Study into the Implications of Smartphone Operating System Security
Study into the implications of Smartphone operating system security

CONTENTS

Executive Summary ................................................................................................................................... 4
Scope of Study .......................................................................................................................................... 4
Introduction .............................................................................................................................................. 5
  The personal remote control for our lives .............................................................................................. 5
  Smartphone ecosystem and mobile app stores ....................................................................................... 7
  Smartphones get more personal ........................................................................................................... 7
Security Threats ....................................................................................................................................... 8
  What is being done to counteract these security threats? .................................................................. 10
  What more can be done? ....................................................................................................................... 13
Report Summary - Key Findings and Recommendations ................................................................. 15
  An investigation into the emerging Smartphone security threats to consumers ......................... 15
  How UK Mobile Network Operators are supporting Smartphone operating system updates ................................................................................................................................. 16
  An examination into the challenges of supporting multiple versions of Smartphone operating systems ........................................................................................................................................... 18
  An Investigation of Smartphone vulnerabilities and how they are being managed .................... 19
  An examination on whether current consumer Smartphone protection practices in the UK are working ................................................................................................................................................. 21
  An Investigation and analysis on how other regions are dealing with Smartphone security .................................................................................................................................................... 22
  An overview and analysis on UK regulatory and institutional responsibilities for Smartphone security ................................................................................................................................. 23
  A look at the impact of emerging mobile technologies to Smartphone security .......................... 25
  An investigation and security analysis into mobile app store (market) security .......................... 26
  An investigation and security analysis into ‘sideloading’ mobile apps ............................................. 27
1. The emerging threat to consumers ...................................................................................................... 28
Study into the implications of Smartphone operating system security

Overview .................................................................................................................................................. 28

Threat analysis and impact to consumers ................................................................................................. 29

2. How UK Mobile Network Operators (MNOs) support Smartphone operating system updates ............................................................................................................................................. 38

Overview .................................................................................................................................................. 38

Analysis of mobile operating system updates .............................................................................................. 39

3. Analysis of how UK Mobile Network Operators (MNOs) manage mobile operating system software updates .................................................................................................................................................. 62

4. Smartphone security vulnerabilities ........................................................................................................... 73

Overview .................................................................................................................................................. 73

Levels of reported Smartphone operating system vulnerabilities ............................................................... 76

Smartphone operating systems vulnerabilities .............................................................................................. 79

5. Current consumer protection practices in the UK ....................................................................................... 92

Overview .................................................................................................................................................. 92

6. How are other regions dealing with Smartphone security? ........................................................................ 100

Overview .................................................................................................................................................. 100

EU ............................................................................................................................................................. 100

United States of America .............................................................................................................................. 103

7. Current UK Smartphone security regulatory and institutional responsibilities ........................................ 108

Overview .................................................................................................................................................. 108

The Information Commissioner’s Office (ICO) .............................................................................................. 108

Telecommunications regulation .................................................................................................................... 109

Fraud and Financial Regulation ................................................................................................................... 110

UK legislation and Smartphone security ....................................................................................................... 111

Summary and Recommendations ................................................................................................................ 112

8. The impact of emerging mobile technology to Smartphone security .................................................... 113

Overview .................................................................................................................................................. 113

Near Field Communications (NFC) .............................................................................................................. 114
Study into the implications of Smartphone operating system security

9. Investigation and security analysis into mobile app market security ........................................ 118
   Overview ................................................................................................................................. 118
   Official App Stores ................................................................................................................ 118
   Third-party Android App stores ............................................................................................ 121

10. Investigation and security analysis into sideloading mobile apps ......................................... 123
    Overview ............................................................................................................................... 123
    Android Sideloding ............................................................................................................... 123

Appendices .................................................................................................................................. 126
   Appendix A: Apple iOS Devices and Operating Systems ....................................................... 126
   Appendix B: Apple iOS Version History ................................................................................. 127
   Appendix C: Apple iOS Wireless Software Update Process ................................................... 129
   Appendix D: Apple iOS iTunes Software Update Process ..................................................... 130
   Appendix E: Google Android version history ......................................................................... 131
   Appendix F: A guide to mobile operating systems ................................................................. 132
      Types of mobile operating systems – mobile models ........................................................... 132
      ROM and Mobile Operating Systems ................................................................................ 132
   Appendix G: Goode Intelligence research methodology and assumptions ......................... 134
   Appendix H: About Goode Intelligence .................................................................................... 137
EXECUTIVE SUMMARY

Scope of Study

Goode Intelligence was commissioned by Ofcom to prepare an independent expert report into emerging risks to users of Smartphones and to further Ofcom’s understanding of how these risks are addressed in this highly dynamic and nascent environment.

Ofcom has a statutory duty to further the interests of citizens in relation to communications matters. Ofcom is also guided by a regulatory principle to research markets constantly and aims to remain at the forefront of technological developments and it is on this basis that this report was commissioned.

This study investigates ten key areas of Smartphone OS security which are:

1. An investigation into the emerging Smartphone security threats to consumers
2. How UK mobile network operators (MNO) are supporting Smartphone operating system updates
3. An examination into the challenges of supporting multiple versions of Smartphone operating systems
4. An investigation of Smartphone security vulnerabilities and how they are being managed
5. An examination of current consumer Smartphone protection practices in the UK and how they are working
6. An investigation and analysis on how other regions are dealing with Smartphone security
7. An overview and analysis on UK regulatory and institutional responsibilities for Smartphone security
8. A look at the impact of emerging mobile technologies to Smartphone security
9. An investigation and security analysis into mobile app store (market) security
10. An investigation and security analysis into ‘sideloading’ mobile apps

This study investigates the four main leading Smartphone operating systems that are currently being used in the UK, namely Apple iOS, BlackBerry OS, Google Android and Windows Phone.

The Smartphone market is currently dominated by two mobile operating systems, Google Android and Apple iOS.

By the end of 2012 Android had 54.4 percent and iOS had 32.4 percent of UK Smartphone sales – combined that equates to just under 87 percent of the UK’s Smartphone market share. The mobile operating systems in third and fourth spots are Blackberry OS (6.4 percent) followed by Windows Phone (5.9 percent).
Introduction

The personal remote control for our lives

Smartphones are having a fundamental impact in how we create and consumer digital information and have become the personal remote control for our lives.

More and more UK consumers are using Smartphones; between 58 percent\(^1\) and 64 percent\(^2\) of the UK population now owns a Smartphone and most new mobile phone sales will be Smartphones.

Smart mobile devices (Smartphones and tablet computers running mobile operating systems) have transformed the way in which we create and consume digital information and rarely leave our sides. They have, and are continuing to, replace other consumer digital equipment including personal computers, laptops and notebooks, televisions, gaming devices / consoles, satellite navigation devices and personal music players. Mobile is now the most popular way to send and receive emails with Apple iOS being the most popular email client\(^3\) and according to figures from IDC PC sales are declining, with global sales falling 14 percent in the first three months of 2013.\(^4\) An average UK Smartphone owner may have the following experience during a typical day.

---

\(^1\) Ofcom consumer research; Taken from Ofcom International Communications Market Report 2012.  http://media.ofcom.org.uk/files/2012/12/2012-ICMR-analyst-presentation.pdf

\(^2\) comScore; UK Digital in Focus 2013

\(^3\) http://www.campaignmonitor.com/resources/will-it-work/email-clients/

\(^4\) http://www.bbc.co.uk/news/business-22103079
The personal remote control for our lives

A typical morning could start with being awoken by the alarm function then a quick check on our digital social and work lives by checking our email (personal and work), Twitter, LinkedIn and Facebook notifications, followed by a summary of news events and what the day’s weather has in store for us – and all before breakfast and the morning shower. For the daily commute into work we have generally ditched the printed daily paper and the book and will receive notifications from our banks on account balances and reminders of our day’s schedule. On our return from home we have already checked to see the state of the transport network and been sent a reminder that the weekly shopping is being delivered at 19:00.

This scenario is happening every day in every city, town and village up and down the length of the UK. And what does mobile technology have in store for us in the coming years? NFC will bring contactless payments and ticketing directly onto our Smartphones, the next generation of Google and Apple devices will be wearable and be able to capture our daily lives in very personal ways – the digital and physical will become one.
Study into the implications of Smartphone operating system security

**Smartphone ecosystem and mobile app stores**

In addition to acting as conventional mobile phones, Smartphones behave like computers with upgradeable operating systems and the ability to run programs (mobile apps).

Smartphones are driven by the mobile app ecosystem with mobile apps being distributed mainly from official app stores such as the Apple Appstore and Google Play. There seems to be a mobile app to help consumers run almost every element of their entire lives.

Smartphones and the mobile app store ecosystem have altered the relationship that consumers have with their mobile network operator (MNO) supplier. Before Smartphones were introduced and gained popularity consumers received most of their services, including messaging and limited data services mainly through the MNO. Smartphones have disrupted this relationship with the introduction of over-the-top (OTT) services being delivered to consumers by service providers via mobile apps. Mobile apps have enabled service providers, such as WhatsApp for messaging services (SMS text replacement), a direct route to market for their products and services without a role for the MNO.

This shift away from the MNO for the delivery of value added mobile services has implications for security and for the regulatory environment that shall be discussed in this study.

**Smartphones get more personal**

Innovation in technology is occurring at an incredibly fast pace and today's high-tech Smartphones may look a little outdated in a short space of time.

Smart mobile devices will become smarter and more personable. Wearable devices with Smartphone features are scheduled to be launched during the next couple of years.
Study into the implications of Smartphone operating system security

These include Google Glass\(^5\), a wearable computer with a head-mounted display (HMD) that is planned to be launched in 2013/2014, and there are predictions that Apple will launch its own wearable device, a smart watch or iWatch, as early as 2013.

**Security Threats**

A combination of increasing Smartphone ownership and the use of more valuable data services on these devices has led to Smartphones becoming a more attractive target for fraudulent and illegal actions.

All forms of computing technology can be vulnerable to security threats and Smartphones are no exception. In the main, Smartphones employ adequate security measures to ensure that consumers are protected against some of the more common security threats such as financial fraud and unauthorised access to personal information.

Vulnerabilities exist on every Smartphone Operating System examined in this study. A vulnerability becomes a problem when it can be exploited. Malware is an example of how a vulnerability is exploited, creating code that exploits weaknesses and bugs, in the Operating System for malicious purposes – to extract personal information or to enact financial fraud on the Smartphone owner. If the vulnerability is not remediated, fixed or patched, in a timely fashion then these exploits will continue and Smartphone owners will be exposed to security threats.

This is why it is imperative to have a robust and efficient Smartphone Operating System software update process that discovers vulnerabilities before the bad guys do, fixes them and then pushes the resultant software update to all affected Smartphone owners before the vulnerability can be widely exploited. This is the first independent study that investigates both the Smartphone Operating System update process and vulnerability management in detail.

In the main, Smartphone Operating System vendors are doing a decent job of handling software updates and vulnerability management. Figure ES2 details the basic Smartphone Operating System update process. There are however, exceptions. The fragmentation issues surrounding Google’s Android OS are not helping this process with the effect of many millions of Android Smartphone owners being potentially exposed to exploitable vulnerabilities.

\(^5\) Google’s Glass website http://www.google.com/glass/start/
Mobile malware numbers are certainly rising, especially on Android, but the risks for UK consumers of being affected are low. The greatest security risk currently for UK Smartphone owners is the threat of a lost or stolen device.

Throughout the UK, Smartphones are being stolen on a daily basis and the problem is growing. According to information that was obtained by The Times newspaper under the Freedom of Information Act, more than 170 iPhones are stolen every day in London.\(^6\) In all, 10,000 mobile phones are stolen every month in London with two thirds of the victims aged between 13 and 16. The rise in stolen Smartphones was also recorded by the fact that in a six-month period between April and September 2012, 28,800 iPhones were reported stolen in London. Overall a total number of 56,680 mobiles were stolen in London between April and September 2012, equating to 341 phones per day.\(^7\)

Other security threats to Smartphones are categorised into two main areas; financial fraud (includes premium rate services and banking fraud) and personal information loss (privacy issues). There is evidence of targeted attacks leading to both financial fraud and personal information loss and with Smartphones becoming a major technology tool then it is probable that these attacks will increase.

---


What is being done to counteract these security threats?

As with all security threats a combination of legislation, regulatory governance, education / awareness and technology control is managing the security threats for Smartphones.

Legislation and Regulatory Governance

Smartphone security threats are controlled by legislation and governed by bodies that have been assigned responsibility to govern them.

UK regulatory and institutional responsibility for Smartphone security is shared across a number of bodies that include:

- Telecommunications regulators:
  - Office of Communications (OFCOM)
  - PhonepayPlus
- Date Protection and Privacy:
  - The Information Commissioner’s Office (ICO)
- Financial regulation:
  - Financial Conduct Authority (FCA)
  - Prudential Regulation Authority (PRA)
- Trading standards:
  - Office of Fair Trading (OFT)
- Fraud:
  - National Fraud Authority (NFA)
  - Police Authorities

The following table, ES3, summarises key UK regulatory and institutional responsibilities for Smartphone security by matching major Smartphone security risks against legislation and its responsible institution.
Table ES3: UK legislation and Smartphone security

<table>
<thead>
<tr>
<th>Smartphone security risk</th>
<th>Applicable legislation</th>
<th>Institution Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unpatched Smartphone</td>
<td>Unclear</td>
<td>Unclear</td>
</tr>
<tr>
<td>Lost and stolen Smartphone (leading to potential loss of privacy, identity and data)</td>
<td>• Criminal law for theft</td>
<td>Shared between:</td>
</tr>
<tr>
<td></td>
<td>• Data Protection Act</td>
<td>• Police Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The ICO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PhonepayPlus</td>
</tr>
<tr>
<td>Lost and stolen Smartphone (leading to potential loss of privacy, identity and data)</td>
<td>• Communications Act 2003</td>
<td>• PhonepayPlus</td>
</tr>
<tr>
<td></td>
<td>• PhonepayPlus Code of Practice</td>
<td>• Ofcom</td>
</tr>
<tr>
<td>Telephony Financial (Premium Rate Services) fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of privacy (due to Spyware and Malware)</td>
<td>• Data Protection Act 1998</td>
<td>• The ICO</td>
</tr>
<tr>
<td></td>
<td>• Communications Act 2003</td>
<td>• Ofcom</td>
</tr>
<tr>
<td></td>
<td>• Computer Misuse Act 1990 (Police and Justice Act 2006)</td>
<td>• CPS</td>
</tr>
<tr>
<td>Financial services (banking) fraud</td>
<td>• Financial Fraud Act 2006</td>
<td>• FCA &amp; PRA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• National Fraud Authority (NFA)</td>
</tr>
</tbody>
</table>

Source: Goode Intelligence © 2013

Ofcom has a statutory duty to further the interests of citizens in relation to communications matters. Ofcom is also guided by a regulatory principle to research markets constantly and aims to remain at the forefront of technological developments.

With the exception of unpatched Smartphones, Goode Intelligence believes that current legislation should be sufficient in dealing with current Smartphone security issues. There does not seem to be any major holes in current legislation that could result in a disparity between the technology and the governing framework.

There may, however, be a need for more clarity around the legal and regulatory responsibility surrounding these issues affecting Smartphones. Goode Intelligence recommends that further analysis be carried out to ensure that the legal and regulatory responsibility is clarified.
Study into the implications of Smartphone operating system security

**Education and Awareness**

Goode Intelligence believes that, although improving, the levels of awareness as to the current security threats affecting UK Smartphone owners is low. Consumers still treat these devices as phones, whose value is the monetary cost of the device, rather than mobile computers that contain valuable personal information.

From an education and awareness point of view, MNOs are not making it easy for consumers to locate vital information that could protect their Smartphones against major security threats, including protection against loss or theft.

There is a good level of communication from organisations such as Get Safe Online and UK Police authorities about major Smartphone threats but there needs to be an analysis of these communication channels in measuring their effectiveness.

**Technology Control**

There are many security features built into both the Smartphone Operating System and within the ecosystem to protect these devices and their owners.

All major Smartphone Operating System vendors treat security seriously and have architected the OS to prevent most of the known security threats. There still are weaknesses, the ability to ‘sideload’ mobile apps onto Android Smartphones and Apple’s struggle with iOS Jailbreaking are two examples, but in the main Smartphones are fairly secure devices.

Mobile app stores are an important component in the Smartphone ecosystem and are the main distribution point for mobile apps.

In general, according to Adaptive Mobile’s Cathal McDaid “app store security ranges from good to poor”. Goode Intelligence believes that out of the top two mobile app stores Apple operates at the good end, Google Play is somewhere in the middle (but edging up towards good all of the time) and the unofficial Android app stores are at the poor end of the spectrum.

There is little evidence that UK consumers are effectively protecting their Smartphones using technology and that they are aware of what the main threats are. Consumers, in the main, do not take personal responsibility for the security of their Smartphones and are relying on the MNOs to be proactive in securing both the device and ensuring the safe transport of information over the radio network.

MNOs are taking steps to protect both their own networks and Smartphone devices by adopting security practices, including technology controls.
What more can be done?

When dealing with security matters it is important to put things into perspective and to provide as much context as possible. Smartphones and tablet computers running mobile operating systems are now an incredibly important tool in managing our ever more connected lives. They contribute to our wellbeing and can enhance our business lives by connecting us to important global networks and by improving productivity.

It is vital to the safety and the economy of the UK that Smartphones are adequately protected against security threats that can lead to loss of personal information and financial fraud.

A lot has already been done to achieve this but Goode Intelligence feels that more can be done to protect UK Smartphone owners from security threats that target these incredibly useful and important electronic devices.

As a result of creating this independent study into the implications of Smartphone Operating System security Goode Intelligence recommends the following:  

1. Concentrate efforts on highest security risks affecting UK consumers. Currently the main threat is lost or stolen Smartphones.
2. Educate UK consumers as to the major threats of using Smartphones using both online and offline communication channels. Treat them as computers not phones.

There is a responsibility for better education and awareness from the UK MNO community. Goode Intelligence recommends that the following basic steps to protect Smartphones be communicated to UK consumers:

a. Better communication at the point of sale, e.g. when the consumer purchases a Smartphone.
b. PINs and passwords are set. Potentially a default setting on new Smartphones.
c. Only install apps from trusted sources and educate as to what is a trusted or untrusted source.
d. Know how to report a stolen phone and that if a device is lost or stolen, it should be reported immediately.
e. Discourage modification of security settings including rooting or Jailbreaking.
f. Encourage secure disposal of Smartphones, including advice on how to wipe data of an old phone before it is donated, resold or recycled.
g. Backup and secure data stored on a Smartphone.
h. Set security settings or install security apps that enable remote location and wiping.
i. Be aware of risks when connecting to open WiFi networks.
j. Understand privacy and app permission settings before accepting them.

**Note** - Some of these recommendations are more easily achieved than others as Smartphones are a worldwide phenomenon with often complex business models and ecosystems. Unilateral action can succeed in some cases but a more bilateral, partnership; strategy is often a better course of action.
3. Review the current gaps in the effectiveness and efficiency of the Smartphone Operating System update process and work with industry stakeholders to remove the gaps. This includes improving the time it takes for vulnerabilities to be discovered, remediated and pushed to Smartphone owners.

4. This includes raising awareness of the importance of downloading and installing the latest software versions.

5. Learn from other regions about how they are managing Smartphone security threats including:
   a. Analysing EU and US examples of how they deal with Smartphone security.
   b. Liaising with the ENISA in the EU and FCC/FTC in the USA to determine the success of their initiatives.

6. UK legislation and regulatory recommendations:
   a. Creation of a cross-regulatory working party to discuss potential issues and gaps in protecting Smartphones, and their associated services. This study could act as the initial reference point for such a group.
   b. Review of Smartphone security risks against UK legislation to determine:
      i. UK legislation related to particular security risk
      ii. UK regulatory body that is responsible for particular security risk
      iii. Gaps
      iv. Action plan to manage security risks.

7. Emerging mobile technology risks. Emerging technology areas are difficult to assess from a security perspective. There may be proof-of-concept attacks on technologies that have not been widely deployed but it is usually only when technologies reach a degree of critical mass that more widespread exploits are discovered.
   a. It is recommended that Ofcom continue monitoring emerging mobile technologies, including NFC, LTE, and wearable devices running Smartphone Operating Systems such as Google Glass, to determine their impact on consumer Smartphone security.

8. Mobile Appstore security recommendations:
   a. Educate consumers about the levels of risk when dealing with app stores.
   b. Consumers should be cautious when using third-party Android app stores and file sharing sites.
   c. Determine if there are practical solutions in minimising the risk of installing rogue or Trojanised apps using Android’s app sideloading feature.

The following section, ‘Report Summary – Key Findings and Recommendations’, summarises the key findings and recommendations from this study in more detail.
An investigation into the emerging Smartphone security threats to consumers

Key Findings

Smartphones have become the remote controls for our ever-important digital lives. We rarely let them out of our sight, even when we are asleep, and perform much of our daily activities on them.

Smartphones access and store much of our digital lives, both personal and business. Smartphones and tablet computers have become the dominant digital device and we now preform much of our social networking, shopping, messaging (iOS has become the number one client for email replacing Microsoft Outlook), banking and business activities on them.

With this increasing reliance on Smartphones comes the possibility of increasing threats and security risk. These threats will replicate what has already been experienced with other forms of information technology (as Smartphone operating systems have commonality with other systems, e.g. Linux Kernel and WebKit) but we shall also see other, mobile-specific, threats that will probe for weaknesses in unique characteristics that Smartphones support.

For instance:

- Accurate location based services, using a combination of GPS and GSM location data to accurately pinpoint where a device and its owner are
- Faster network access through 4G (LTE) and future fast radio-based networks
- Using a Smartphone as a payment source either at the physical Point-of-Sale (POS) using Near Field Communications (NFC) or using other mobile payment solutions for in-app payment/billing and peer-to-peer (P2P) payment between one device and another
- Capturing biometric data via embedded sensors such as fingerprint readers, conventional and bespoke cameras for facial, iris and retinal scanning, in-built microphones for capture of voiceprints (some of which can be captured by an in-built voice sensor) and sensors to capture and record other biometrics such as pulse, blood pressure and ECG

Goode Intelligence believes that the threats to Smartphone consumers can be broken down into these main areas:

- Lost and stolen Smartphones
- Financial fraud
- Privacy

These threats are interconnected as a lost or stolen Smartphone can lead to other threats being exposed including financial fraud and privacy issues (including data and identity theft).
Study into the implications of Smartphone operating system security

According to Kevin Mahaffey, co-founder and Chief Technology Officer (CTO), of mobile security vendor Lookout Mobile Security, lost and stolen Smartphones is currently the number one threat to consumers. This thought is echoed by many mobile security professionals.

Whether it is losing a phone in a taxi after a night out or being a victim of a mugging in which a Smartphone is stolen this is the greatest threat to Smartphones.

In reference to mobile malware, although examples of mobile malware are rising especially on the Android platform, there is still a low risk of UK consumers being affected by this threat.

Recommendations

So far, we have not seen a major security threat that has caused widespread disruption to UK Smartphone owners. This includes the threat of mobile malware.

As threats to Smartphones are an emerging area, a constant review of the threat landscape must be performed by industry bodies including Ofcom.

It is recommended that efforts are invested towards the current major threats to Smartphone owners, especially the threat of Smartphone loss and theft.

The next section shall investigate current Smartphone protection practices that are attempting to control the security threat to UK consumers.

How UK Mobile Network Operators are supporting Smartphone operating system updates

Key Findings

A major goal for Smartphone operating system software updates is to get the updates and security fixes installed on smartphones as quickly and as smoothly as possible without interfering with the usual running of the device and the mobile network – to balance security needs with usability.

Smartphone operating system lifecycles are usually shorter than for desktop computers. For instance, Microsoft announced in March 2013 that Windows Phone 7.8 and 8 will be unsupported by the end of 2014 – an eighteen month OS lifecycle. This compares with Windows XP that had a lifecycle of over 7 years (released October 2001 and unsupported by April 2009).
There are many stakeholders involved in the process of developing, testing, distributing and installing Smartphone operating system software updates. These include the operating system developer (the platform owner), the Smartphone manufacturer (device Original Equipment Manufacturer (OEM)), the MNO and the Smartphone owner.

The Smartphone OS ecosystem is detailed in figure ES4 below.

**Figure ES4: Smartphone Operating System Ecosystem**

UK MNOs are an integral part of this process in ensuring that their own networks and their customer’s Smartphones are not affected as a result of a new Operating System version. They support this process but are reliant on receiving Operating System updates from the Smartphone OEMs. The process is at its smoothest when there are fewer intermediaries involved in the end-to-end process and the Smartphone operating system vendor is proactive in patching vulnerabilities and then distributing these software updates swiftly to the Smartphone owner.

Where you introduce more intermediaries into the process you can introduce complexity that can lead to an adverse impact on the fluidity of the update process. Where this is most acute is with Android. Google is heavily reliant on third-party Smartphone OEMs that take the base Android firmware and then customise it for use on their hardware platform. The so-called ‘Android Fragmentation’ issue results in a situation where Google releases a software update and then pushes it out to its own-brand devices but then has to rely on its other hardware partners to manage the software update themselves. This can result in a delay in Android device manufacturers releasing software updates to its device community. There is a risk to consumers being exposed to harm.


**Recommendations**

There are a number of industry initiatives, including one run by the GSMA, to improve and speed up the process of delivering Smartphone operating system updates to the end user.

These initiatives need cross-industry support and buy-in to ensure that any blockages in the system are removed to ensure that consumers are not disadvantaged by unnecessary delays in receiving Smartphone operating system software updates.

**An examination into the challenges of supporting multiple versions of Smartphone operating systems**

**Key Findings**

There are currently four major Smartphone operating systems but there are also other ‘legacy’ platforms, e.g. Symbian and Palm OS, that still need to be supported. There are also new Smartphone operating systems that are coming to market including Mozilla’s Firefox OS and Samsung’s Bada.

Challenges for MNOs in supporting multiple versions of Smartphone operating systems include:

- **Lack of control**: The MNOs are reliant on their suppliers, e.g. handset manufacturer/platform owner for managing the end-to-end mobile operating system software lifecycle and process

- **Support burden**: By owning the Smartphone customer, mobile operators will receive the bulk of support calls in relation to the software update process even though in many cases they do not own or control the process

- **Testing / Approval responsibility**: Mobile operators are responsible for the mobile network, its integrity, availability (Quality of Service or QoS) and security. As a Smartphone will be connected to a mobile network, they must ensure that any new device or software update does not adversely interfere with the network’s operation. This includes supporting older Smartphones and running older versions of the mobile operating system

**Recommendations**

Although UK MNOs recognise that there are challenges in supporting multiple versions of Smartphone operating systems they consider this as part of their “business as usual” process.

This problem could get worse as there are new Smartphone operating systems, e.g. Firefox OS, being announced on a regular basis
Study into the implications of Smartphone operating system security

Goode Intelligence recommends that cross-industry representatives should liaise with UK MNOs to assist them in any cross-operator initiatives to improve the process in supporting multiple versions of Smartphone operating systems.

**An Investigation of Smartphone vulnerabilities and how they are being managed**

**Key Findings**

Security vulnerabilities exist in every example of computer software and Smartphone operating systems are not exempt from this rule.

Vulnerability management is the process or lifecycle that aims to manage computer vulnerabilities. There will be many vulnerability management models but essentially the main parts of the vulnerability management process are:

1. Identification (Including Disclosure)
2. Classification
3. Remediation (fixing or mitigation)

Effective Smartphone vulnerability management is essential in how effectively vulnerabilities are discovered, disclosed, fixed and patched. If security vulnerabilities are not efficiently remediated (fixed) then the risk of them being effectively exploited will increase. This increases the risk to consumers.

The actual risk to Smartphone owners to these vulnerabilities will be dependent on a number of factors including:

- The nature and risk level of the vulnerability, e.g. will the vulnerability lead to widespread disruption, potential financial fraud or identity theft?
- Who knows about the vulnerability? Is knowledge of the vulnerability restricted and confined to a criminal organisation or hostile nation state?
- How easy is it to exploit the vulnerability and has the exploit been automated and shared throughout the security research community?
- The speed for the vendor that is affected by the vulnerability to initially fix (patch) and then to distribute the remediated software to Smartphone owners
- Quality of communication. Is news about the vulnerability efficiently distributed to those parties that are affected by it?
- The willingness of the Smartphone owners to download and install the revised software update

Smartphone operating system vulnerabilities are being discovered either by the operating system vendor themselves, by security research companies that specialise in vulnerability discovery and by individual security researchers.

Computer Emergency Response Teams (CERTs) have been an important part of the vulnerability management landscape, especially in the enterprise environment. By
communicating vulnerability information to system administrators and security professionals and by providing a searchable database of known vulnerabilities nationally managed CERTs, including the UK’s own GovCertUK, are important centres for vulnerability management.

From Goode Intelligence’s research CERT’s are currently performing a limited role in the Smartphone operating system security and vulnerability management process.

In discussion with a number of the UK’s mobile operators they had little involvement with CERTs including GovCertUK.

Smartphones and other smart mobile devices have definitely started to turn up on the radar of CERTs. US-CERT has published a number of security publications specifically on mobile security that act as advisories.

**Recommendations**

This is a constantly evolving landscape and there is a need to reach out to industry stakeholders to ensure that they are kept informed of the latest vulnerabilities that can affect UK consumers.

Goode Intelligence believes that all of the major Smartphone operating system vendors are proactive in vulnerability management. They are doing a pretty good job of discovering and remediating vulnerabilities.

However, there can be problems in pushing out ‘fixed’ or patched software updates to millions of Smartphone users in an appropriate period of time. There can be instances where vulnerabilities go unpatched for many months. This can lead to Smartphone owners being exposed to exploitable vulnerabilities for an excessive period of time. This situation is more acute with Android and is a consequence of the platform’s ‘fragmentation’ issue.

As national CERTs are currently playing a limited role in the Smartphone operating system vulnerability management process they may want to improve their role by taking a more proactive stance and by improving their relationships with UK MNOs.
An examination on whether current consumer Smartphone protection practices in the UK are working

Key Findings

Smartphone security is an emerging area of technology, as are the threats against them.

Consumer protection practices in the UK are currently a combination of technology initiatives and consumer awareness.

There is little evidence that UK consumers are effectively protecting their Smartphones using technology and that they are aware of what the main threats are. Consumers, in the main, do not take personal responsibility for the security of their Smartphones and are relying on the MNOs to be proactive in securing both the device and ensuring the safe transport of information over the radio network.

MNOs are taking steps to protect both their own networks and Smartphone devices by adopting security practices, including technology controls.

From an awareness point of view, MNOs are not making it easy for consumers to locate vital information that could protect their Smartphones against major security threats, including protection against loss or theft.

There is a good level of communication from organisations such as Get Safe Online and UK Police authorities as to the major Smartphone threats but there needs to be an analysis of these communication channels in measuring their effectiveness.

Recommendations

A combination of technology control and education is recommended in combatting the threat to UK Smartphone owners.

Better consumer education is at the heart of any protection practice that aims to protect Smartphone users. This can be achieved with the close cooperation of UK stakeholders that includes MNOs, Get Safe Online, The ICO, Ofcom, PhonePayPlus and UK Police Service.

Ensure that MNOs are taking adequate safeguards to protect consumer Smartphones and the mobile network infrastructure. This includes appropriate levels of consumer communication.

Basic steps to protect Smartphones include:

- Better communication at the point of sale, e.g. when the consumer purchases a Smartphone
- PINs and passwords are set. Potentially a default setting on new Smartphones
- Only install apps from trusted sources and education as to what is a trusted or untrusted source
An Investigation and analysis on how other regions are dealing with Smartphone security

Key Findings

Regions such as the European Union (EU) and the United States of America have been proactive in managing the Smartphone security threat.

In the EU, the European Network and Information Security Agency (ENISA) has been set up by the EU to be the “pace-setter for Information Security in Europe” with a mission “to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union”.

The agency has been actively offering support to EU member states on Smartphone security since 2010 when they first published a report assessing the security risk from using Smartphones and offering “practical recommendations on how to address these risks”.

US regulators and other government bodies, including the FCC and the FTC, have been proactive in managing the Smartphone security threat, by reaching out to industry partners, establishing clear guidelines and enforcing current regulations and legislation.

The FCC has also been directly involved in attempting to raise awareness for Smartphone security through a number of campaigns.

These include “Ten Steps to Smartphone Security for Android” and the “FCC Smartphone Security Checker”.

Recommendations

Analyse EU and US examples of how they are dealing with Smartphone security.

Liaise with the ENISA in the EU and FCC/ FTC in the USA to determine the success of these initiatives.

---

An overview and analysis on UK regulatory and institutional responsibilities for Smartphone security

Key Findings

UK regulatory and institutional responsibility for Smartphone security is shared across a number of bodies that include:

- Telecommunications regulators:
  - Office of Communications (OFCOM)
  - PhonepayPlus
- Date Protection and Privacy:
  - Information Commissioner’s Office (ICO)
- Financial regulation:
  - Financial Conduct Authority (FCA)
  - Prudential Regulation Authority (PRA)
- Trading standards:
  - Office of Fair Trading (OFT)
- Fraud:
  - National Fraud Authority (NFA)
  - Police Authorities

The following table, ES5, summarises key UK regulatory and institutional responsibilities for Smartphone security by matching major Smartphone security risks against legislation and its responsible institution.
Table ES5: UK legislation and Smartphone security

<table>
<thead>
<tr>
<th>Smartphone security risk</th>
<th>Applicable legislation</th>
<th>Institution Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unpatched Smartphone</td>
<td>Unclear</td>
<td>Unclear</td>
</tr>
<tr>
<td>Lost and stolen Smartphone (leading to potential loss of privacy,</td>
<td>Criminal law for theft</td>
<td>Shared between:</td>
</tr>
<tr>
<td>identity and data)</td>
<td>• Data Protection Act</td>
<td>• Police Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The ICO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PhonepayPlus</td>
</tr>
<tr>
<td>Lost and stolen Smartphone (leading to potential loss of privacy,</td>
<td>Communications Act 2003</td>
<td>Shared between:</td>
</tr>
<tr>
<td>identity and data)</td>
<td>• PhonepayPlus Code of Practice</td>
<td>• Police Service</td>
</tr>
<tr>
<td></td>
<td>• Data Protection Act 1998</td>
<td>• The ICO</td>
</tr>
<tr>
<td></td>
<td>• Communications Act 2003</td>
<td>• Ofcom</td>
</tr>
<tr>
<td></td>
<td>• Computer Misuse Act 1990 (Police and Justice Act 2006)</td>
<td>• CPS</td>
</tr>
<tr>
<td>Loss of privacy (due to Spyware and Malware)</td>
<td>Financial Fraud Act 2006</td>
<td>FCA &amp; PRA</td>
</tr>
<tr>
<td>Financial services (banking) fraud</td>
<td>• PhonepayPlus</td>
<td>National Fraud Authority (NFA)</td>
</tr>
<tr>
<td></td>
<td>• Ofcom</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CPS</td>
<td></td>
</tr>
</tbody>
</table>

Source: Goode Intelligence © 2013

Ofcom has a statutory duty to further the interests of citizens in relation to communications matters. Ofcom is also guided by a regulatory principle to research markets constantly and aims to remain at the forefront of technological developments.

Goode Intelligence believes that current legislation should be sufficient in dealing with current Smartphone security issues. There does not seem to be any major holes in current legislation that could result in a disparity between the technology and the governing framework.

However, this must be constantly reviewed in light of emerging, sometimes disruptive, technology that could alter the effectiveness of regulation and legislation.

Related to legislation is education (engagement) and enforcement; educating affective parties as to the nature of legislation by engaging with all parts of the ecosystem and enforcement once there has been a breach (either intentional or unintentional).

There is a question on whether providers of Smartphone services, including the Smartphone OS vendors, Smartphone OEMs and mobile app developers (including suppliers of OTT services) are adequately regulated.
Study into the implications of Smartphone operating system security

**Recommendations**

Goode Intelligence recommends the following at, at a minimum:

1. Creation of a cross-regulatory working party to discuss potential issues and gaps in protecting Smartphones, and their associated services. This study could act as the initial reference point for such a group.
2. Review of Smartphone security risks against UK legislation to determine:
   a. UK legislation related to particular security risk
   b. UK regulatory that is responsible for particular security risk
   c. Gaps
   d. Action plan to manage security risks
3. Review on whether all of the Smartphone ecosystem is adequately regulated

**A look at the impact of emerging mobile technologies to Smartphone security**

**Key Findings**

Innovation in mobile computing including Smartphones is happening at a spellbinding pace.

Each time a major Smartphone operating system version or new device arrives it heralds the arrival of the latest innovative technology.

Near Field Communication (NFC) and Long-Term Evolution (LTE) are examples of two emerging technologies that may impact Smartphone security.

**Recommendations**

Emerging technology areas are difficult to assess from a security perspective. There may be proof-of-concept attacks on technologies that have not been widely deployed but it is usually only when technologies reach a degree of critical mass that more widespread exploits are discovered.

It is recommended that Ofcom continue monitoring emerging mobile technologies to determine their impact on consumer Smartphone security.
An investigation and security analysis into mobile app store (market) security

**Key Findings**

App stores are the main delivery mechanism for mobile apps and are are divided into official, those that are approved and usually run by the mobile operating system vendor, and unofficial, everything else.

The two most popular mobile app stores are provided by Apple and Google and are tied to iOS and Android Smartphone operating systems respectively.

Apple iOS users cannot use an app store from a competing mobile platform. A developer creating a native iOS app must distribute this app through the official app store. The same lock-in to the operating system vendor’s app store is seen for Blackberry OS, BlackBerry World app store, and Windows Phone 8, Windows Phone app store.

This differs from Android where an Android developer is not tied to Google Play. They can distribute their app through a wide variety of distribution channels including unofficial app stores, e.g. Amazon Android app store, file sharing sites, e.g. BitTorrent, and even by sideloading an app from a connected desktop. Android really is an open platform.

According to Adaptive Mobile’s Cathal McDaid “app store security ranges from good to poor”. In Goode Intelligence’s opinion, out of the top two mobile app stores Apple operates at the good end, Google Play is somewhere in the middle (but edging up towards good all of the time) and the unofficial Android app stores are at the poor end of the spectrum.

**Recommendations**

- Educate consumers as to the levels of risk when dealing with app stores
- Consumers should be cautious when using third-party Android app stores and file sharing sites

Additionally, Goode Intelligence believes that ENISA’s advice against the threat of mobile malware in a report published in September 2011 entitled “Appstore security – 5 lines of defence against malware” is relevant for app store security and could form the basis of minimum levels of protection for mobile app stores.

In this report ENISA identifies these five lines of defence against mobile malware (app store security mechanisms):

1. App review: App stores should review apps before admitting them to the app store.
2. Reputation mechanism: App stores should show the reputation of apps and app developers.

---

Study into the implications of Smartphone operating system security

4. Device security: Includes supporting sandboxes to install and run apps “to reduce the impact of malware”.
5. Jails (or walled gardens): This is closing the sideloading feature. ENISA recommends that “the Smartphone should either be blocked from using untrusted app stores or, for expert users, present clear warnings about installing from untrusted sources”.

**An investigation and security analysis into ‘sideloading’ mobile apps**

**Key Findings**

The “sideloading” of mobile apps is defined as a user installing an app without using the official platform app store or app market.

The ability to install mobile apps from outside of the ‘official’ platform app stores is only officially supported on one Smartphone operating system, Google’s Android.

By allowing a user to install an app from any source you break this model and as a result greatly increase security risk.

Most Android devices will be delivered ‘out-of-the-box’ with the option to sideload turned off.

**Recommendations**

- Educate consumers as to the risks of sideloading mobile apps onto their devices
- This is also related to Jailbreaking Apple iOS devices and consumers should be persuaded not to jailbreak their Apple Smartphones as this removes most of the in-built security protection that iOS offers
- Working with UK MNOs to ensure that sideloading, by default, is switched off

Liaising with Google to determine whether there are other workable ways to support third-party Android app stores that improves security and doesn’t impact their app distribution business model
1. THE EMERGING THREAT TO CONSUMERS

Overview

Smartphones have become the remote controls for our ever-important digital lives. We rarely let them out of our sight, even when we are asleep, and perform much of our daily activities on them.

Smartphones access and store much of our digital lives, both personal and business. Smartphones and tablet computers have become the dominant digital device and we now preform much of our social networking, shopping, messaging (iOS has become the number one client for email replacing Microsoft Outlook), banking and business activities on them.

There is also a question whether consumers have changed their risk behaviour to adapt to how we are using Smartphones. Tony Neate, CEO, Get Safe Online, believes it has taken many years for consumers to change their behaviour to adapt to using desktop-based electronic services but “with mobile we have a whole new mountain to climb”. Neate feels that “there is a different behaviour when we use our Smartphones to that of desktop computers” and a “new behavioural change is required”.

With this increasing reliance on Smartphones comes the possibility of increasing threats and security risk. These threats will replicate what has already been experienced with other forms of information technology (as Smartphone operating systems have commonality with other systems, e.g. Linux Kernel and WebKit) but we shall also see other, mobile-specific, threats that will probe for weaknesses in unique characteristics that Smartphones support.

For instance:

- Accurate location based services, using a combination of GPS and GSM location data to accurately pinpoint where a device and its owner are
- Faster network access through 4G (LTE) and future fast radio-based networks
- Using a Smartphone as a payment source either at the physical Point-of-sale (POS) using Near Field Communications (NFC) or using other mobile payment solutions for in-app payment/billing and peer-to-peer (P2P) payment between one device and another
- Capturing biometric data via embedded sensors such as fingerprint readers, conventional and bespoke cameras for facial, iris and retinal scanning, in-built microphones for capture of voiceprints (some of which can be captured by an in-built voice sensor) and sensors to capture and record other biometrics such as pulse, blood pressure and electrocardiogram (ECG)

Goode Intelligence believes that the threats to Smartphone consumers can be broken down into these main areas:

- Lost and stolen Smartphones

---

Tony Neate interview with Goode Intelligence, 15th March 2013.
Study into the implications of Smartphone operating system security

- Financial fraud
- Privacy

These threats are interconnected as a lost or stolen Smartphone can lead to other threats being exposed including financial fraud and privacy issues (including data and identity theft).

The following section - ‘Threat analysis and impact to consumers’ examines these areas in more detail.

**Threat analysis and impact to consumers**

**Lost and Stolen Smartphones**

According to Kevin Mahaffey, co-founder and Chief Technology Officer (CTO), of mobile security vendor Lookout Mobile Security, lost and stolen Smartphones is currently the number one threat to consumers. This thought is echoed by many mobile security professionals.

Whether it is losing a phone in a taxi after a night out or being a victim of a mugging in which a Smartphone is stolen this is the greatest threat to Smartphones.

Throughout the UK, Smartphones are being stolen on a daily basis and the problem is growing. According to information that was obtained by The Times newspaper under the Freedom of Information Act, more than 170 iPhones are stolen every day in London.\(^\text{12}\) In all, 10,000 mobile phones are stolen every month in London with two thirds of the victims aged between 13 and 16. The rise in stolen Smartphones was also recorded by the fact that in a six-month period between April and September 2012, 28,800 iPhones were reported stolen in London. Overall a total number of 56,680 mobiles were stolen in London between April and September 2012, equating to 341 phones per day.\(^\text{13}\)

This is not just a London problem. According to the same source between 2009 and 2011, Hertfordshire Police had 11,027 cases of mobile phone theft and Thames Valley Police had 34,439 cases.

The police categorise Smartphones as C.R.A.V.E.D (concealable, removable, available, enjoyable and disposable).

**What is driving this?** According to law enforcement experts the rise in Smartphone theft in the UK is being driven by the value of the device and not the value of the information that is stored (or can be accessed) on the device.


Study into the implications of Smartphone operating system security

For instance a locked (tied to a MNO) iPhone 5 (16GB model) can be sold on online auction sites such as eBay for between £350.00 and £400.00. That is a very good resell price as to buy a brand new 16GB iPhone 5 direct from Apple costs £529.00.\footnote{Cost as at 16\textsuperscript{th} March 2013 and obtained from www.store.apple.com}

In the main, reselling stolen Smartphones will not be via legitimate auction sites such as eBay and usually the actual thief will not sell the stolen goods themselves. It is easy to see how the high second-hand demand for these devices is driving the trend of rising stolen Smartphone numbers.

Source: National Mobile Phone Crime Unit

Get Safe Online’s Tony Neate, once a police officer himself, believes that the driver for theft is the “actual value not the value of the information on it”. However, Neate thinks that this may change when the thieves begin to understand that there may be more value in selling these devices to organised crime gangs who may be more interested in the value of extracting potentially valuable identity, personal and financial data from the device.

For this to happen criminals need to believe that the value of this information has a higher value than the resell value of the device itself. Alternatively, if it becomes extremely difficult to resell stolen Smartphones it may force criminals to rethink their business model.

\textbf{Is information safe on a Smartphone?} But once a Smartphone is lost or stolen how easy is it to get access to the device and extract information from it?

Consumer survey research from security vendors Norton (owned by Symantec) discovered that 35 percent of Smartphone owners used no PIN or password to protect their devices and a similar study by McAfee stated that the figure was as high as 50 percent.\footnote{Hackers, viruses, phishing: why all smartphone and tablet users need to know about mobile security. www.broadbandgenie.co.uk, 8\textsuperscript{th} March 2013: http://www.broadbandgenie.co.uk/blog/20130308-hackers-viruses-phishing-why-all-smartphone-tablet-users-need-know-about-mobile-security}

\textbf{No PINS or Passwords:} Most Smartphones will have an option to lock the device, usually after a defined period of inactivity or after the user puts it into standby mode. To unlock the device the user will be required to authenticate into the Smartphone, usually by using a PIN or a password. The problem is that not all Smartphone owners will set-up a PIN or password and if they do this protection may be easily bypassed by using a weak PIN or password that can be guessed.
Study into the implications of Smartphone operating system security

**Weak PINS:** Research in 2011 by mobile app developer Daniel Amitay\(^\text{16}\) discovered that 15 percent of monitored iPhone users were using ten easy-to-guess PINs. The ten PINs were 1234, 0000, 2580 (straight down the middle of the keypad), 1111, 5555, 5683 (spells out LOVE), 0852 (straight up the middle of the keypad), 2222, 1212 and 1998. If a thief were to enter in these PINs they could possibly gain access to around 15 percent of Smartphones.

**Financial Fraud**

There is evidence of financial fraud targeting Smartphones in at least two sectors, telephony Premium Rate Services (PRS) and financial services, including banking and payment.

As commerce and financial services move onto mobile platforms than there will be more opportunity to attempt financial fraud on Smartphones. This will lead to other services that deal with finance and money, such as retail, becoming targets.

**Telephony Premium Rate Services (PRS) Fraud**

Premium Rate Services offer one way in which criminals can attack Smartphone in an attempt to undertake financial fraud.

There is evidence that there have been attacks made against Smartphone-based Premium Rate Services (PRS) in the UK.

In two separate reports\(^\text{17}\), commissioned by the UK’s PRS regulator, PhonepayPlus, Goode Intelligence determined that there was a link between mobile malware and Smartphone PRS fraud. This concurred with what PhonepayPlus was seeing as part of investigations carried out by the regulator after they had received consumer complaints of unsolicited PRS payments being charged to their mobile phone bills.

During the winter and spring of 2011/2012 PhonepayPlus recorded an increase in consumer complaints related to unsolicited PRS charges on their Smartphone bills. Unsuspecting users were being charged £15.00 every time (charged as three separate £5.00 premium rate texts) they tried to open a ‘free’ app that had been downloaded to their Android Smartphones from Android App store, including Google’s official App store (Google Play). The free apps were fake versions of popular games such as Angry Birds, Assassins Creed and Cut the Rope.

The subsequent investigation by PhonepayPlus resulted in action against a PRS provider, A1 Agregator Limited, who “had control of, and responsibility for, the premium rate payment system which enabled the malware to fraudulently charge consumer’s mobile phone.

---

\(^{16}\) Why your Smartphone’s PIN is Far More Vulnerable Than You Think. CBS News, 22\(^\text{nd}\) June 2011: http://www.cbsnews.com/8301-505143_162-28651662/why-your-smartphones-pin-is-far-more-vulnerable-than-you-think/

Study into the implications of Smartphone operating system security

accounts. A1 Agregator Limited was fined £50,000.00 and ordered to directly refund all of the consumers affected in the UK.

Patrick Guthrie, PhonepayPlus’ Director of Strategy and Communications said:

“We will continue to clamp down on those who wish to take advantage of UK smartphone customers. We are very pleased that the tribunal ordered that everyone affected will get their money back and that a strong fine was imposed. The digital economy is vital to the UK’s future and we will continue to take action to maintain the confidence of the public.”

**Figure 1.1: Screenshot from Android Market (Google Play) detailing fake (rogue) versions of popular premium games**

---

In a separate incident, PhonepayPlus fined a company called Connect Limited a total of £50,000.00 for publishing an Android app that caused the user to click on a weblink that resulted in a £10.00 premium rate text message. An estimated £250,000.00 was lost by UK consumers as a result of this fraud. Connect Limited was ordered to recompense all of the consumers that had lost money as a result of this fraud.

Paul Whiteing, chief executive of PhonepayPlus, said in a statement:

"PhonepayPlus has a strong track record of protecting consumers from misleading apps that charge using premium rate services. We will continue to work with the telecoms and security industries to understand threats to consumers and to take robust regulatory action where appropriate. We want to make sure phone users can use apps with confidence."

There is a continuing threat against Smartphone users who are accessing PRS services on their devices. Thankfully, PhonepayPlus and industry representatives including MNOs and security vendors are constantly monitoring the situation. By taking quick and direct action against companies involved in this fraud, a clear message is being sent out to other companies and individuals who may be contemplating initiating a fraud campaign.

---

Financial Services fraud

Banks are targeting Smartphone owners because they represent good business, being generally younger or more affluent.

As financial services move increasingly to the mobile channel then Smartphones will be targeted.

This is an emerging threat area and there have been a small number of examples where Smartphones have been targeted. One of the most high-profile attacks to date has been the adaptation of the Zeus financial Trojan to target Smartphones. Throughout its five year history, Zeus has successfully defrauded bank users of hundreds of millions of Pounds. In 2010 the FBI announced that it had discovered a major international cybercrime network that had used Zeus to steal around US$70 million. In this case the FBI successfully arrested this cybercrime network with the help of law enforcement partners in the UK, the Ukraine and the Netherlands.\(^{20}\)

Zeus has been upgraded to support Smartphones with the Zeus in the Mobile (ZitMo) variant. ZitMo targets the SMS-delivered two-factor-authentication (2FA) one-time-passwords (OTP), or Transaction Authentication Number (TAN), that banks use to enhance the security of their online banking services. ZitMo is designed to infect a bank customer’s device and then harvest these OTPs to then access the defrauded customer’s bank account. ZitMo has been seen on Android, BlackBerry and Symbian devices.

According to a report published by security vendors Check Point Technologies and Versafe ZitMo has been very successful and was involved in fraud to the value of £31 million (see the Eurograbber case study below).

Eurograbber case study: The case of Eurograbber grabbed the headlines in 2012 mainly because of the ‘reported’ high value of the financial fraud. A white paper published jointly by the security vendors Versafe and Check Point Software Technologies\(^{21}\) reported that Eurograbber, a variant of Zeus, managed to steal “an estimated 36+ million Euros from more than 30,000 bank customers from multiple banks across Europe”. That equates to just over £31 million. The report details that there is a mobile component to Eurograbber that is designed to steal mobile-based TANs sent to bank customers’ phones via SMS. The report does not detail the extent of the mobile-based attack and whether all of the £31 million fraud was a direct result of the TAN-stealing mobile Trojan. What it does tell us is that Smartphones can be vulnerable to targeted attacks that successfully use mobile malware.


How ZitMo works? The Zeus Trojan has been described by McAfee as “probably the most prevalent and active Trojan “Banker” families seen in the wild”\textsuperscript{22}. The Zeus Trojan attempts to steal banking information, including authentication credentials, using man-in-the-browser (MitB) keystroke logging. ZitMo is a reaction to the banks’ mobile Two-Factor Authentication (2FA) security mechanism where customers are sent one-time-passwords (OTPs), mobile transaction authorisation numbers (mTANs), to mobile phones via SMS text messaging. As part of the electronic banking login process bank customers will use this mTAN to prove that it is the authorised bank user accessing their account. ZitMo is designed to steal these mTAN codes in tandem with the main Zeus Trojan. Kaspersky Labs, in a blog entitled “Teamwork: How the ZitMo Trojan Bypasses Online Banking Security”\textsuperscript{23}, outlines how the Trojan operates:

- “Cyber criminals use the PC-based Zeus to steal the data needed to access online banking accounts and client mobile phone numbers
- The victim’s mobile phone receives a text message with a request to install an updated security certificate, or some other necessary software. However, the link in the text message will actually lead to the mobile version of Zeus
- If the victim installs the software and infects his phone, then the malicious user can then use the stolen personal data and attempt to make cash transactions from the user’s account, but will need an mTAN code to authenticate the transaction
- The bank sends out a text message with the mTAN code to the client’s mobile phone
- ZitMo forwards the text message with the mTAN code to the malicious user’s phone
- The malicious user is then able to use the mTAN code to authenticate the transaction

Privacy

Privacy and mobile phones has been a very sensitive topic in the UK over the last couple of years with various phone hacking scandals. Privacy of voicemail and SMS text messages have been violated as a result of mobile phone hacking by individuals working both directly and indirectly for some sections of the UK press. The public outcry led to a public enquiry that has made the subject of privacy and mobile phones an incredibly high-profile issue. For many cases in the phone hacking scandal privacy, breaches were a direct consequence of mobile phone theft.

For this study, privacy is related to security in terms of appropriate protection of our private lives, including our personally identifiable information (PII)\textsuperscript{24}. Privacy is also linked to data and identity theft and conversely data protection.


\textsuperscript{24} Personally Identifiable Information (PII) is defined as information that can be used to identify, contact or locate an individual. This includes name, government record IDs such as passport number,
Study into the implications of Smartphone operating system security

It is an important issue with examples of both wilful and accidental loss of privacy in both the Smartphone operating system software and within mobile apps.

Privacy issues on Smartphones include:

- **Surveillance in the form of Spyware:** Where commercially available software that can record activity on the device is installed on the Smartphone without the user’s consent. Examples of this are FinFisher and FlexiSPY. Reasons why Spyware is installed on a device include:
  o Corporate espionage
  o To catch “cheating partners” as FlexiSPY advertises

- **Location information:** This is where a system component or mobile app will collect location information and then transmit this information to a central database. There are many reasons for capturing location information, many of them as part of a legitimate service. For instance, a consumer takes a photograph with their Smartphone and tags where it was taken using the phone’s location. The grey area is what is classified as legitimate or illegitimate and what has the consent of the Smartphone owner. The EU is currently investigating location-based services as part of its Data Protection legislation review. This includes the creation of the Article 29 Working Party (Art. 29 WP), set up under Directive 94/46/EC of the European Parliament and of the Council of 24 October 1995 on “the protection of individuals with regard to the processing of personal data”\(^{25}\). Article 29 WP has released an opinion on a range of matters that include:
  o Opinion 02/2013 on apps on smart devices
  o Opinion 03/2012 on facial recognition in online and mobile services
  o Opinion 13/2011 on Geolocation services on smart mobile devices

- **Data and Identity theft/loss:** Again this can include wilful and accidental loss. It can also be related to Spyware. Examples of wilful loss of data and identity information includes:
  o After the theft or loss of a device when information is extracted from the device. This could be private and personal information that could be sensitive, e.g. personal photographs
  o Through a malicious app (malware) whose intention is to steal personal data
  o Through an app that has been poorly written and is extracting personal information that it doesn’t need
  o As part of a feature of the Smartphone operating system. In 2009 Etisalat, a middle-eastern MNO, was accused of pushing out a custom BlackBerry software update to customers in the United Arab Emirates that could intercept email and text messages\(^{26}\). Additionally HTC, the handset manufacturer, recently settled a court case brought by the US’ Federal Trade Commission

---

26 BlackBerry update bursting with spyware. The Register, 14 July 2009: http://www.theregister.co.uk/2009/07/14/blackberry_snooping/
Study into the implications of Smartphone operating system security

(FTC) were HTC was accused of installing software, Carrier-IQ, that tracks device logs or user location\(^{27}\)

It is worth noting that there are many forensic tools that enable trained and semi-trained individuals to retrieve data and information from a Smartphone even when the device has been locked.

\(^{27}\) HTC settles with FTC over leaving Carrier IQ and other logging tools open to hackers. The Verge, 22 February 2013: http://www.theverge.com/2013/2/22/4017746/htc-settles-with-ftc-over-insecure-logging-software
2. HOW UK MOBILE NETWORK OPERATORS (MNOS) SUPPORT SMARTPHONE OPERATING SYSTEM UPDATES

Overview

A major goal for Smartphone operating system software updates is to get the updates and security fixes installed on smartphones as quickly and as smoothly as possible without interfering with the usual running of the device and the mobile network – to balance security needs with usability.

There are many stakeholders involved in the process of developing, testing, distributing and installing Smartphone operating system software updates. These include the operating system developer (the platform owner), the Smartphone manufacturer (device OEM), the MNO and the Smartphone owner. This process is represented in figure 2.1 below.

Figure 2.1: Smartphone Operating System Update Process Management

MNOs (MNOs) are an important part of the Smartphone operating system update process.

The majority of Smartphones purchased in the UK will be made through an MNO and as such they will have a role in the operating system update process.

From a consumer point of view, the MNO will usually be the first point of contact for any support contact that they will make as a result of a problem with a mobile device, including operating system updates and patching issues.

The role of the MNO in supporting Smartphones on their network can include Smartphone operating system customisation, where this is permissible. In the UK, Smartphone
Study into the implications of Smartphone operating system security

customisation may include the development of operator-specific mobile Apps that will be tied into a service. This can include mobile Apps that enable the device owner to access an MNO-branded mobile App store.

There will be a number of Smartphones that are not purchased from a MNO and these unlocked devices will not be customised to work on a particular MNO network and may not be part of a MNOs update process. A consumer will purchase the unlocked Smartphone from a retailer and then they will access the mobile network by inserting a SIM card into the device. These devices are not customised to work on a particular network and the operator will usually have no knowledge of, or management responsibility for them. In these cases the question is. What is the risk to the MNO of having Smartphones connected to their network that the MNO does not directly manage? There are also scenarios when a consumer will purchase a connected smart mobile device (SMD), e.g. a tablet or “phablet”\(^2\), through a general retailer – not through the MNO. If this is a WiFi-only device it cannot support a SIM and therefore cannot access the mobile network (unless it uses a GSM dongle or Mobile WiFi device). In these cases, the consumer will liaise with the retailer for warranty related issues and then directly with the device manufacturer for operating system issues, including updates.

**When are Smartphone operating system updates released?**

There are two main reasons why mobile operating systems are updated:

1. Feature and functionality change.
2. Emergency patch as a result of a system bug or security vulnerability

**Analysis of mobile operating system updates**

**Introduction**

This section provides an analysis of generic mobile operating system updates.

There may be local (regional) and MNO variations to this process but in the main this section will detail how mobile operating system updates are managed on a mobile platform by platform basis.

The section also includes background information about each mobile operating system including a brief history and statistics.

This section should not be viewed as a support guide to install mobile operating system updates. Information and ‘how-to’ guides can be obtained from a number of sources including MNOs, handset manufacturers and mobile operating system providers (owners of the mobile platform).

---

\(^2\) A Phablet is a merging of the words phone and tablet to describe a device that is too large to be described as a phone and too small to be described as a tablet. Phablet screen sizes range between 5 and 7 inches. The Samsung Galaxy Note is an example of a Phablet.
Study into the implications of Smartphone operating system security

Before we explore how the four major Smartphone platforms manage their operating system update process we shall examine a basic view of a generic update process.

**Basic view of generic update process**

For Smartphones that are purchased from an MNO and are connected to an operators' cellular (GSM29) network the generic model for Smartphone operating system updates works along these lines:

1. Mobile operating system owner (the mobile platform builder) develops the operating system software (firmware) update
2. The mobile operating system owner then distributes the source code to the hardware manufacturer (the Original Equipment Manufacturer – OEM). Please note that the OEM can also be the operating system owner as is the case for Apple and BlackBerry Smartphones
3. The mobile operating system update will be made available to MNOs for testing
4. The MNO tests that the software update is compatible to its range of devices. Testing will ensure the device can function on the MNO’s network without problems.
5. Software update is pushed out, usually by the Smartphone manufacturer. Using Firmware Over-The-Air (FOTA)30 technology where supported.

**A guide to mobile operating system updates according to platform**

**Introduction**

There are different update models that each of the four main Smartphone operating system vendors have adopted. Dependent on the model adopted there will be lower and higher degrees of complexity in this process.

It is generally the case that where the platform owner is also the hardware manufacturer then the process is less complex.

The more complex model is when you have platform owner that either does not own the manufacturing component of building a Smartphone itself and/or when that platform owner does not have strict controls over how hardware manufacturers build their mobile devices.

This complexity can be further heightened if a MNO has the ability to make further changes to the operating system prior to delivery to the consumer.

---

29 Global System for Mobile Communications (GSM). Originally Groupe Special Mobile is the standard developed by the European Telecommunications Standards Institute (ETSI) to define the protocols for second generation (2G) mobile phone networks.

30 Firmware Over-The-Air (FOTA) is used for software updates on mobile phones and tablet computers. The Open Mobile Alliance has released a testing process specification on Firmware Update Management which standardises testing methods for FOTA.
Study into the implications of Smartphone operating system security

Analogies can be made with the personal computer model and lessons can be learnt from organisations like Microsoft and Apple. Both of these technology companies have over 30 years of operating system management experience.

Each section will be complemented by additional, technical, information that will be available in the appendix.

**Apple iOS**

---

**History of Apple iOS**

---

Apple’s iPhone OS (quickly renamed to iOS) was originally released (version 1.0) in June 2007 for two Apple devices, the iPhone and the iPod Touch. These are handheld devices that use touch as the main user interface.

iOS is derived from OS X\(^3\) and both are based on the Darwin\(^2\) open source operating system (UNIX-based operating system) released by Apple in 2000.

In 2010 Apple announced the iPad, a new device running iOS, featuring a larger screen than the iPhone and the iPad.

The latest versions of Apple TV, Apple’s digital media receiver, also run iOS (second and third generation Apple TVs run iOS 6.1.1 – released November 2012).

---

\(^3\) Apple OS X, previously Mac OS X, is an Apple operating system designed for Apple Mac computers. It is based on UNIX and has been pre-loaded on Mac computers since 2002.

\(^2\) Darwin is an open-source POSIX-compliant operating system with code derived from NeXTSTEP and BSD (Berkeley Software Distribution or Berkeley Unix) open source projects.
Study into the implications of Smartphone operating system security

Apple devices that run iOS include:

- iPhone
- iPod Touch
- iPad
- iPad Mini
- Apple TV

See Appendix A for a table that lists iOS devices and operating systems that they were initially launched with along with the highest supported operating system.

Apple has released six full versions of the iOS Operating system since June 2007 (a little more than one full release per year). See Appendix B for a table that details Apple iOS version history.

**Apple iOS Stats**

- There are over 800,000 apps available to iOS devices
- Worldwide Apple App Store customers have downloaded over 40 billion apps
- iOS6 is used on nearly 300 million devices worldwide
- The Apple App Store has over 500 million active accounts worldwide

---

Study into the implications of Smartphone operating system security

- UK sales (market share) of iPhones at January 2013 is estimated at 30.6 percent\textsuperscript{35} making iOS the second most popular Smartphone platform
- By January 13 2013, 60 percent of iOS install base had updated their devices to latest version, iOS 6.0\textsuperscript{36}, in less than a four month period

**Operating system updates**

This section details how Apple manages software updates for iOS devices.

Apple will push out iOS updates for a variety of reasons including major functionality changes (full releases), minor functionality changes and emergency patches as a result of reported bugs or security vulnerabilities.

Users will be notified that a new release is available usually via a message displayed on the iOS device. An example is shown below in figure 2.2.

**Figure 2.2: Software update notification on iPhone 4GS**

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{software_update_notification.png}
\caption{Software update notification on iPhone 4GS}
\end{figure}

\textit{Source: Apple}

\textsuperscript{35} Kantar Worldpanel figures: http://www.kantarworldpanel.com/global/News/news-articles/Smartphone-Competition-Hots-Up
\textsuperscript{36} Interview with Apple on Friday 8\textsuperscript{th} March 2013
Study into the implications of Smartphone operating system security

Dependent on the policy adopted by a MNO, iOS users may be notified of a new release via email or even SMS text messaging. The role of MNOs in mobile operating system upgrades is discussed in more details in subsequent chapters.

Apple has devised two ways in which a consumer can update the operating system of an iOS device.

1. Wirelessly using an FOTA update process from the device itself (available from iOS 5.0, released 12 October 2011)
2. Via Apple’s iTunes media application

**WIRELESS - OVER-THE-AIR (OTA) - IOS UPDATE PROCESS**

FOTA software updates for iOS devices have been available since iOS 5 was released during October 2011.

This feature was part of Apple’s wireless and cloud strategy that untethered the device from a personal computer. Users no longer had to connect their iOS device to a personal computer for synching and operating system updates.

Not all iOS updates are available as FOTA updates.

See Appendix C for details on how this process currently works.

**APPLE ITUNES IOS UPDATE PROCESS**

Previous to the release of iOS 5.0 users had to physically connect their devices to Apple iTunes, via a personal computer, to allow system updates. This function is still available and is examined in full in Appendix D.
Study into the implications of Smartphone operating system security

Google Android

History of Google Android

Android is a Linux-based operating system originally developed by Android Inc., a company founded in 2003 by Andy Rubin. Google initially funded then acquired Android Inc. in 2005, making it a wholly-owned subsidiary.

The Android operating system was launched in 2007, becoming the first product of the Open Handset Alliance (OHA)\(^\text{37}\), a consortium of companies that included device manufacturers such as Samsung and HTC, MNOs including Sprint Nextel and T-Mobile and chipset makers such as Qualcomm and Texas Instruments.

\(^{37}\) The Open Handset Alliance is a consortium of firms set up to develop open standards for mobile devices. The OHA was established in November 2007 by Google.
Study into the implications of Smartphone operating system security

Android is an open source software product with Google releasing the code under the Apache License Foundation (ASF)\textsuperscript{38}.

Unlike Apple iOS that is only available on hardware designed and manufactured by Apple, Android is available on a variety of different manufacturers’ devices. Android source code is licensed (for free) to hardware manufacturers through the Apache License and the GNU\textsuperscript{39} General Public License\textsuperscript{40} (Linux Kernel distribution).

In addition to Google’s own-brand range of ‘Nexus’ devices, Android has been licensed to some of the biggest names in technology manufacturing including:

- Asus
- Dell
- HTC
- LG
- Huawei
- Kyocera
- Motorola
- Samsung
- Sharp
- Sony
- ZTE

Android is running on a variety of devices including Smartphones, tablet computers and phablets Android is a flexible operating system that can run on other electronic devices that can benefit from its low power consumption and touch-screen user interface including watches, smart TVs, cameras and within in-car entertainment systems.

Google has released four full versions of its Android operating system since October 2008 (although Android beta was released in November 2007).

Android versions, since April 2009, have been assigned a codename in addition to a version number. These codenames have a food theme and include Gingerbread and Ice Cream Sandwich. Android’s version history can be found in Appendix E.

Google Android 5.0 Key Lime Pie is reported to be scheduled for release in the second quarter of 2013.

\textsuperscript{38} Apache Software Foundation is a non-profit corporation that supports Apache software projects, including the Apache HTTP Server. The Apache License is a free open-source license for software.

\textsuperscript{39} GNU Unix was developed by the GNU Project.

\textsuperscript{40} GNU General Public License is a free software licensing using the copyleft framework which means that derived works can only be distributed under the same license terms. Source: http://en.wikipedia.org/wiki/GNU_General_Public_License
**Android iOS Stats**

- There are more than 600,000 apps available on Google Play
- Android users download more than 1.5 million apps from Google Play every month
- Android has the largest install base of any mobile platform
- Every day more than one million new Android devices are activated worldwide
- UK sales (market share) of Android devices at January 2013 is estimated at 56.2 percent making it the number one mobile platform by sales in the UK\(^\text{41}\)
- Samsung is the largest manufacturer of Android devices with an estimated 40.2 percent of Android Smartphone market and 27.9 percent of the Android tablet market during the fourth quarter of 2012\(^\text{42}\)

**Figure 2.3: Android growth in device activations – 2009-2012**

---


\(^\text{42}\) Figures from IDC reported in Wall Street Journal: http://blogs.wsj.com/digits/2013/02/25/can-samsungs-android-rivals-catch-up/
Study into the implications of Smartphone operating system security

**Version distribution**

As the following table and pie-chart details, Table 2.1, 45.6 percent of Android users are running version 2.3 (Gingerbread), initially released in December 2010.

**Table 2.1: Current distribution of Android versions (collected 4 February 2013)**

<table>
<thead>
<tr>
<th>Version</th>
<th>Codename</th>
<th>API</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.6</td>
<td>Donut</td>
<td>4</td>
<td>0.2%</td>
</tr>
<tr>
<td>2.1</td>
<td>Eclair</td>
<td>7</td>
<td>2.2%</td>
</tr>
<tr>
<td>2.2</td>
<td>Froyo</td>
<td>8</td>
<td>8.1%</td>
</tr>
<tr>
<td>2.3 - 2.3.2</td>
<td>Gingerbread</td>
<td>9</td>
<td>0.2%</td>
</tr>
<tr>
<td>2.3.3 - 2.3.7</td>
<td></td>
<td>10</td>
<td>45.4%</td>
</tr>
<tr>
<td>3.1</td>
<td>Honeycomb</td>
<td>12</td>
<td>0.3%</td>
</tr>
<tr>
<td>3.2</td>
<td></td>
<td>13</td>
<td>1.0%</td>
</tr>
<tr>
<td>4.0.3 - 4.0.4</td>
<td>Ice Cream Sandwich</td>
<td>15</td>
<td>29.0%</td>
</tr>
<tr>
<td>4.1</td>
<td>Jelly Bean</td>
<td>16</td>
<td>12.2%</td>
</tr>
<tr>
<td>4.2</td>
<td></td>
<td>17</td>
<td>1.4%</td>
</tr>
</tbody>
</table>

*DATA COLLECTED DURING A 14-DAY PERIOD ENDING ON FEBRUARY 4, 2013 SOURCE: GOOGLE*

Operating system updates

OVERVIEW

Android does not have a generic, single, method for managing operating system software updates. By licensing the platform based on an open-source software method, Google does not have full control over the method in which its licensees manage the software update and emergency patch process.

Google has some degree of control over the Android ecosystem. It manages the development of new versions of the Android operating system and ensures that third-party companies (hardware OEMs) using it in their devices adhere to the Compatibility Definition Document (CDD).

Section 11 of the Android 4.2 CDD references software updates and states:

“Device implementations MUST include a mechanism to replace the entirety of the system software. The mechanism need not perform "live" upgrades - that is, a device restart MAY be required.

Any method can be used, provided that it can replace the entirety of the software preinstalled on the device. For instance, any of the following approaches will satisfy this requirement:

- FOTA downloads with offline update via reboot
- "Tethered" (physically connecting a Smartphone to a PC) updates over USB from a host PC
- Offline" updates via a reboot and update from a file on removable storage

The update mechanism used MUST support updates without wiping user data. That is, the update mechanism MUST preserve application private data and application shared data. Note that the upstream Android software includes an update mechanism that satisfies this requirement.

If an error is found in a device implementation after it has been released but within its reasonable product lifetime that is determined in consultation with the Android Compatibility Team to affect the compatibility of third-party applications, the device implementer MUST correct the error via a software update available that can be applied per the mechanism just described.”

This section gives Android OEMs a good degree of flexibility in defining the process for operating software updates.

44 Android compatibility program. Android 4.2 Compatibility Definition, revision 2, updated 17 February 2013.
By having an open source model Google does lose a degree of control in the operating system update process. What it gains in openness and flexibility by being available on millions of devices from different hardware manufacturers it loses in control over the software update management process.

Currently Google does not mandate when a software update is put on a partner's device or when that partner pushes it out to its device owners. This results in a situation where Google releases a software update and then pushes it out to its own-brand devices but then has to rely on its other hardware partners to manage the software update themselves. This can result in a delay in Android device manufacturers releasing software updates to its device community.

Except for Google-branded Android devices, the Android hardware manufacturer (OEM) is responsible for the software update lifecycle and management process.

Android operating system software is pushed into the Android Open Source Project (AOSP) repository by Google. From here hardware manufacturers, who want to use and license Android, can download the source code. The hardware manufacturer may want to adapt the source code and add additional features that make their Android devices unique. This creates a new version of the firmware based on the source code that is held in the AOSP repository.

Google has also created a standard that all hardware manufacturers must meet before they can use Google’s Android trademark. This standard is defined in the Compatibility Definition Document (CDD). Compatibility with the CDD also means that the hardware manufacture is eligible to license Google applications including Google Play (Google's mobile App store) and Google Maps. Google has created a test process, with tools, that enables hardware manufacturers (OEMS) to test new software updates and security patches. At the heart of this test process is the ‘Google Compatibility Test Suite (CTS)’.

As there are over 20 hardware manufacturers licensing the Android platform for use in their devices it would be difficult to investigate how they individually manage software updates. Instead, this report details how two device owners (manufacturers) manage this process. Firstly, how Google manages this process for its own-branded devices (in practice this is Google’s reference model for software management and as such is called “Pure Google”) and secondly how the current number one Android device manufacturer, Samsung, deals with operating system software updates.
Android Fragmentation – Cause for concern?

Android's fragmentation issue does have an adverse effect on its ability to successfully manage the end-to-end operating system software update process. This is more acute for ensuring that Android Smartphones are patched against the latest security vulnerabilities. There are millions of Android Smartphones that are either running earlier versions of Android (especially Android Gingerbread) and do not have a way to update their devices, unless they 'root' them, or cannot update to later versions because the hardware cannot support more up-to-date versions of the Android firmware.

Google are well aware of the fragmentation issue and have attempted to solve the problem. At the 2011 Google I/O conference, they announced the creation of the ‘Android Update Alliance’, an initiative to overcome the fragmentation issue with the help of their hardware manufacturing partners. The Alliance’s aims included mandating that Android mobile devices would receive software updates for at least 18 months after their introduction.

In contrast Apple iOS provides Smartphones with a longer software update lifecycle. The original iPhone was provided with 32 months of software updates; originally released in June 2007 the last software update, iOS 3.1.3, for this Smartphone was released February 2010. It is questionable how influential this Alliance has been as there has been little public news since the original announcement in 2011.

The latest attempt by Google to solve this problem was in January 2012 when Google changed the terms of service (TOS) of the Android SDK (used by developers to create Apps to run in Android) and introduced a new clause that states:

“3.4 You agree that you will not take any actions that may cause or result in the fragmentation of Android, including but not limited to distributing, participating in the creation of, or promoting in any way a software development kit derived from the SDK.”

Unfortunately, the flip-side of Android’s open source model and its availability on many different manufacturer’s mobile devices has resulted in less direct control over both the handset manufacturers who have licensed Android and the MNOs who are allowed to customise the platform prior to delivery to the majority of the UK’s Android user base. Android fragmentation does have a direct, negative, impact on the operating system update process.”
Google’s own-brand Android device range, Nexus, is available in three form factors:

- Smartphone: Nexus 4 (manufactured by LG). Released November 2012
- Small Tablet: Nexus 7 (manufactured by Asus). Released June 2012
- Large Tablet: Nexus 10 (manufactured by Samsung). Released October 2012

Nexus One, the first Google Android Smartphone manufactured by HTC, was released in January 2010, running Android 2.1 Eclair, although it decided to drop support of the device due to poor screen rendering when running the 2D acceleration engine found in Android 4.0 Ice Cream Sandwich.

It is interesting that Google makes a marketing point in that its Nexus range of smart devices “comes with the latest version of Android and gets updates directly from Google, so you’ll always have the fastest, most up-to-date software on your phone.”

It is important to note that Google information relating to Android operating system updates is hard to track down. There is no obvious place within Google’s support website or within the user manuals for any of the latest crop of Nexus devices that states how this process works.

The only obvious information on this process was found in the “Software Updates” section of the ‘Google Play’ support website. This states:

“Devices purchased on Google Play are Pure Google and among the first to receive the latest software updates from Google. We are pushing out updates to Nexus devices as quickly as possible and we will continue to provide the latest updates to these devices going

45 Google marketing: http://www.google.com/nexus/4/
Study into the implications of Smartphone operating system security

forward. For devices purchased on Google Play, you can expect software updates to come directly from Google. 46

In an attempt to obtain information on this process the report author called Google Play Device Technical Support. Unfortunately they were unable to explain the process or to make available any support documents that may have assisted a Nexus user in understanding more about the update process.

There has also been debate on some mobile developer forums that in some cases the software update is not being delivered by Google themselves but by the hardware manufacturer. This has been reported with some Google Nexus devices manufactured by Samsung running in certain regions. 47

HOW IT WORKS

There are two major ways in which a Nexus device is able to perform an operating system update:

1. Wirelessly using an FOTA process
2. Manually by downloading the factory image from the official Google Developers website

Google will automatically push out operating system updates using an Over-The-Air (OTA) procedure to its Nexus range of smart mobile devices.

If, for some reason, a Google OTA update fails to work or is not available on a particular model or through a certain mobile network then there is a manual method to download and install the updates software.

The manual method is not a recommend approach for Nexus owners who may not be technically proficient.

This manual procedure does not come without an element of risk - If a Nexus owner does not follow the manual update procedures correctly than there is a possibility that the device may be 'bricked', e.g. it will no longer work and could become completely unusable.


46 http://support.google.com/googleplay/bin/answer.py?hl=en&answer=2589788
47 Not all GSM Galaxy Devices will be updated directly by Google: http://androidandme.com/2011/12/devices/not-all-gsm-galaxy-nexus-devices-will-be-updated-directly-by-google/
Study into the implications of Smartphone operating system security

SAMSUNG ANDROID DEVICES

Samsung uses a personal computer (PC) program (available for both Windows and Mac PCs) called ‘Samsung Kies’ to manage Android operating system updates.

Users are required to download the program to their PCs and then either physically connect the device to the PC or use an Android App, ‘Kies Air’ on the device itself to connect to the PC software using WiFi.

Figure 2.4: Samsung Kies screenshot showing Android firmware update information

Source: Samsung
BlackBerry

History of BlackBerry

BlackBerry OS is a proprietary mobile operating system developed by BlackBerry (formally known as RIM) and used on the BlackBerry range of Smartphones.

BlackBerry devices are best known as enterprise Smartphones that are capable of receiving corporate email wirelessly achieved through synchronisation with the most popular enterprise email servers including Microsoft Exchange, Lotus Domino and Novell GroupWise. Wireless enterprise services are achieved using a middleware solution, the BlackBerry Enterprise Server (BES).

BlackBerry OS was first launched in January 1999 with the release of version 1.0 for a Paging device, Pager BlackBerry 850 (see figure 2.5 below).

Figure 2.5: Pager BlackBerry 850

Source: BlackBerryOS.com

The latest version of BlackBerry OS is 7.1.0.8661 released on 6 February 2013. However, a revised operating system, Blackberry X (10), was announced in October 2011 that replaced the java based operating system previously used.

BlackBerry has been famous for its easy-to-use physical keyboards that sit well with its use as a wireless messaging device. Recent BlackBerry devices, including the latest BlackBerry Z10 (see figure 2.6 below), have gone for a pure touchscreen interface, i.e. no physical keyboard. The Z10 has been released alongside a more traditional BlackBerry device that has a physical keyboard, the BlackBerry Q10.
Study into the implications of Smartphone operating system security

Figure 2.6: BlackBerry Z10 and Q10

BlackBerry OS Stats

- UK sales (market share) of BlackBerry OS devices at January 2013 is estimated at 5.8 per cent making it the fourth most popular Smartphone platform by sales in the UK\(^48\), only slightly behind Windows Phone who had 6.2 per cent of sales
- BlackBerry World (BlackBerry’s mobile App store has had 90,000 app uploads as at mid-2012)\(^49\)
- BlackBerry Smartphones and PlayBook (tablet) users had downloaded over 3 billion apps since Blackberry World was launched in April 2009\(^50\)

---


\(^{49}\) http://crave.cnet.co.uk/software/windows-phone-store-hits-150000-apps-doubled-in-last-year-50010072/

\(^{50}\) BlackBerry blog; “3 billion and counting”: http://devblog.blackberry.com/2012/07/three-billion-and-counting/
Study into the implications of Smartphone operating system security

Operating system updates

HOW IT WORKS

BlackBerry has three methods which it uses to deliver operating system updates to its Smartphone owners.

1. Through the web for Windows PC users

2. By physically connecting a BlackBerry device to a PC and initiating the software download and update process using either BlackBerry Desktop Software (BlackBerry 7.1 OS and earlier) or BlackBerry Link for BlackBerry 10 OS

3. Wirelessly using BlackBerry’s Over-The-Air Software Loading (OTASL) service
Study into the implications of Smartphone operating system security

**Notification:** An email notification service is available for Blackberry software updates that device owners are required to subscribe to.

There is also a notification that can appear through the BlackBerry Desktop Software informing the device owner that an updated version of the BlackBerry device software is available to download. – the new version number will be listed on the screen.

Updates to BlackBerry Playbook users is achieved using an OTA service as detailed in Figure 2.7 below.

**Figure 2.7: Updating BlackBerry PlayBook OS devices**

![Source: BlackBerry](source.jpg)
Study into the implications of Smartphone operating system security

**Microsoft Windows Phone**

Windows Phone is a proprietary mobile operating system developed by Microsoft and is the successor to Windows Mobile.

In its latest version, Windows Phone 8 (WP8), it is based on the Windows NT kernel and shares many components of the desktop version of Windows 8.

Microsoft licenses Windows Phone to mobile phone manufacturers (OEMs) in a similar manner to its desktop business model.

Notable mobile phone manufacturers include Nokia (who it has a formal partnership arrangement with), HTC, Huawei, LG and Samsung.

The Windows Phone Store is the digital distribution platform, mobile App store, for Windows Phone devices.

**History of Windows Phone**

Source: Microsoft
Study into the implications of Smartphone operating system security

Windows Phone was first launched in November 2010 and follows in the footsteps of a long line of Windows mobile operating systems going back to 2000 Windows Mobile and the Pocket PC range of devices.

Windows Phone has had two major operating system versions since its launch in 2010. Windows Phone 7 and Windows Phone 8.

The Windows Phone Store was launched in its ‘Marketplace’ name in October 2010. It was renamed ‘Store’ in August 2012.

Microsoft has announced its intention to stop supporting Windows 7.8 and 8 by the second half of 2014. Microsoft’s operating system timetable means that each version of the operating system gets 18 months of support from launch. Hopefully this means that Smartphones purchased during this 18 month timetable will have the ability to be upgraded to newer versions of the operating system.

Windows Phone 7

- Publically launched in the USA during November 2010
- Updated versions:
  - Windows Phone 7.5 (Mango) released May 2011
  - Windows Phone 7.5 (Tango) released 2012
  - Windows Phone 7.8 released January 2013
- A full version history for Windows Phone 7 is available from Microsoft at http://www.windowsphone.com/en-GB/How-to/wp7/basics/update-history

Windows Phone 8

- Windows Phone 8 (Apollo) Released 29 October 2012 with Metro user interface
- A minor bug-fix software update 8.01.10211.204 was released 11 December 2012

Windows Phone iOS Stats

- There are 130,000 apps available in the Windows Phone Store 51
- Windows Phone 7 accounts for 81 percent of Windows Phone market 52
- Nokia has the largest share of the Windows Phone market with 76 percent of the UK market 53
- UK sales (market share) of Windows Phone devices at January 2013 is estimated at 6.2 percent making it the third most popular Smartphone by sales in the UK 54

---

51 http://www.neowin.net/news/microsoft-130000-windows-phone-apps-now-available
52 http://blog.adduplex.com/2013/01/windows-phone-device-stats-for-january.html
53 http://blog.adduplex.com/2013/01/windows-phone-device-stats-for-january.html
Operating system updates

HOW IT WORKS

Microsoft manages Windows Phone software updates and will release updates on a staggered schedule throughout the world. When a Windows Phone device owner will get an update is dependent on different factors including type of device and what MNO is being used.

There is a different update process for Windows Phone 7 and Windows Phone 8.

WINDOWS PHONE 7

Windows Phone 7 software update information is made available through the update central website.

When a Windows Phone 7 software update is available a message will appear on the device informing the owner that an update is available.

Windows Phone 7 updates are managed through a personal computer application called ‘Zune’ and the device owner will be required to physically connect. Zune is available only for Windows users and a separate Windows Phone application is needed for Mac users.

WINDOWS PHONE 8

Windows Phone 8 software update information is made available through the update central website.

When a Windows Phone 8 software update is available a message will appear on the device informing the owner that an update is available.

Windows Phone 8 supports OTA software updates and also has an automatic update feature that allows the software update to be automatically updated. This feature automatically checks that the battery life is good enough to support the entire update process.

There is also a manual feature that allows the user to check for available Windows Phone 8 software updates.
Study into the implications of Smartphone operating system security

3. ANALYSIS OF HOW UK MOBILE NETWORK OPERATORS (MNOS) MANAGE MOBILE OPERATING SYSTEM SOFTWARE UPDATES

Overview

This section analyses how UK MNOs manage the mobile operating system software update process, including the frequency of software updates and how these updates are communicated to Smartphone owners.

As part of the research for this study, Goode Intelligence has interviewed representatives from some of the UK's MNO community to determine what involvement they have in the Smartphone operating system update process. Their involvement in this process is largely uniform on an operator by operator basis. Where it differs is between the different Smartphone operating systems.

There is no standard Smartphone operating system update process. There is a different process, and therefore a different level of operator involvement, for each Smartphone operating system. For instance, Apple, Blackberry and Windows Phone will largely manage the operating system software update process themselves.

That is not to say that the operators have no involvement in this process. In an interview between Apple and Goode Intelligence as part of this research, a spokesperson stated Apple "works closely with carriers (MNOs) to ensure that the updated operating system works on their network". Additionally if a software update affects the radio stack (the part of the operating system that manages communication between the Smartphone and the Operator's cellular (radio) network), then the MNO will be involved in ensuring that the change has not affected the device's ability to connect to their cellular network.

The MNOs are largely unable to make any changes to the operating system but will authorise that the software updates are compatible with the network. Conversely, MNOs have much more involvement in testing software updates for Android Smartphones and to a lesser degree with Windows Phone 7 (Windows Phone 8 does have an option to take updates directly from Microsoft but only if users agree not to contact the MNO's directly for any support problems with the operating system).

There have been criticisms with the role of the operator in this process, in particular with the delay between the software update being available by the mobile operating system owner/OEM to it being pushed out by the operator. In the following sections we shall investigate whether this criticism is well-founded and look at the reasons why delays occur and its impact on Smartphone owners.

---

55 Goode Intelligence thanks Telefonica O2 and Vodafone for their support
56 Apple interview: Friday 8 March 2013.
The role of MNOs in managing mobile operating system updates

UK MNOs are responsible for ensuring that the mobile phone network is reliable and available.

With modern 3G and 4G networks UK operators have to ensure that the reliability and availability of the network is not just pertinent to voice communications but data traffic as well.

Management of data traffic, including mobile broadband, within the mobile network is becoming an essential, and increasingly used (see figures from Ofcom below), part of an Operator’s service.

**Ofcom data from 2012 Communications Market Report**

“Growth in Smartphone take-up resulted in increasing use of mobile data in the year to Q1 2012. The average time spent using mobile data services was 2.1 hours a month in 2011, 25 minutes per month (24.7%) more than in 2010, while the volume of data consumed more than doubled in the 18 months to January 2012.”

To ensure that the quality and integrity of the UK’s mobile phone network is maintained MNOs have to ensure that mobile devices that are connecting into their networks are controlled and do not unduly effect the network’s operation in any way. This includes both the cellular (radio) and data networks.

As, in the majority of UK cases, the MNO owns the Smartphone and manages the connectivity to the radio network, they want as much control in software updates, including testing as is possible and allowable. Some Smartphone manufacturers, including BlackBerry, make it easier for operator testing by separating out the Smartphone’s system software into two categories; the radio stack and the operating system (no or little involvement in connecting to the radio network).

For BlackBerry OS if there are no changes to the radio stack but changes to the operating system then the MNO will have no or little involvement in the software update process and there will be no operator testing. In this scenario, the BlackBerry Smartphone owner will be notified directly by BlackBerry of the need to update the operating system software. This results in a potentially speedier software update schedule as there are no delays as a result of operator involvement in this process.

In other cases the MNO will get involved in Smartphone testing and these will occur every time an operating system update is made. They will ensure that changes to the Smartphone operating system will not adversely affect both the stability of the device, ensuring that customer data is not corrupted, and the operation of the network – the technology aspects

---

57 Ofcom 2012 Communications Market Report Page 14
Study into the implications of Smartphone operating system security

that the operator controls. On average the testing phase will take approximately eight weeks. There will be variations to this time period based upon the Smartphone type and if many defects are found during testing.

MNOs have discovered problems during this testing phase and this has been as serious as rendering the device completely unusable, e.g. ‘bricking’, the Smartphone under test.

The typical process for releasing mobile operating system updates to MNO customers involves three main steps (see figure 3.1):

1. The Smartphone operating system software will be updated by the owner / builder and released to the MNO community. Where the operating system builder/owner is different from the handset manufacturer then this will be a two-step process.
2. The MNO will receive the update and will either fully test or authorise the release. This stage may include making changes to the operating system that are required to ensure that the operating system is compatible with the Operator’s network and testing to ensure that any Operator mobile Apps are not affected by the changes.
3. Once tested and authorised the MNO will push the operating system update out to its customers and monitor for any feedback. Most MNOs will have a group of ‘Friendly Users’ that receive the updated software in advance of the main push out to the remaining customers. If the Smartphone can support FOTA updates than this will be used if not the customer will be required to download the update through a specific mobile operating system utility tool that will be loaded onto a PC, e.g. Samsung Kies or Apple iTunes.

**Figure 3.1: Typical Smartphone Operating System Update Process**

[Diagram of the typical smartphone operating system update process]

*Source: Goode Intelligence © 2013*
Study into the implications of Smartphone operating system security

*Frequency of Smartphone operating system updates provided by UK Mobile Network Operators (MNOs) and the impact on security patching*

The frequency of operating system updates provided by UK MNOs is by-and-large governed by the mobile operating system vendors and the handset manufacturers. They own the platform and manage the update process.

However, as MNOs manage the direct relationship with the customer - the majority (71 percent 58) of UK smartphone owners will have purchased their device either through the operator directly, via a reseller or through an Mobile Virtual Network Operator (MVNO), e.g. Virgin Mobile, that is running on top of the operator network - the final leg of the update process, delivery to smartphone owners, will be managed by the operator.

There will be a delay from when the operating system update will be released by the owner to when the operator will push out to smartphone owners. This delay can be frustrating to some smartphone owners who are keen to have the latest version of the mobile operating system. It also has an impact on the security of the device in that unpatched operating systems can be at risk to known security vulnerabilities. In fact, many emergency software updates, patches, are often the direct result of patching discovered security vulnerabilities.

This means that the delay in pushing out security patches to Smartphone operating systems by MNOs has a direct impact on Smartphone security and can result in increased risk to those devices still running older, unpatched, operating system versions.

*Challenge of supporting multiple versions of Smartphone operating systems*

As part of this research, Goode Intelligence contacted all UK MNOs with Telefonica 02 and Vodafone responding to our request with information. They claim that although supporting multiple versions of Smartphone operating systems is very challenging, it is part of their normal “business as usual process”. The challenges include:

- **Lack of control**: The MNOs are reliant on their suppliers, e.g. handset manufacturer/platform owner for managing the end-to-end mobile operating system software lifecycle and process
- **Support burden**: By owning the Smartphone customer, MNOs will receive the bulk of support calls in relation to the software update process even though in many cases they do not own or control the process
- **Testing / Approval responsibility**: MNOs are responsible for the mobile network, its integrity, availability (Quality of Service or QoS) and security. As a Smartphone will be connected to a mobile network, they must ensure that any new device or software update does not adversely interfere with the network’s operation. This includes

---

58 comScore MobiLens, January to December 2012, 3 month average
Study into the implications of Smartphone operating system security

supporting older Smartphones and running older versions of the mobile operating system

How they are responding?

It is early days in terms of a coordinated effort from the MNO community in response to this problem. They know they have a problem and are actively seeking a solution to manage different operating systems from a wide range of handset manufacturers, all with their own unique way of dealing with software updates and handset management.

Some operators, such as Telefonica O2, have reacted to this problem by setting up a Smartphone forum that holds monthly meetings to find ways in which to best deal with this issue.

The MNO’s industry trade organisation, the GSMA, is also attempting to deal with this problem and has set the wheels in motion by setting up a working group, under the control of the GSMA’s Security Group (SG) to develop a cross-network, platform agnostic, solution that solves the problem of delivering critical security updates to Smartphones and to investigate how best to manage the process.

GSMA Facts

The GSMA’s mandate is to represent “the interests of MNOs worldwide”. Its members include nearly 800 of the world’s MNOs in some 220 countries. Membership is also open to the broader mobile ecosystem including handset manufacturers, software companies and equipment providers. The GSMA manages industry-leading mobile events such as Mobile World Congress (MWC) held annually in Barcelona, Spain. The GSMA Fraud and Security groups are made up of industry experts and regularly meet to ensure that mobile fraud and security issues are resolved.

Criticism of Mobile Network Operators in the software update process

There has been criticism from a number of quarters to the way that MNOs seemingly delay the release of mobile operating system updates.

Much of the criticism has especially been targeted at how they manage Android system updates. Is this a problem of the MNOs’ making or are they victims to Android’s fragmentation problem and the complexity of having to manage customised Android instances that include manufacturer-specific User Interfaces or Skins?
There are examples of security vulnerabilities being patched by Google in a timely manner and then releasing software patches to the AOSP. For example, during October 2012 security researchers at North Carolina State University informed Google of a SMS text security vulnerability. Google quickly acknowledged the vulnerability and within days had fixed the bug incorporating it into Android Jelly Bean 4.2 and also including it in as a patch for earlier versions. However, many experts believe that this security patch, and many others, has not found its way to the majority of Android Smartphone users. Either, because of the time it gets the Android hardware OEMs to incorporate the patch into their versions of the operating system or due to the time it takes for the MNO community to receive and test out the patches. In another example with Android (the Samsung Exynos kernel exploit referenced earlier in this study), this time with Samsung, it took around 3 months from the vulnerability being discovered to the patch being pushed out to actual Smartphones. Although Samsung must be commended for fixing this vulnerability in good time it is unclear how many devices that were affected by this vulnerability have been successfully patched and whether the patch has been pushed to all affected devices.

In research\(^59\) that was presented to the BlackHat conference in 2011, mobile security vendor Lookout Mobile Security asked the question “If a new Android vulnerability is discovered today, when will the phone in your pocket be patched?” Lookout admit that “Google has developed an extremely fast response to push updates and fix security flaws on the Android OS – often within days or weeks of discovery”. However, they go on to say that the complexity of the Android ecosystem and the fragmentation issue means that Android software updates can take their time for being pushed out to Android Smartphones. Lookout believe that the main factors that affect the length of update and patch cycles on Android include:

- Time it takes Google to release the patch to the Android Open Source Project (AOSP) repository
- The level of commitment by OEM manufacturers and carriers (operators) to update devices with the latest release
- The number of customisations on devices and time it takes to flash each firmware build with the updated OS release

Goode Intelligence believes that rather than blame MNOs, i.e. one part of the ecosystem, for the failure in properly patching Android Smartphone devices it is the process and the operating system management lifecycle that is responsible for this issue. It is the responsibility of all stakeholders in the Android ecosystem to collectively resolve these issues and ensure that software updates and security vulnerability patching is successfully delivered to the majority, not the minority, of Android Smartphone devices.

There are some situations where this cannot happen. Some older Smartphone OS versions cannot be updated. In these situations, it is also the responsibility of the industry to educate Smartphone users to the risks involved in using devices that cannot be updated to latest versions of the OS.

Study into the implications of Smartphone operating system security

There has also been criticism of Microsoft in the time it takes for Windows Phone owners to get patches to security vulnerabilities. Back in 2011 there was criticism of a patch to Windows Phone 7.5 that was released by Microsoft in February 2011 but was seen to be slow in getting delivered to affected Smartphone owners. Some Windows Phone 7.5 owners were still waiting for the patched release in April 2011. Microsoft initially put the blame on the MNOs in delays in the testing and assurance process and subsequently updated the communications saying that a combination of “glitches” in some of the early versions of the updated version on certain manufacturer’s (including Samsung, LG and HTC) devices. Microsoft’s top mobile executive, Joe Belifore, responded with this statement:

“"One thing we struggled with is each of these things involves us and the OEMs or handset manufacturers and the MNOs, and it's hard to coordinate which things we can say about what other people are doing.""60

This is a very good example of how the complexity of certain Smartphone operating system vendors’ ecosystem adversely affects their ability to push out patched software to the actual devices – putting fixed software into the hands of those that really matter, the end user. In situations where vendors have complex partner management relationships it can be difficult to control the end-to-end process for software update and vulnerability management.

In summary, there are still unanswered questions in relation to the length of time that it can take for operating system updates to be distributed to Smartphones. This is most acute on Android where users have been known not to receive a single software update in the time that they own the device – in some cases for between eighteen and twenty-four months.

When things go wrong and the impact to the consumer

Software does go wrong from time to time and despite extensive testing by mobile operating system vendors, handset manufacturers and MNOs new bugs can be introduced as a result of a new software update.

For instance, Apple’s iOS 6.1 update, released by Apple on 28th January 2013, included fixing wireless connectivity issues. Unfortunately, it also introduced a new set of bugs that included issues with iOS 6.1 devices connecting to Microsoft’s Exchange ActivSync servers for push emails, a security related bug that allowed user’s to bypass iOS lock screen security and reports of battery degradation problems.

To Apple’s credit, the ActivSync connectivity issue was quickly resolved with a follow up patch, iOS 6.1.2 that was released by Apple on 19th February 2013. To our knowledge the lock screen bypass issue was not fixed in 6.1.2 and there are indications that 6.1.3 will fix this security issue. 6.1.3 is also rumoured to fix a well-known iOS Jailbreak61 called the

---

60 Crisis expert grades Microsoft’s Windows Phone 7 update mea culpa: Computerworld article from 15th April 2011: http://www.computerworld.com/s/article/9215850/Crisis_expert_grades_Microsoft_s_Windows_Phone_7_update_mea_culpa
61 iOS Jailbreak is a term to denote the process of removing the limitations on Apple devices running iOS. Jailbreaking allows root access to the iOS operating system and enables the device to download
Study into the implications of Smartphone operating system security

**Evasi0n Jailbreak**[^62]. There are concerns that the ability to Jailbreak an iOS device can lead to malicious use whereby a device could be surreptitiously Jailbroken without the user’s knowledge. This may lead to unauthorised control of the device.

![Evasi0n Jailbreak](http://www.gottabemobile.com/)

These patches were quickly made available through at least two of the UK’s MNO’s iOS devices running on T-Mobile UK (EE) and Vodafone.

For these iOS patches there was no notification directly from one of the MNOs, T-Mobile UK. For T-Mobile the communication to the device owners that a patch was available was directly from Apple via the update notification service within ‘Settings’.

Vodafone pushed out SMS notification messages to its iPhone 4s users that informed the owner that a new version of iOS was available that fixed network performance issues (see figure x below). This was after Vodafone had issued an advisory to its Apple iPhone 4s customers not to install iOS 6.1.[^63]

[^62]: The Evasi0n Jailbreak is a software package that allows an Apple iOS user to Jailbreak a device running iOS 6.0 to 6.1.2. It is estimated that more than seven million copies of Evasi0n were downloaded in the first four days of its release.

[^63]: Vodafone advisory to iPhone 4s users: [http://forum.vodafone.co.uk/t5/Apple/iOS-6-1-update/td-p/1425278](http://forum.vodafone.co.uk/t5/Apple/iOS-6-1-update/td-p/1425278)
Study into the implications of Smartphone operating system security

**Figure 3.2 Vodafone SMS notification of iOS 6.1.1 download**

Although there was a degree of confusion in the messaging between Apple and Vodafone for this particular software update, Vodafone should be applauded for its handling of this update.

This is an example of the platform and Smartphone owner, in this case Apple, having direct control over the software update process and then working with its Operator partners to ensure that all relevant Smartphone owners are notified as quickly as possible of the need to update, or not as was the case for iOS 6.1, their operating system versions.

Goode Intelligence believes that it is the responsibility of all of the stakeholders in Smartphone operating system management to offer a coordinated approach to customer relationship, including offering timely and well-informed notifications using all available channels; Web-based support forums, social networking including Twitter, push notification messages through a branded mobile app and direct SMS text messages.
The importance of the consumer in the Smartphone operating system software update process – Do they understand the process and responsibility?

The consumer is a vital component in the Smartphone operating system update process.

The whole software update model is reliant on consumer willingness to update their Smartphones.

There is anecdotal evidence that consumers have a mixed understanding of how Smartphone operating system updates work, e.g. when, why, how they should update and what the difference is between a major update and an emergency security update?

It is the belief of Goode Intelligence that the majority of Smartphone owners will feel that the main point of contact for any Smartphone operating system question or issue will be their MNO. In the majority of cases this view will be correct but as this report has discovered in some cases the role of the operator in managing this process is very limited, e.g. the differences between Android and iOS updates.

This situation is not helped by a lack of clear communication to consumers from the MNOs. Most UK Smartphones will be purchased either directly or indirectly from MNOs to run on their networks and there is an opportunity at the point of purchase to educate consumers as to who is responsible for what. Education is key in ensuring that consumers know who is responsible for what and for them to understand their own role in the operating system update process.

There are questions over how consumers view the update process and whether they understand the differences between the different software components of a Smartphone. They are used to receiving regular updates for Smartphone Apps, some of which are automatically updated each time the App Developer has an updated version to push out, but may find it difficult to understand the difference between these updates (that don't require the device to power-down) and whole operating system updates.

In an interview with Darren Gale, EMEA lead for Mobile at Symantec, he gave first-hand experience from a family member that exemplifies this issue; “some Smartphone owners are terrified to update their devices as they are unsure as to what the end result will be. They may have only got used to characteristics of a particular Smartphone OS version and then are being asked to update it without knowing what the consequences are. This is a very big challenge”.

More research needs to be carried out to gauge consumer awareness and their understanding of the operating system software update process. There is anecdotal evidence that consumers may be delaying updating their devices and thus increasing the security risks of using their Smartphones. This anecdotal evidence includes:

- Apple iOS device owners delaying updating to iOS 5.0 due to negative reaction to Apple’s decision to replace Google Maps with their own mapping application
Consumers conservatism by not wanting to update their Smartphones because they were content with the current version and feared that the updated operating system ‘look and feel’ would be radically different from the current version

Not understanding the software update process and ignoring requests to update new versions of the operating system either by OTA or PC-Synching means (Note. GI believes that OTA updates are more user friendly and greatly improve the user experience. If a Smartphone operating system does not support OTA software updates then it is less likely that the update will take place)
4. SMARTPHONE SECURITY VULNERABILITIES

Overview

Security vulnerabilities exist in every example of computer software, from computer operating systems including Windows, Mac OS and UNIX to web browsers and databases. They also exist in every Smartphone operating system.

What are security vulnerabilities?

Vulnerabilities are weakness, flaws, in a computer system or even poorly configured systems or networks.

An exploit is a piece of software or a technique that takes advantage of a security vulnerability. An example of an exploit is a virus or malware.

In information security an attacker, or hacker, can exploit a vulnerability to create a threat. Threats are numerous and can result in unauthorised access to a computer system and the infection of a computer system by virus or Malware that can lead to financial fraud and identity or Intellectual Property (IP) theft. One of the major information security standards, ISO 27005, defines vulnerability as;

“A weakness of an asset or group of assets that can be exploited by one or more threats where an asset is anything that can has value to the organization, its business operations and their continuity, including information resources that support the organization’s mission”\(^{64}\)

Figure 4.1: OWASP (The Open Web Application Security Project) security vulnerability (weakness) model

---

\(^{64}\)British Standard Institute, Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management BS ISO/IEC 13335-1-2004
What is Vulnerability Management (VM)?

Vulnerability management is the process or lifecycle that aims to manage computer vulnerabilities. There will be many vulnerability management models but essentially the main parts of the vulnerability management process are:

1. Identification (Including Disclosure)
2. Classification
3. Remediation (fixing or mitigation)

Identification

The initial part of the Vulnerability Management process is when the vulnerability is identified (discovered). This part can also include Disclosure where the security researcher who identifies the Vulnerability discloses their findings to either the computer system owner (could be a Smartphone operating system owner) or into the public domain.

Classification

Security vulnerability classification does not have a true global standard. There have been attempts at standardisation by governing bodies such as the USA’s NIST (National Institute of Standards and Technology), SANS Institute or OWASP (The Open Web Application Security Project) but in the main classification is largely left to the technology vendor that the vulnerability affects.

Linked to the above efforts to classify security vulnerabilities is the Common Weakness Enumeration (CWE) project sponsored by the US-based not-for-profit organisation the Mitre Corporation, a formal list of software weakness types whose aims are to:

- Serve as a common language for describing software security weaknesses in architecture, design, or code
- Serve as a standard measuring stick for software security tools targeting these weaknesses
- Provide a common baseline standard for weakness identification, mitigation, and prevention efforts

The CWE project provides a universal online dictionary of software weaknesses or vulnerabilities that can be interrogated either manually or programmatically. Its aims are; “The main goal of the CWE initiative is to stop vulnerabilities at the source by educating software acquirers, architects, designers and programmers on how to eliminate the most common mistakes before software is delivered.”

---

65 CWE FAQs: http://cwe.mitre.org/about/faq.html#A.2
Is there a conflict of interest in vulnerability disclosure for Smartphones?

Some commentators, including the mobile security vendor, Lookout Mobile Security, have suggested that there may be a conflict of interest in the Smartphone operating system vulnerability disclosure process that may have led to reluctance in some security researchers to disclose vulnerabilities.

There are possible reasons behind this reluctance. These include a theory that vulnerabilities may be the only way to either root or jailbreak a Smartphone and if the security researcher was to disclose this vulnerability then it would automatically close off the method in which to root or jailbreak the device. This viewpoint was backed up by Wolfgang Kandek, Chief Technology Officer (CTO) of vulnerability management vendor Qualys who stated that Smartphone vulnerabilities were less likely to be disclosed as a result of the value (including monetary) of these vulnerabilities. Lookout’s CTO, Kevin Mahaffey, stated that the current value of a iOS zero day vulnerability is US$500,000.00 making it less likely for a security researcher to disclose (free of charge) a vulnerability. It is known that Apple, unlike Google, rarely pays ‘bounty’ money for zero day vulnerabilities. As Lookout stated in its blog “This conflict of interest between vulnerability disclosure and the ability for people to fully control their own device poses a great security issue. Once a vulnerability being used to root or jailbreak devices becomes public knowledge it may also be used by malicious attackers, like DroidDream.”

Another explanation is the frustration by some security researchers that even though they are disclosing vulnerabilities in the public domain (and to Google) they are not being fixed quick enough by Google and, in particular, the handset manufacturers. This frustration is reported in many blogs and security vulnerability lists that Goode Intelligence has uncovered as part of this research. The argument goes along these lines; why should I fully disclose an Android vulnerability or exploit when it isn’t being fixed quickly enough, or not at all, by the handset manufacturers. Yes Google are accepting that it is in an issue and fixing it but it is not getting into the hands of Android Smartphone users and could potentially be exploited.

Remediation

Software vendors want to fix vulnerabilities as quickly as possible, before they can be exploited and used maliciously. They will either discover the vulnerability directly as part of their own security testing process - most Smartphone operating system vendors will have specialist security engineers that will have responsibility for vulnerabilities.

BlackBerry reportedly has some 160 security specialists working for them) or it will be disclosed to them by either independent security researchers (sometimes referred to white hat hackers) or specialist security vendors.

66 A zero-day (0-day) vulnerability is an attack or threat that exploits a previously unknown vulnerability. It is related to the ‘Vulnerability windows’ that is the windows that exists in time between when a vulnerability is first exploited to when it is fixed.
67 http://www.evad3rs.net/2013/03/ios-7-jailbreak-price-500000.html
Once the security vulnerability is fixed then it can be incorporated (built) into a new version of the software and then released in accordance to the vendor’s software update lifecycle.

**Levels of reported Smartphone operating system vulnerabilities**

This section examines the levels of Smartphone operating system vulnerabilities and whether they are being managed by vulnerability management bodies such as CERT (Computer Emergency Response Team). We shall first investigate the role of a CERT.

**The role of Computer Emergency Response Teams (CERTs)**

A Computer Emergency Response Team (CERT) was originally the name of the first CERT from Carnegie Mellon University (CMU), USA. CERT is now a registered name of CMU that is licensed to other teams around the world, usually state-funded and run. It can also be referred to as CSIRT (Computer Security Incident Response Team).

CMU CERT is also known as US-CERT acting as the emergency response team for US Cybersecurity threats. Part of CMU CERT Program is the Coordination Center (CERT/CC) that partners with government, law enforcement, industry and academia to coordinate security threats.

A major role of a CERT is Vulnerability Management, including analysis, discovery and remediation. Educating security professionals is another key role of the CERT.

The CERT Charter is to:

- Provide a reliable, trusted, 24-hour, single point of contact for emergencies
- Facilitate communication among experts working to solve security problems
- Serve as a central point for identifying and correcting vulnerabilities in computer systems
- Maintain close ties with research activities and conduct research to improve the security of existing systems
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and services providers

**GovCertUK**

More than 50 other CERTs/CSIRTs with national responsibility have been established around the world including the UK’s own CERT, GovCertUK, run as part of CESG. GovCertUK’s primary role is to coordinate emergency security responses for UK government bodies. GovCertUK is responsible for Computer Security Incident Response within UK Government, and provides an emergency response capability to public sector organisations that may require technical support and advice during periods of electronic attack or other network security incidents. The CESG GovCertUK Incident Response team provides a 24 hours a day, 7 days a week operation.
GovCertUK state that all public-sector computer security incidents should be logged with them and offer assistance in the identification and categorisation of information security events. They have published Incident Response Guidelines, available as a downloadable PDF from its website, that educate public sector organisations on how to deal with security incidents.

The guidelines do not refer specifically to Smartphone vulnerabilities and threats although most of the guidance is applicable to all computer systems and services. The guidelines include advice on classifying incidents into four categories:

- Critical
- Significant
- Minor
- Negligible Impact

Goode Intelligence contacted GovCertUK to enquire about their experience of dealing with Smartphone security incidents and managing vulnerabilities. Unfortunately, they were not able to deal with the enquiry and replied with “Our engagement is restricted as to whom we can engage with, and hence we are unable to provide you with further details on our processes and relationships with other CERTs, or any work with vulnerabilities.”

**The role of CERTs in Smartphone operating system software security**

From Goode Intelligence’s research CERT’s are currently performing a limited role in the Smartphone operating system security and vulnerability management process.

In discussion with a number of the UK’s MNOs they had little involvement with CERTs including GovCertUK.

Smartphones and other smart mobile devices have definitely started to turn up on the radar of CERTs. US-CERT has published a number of security publications specifically on mobile security that act as advisories.

The information is aimed at a wide-range of communities including IT professionals, government users, businesses and home users. They include:

- Cyber Threats to Mobile Phones: Published 2011

In terms of receiving information about Smartphone vulnerabilities this was most likely to come directly from the operating system vendors and handset manufacturers. Other bodies that were referenced by UK MNOs for information and advice on Smartphone vulnerabilities and threats were the GSMA Mobile Malware Group (MMG) and the NIST National Vulnerability Database (NVD) (which was unfortunately offline at the time of writing this report).
Study into the implications of Smartphone operating system security

The GSMA MMG is a cross-industry working group that meets to share intelligence on mobile malware. The GSMA makes this statement on the MMG; “Although mobile malware has not reached predicted epidemic levels, the GSMA is aware of the potential threats and has established a Mobile Malware Group to coordinate the operator response to identified threats. The group facilitates the prompt exchange of information between industry stakeholders and encourages best practice to manage and handle malware by producing comprehensive guidelines for its members.”69 The GSMA MMG has been favourably cited by the MNOs that Goode Intelligence has spoken to. The MMG regularly meets and shares information. However, the nature of the group has its limitations handling emergency scenarios that require a quick reactive response. It is Goode Intelligence’s belief that it doesn’t currently offer a CERT-like early warning system that allows real-time exchange of intelligence specifically aimed at mobile malware.

The UK’s Premium Rate Services (PRS) regulator PhonepayPlus has presented at this forum to discuss their research, aided by Goode Intelligence, into the threat of mobile malware to the UK’s PRS industry.

Other Vulnerability Management Resources

There are other government run databases for vulnerability management including the National Vulnerability Database (NVD) and the Common Vulnerabilities and Exposures (CVE) database.

**NIST NVD**

The National Vulnerability Database is run by the US Government’s National Institute of Standards and Technology (NIST) and is a searchable (using the Security Content Automation Protocol (SCAP)) repository of standards-based vulnerability management data. The NVD does contain Smartphone operating system vulnerabilities but it may take a while for the latest vulnerabilities to be uploaded and for them to be matched against any patch that the operating system vendor may have released.

**CVE**

The Common Vulnerabilities and Exposures is a resource run by The MITRE Corporation and is a dictionary of publically known information security vulnerabilities and exposures. It is not a vulnerability database.

Each vulnerability is allocated a CVE common identifier that has become a de facto standard for identifying vulnerabilities. The CVV common identifier is used by the NVD.

---

FIRST is the Forum of Incident Response and Security Teams and was founded in 1989.

It is an international confederation of “trusted computer incident response teams” that allows incident response teams to respond to security incidents.

FIRST initiated the Common Vulnerability Scoring System (CVSS). This is a system that provides an open and standardised method for rating computer vulnerabilities.

**Smartphone operating systems vulnerabilities**

All Smartphone operating systems will have vulnerabilities and the more popular an operating system becomes the more likely it will come under attack and those vulnerabilities disclosed.

The actual risk to Smartphone owners to these vulnerabilities will be dependent on a number of factors including:

- The nature and risk level of the vulnerability, e.g. will the vulnerability lead to widespread disruption, potential financial fraud or identity theft?
- Who knows about the vulnerability? Is knowledge of the vulnerability restricted and confined to a criminal organisation or hostile nation state?
- How easy is it to exploit the vulnerability and has the exploit been automated and shared throughout the security research community?
- The speed for the vendor that is affected by the vulnerability to initially fix (patch) and then to distribute the remediated software to Smartphone owners
- Quality of communication. Is news about the vulnerability efficiently distributed to those parties that are affected by it?
- The willingness of the Smartphone owners to download and install the revised software update

This section details specific Smartphone operating system vulnerabilities on a per-platform basis. It investigates the levels of reported vulnerabilities associated with each Smartphone operating system that has been discussed in this report. There will be reference to mobile malware and its impact on each platform.

Before we dive down into each platform it is worth taking some time to discuss mobile malware in general.
Study into the implications of Smartphone operating system security

**Mobile Malware**

According to some security vendors and commentators 2013 will be the year of mobile malware. However, this was stated at the beginning of 2012, 2011 and 2010. When reading mobile threat reports that are created by security vendors it is recommended that the reader is cautious and attempt to validate the claims from other sources.

That said, the facts do point to a steady increase in mobile malware since 2008/09. The numbers are still relatively small, especially when compared with the numbers seen in the personal computing space, but the trend is upwards and there have been a number of high-profile examples that have resulted in financial fraud and identity theft.

If we take a look at figure x below from F-Secure’s Q4 2012 Mobile Threat Report\(^{70}\) you can see that Android is the number one Smartphone operating system for reported mobile malware.

Goode Intelligence believes that this is because of the following reasons:

1. It is the number one Smartphone operating system in the world and could surpass Microsoft Windows as the most commonly used operating system.
2. Android is a more open platform and allows users to ‘sideload’ apps onto the Smartphone from unofficial Android App stores. These third-party App stores may not have the levels of control that is reducing the distribution of malware.
3. Malware has been distributed from Google’s official App store (initially Google Market and now named Google Play). Google are getting better at detecting malware and rogue apps in their official App store and have deployed ‘gatekeeper’ type solutions to detect and remove malware (Google Bouncer\(^{71}\)).
4. Most Android users (over 40 percent) are using older versions of the operating system software (mainly Android Gingerbread) that are known to have vulnerabilities that have been exploited. Newer versions of Android are better equipped to deal with vulnerabilities including malware and have better security features including ASLR\(^{72}\) and rudimentary anti-malware tools.

We shall take a further look at Android malware in the ‘Google Android’ section below.

According to the latest figures from F-Secure the majority (66.1 percent) of mobile malware were Trojans and of these many were financial motivated and attacking Premium Rate Services (PRS).

---


\(^{71}\) Google Bouncer checks Apps in Google Play and aims to prevent the distribution of malware from Play. According to Google, Bouncer has been responsible for a 40% drop in the number of malicious apps in Play since being introduced late in 2011.

\(^{72}\) ASLR, Address Space Layout Randomization is a security model that randomly arranges the positions of key data areas. It hinders security attacks by making it harder for an attacker to predict target addresses. This was available in a limited form from Android 4.0 Ice Cream Sandwich (October 2011) with a better implementation seen in Android 4.1 Jelly Bean (July 2012). ASLR was introduced in Apple iOS from version 4.3. (March 2011).
Study into the implications of Smartphone operating system security

**Figure 4.2: New Mobile Threat Families and Variants Received per quarter (2012)**

Please note: Figure x above. The threat statistics used are made up from families and variants of unique files. For instance, if two samples are detected as **Trojan:Android/GinMaster.A**, they will only be counted as one in the statistics.

The vast majority of mobile malware detections have been in three regions, China, Ukraine and Russia. Infection rates have been estimated to be as high as 40 percent of mobile devices[^73]. A combination of lighter regulatory control and consumer use of ‘unofficial’, less secure, mobile app stores have contributed to this problem.

This compares to an estimated figure from Lookout Mobile Security of less than one percent of US devices infected.

Study into the implications of Smartphone operating system security

The figures from security vendors operating in the anti-virus sector rarely rarely give an indication on actual infection rates, e.g. how many Smartphone are actually being infected by malware. A study by Georgia Tech University in the USA that used a machine learning technique called Multiple Correspondence Analysis (MCA) in an attempt to get to a “ground truth” about how pervasive mobile malware found “little evidence of significant malware infection in the mobile world.”

It is Goode Intelligence’s belief that all though mobile malware is effecting UK Smartphone users, the numbers of UK Smartphone’s that have been infected remain low.

**Apple iOS**

According to Symantec’s Darren Gale “Apple is getting proactive in its vulnerability management approach”.

Goode Intelligence believes that Apple does offer a comprehensive approach to vulnerability management that is linked to an effective operating system security update process.

Goode Intelligence discovered 179 unique CVE entries whilst performing a search on ‘Apple iOS’ on the CVE vulnerability database. The latest CVE entry (CVE-2013-0974) was added on 10 January 2013 and was related to an iOS Safari vulnerability. The first vulnerability (CVE-2010-1387) was recorded in April 2010 for vulnerability in JavaScriptCore in WebKit on iOS devices pre-version 4.

Apple has stated that it does not offer any large bounties to security researchers for disclosing iOS vulnerabilities. Other vendors, including Google, do offer a bounty scheme whereby cash will be offered in return for disclosing vulnerabilities to them.

To report a security issue or vulnerability to Apple a generic email address, product-security@apple.com is used. The emails can be encrypted using Apple’s product security PGP key.

Apple product security notifications are sent out via email, using the ‘security-announce’ mailing list, or via a RSS feed

To ensure that Apple security advisories are authentic Apple uses an ‘Apple Product Security PGP key’ to encrypt and sign.

Apple works with the formal incident response community to distribute information on vulnerabilities and is a member of FIRST.

Apple lists all of its platform (not just iOS) security updates on a central website that can be found here.

There are no security specific Apple iOS software updates but many releases will have fixes to known security vulnerabilities. For instance, in the recent iOS 6.1 release there were

---


75 You can find the CVE entry here: [http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0974](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0974)
some 27 security vulnerabilities that were fixed. This included 20 remote code execution errors in the WebKit browser engine.

The WebKit browser engine is not just used within the Apple web browser, Safari, but it is contained in Google Chrome and within BlackBerry 10. That is why the vulnerability was discovered by a Google Chrome software engineer. Each of the vulnerabilities fixed in iOS 6.1 was referenced by its CVE number.

### Jailbreaking

Jailbreaking is a term to denote the process of removing the limitations on Apple devices running iOS. Jailbreaking makes use of vulnerabilities within the iOS operating system.

Jailbreaking allows root access to the iOS operating system and enables the device to download applications outside of the official Apple App store, e.g. from unofficial App store providers like Cydia.

There is a debate as to whether Jailbreaking is legal or not.

Popular Jailbreak tools include redsn0w, JailbreakMe and Evasi0n.

**Why Jailbreak?** There are many reasons to Jailbreak an Apple iOS device but fundamentally it allows the user to bypass many of Apple’s control mechanisms. For instance it allows the user to develop their own software without having to release it via Apples official App store or to bypass operator locks. It is dangerous as it removes many of the security control mechanisms that have been put in place to prevent vulnerabilities and exploits such as Malware. It is no surprise that some of the only examples of iOS malware has been discovered on Jailbroken devices, for instance the infamous ikee.

**How many jailbreaking devices?** It is difficult to get a truly accurate picture on exactly how many iOS devices have been Jailbroken. Estimates range from two to five million (roughly seven to ten percent of all iPhones devices shipped) and China is thought to be the leading country in the number of Jailbroken devices (Goode Intelligence has seen figures that estimate that up to 34 percent of all iPhone users in China are Jailbroken). An article in the Washington Post from 2011 suggested that Cydia was earning some $10 million in annual revenue and had approximately 4.5 million active weekly users.

---

76 About the security content of iOS 6.1 Software Update: [http://support.apple.com/kb/HT5642](http://support.apple.com/kb/HT5642)
77 Cydia ([http://cydia.saurik.com/](http://cydia.saurik.com/)) is an alternative to Apple App Store and allows Jailbroken iOS devices to download and install mobile Apps.
78 For more information on ikee go to F-Secure’s website: [http://www.f-secure.com/v-descs/worm_iphonesos_ikee.shtml](http://www.f-secure.com/v-descs/worm_iphonesos_ikee.shtml)
iOS Mobile Malware

It is Goode Intelligence’s belief that there have been no reported instances of mobile malware on iOS devices.

The combination of a strong security model, rigorous mobile app control within Apple's official App store - every app is reviewed for malware and determined if it is illegal or rogue - ensures that Apple iOS devices have been free of malware to date.

There have been attempts to load malicious apps onto Apple's App store but in the main their defence systems and procedures have held up. One notable exception was from renowned Apple security researcher, Charlie Miller, who in 2011 managed to get a proof-of-concept malicious app, called ‘Instastock’, loaded onto Apple’s App store. Apple quickly removed the offending App and fixed the flaw. As a result of his action Miller had his Apple Developer license revoked.

Mobile malware has, however, been seen on Jailbroken iOS devices. Jailbreaking upsets the security model for Apple iOS devices and allows Apps to be installed from unofficial sources such as Cydia.

As Jailbreaking is unofficial it is difficult to get an accurate picture of the proliferation of mobile malware in Jailbroken devices.

Probably the most infamous examples of mobile malware on Jailbroken iOS devices was ‘Ikee’. Ikee was written by an Australian hacker and uses the default SSH password (“alpine”) of the Jailbroken iPhone to log onto the device and to deliver its payload.

The Ikee MM changes the wallpaper to a picture of the 1980s singer Rick Astley (a prank known as “Rickrolling”), deletes the SSH daemon (code) and begins scanning the network for other vulnerable phones in a predetermined IP range.

---

Later on in November 2009 a variant of the Ikee virus, “Ikee.B” or “Duhi”, started to spread from Holland out to Jailbroken iPhone devices in countries including Portugal, Australia, Austria and Hungary. This has more malicious intentions than the original Ikee MM. The “Ikee.B” MM takes control of the device and enables a botnet, hosted in Lithuania, to perform any commands on the device. The malware edited the Hosts file to redirect *.ing.com to a site in Tokyo that was a mock-up of the real *.ING site. It then harvested account credentials and account details.
Study into the implications of Smartphone operating system security

BlackBerry

BlackBerry is renowned for its device and operating system security. In a recent interview with BlackBerry, a spokesperson told Goode Intelligence that “BlackBerry has a moral obligation to protect their user’s security and privacy”.

It is still the only Smartphone that has been accredited by CESG, using CESG’s Assisted Products Service (CAPS), for handling UK Government (HMG) ‘Restricted’ information.81

In an interview with BlackBerry in March 2013, Goode Intelligence was informed that for vulnerability management:

- BlackBerry holds regular security meetings and conferences where independent security researchers will attend and discuss the latest vulnerabilities and threats
- BlackBerry has a security team of around 160 people and a good proportion of these will be security researchers (white hats). They will be looking at the latest threats and exploits
- Enterprise users will be pushed vulnerability advisories, using RSS, and these advisories will also be sent to national CERTs and other vulnerability databases "as soon as possible"
- Consumer users will be notified using public notification channels including BlackBerry’s Knowledge Base

Goode Intelligence discovered only three unique CVE entries whilst performing a search on the CVE vulnerability database for ‘BlackBerry OS’, 33 entries were discovered for ‘RIM’ and 41 when ‘BlackBerry’ was used. The search term ‘BlackBerry’ also included vulnerabilities recorded for the BlackBerry Enterprise Server (BES).

The BlackBerry Security Incident Response Team (BSIRT) provides 24/7 monitoring, vulnerability analysis, remediation and guidance in order to help keep BlackBerry customers protected from security issues.

BBISRT addresses both internally and externally identified vulnerabilities through a triage and monitoring process. Once a potential issue is identified, BBSIRT uses the Common Vulnerability Scoring System (CVSS) internally to rank and prioritise security vulnerabilities in BlackBerry products. If an issue is classified through CVSS as critical or severe, BlackBerry will begin the process to develop a security update to address the issue.

Depending on BlackBerry’s analysis on the threat landscape, they may release a security notice while the security update is being developed to help protect customers by providing them with available mitigations.

Once the security update is ready for customers, they will release a security advisory that details the vulnerability, the fix, and any applicable mitigations and workarounds.

BlackBerry follows the ‘Patch Tuesday’ schedule for releasing software updates by releasing on the second Tuesday of the month. The security update information is widely shared through several communication channels, such as the external BlackBerry website,

---

81 BlackBerry OS 7.1 was accredited by CESG in November 2012: http://www.cesg.gov.uk/News/Pages/BlackBerry-7.1-OS-now-Approved.aspx
Study into the implications of Smartphone operating system security

www.blackberry.com/bbsirt, RSS feeds, Twitter, media statements and direct customer communications.

BlackBerry OS Mobile Malware

There have been very few examples of malware affecting BlackBerry OS. In the ‘F-Secure Mobile Threat Report Q4 2012’ only 0.3 percent of recorded mobile malware is targeting BlackBerry OS.

There has been only a handful of recorded malware affecting the BlackBerry OS platform with more attacks seen on the BES.

As BlackBerry has been a piece of essential enterprise kit for so many years malware examples have included Spyware,82 financial services threats and malware with a corporate espionage theme.

Spyware designed for BlackBerry has the ability to record all of the user’s actions on the device including monitoring app usage, record SMS text messages, voice calls and BBM83 messages.

The FinFisher84, not classified as malware but commercially available as a surveillance tool, cyber espionage tool has mobile versions that include BlackBerry.

It is difficult to install Spyware-type software onto a BlackBerry OS device and would require an existing exploit, or use social engineering. If an attacker has physical access to the BlackBerry device then that would make the task a little easier but they would still need to bypass BlackBerry’s authentication.

The Zeus Trojan has been targeting retail banking services since 2007. It steals banking information using a Man-in-the-Browser (MitB) attack that grabs information that an electronic bank user is typing into a web browser. Zeus has a mobile variant called Zeus-in-the-Mobile (ZitMo) and BlackBerry OS devices have been targeted and infected.

ZitMo shall be discussed in more detail in the section on ‘Emerging threat to consumers’.

82 Spyware is software whose purpose is to gather information from a person or organisation without their consent and knowledge. Typical spyware is categorised as ‘keyloggers’ that monitors a user’s computer behaviour including capturing keystrokes (information that is typed into a keystroke).
83 BBM is BlackBerry Messenger
84 FinFisher is a commercially available surveillance tool that in its mobile version monitors app usage, text messages and voice calls.
Google Android

Android is being labelled as the new Microsoft Windows. This is both a blessing and a curse as Microsoft Windows has been the most successful desktop operating system in the world but has been criticised for the extent of its vulnerabilities and exploits.

Goode Intelligence discovered 320 unique CVE entries whilst performing a search on ‘Android’ on the CVE vulnerability database. The latest CVE entry (CVE-2013-1773) was added on 19 February 2013 and was related to Linux Kernel 3.3 vulnerability.

As Android is based on the version of the Linux Kernel, version 3.x for Android 4.0 onwards and version 2.6 for all other versions, Android will share some vulnerabilities with Linux, as CVE-2013-1773 shows us.

Issues with Android, including security vulnerabilities, are logged with Google via the Open Handset Alliance Project (There is an ‘Issues’ area of the website - https://code.google.com/p/android/issues/list). They will be allocated an ID and a Type (categorised into ‘Defect’ or ‘Enhancement’), along with a summary of the issue and the owner. Google will analyse the issue and if it is a security vulnerability that needs remediating will schedule in the fix according to the severity of the issue.

It is accepted that this process works relatively well and that Google have an adequate vulnerability management process. Where the process has problems is in the relationship between Google, the third-party handset manufacturers and the operators.

Goode Intelligence believes that the critical relationship that is causing much of the issue is the Google-Android handset manufacturer relationship.

As there is a degree of customisation of Android by the handset manufacturer community then each OEM has their own vulnerability management process. They will also have their own unique vulnerabilities. For instance in December 2012 it was widely reported that Samsung had introduced a flaw in its Android Kernel implementation. The flaw, named the Samsung Exynos kernel exploit, resulted in a vulnerability that could allow a malicious application to gain control over the device. Android devices that were affected included the S2 and S3 Galaxy Smartphones. Samsung acknowledged the vulnerability and posted a response:

“Samsung is aware of the potential security issue related to the Exynos processor and plans to provide a software update to address it as quickly as possible.

The issue may arise only when a malicious application is operated on the affected devices; however, this does not affect most devices operating credible and authenticated applications.

---

65 You can find the CVE entry here: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1773
66 Samsung devices vulnerable to dangerous Android exploit (article from Computerworld).
http://www.computerworld.com/s/article/9234778/Samsung_devices_vulnerable_to_dangerous_Android_exploit
Study into the implications of Smartphone operating system security

In early January Samsung did manage to push out a software update to Galaxy S3 devices (I9300XXELLA) that fixed the Exynos vulnerability. The UK was one of the first countries to receive this patch that was released via Kies. The following month, February, saw Samsung roll out this release to US consumers after carrier testing.

Although Samsung must be commended for fixing this vulnerability in good time it is unclear how many devices that were affected by this vulnerability have been successfully patched and whether the patch has been pushed to all affected devices.

The complexity of the Android ecosystem is still creating confusion in how vulnerabilities are managed. If a vulnerability is discovered on a Samsung Android device and the vulnerability is to a core component of the Android operating system (not as part of a Samsung Customisation) then the core Android operating system needs to be fixed by Google and then, once remediated, needs to be distributed to the AOSP for onward distribution to all of the handset manufacturers. As this is a complex ecosystem then it is no wonder that Android operating system vulnerability management is not as streamlined as other mobile platforms and consumers will sometimes not receive software patches in a timely manner.

Android Mobile Malware

According to recently published threat reports in the major anti-virus security vendors sector, Android is currently the number one choice for mobile malware authors.

When we talk about the rising threat of mobile malware we are effectively talking about the rising threat of Android malware

Making sense of the figures

There doesn’t seem to be a week that goes by without receiving news issued from a security vendor announcing rising figures with Android malware. Goode Intelligence has collated a sample of recent Android malware figures:

- According to F-Secure Android accounted for 79 percent of all mobile malware discovered in 2012.
- In the July-September 2012 quarter alone, Blue Coat Security Labs saw a six hundred percent increase in Android malware over the same period in 2011. In June

---

Study into the implications of Smartphone operating system security

2012, requests to malware targeting Android devices reached more than one thousand88

- From McAfee Threats Report: Fourth Quarter 201289:
  o Android represents 97 percent of all mobile malware
  o A total of 36,699 mobile malware samples gathered with 95 percent of that arriving in 2012 compared to 792 samples in 2011
  o This compares to 113 million samples in McAfee’s general malware database
- Kaspersky echoes other reports by stating that 99 percent of all mobile malware targets Android90 and stated that during 2012 Android malware rose more than eight times

These figures are largely detection figures taken from both official and unofficial App stores and file sharing sites whose security leave a lot to be desired where rogue apps and malware sit side by side with pirated films and music. The ability to sideload mobile apps onto an Android device means that users can download and install apps from a variety of ‘unofficial’ sources when security control is light.

So what about infection rates? Figures of actual devices being infected with malware is hard to find – for one thing adoption of mobile security apps that include anti-virus controls is currently low so security vendors do not have a great deal of metrics that they can gather from the endpoint itself.

The exponential growth of Android malware detected by security vendors has, so far, not resulted in an increased risk of a Smartphone being infected. In their Emerging Cyber Threat Report 2013, Georgia Tech University91 references a research project that they performed “analyzing three weeks of DNS traffic from a large cellular provider”. The Georgia Tech University security researchers “found that only a very small number of devices—about 0.002%—are showing signs of infection in the United States.”

In summary; Android is the most targeted Smartphone operating system for malware and the numbers of detected malware is increasing month-by-month, year-by-year. However, it is debatable whether the rise in detected Android malware is resulting in an increase in actual device infection rates. The risk to UK Android Smartphone owners is currently low despite the rise in detected malware examples.

---

88 Blue Coat Security Labs 2013 Mobile Malware Report:
90 Kaspersky Security Bulletin 2012:
Study into the implications of Smartphone operating system security

Windows Phone

Windows Phone is a relatively new Smartphone operating system but there have been versions of Microsoft, Windows CE and Windows Mobile, running on Smartphone since 2000.

In the early days of Smartphone adoption, Windows Mobile and Symbian were two of the most popular Smartphone operating systems. As such, these platforms were frequently attacked and vulnerabilities were exposed. Some of these vulnerabilities led to the development of early mobile malware that took advantage of these exploits.

Goode Intelligence discovered just seven CVE entries whilst performing a search on 'Windows Phone' on the CVE vulnerability database, ranging from 2007 until 2012. The latest CVE entry (CVE-2012-2993) was added on 30 May 2012 and was related to a Windows Phone 7 vulnerability in the way that it verifies the domain name in an X.509 digital certificate that could lead to man-in-the-middle attacks.

As the latest version of Windows Phone, version 8, share parts of the core software components with the desktop version there could be situations where vulnerabilities discovered on the desktop version could be applicable to the phone version.

Windows Phone Mobile Malware

Windows Smartphones have had examples of malware written for them over the years. As Windows Smartphones were one of the most popular device pre-iOS and Android then they were targeted.

There is little evidence of malware being written in any great numbers for the Windows Phone platform. There have been examples of malware proof-of-concepts for Windows Phone 8 but no real examples of malware in the wild infecting Windows Phone 8 owners.

This may be a testament to the strength of the Windows Phone security mechanisms or, more realistically, due to the relatively small numbers of Windows Phone users.

As Windows Smartphones have lost market share then the percentage of malware that is explicitly targeting this operating system has also fallen with only a handful of specific Windows Phone 7 and 8 examples being detected.

This situation may change if Windows Phone market share grows.

---

5. CURRENT CONSUMER PROTECTION PRACTICES IN THE UK

Overview

Smartphone security is an emerging area of technology, as are the threats against them.

Consumer protection practices in the UK are currently a combination of technology initiatives and consumer awareness.

This section will exclude policy and regulatory control as this is covered in the section entitled “Current UK Smartphone security regulatory and institutional responsibilities”.

Technology initiatives

Technology initiatives to protect UK consumer Smartphones are a combination of endpoint (Apps installed on the Smartphone) and network-based controls (mainly technology controls deployed by the MNO).

Endpoint Technology

Endpoint technology that protects Smartphones from threats and vulnerabilities are usually termed mobile security apps and are usually developed by security vendors that have traditionally been active in protecting desktop computers against threats. These threats include viruses and malware, unauthorised access to devices and data and data leakage.

Security vendors that have consumer products in this space include:

- AVG
- AVAST
- Bitdefender
- BullGuard
- ESET
- F-Secure
- Lookout Mobile Security
- Kaspersky Labs
- McAfee
- NQ Mobile
- Panda
- Symantec (Norton brand)
- Trend Micro
- TrustGo

Please note that this is not an exhaustive list. This is a very competitive market and as such there are many vendors operating in the mobile security sector.
Study into the implications of Smartphone operating system security

**What does it protect against?**

Third-party Smartphone security products are reliant on the security framework (Application Programming Interfaces - APIs) of the platform in terms of what functionality is supported. Each platform will have security APIs that allow some security functionality and features to be supported.

As the security model and system architecture of the Smartphone operating system varies between platforms there will be variations in what security functionality can be supported. This means that Apple iOS, BlackBerry and Windows Phone operating systems have limited support for third-party security apps whilst Android offers a richer set of security features to be supported.

As a result of this, the bulk of the products and market for third-party Smartphone security apps is for Android devices. In fact, when we talk about the market for Smartphone security apps and services we are in effect talking about the market for Android security apps and services, and to a lesser degree Symbian Smartphones. Some vendors have even taken the strategic step of developing apps and tools primarily for Android.

There are a handful of Apple iOS security apps with limited functionality, mainly aimed at the lost and stolen device problem but also including public WiFi protection and cloud backup. Some of these features are add-ons to existing iOS operating system features. For instance from iOS, Apple provided cloud backup and the ‘Find My iPhone’ feature to locate the device if lost and stolen and then to initiate a remote deletion of the data.

As with the desktop security business some security vendors will offer a free (the ‘freemium’ model) versions of their security apps. The free versions will include base functionality but still offer basic protection.

**ANDROID MOBILE SECURITY APPS**

Android mobile security solutions protect against a wide-variety of threats and commonly they provide the following features (Please note that as this is a competitive market there will be variations to these features):

- Anti-Malware
- Anti-Theft (usually associated with some sort of location-based service utilising GPS and includes remote lock and wipe)
- Data Backup
- Personal Firewall

There are other features that are usually confined to the premium versions that include:

- File encryption
- Web browser protection (URL checking against blacklists)
- QR Code validation
- Ad network detection (although the legality of this has been questioned)
Study into the implications of Smartphone operating system security

- Privacy controls
- App reputational services

Android mobile security products operate in a similar fashion to their desktop cousins with background processing, where the platform supports it, signature-file checking, regular signature file updates (usually OTA) and checks on messaging, removable media, mobile internet and mobile App installation and execution.

**How effective are they?**

There has been debate as to the effectiveness of mobile security apps but it all depends on what you are trying to protect against.

Using a locate and wipe app to find a Smartphone after it has been lost and stolen and then to wipe the data on it is a useful utility whether it is a native (part of the operating system) or provided by a third party. Although there have been questions as to how effective these services are and whether they are reliant on the SIM card still being present in the device for location purposes – Note: one of the first things that a phone thief may do is to pull out the SIM card from the device and to disable the WiFi services.

The fiercest debate has been around the effectiveness of anti-malware on the device. Executives at Apple and Google have long criticised the anti-virus industry stating that the security of the operating system and ecosystem is more effective at preventing the spread of malicious code.

The security vendors themselves will admit that there are problems in running anti-malware services on the Smartphone. In an interview with Rapid 7, a security vendor, their CEO and Founder Giri Sreenivas stated that there is a “weakness in mobile anti-malware products in that they cannot be run in a privileged state on the device restricting their ability to detect all malware and vulnerabilities”.

A further problem is with the limited battery life of Smartphones. Lookout Mobile Security’s CTO and Co-Founder, Kevin Mahaffey, told Goode Intelligence that “Smartphone battery life is an issue for us as it prevents us from continuously checking for Malware. We don’t want to drain the battery so we have to resort to other techniques such as scanning for Malware when a user downloads or updates an App”.

The German-based independent anti-virus test organisation, AV Test, have been testing Android anti-malware products and their recent study of 22 products was published in January 2013. The good news is that only one of the products failed the test and did not receive the AV Test certificate. The products are tested for protection usability and additional security functions. Top points were awarded to products from TrustGo, Lookout, Symantec and Trend Micro.

---

93 The full test results can be found here (http://www.av-test.org/fileadmin/pdf/avtest_2013-01_android_testreport_english.pdf) in PDF format from the AV Test website
Study into the implications of Smartphone operating system security

**Network-based Technology**

Network-based protection technologies serve two main purposes:

1. Protect the MNO’s infrastructure from security threats
2. Protect their customer’s mobile devices from security threats

This includes protection against spam and malware. There are also solutions to detect and manage fraud before it gets to the Smartphone.

There are also ancillary benefits to the MNO and these are mainly related to Quality of Service (QoS) purposes. Spam and Malware is taking up valuable bandwidth on the MNO networks and technology that prevents malware and spam from infecting customers’ Smartphones can be used to remove traffic that is classified as non-generating revenue.

There are a number of technology vendors that are successful in this sector including:

- Blue Coat Technologies
- Adaptive Mobile
- Cloudmark

The technology can scan the MNO’s network in an attempt to prevent and contain spam and increasingly, malware. Scanning can take place at both the messaging, for SMS, MMS and email, or at the mobile internet levels.

They all develop solutions that generally tightly integrate with core network infrastructure supplied by vendors such as Ericsson and Huawei.

**Fraud Management**

Related to anti-spam and anti-malware network protection is fraud detection and management, commonly known as Fraud Management Systems (FMS).

According to one of the leading suppliers of network-based anti-fraud solutions, Subex, “global fraud loss is estimated to be approximately 5 percent of telecoms revenue annually”.

To combat fraud within the network, MNOs have adopted technology that allows them to be proactive for both detection and prevention.

Network-based anti-fraud measures include:

- Stopping fraudsters at the point of activation
- Minimising fraudster’s time on the network
- Building strong profiles of fraudster credential and behaviour to quickly recognise repeat offenders
Study into the implications of Smartphone operating system security

- Enforcing strong governance, thereby deterring internal employees from committing or colluding in fraud
- Implementing efficient and early fraud detection
- Continuously monitoring both internal and external entities
- Employing strong deterrents, including taking action against employees and legal proceedings against external fraudsters, both externally and internally, to minimise future frauds

**Blocking lost and stolen Smartphones**

Lost and stolen Smartphones are probably the biggest mobile phone security threat within the UK at the moment.

If you can render that lost or stolen device useless once the customer has reported its loss then that device can lose its resell value.

MNOs have the ability to block stolen devices. All mobile phones, including Smartphones, have a unique number called the IMEI. The GSMA maintains a global database of lost or stolen devices, a ‘blacklist’ using the IMEI as the unique identifier. This is called the GSMA IMEI DB. MNOs can access this database to check whether a device that is not on their own database has been blacklisted.

MNOs can choose to operate their own database of lost and stolen database and this is commonly referred to as ‘Equipment Identity Registers (EIR)’. Operators have the option of connecting their local EIR to the GSMA IMEI DB.

Every time a Smartphone connects to the mobile network it will transmit its own unique IMEI number and during this process should check the EIR to verify whether the device has been blacklisted, e.g. is categorised as being lost or stolen. This is classified as having a mobile phone ‘blocked’. It is illegal and a criminal offence in the UK to ‘unblock’ or offer to ‘unlock’ a phone.

If implemented and enforced correctly than this system for blocking lost and stolen Smartphones offers a serious countermeasure to the threat of lost and stolen Smartphones.

**Consumer awareness**

Consumer awareness, in partnership with technology controls, is an important aspect in preventing and controlling threats to the security of Smartphones.

This section outlines some of the consumer awareness practices that are currently place in the UK.

It is difficult to gauge the effectiveness of consumer awareness practices without carrying out very specific consumer market surveys.
Consumer awareness practices and programmes are currently being offered by a number of stakeholders including MNOs, government-sponsored bodies and law enforcement agencies including UK Police.

Most, if not all, of MNO initiated communication to consumers on Smartphone threats is via their websites.

There is an opportunity to advise UK consumers on the latest threats to Smartphones when a consumer purchases a phone and network plan but from experience this is not happening.

Unfortunately, security advice is not easy to find on these websites and is usually buried away in the support pages. It is our belief that most consumers will not go looking for information and advice on security.

There is an obligation for an organisation to have a statement on ‘privacy’ on their websites why not for ‘security’?

The following is a summary of Goode Intelligence’s findings when searching for Smartphone security advice on the websites of the major UK MNOs. It is not intended to be a comprehensive review of the ability of UK MNOs to offer security advice to its consumer customers.

**T-Mobile**

There was no obvious location for security questions and concerns about Smartphone security. On a Google search for “T-Mobile Smartphone security” an FAQ on security was displayed and this can be viewed here. The security FAQ detailed a number of general security facts on topics including:

- What do I do if my phone is lost or stolen?
- What should I do if I discover illegal material online?
- What does T-Mobile do to prevent identity fraud?
- How does identity fraud happen?

**Telefonica O2**

Similarly to T-Mobile there is no obvious area of the website where security advice is offered.

There are facts and advice on the support pages of the O2 UK website that deal with:

- How do I wipe a Blackberry of personal information?
- Is O2 Wallet secure?
- The security code for my mobile isn’t working

**Orange**
Study into the implications of Smartphone operating system security

On its UK website, Orange doesn’t specifically offer any obvious messages and advisories on Smartphone security. A search on “Smartphone security” did not return anything specific and included links to articles on:

- Is mobile broadband secure?
- How secure are mobile contactless payments?
- Why do I have problems viewing secure sites?

Vodafone

There were no clear messages on consumer Smartphone security on Vodafone’s UK website. There was some specific information on certain Smartphones, such as “How do I change my SIM PIN” but no obvious place where advice was on keeping Smartphones safe.

Three

A search on the Three’s support website for “Smartphone security” came back with no suggestions and this message “Sorry, No results were found.”

A similar search on “security” came back with 30 suggestions and they included:

- Voicemail security
- Staying secure online
- Removing viruses from your computer

Mobile Virtual Network Operators (MVNOs)

MVNOs, including Virgin Media, are similar to MNOs in that they offer little advice on how consumers should and can protect their Smartphones.

Government-sponsored bodies

The main government-sponsored body for raising consumer awareness for security issues for Information Technology and computing is Get Safe Online.

Get Safe Online is a public-private partnership whose aim is to be “the UK’s leading source of unbiased, factual and easy-to-understand information on online safety”.

Goode Intelligence © 2013
Study into the implications of Smartphone operating system security

It has a specific page on “Smartphone and Tablets” where advice on physical security (lost and stolen devices), QR codes, safe disposal, transferring money, viruses and spyware and wireless networks and hotspots is offered.

**UK Police**

UK Police has been proactive in dealing with the rising threat of stolen Smartphones, mainly stolen as a result of street crime and muggings.

Various UK Police services offer advice on how to prevent Smartphone theft. This is offered through websites and using campaigns that involve posters (see figure x below)

**Figure 5.1: Metropolitan Police Service Smartphone theft poster**

![Metropolitan Police Service Smartphone theft poster]

Source: Metropolitan Police Service

Websites that offer advice on Smartphone theft include:

- Mobile theft – MPS website  
  http://safe.met.police.uk/personal_theft/get_the_facts.html
- National mobile phone crime unit (MPS) http://www.met.police.uk/mobilephone/
- Checking whether a mobile phone is stolen from http://www.checkmend.com/uk/
6. HOW ARE OTHER REGIONS DEALING WITH SMARTPHONE SECURITY?

**Overview**

This section is a companion to sections that detail how the UK is responding to Smartphone security issues.

It will discuss the role of policy and regulation in managing Smartphone security and reviews whether there are any lessons that can be learnt from how other regions are making consumers aware.

This section focuses on two regions, the European Union (EU) and the USA, both with strong Smartphone adoption.

**EU**

**European Network and Information Security Agency**

The European Network and Information Security Agency (ENISA) has been set up by the EU to be the “pace-setter for Information Security in Europe” with a mission to “to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union”.

The agency has been actively offering support to EU member states on Smartphone security since 2010 when they first published a report assessing the security risk from using Smartphones and offering “practical recommendations on to address these risks”.94

In December 2010, ENISA identified the top ten Smartphone security risks in an attempt to “convey the risk in relation to others”95. Even though the risks were created over two years

---


ago they still offer a fair representation on current threats and risks. They are represented in the following table, table 6.1.

**Table 6.1: ENISA Top Ten Smartphone Security Risks**

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data leakage resulting from device loss or theft</td>
<td>High</td>
<td>The Smartphone is stolen or lost and its memory or removable media are unprotected, allowing an attacker access to the data stored on it.</td>
</tr>
<tr>
<td>2</td>
<td>Unintentional disclosure of data</td>
<td>High</td>
<td>The Smartphone user unintentionally discloses data on the Smartphone.</td>
</tr>
<tr>
<td>3</td>
<td>Attacks on decommissioned Smartphones</td>
<td>High</td>
<td>The Smartphone is decommissioned improperly allowing an attacker access to the data on the device.</td>
</tr>
<tr>
<td>4</td>
<td>Phishing attacks</td>
<td>Medium</td>
<td>An attacker collects user credentials (such as passwords and credit card numbers) by means of fake apps or (SMS, email) messages that seem genuine.</td>
</tr>
<tr>
<td>5</td>
<td>Spyware attacks</td>
<td>Medium</td>
<td>The Smartphone has spyware installed, allowing an attacker to acces or offer personal data.</td>
</tr>
<tr>
<td>6</td>
<td>Network Spoofing Attacks</td>
<td>Medium</td>
<td>An attacker deploys a rogue network access point (WiFi or GSM) and users connect to it.</td>
</tr>
<tr>
<td>7</td>
<td>Surveillance attacks</td>
<td>Medium</td>
<td>An attacker keeps a specific user under surveillance through the target user’s Smartphone.</td>
</tr>
<tr>
<td>8</td>
<td>Diallerware attacks</td>
<td>Medium</td>
<td>An attacker steals money from the user by means of malware that makes hidden use of premium rate SMS services or numbers</td>
</tr>
<tr>
<td>9</td>
<td>Financial malware</td>
<td>Medium</td>
<td>The Smartphone is infected with malware specifically designed for stealing credit card numbers, online banking credentials or subverting online banking or ecommerce transactions</td>
</tr>
<tr>
<td>10</td>
<td>Network congestion</td>
<td>Low</td>
<td>Network resource overload due to Smartphone usage leading to network unavailability for the end-user.</td>
</tr>
</tbody>
</table>

*Source: ENISA*

ENISA’s advice and support is technology focused and offers support for Smartphone security currently with a number of activities including:
Study into the implications of Smartphone operating system security

1. Secure app development
2. App store security

Secure app development

ENISA has drafted, together with the Open Web Application Security Project (OWASP) mobile security project, security guideline for app developers.96

Written in 2011, the guidelines have been written for developers of Smartphone apps as a guide to developing secure mobile apps.

It offers practical advice on securing mobile apps with ten control mechanisms:

1. Identify and protect sensitive data on the mobile device.
2. Handle password credentials securely on the device.
3. Ensure sensitive data is protected in transit.
4. Implement user authentication and authorisation (including session management).
5. Securing backend APIs (services) and the platform (server) secure.
6. Secure data integration with third party services and applications.
7. Pay specific attention to the collection and storage of consent for collection and use of user’s data.
8. Implement controls to prevent unauthorised access to paid-for resources (wallet, SMS, phone calls etc.).
9. Ensure the secure distribution and provisioning of mobile apps.
10. Checking for runtime interpretation of code for errors.

App store security – Mobile malware

ENISA offers advice against the threat of mobile malware in a report published in September 2011 entitled “Appstore security – 5 lines of defence against malware”.97

In the report ENISA identifies these five lines of defence against mobile malware:

1. App review: App stores should review apps before admitting them to the app store.
2. Reputation mechanism: App stores should show the reputation of apps and app developers.
4. Device security: Includes supporting sandboxes to install and run apps “to reduce the impact of malware”.

---

5. Jails (or walled gardens): This is closing the sideloading feature. ENISA recommends that “the Smartphone should either be blocked from using untrusted app stores or, for expert users, present clear warnings about installing from untrusted sources”.

**United States of America**

**Government policy and regulation**

According to Lookout Mobile Security’s Tim Wyatt the US Government is “getting more involved in Smartphone security with the regulator getting more involved with privacy issues around the use of these devices.”

**FTC vs. HTC**

A clear indication of the US regulatory bodies “getting more involved” was the recent legal action against Taiwanese Smartphone manufacturer, HTC.

In February 2013, the US’ Federal Trade Commission (FTC), similar to the UK’s Office of Fair Trading (OFT), announced a settlement made by HTC after facing charges from the FTC that “it failed to secure millions of mobile devices shipped to consumers”. As a result of the settlement it was required to patch vulnerabilities on HTC Smartphones and tablet computers and to “establish a comprehensive security program designed to address security risks during the development of HTC devices”.

According to a FTC press release, HTC “failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers, introducing security flaws that placed sensitive information about millions of consumers at risk.”

In a very indicting statement the FTC statement went on to say that “HTC America failed to employ reasonable and appropriate security practices in the design and customization of the software on its mobile devices” and “failed to follow well-known and commonly accepted secure coding practices, and failed to establish a process for receiving and addressing vulnerability reports from third parties”.

Study into the implications of Smartphone operating system security

The FTC complaint revealed specific vulnerabilities that had been found on HTC’s devices including:

- Insecure implementation of two logging applications, Carrier IQ and HTC Loggers
- Programming flaws that would allow third-party applications to bypass Android’s permission-based security model

This action by the FTC has been considered to be a milestone in Smartphone security. A government body taking legal action against a Smartphone manufacturer for poor security implementation. If the FTC has decided to intervene against HTC in its duty to protect USA consumers against Smartphone security threats, the question has to be asked “is this just the start of legal action and who could be next?” It sends out a clear warning to other vendors operating in this sector not to treat security lightly.

As a follow-up to this case the FTC is planning to hold a public forum on malware and other mobile security threats on 4 June 2013.

**Federal Communications Commission (FCC) Smartphone Initiatives**

Another US Government body, the Federal Communications Commission (FCC) has responded to the Smartphone security threat with a number of initiatives that were started in April 2012. The FCC is Ofcom’s US counterpart who regulates “interstate and international communications by radio, television, wire, satellite and cable”.

In April 2012, the FCC announced new initiatives to “combat massive smartphone and data theft”. In a joint announcement with US State Police Departments and the Mayor of Washington D.C., Vincent Gray, the FCC highlighted the problem of Smartphone theft quoting New York City Police figures that “more than 40 percent of all robberies in New York City involve Smartphones”. A new initiative was announced, with the support of the US MNO (carrier) community, to “implement a database to prevent use of stolen Smartphones”. The central stolen Smartphone database was to be rolled out in an 18 month timeframe.

Alongside the stolen Smartphone database initiative the FCC announced a number of other initiatives that aimed to raise consumer awareness through channels such as the US MNO (carrier) and handset manufacturer communities. These included (and the following is a direct quote from the FCC press release):

- “Encourage users to lock their phones with passwords:
  - Smartphone makers will notify and educate users in the most highly visible ways — through messages on the Smartphone itself and through “Quick Start” user guides — about how to use passwords to deter theft and protect their data

- Educate users in lock/locate/wipe applications:

---

Study into the implications of Smartphone operating system security

- Wireless providers [MNOs] will directly inform their customers about how to find and use applications that enable customers to lock/locate/and wipe smartphones remotely

- **Public education campaign on how to protect your Smartphone and yourself:**
  - The wireless industry will launch a campaign, with media buys, to educate consumers on how to protect their smartphones and themselves from crime

- **Progress benchmarks and ongoing dialog:**
  - The wireless industry will publish quarterly updates and submit them to the FCC on progress on these initiatives

- **Accountability:**
  - The FCC will engage the public safety community and wireless carriers in an ongoing dialog, with regular, quarterly meetings, to ensure that the most effective technological processes are in place to deter smartphone theft and data exposure
  - The FCC will launch a proceeding if progress on the above deliverables falls behind schedule

- **Legislation expected to criminalize tampering with unique hardware IDs on cell phones:**
  - Members of Congress are planning to introduce legislation that will make it a federal crime to take steps to evade the effective deployment of a stolen phone database, including by tampering with hardware identifiers on wireless devices
  - Criminalizing tampering with unique hardware identifiers has been an integral part of successful foreign deployments of stolen cell phone databases and the deterrence of cell phone theft

Goode Intelligence does not know how effective these initiatives have been in deterring Smartphone theft and for raising consumer awareness. A quick check of some of the major US carriers’ websites does not find anything obvious in the way of advice on Smartphone security and theft.

Goode Intelligence recommends that Ofcom contact the FCC to determine the success of these initiatives and if there are any lessons that can be learnt
Study into the implications of Smartphone operating system security

**Consumer awareness**

The FCC has also been directly involved in attempting to raise awareness for Smartphone security through a number of campaigns.

These include “Ten Steps to Smartphone Security for Android” and the “FCC Smartphone Security Checker”.

![FCC Logo]

This is also being included in the Department of Homeland Security’s (DHS) “Stop.Think.Connect” (STC) campaign, “a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online.” The campaign was launched on 4 October 2010 after a presidential Cyberspace Policy Review.

**Ten Steps to Smartphone Security for Android**

The FCC recommends these ten steps to protect Android Smartphones:

1. Set PINs and passwords
2. Do not modify your smartphone’s security settings
3. Backup and secure your data
4. Only install apps from trusted sources
5. Understand app permissions before accepting them
6. Install security apps that enable remote location and wiping
7. Accept updates and patches to your smartphone’s software
8. Be smart on open Wi-Fi networks
9. Wipe data on your old phone before you donate, resell or recycle it
10. Report a stolen smartphone

**FCC Smartphone Security Checker**

The FCC Smartphone Security Checker is an online tool set up by the FCC “to help many smartphone owners who aren’t protected against mobile security threats”.

This was launched in December 2012 with assistance from companies such as Lookout, BlackBerry, Sophos, McAfee and Symantec.

---

99 The full advisory can be found here [http://www.fcc.gov/smartphone-security/Android](http://www.fcc.gov/smartphone-security/Android)
Study into the implications of Smartphone operating system security

The aim of the online tool is to educate US Smartphone users on how best to secure their Smartphones.

The free security checker tool supports Apple iOS, BlackBerry, Google Android and Windows Phone mobile operating systems.

FCC Chairman Julius Genachowski said, “With less than half of smartphone owners using passwords to protect their devices, this new tool will be of particular value to millions of Americans. The holiday gift-giving season is a perfect time to remind consumers to take simple steps, like setting a password, to protect themselves from mobile security threats.”

7. CURRENT UK SMARTPHONE SECURITY REGULATORY AND INSTITUTIONAL RESPONSIBILITIES

Overview

Regulation and enforcement in a constantly evolving sector can be difficult. This is especially difficult with the trans-regional nature of modern digital services. For instance, you may have a scenario in which a UK consumer is accessing a UK MNO network using a mobile banking app developed in Australia with data stored across south-east Asia and Europe from a South Korean Smartphone that is running an open source operating system developed in the USA. What if something goes wrong and the UK consumer finds themselves out of pocket as a result of some financial fraud. Who do they turn to? Is it to the MNO? the handset manufacturer? or the financial services supplier? And in whose regulatory jurisdiction does this operate in?

Regulation does have an important part to play for Smartphone security but cannot be the answer in all cases. It is the joint responsibility of the consumer (someone has to lock the front door of the house), technology developers and device vendors to ensure that they are aware of their own responsibilities.

This section will briefly investigate the state of regulatory and institutional responsibilities and to identify any gaps that may exist. It does not aim to provide an in-depth analysis of the suitability of current UK regulation to Smartphones.

Before we do this we shall introduce three UK regulatory bodies that are responsible for enforcing much of the legislation that governs Smartphone security; The Information Commissioner’s Office (ICO), Ofcom and PhonepayPlus.

The Information Commissioner’s Office (ICO)

Goode Intelligence interviewed Dr Simon Rice, technology policy advisor, and Dave Evans, Group Manager, Business and Industry, Information Commissioner’s Office (ICO).

ICO is the UK’s “independent public body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals”. They enforce key pieces of UK data protection and privacy legislation including the Data Protection Act (DPA) 1998, the Privacy Electronic Communications (EC Directive) (Amendment) Regulations 2011 and the Freedom of Information Act 2000.
Study into the implications of Smartphone operating system security

In relation to Smartphone security they are responsible for data protection and privacy issues in the same way that they enforce legislation in other aspects of Information Technology.

With reference to Smartphones ICO believes that “location data is a concern” particularly from a privacy point of view.

ICO feels that “although the current framework is technology neutral there are areas where the legislation is catching up with changes to the technical landscape” such as with Smartphone technology and with the EU’s Article 29 working party (revised EU Data Protection legislation) investigating location based services (Geolocation). Revised legislation will better reflect the latest technological innovations.

Where ICO has its greatest concern for Smartphone security is in the following areas; the capture of personal data, including location data, and the transparency of where Smartphone generated data is going, who is using it and for what purpose. This is seen as a problem area especially when location information is captured on a 24/7 basis. Whether this is wilful or accidental collection is largely unknown.

When asked whether the UK could mirror the US in taking legal action against a technology company for lapse Smartphone security practices, ICO responded by saying that it could, but action would depend on the specific circumstances. It would be more likely to be taken in the case of a malicious or poorly written app rather than for a security vulnerability in the core of the OS.

ICO are currently taking steps to educate mobile app developers to ensure that they are aware of the some of the privacy issues that may be introduced. ICO are aiming to ensure that developers factor in “privacy by design” and design apps “with privacy and data protection in mind and not collect data just for the sake of it – without having a legitimate use for it”.

Telecommunications regulation

Ofcom

Ofcom is the UK’s main independent regulator and competition authority for the UK’s communications industries and is responsible for regulating both fixed and mobile telecommunications service providers.

Ofcom has a statutory duty to further the interests of citizens in relation to communications matters. Ofcom is also guided by a regulatory principle to research markets constantly and aims to remain at the forefront of technological developments.
PhonepayPlus

PhonepayPlus is the organisation that regulates phone-paid (premium rate services or PRS) services in the UK.

Under the Communications Act 2003, Ofcom has responsibility for the regulation of premium rate services. In December 2007, it was confirmed that PhonepayPlus will act as the agency which carries out the day-to-day regulation of the PRS market on Ofcom’s behalf.

PhonepayPlus regulates the PRS industry using a Code of Practice (revised 12th edition published 1 September 2011).

Goode Intelligence has assisted PhonepayPlus in analysing the threat of mobile malware to PRS fraud and the regulator has been actively monitoring the on-going threat to UK consumers.

**Fraud and Financial Regulation**

There has been recent activity in the organisational structure for fraud and financial regulation.

In 2013 The National Fraud Authority (NFA) was set up to “coordinate the fight against fraud in the UK”. Part of their remit is manage ‘Action Fraud’, the UK’s national fraud and internet crime and reporting centre.

The NFA works with a number of UK Government bodies including:

- Department of Business, Innovation and Skills (BIS)
- Crown Prosecution Service (CPS)
- Department of Work and Pensions (DWP)
- Financial Conduct Authority (FCA)
- Prudential Regulation Authority (PRA)
- Home Office
- HM Revenue and Customs
- Office of Fair Trading
- Serious Fraud Office
- Serious Organised Crime Agency (SOCA)
Study into the implications of Smartphone operating system security

- Attorney General’s Office (AGO)
- National Fraud Intelligence Bureau (NFIB)
- City of London Police

**UK legislation and Smartphone security**

This section investigates current UK legislation and Smartphone security threats and vulnerabilities that have been discussed in this report.

It maps relevant UK legislation and Smartphone security risk to the bodies that are responsible for governing it.

**Table 7.1: UK legislation and Smartphone security**

<table>
<thead>
<tr>
<th>Smartphone security risk</th>
<th>Applicable legislation</th>
<th>Institution Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unpatched Smartphone</td>
<td>Unclear</td>
<td>Unclear</td>
</tr>
<tr>
<td>Lost and stolen Smartphone (leading to potential loss of privacy, identity and data)</td>
<td>• Criminal law for theft</td>
<td>Shared between:</td>
</tr>
<tr>
<td></td>
<td>• Data Protection Act</td>
<td>• Police Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The ICO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PhonepayPlus</td>
</tr>
<tr>
<td>Telephony Financial (Premium Rate Services) fraud</td>
<td>• Communications Act 2003</td>
<td>PhonepayPlus</td>
</tr>
<tr>
<td></td>
<td>• PhonepayPlus Code of Practice</td>
<td>Ofcom</td>
</tr>
<tr>
<td>Loss of privacy (due to Spyware and Malware)</td>
<td>• Data Protection Act 1998</td>
<td>The ICO</td>
</tr>
<tr>
<td></td>
<td>• Communications Act 2003</td>
<td>Ofcom</td>
</tr>
<tr>
<td></td>
<td>• Computer Misuse Act 1990</td>
<td>CPS</td>
</tr>
<tr>
<td></td>
<td>(Police and Justice Act 2006)</td>
<td></td>
</tr>
<tr>
<td>Financial services (banking) fraud</td>
<td>• Financial Fraud Act 2006</td>
<td>FCA &amp; PRA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>National Fraud Authority (NFA)</td>
</tr>
</tbody>
</table>

*Source: Goode Intelligence © 2013*
Study into the implications of Smartphone operating system security

Summary and Recommendations

Smartphones have become the remote control for our digital and non-digital lives, replacing desktop computers, notebooks and even TVs and personal music players. As such, they are subject to the same threats that have affected consumers for many years.

These threats are controlled by legislation and governed by bodies that have been assigned responsibility to govern them.

Governing bodies need to understand the nature of these threats. Many of the current threats are old ones adapted for Smartphones, e.g. Dialler fraud.

There are threats that are either unique to the Smartphone or are amplified as a result of the characteristics of the Smartphone. A Smartphone is more likely to be lost and stolen and when it gets into the hands of unauthorised users more likely to be poorly protected by either no passcodes or weak ones.

From table 7.1 above, we have identified the current Smartphone security risks and matched them against relevant legislation and the bodies responsible for governing them.

Goode Intelligence believes that current legislation should be sufficient in dealing with current Smartphone security issues. There does not seem to be any major holes in current legislation that could result in a disparity between the technology and the governing framework.

However, this must be constantly reviewed in light of emerging, sometimes disruptive, technology that could alter the effectiveness of regulation and legislation.

Related to legislation is education (engagement) and enforcement; educating affective parties as to the nature of legislation by engaging with all parts of the ecosystem and enforcement once there has been a breach (either intentional or unintentional).

Recommendations

Goode Intelligence recommends the following:

1. Creation of a cross-regulatory working party to discuss potential issues and gaps in protecting Smartphones, and their associated services. This study could act as the initial reference point for such a group.

2. Review of Smartphone security risks against UK legislation to determine:
   a. UK legislation related to particular security risk
   b. UK regulatory that is responsible for particular security risk
   c. Gaps
   d. Action plan to manage security risks
8. THE IMPACT OF EMERGING MOBILE TECHNOLOGY TO SMARTPHONE SECURITY

Overview

Innovation in mobile computing including Smartphones is happening at a spellbinding pace.

Each time a major Smartphone operating system version or new device arrives it heralds the arrival of the latest innovative technology.

So far the development of the Smartphone has brought us more accurate location-based services with GPS, faster communication speed with the arrival of 3G+, motion-awareness with the introduction of the accelerometer sensor and the replacement of a physical keyboard with touchscreens.

The next phase of smart mobile devices (SMD) is planning to introduce us to biometric sensors that capture or track our eye movements, record our voice and enable us to lock our devices with the swipe of the finger.

Even the form factor of the Smartphone is changing. Apple and Google promise us wearable devices in the form of a watch\textsuperscript{101} and glasses\textsuperscript{102} respectively. Agile, always on (both switched on and on us), devices running Smartphone operating systems that offer a far more personal experience then Smartphones.

With the fast pace of technology innovation that is being experienced with smart mobile devices there is sometimes a period where security and privacy issues/concerns play catch up. If security has not been built in or hard-baked into the product then there is a possibility that vulnerabilities will be exposed by an equally innovative and increasingly well-funded security research community.

The following sections investigate the potential security implications of three technology innovations and trends that are starting to impact Smartphones; Near Field Communications (NFC), LTE (long-term evolution) or 4G and the trend of Bring Your Own Device (BYOD) and the Consumerisation of IT.

\textsuperscript{101} Rumours of an Apple iWatch are strongly gain ground. See this piece from Forbes entitled “What if an iWatch Replaced Most Of The iPhone’s Functions? Published 13 February 2013: http://www.forbes.com/sites/anthonykosner/2013/02/13/what-if-an-iwatch-replaced-most-of-the-iphones-functions/

\textsuperscript{102} Refers to Google’s ‘Glass’ project - http://www.google.com/glass/start/
Near Field Communications (NFC)

What is it?

NFC is a set of standards for devices, including Smartphones, to enable two-way short-range radio communication between NFC-enable devices. They are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443 and Sony’s FeliCa.

The typical range of the communication is a distance of 10 cm or less (although this can be extended to 20 cm)

The NFC standards have been defined by the NFC Forum, which was founded in 2004 by Nokia, Philips and Sony.

For a Smartphone to support NFC it either needs an embedded NFC chip or a NFC-enabled sleeve or sticker can be attached to the device.

There is a wide range of use cases for NFC. NFC is being used in contactless payment systems (mobile payment at the physical point of sale) and electronic ticketing.

Google Wallet is an example of a Smartphone-based payment solution that uses NFC and is being pre-installed on Google’s Nexus range of Smartphones that support NFC. There are other competing mobile wallet solutions that use NFC and also support existing payment services from MasterCard (PayPass) and Visa.

For ticketing, Austria, Finland, Italy, New Zealand and Germany have all trailed NFC ticketing systems for public transport.
Potential security threat

With greater use of NFC we will see attempts to undermine its security and attack devices through this communication channel.

As NFC can be used for commercial purposes, including payment then there will be attempts to attack this communication method for malicious purposes.

By opening up a new channel for communication it offers another route onto the device that could be attacked. Security vendors such as Symantec believe that there will be security issues in terms of eavesdropping. However, it is more difficult to attack NFC as the range is far less (10 cm) than other wireless communication technologies such as WiFi. An attacker would have to get close to its victim to perpetrate a successful attack and as NFC signals can be sensitive in terms of direction, a moving target would be difficult to hit.

A potential risk is in reprogrammed or fake NFC smart tags. An NFC tag can be embedded in a promotional poster or at an information point and the user would tap their NFC-equipped Smartphone to read the information that had been programmed onto the tag. It is similar to using a camera’s phone to read a barcode that may have been printed onto a poster or within a magazine. There is a potential for hackers to corrupt or reprogram NFC tags for their own purposes. They would have to break the tag’s encryption to achieve this.

There is also the potential for criminals and hackers to place their own NFC tags in public places. These tags could be programmed to take the user to a malicious site that may be attempting to distribute malware. A user can take precautions to counteract this. For instance do not tap any tags that are not physically protected, either behind glass or plastic, or check that a poster has not been tampered with. However, as this is new technology then education about what is legitimate or fake is difficult to determine and there will be instances when a consumer will tap on a tag whose purposes is malicious or illegal.

McAfee predicts in its “McAfee Mobile Security: McAfee Consumer Trends Report” that in “2013, we expect to see criminals abuse the tap-and-pay NFC technology used in mobile payment programs, or “digital wallets.” This scam uses worms that propagate through proximity, a process we can call “bump and infect.” The distribution path can quickly spread malware through a group of people such as in a passenger-loaded train or at an amusement park. When the newly infected device is used to “tap and pay” for the next purchase, the scammer collects the details of the wallet account and secretly reuses these credentials to steal from the wallet. Worm malware like this will spread by exploiting vulnerabilities on devices. This development would monetize the 11.8 per cent of malware families that already contain exploit behaviours."

As NFC is in its early days of deployment it is still too early to accurately predict whether there will be large-scale attacks on vulnerabilities on NFC deployments.

Goode Intelligence believes that the security risk to UK consumers is currently low mainly as a result of a lack of wide-scale adoption and to the physical limitations of attacking a device from a short range.
Study into the implications of Smartphone operating system security

Goode Intelligence recommends that Ofcom monitor NFC security and to draft consumer guidelines as to safe use of the technology especially around the use of smart NFC tags.

**LTE (4G)**

**What is it?**

LTE or long-term evolution is the latest standard for wireless communication of high-speed data for mobile phones. Often called 4G it provides faster and more reliable mobile network speeds.

The standard has been developed by the 3GPP (3rd Generation Partnership Project).

The UK is beginning to see the role out of LTE services with EE (T-Mobile and Orange) being the first network to offer LTE services in certain metropolitan centres late in 2012.

The latest LTE standard provides for peak speeds of 100 Mbit/s for high mobility and 1 Gbit/s for low mobility communication. Test speeds on early deployments in the USA has seen download speeds of over 50 Mbit/s and upload speeds of 15 Mbit/s.\(^\text{103}\) Testing by ‘engadget’ (an online tech magazine) saw average download speeds of around 38 Mbit/s and upload speeds of around 20 Mbit/s in tests on the EE 4G network in the UK.\(^\text{104}\)

The LTE standards offer enhanced security including more robust authentication, supporting greater cryptographic key sizes (maximum of 128 bit key lengths at present). There are also security enhancements to offer improved protection of the Backhaul and Relay Nodes within the mobile network architecture. This should lead to improved network security making it more difficult to intercept voice and data communication over the LTE network.

**Potential security threat**

Most security experts believe that there are no inherent security risks directly as a result of LTE.

However, there is acknowledgement that the bigger the pipe the greater the risk. We have seen with the evolution of faster fixed line networks, such as ADSL and Fibre-optic speed broadband, a corresponding increased security risk that has led to an increase in viruses and malware infecting these connected PCs. Will LTE result in a similar story? Some security experts believe so and that we could see an increase in mobile botnets.

Symantec feel that LTE could lead to the development of bigger and more sophisticated malware payloads. Tom Schroeder, Senior Specialist, Enterprise Mobility Solutions, Symantec, believes there is an urgent “need for a clean pipe”, referring to the LTE mobile

\(^{103}\) T-Mobile LTE Speed Tested. PC Magazine, 18 March 2013. http://www.pcmag.com/article2/0,2817,2416660,00.asp

\(^{104}\) We test speeds on EE, the UK’s first LTE network! Engadget, 11 September 2012: http://www.engadget.com/2012/09/11/ee-lte-speed-test-4g/
network, that filters out unwanted communication including spam and malware. Schroeder also says that there will be "more connected devices and the expansion of Mobile-to-Mobile (MDM) as a result of LTE" and this could lead to increased "unmanaged" devices on the mobile network.

Cathal McDaid, Security Consultant, Adaptive Mobile, says that "LTE will see very little from a security threat perspective." McDaid believes that one possible change could be that "spyware will be easier as the greater network speeds mean that any video/audio spying can be relayed back to a Command and Control (C&C) node.

As LTE is being rolled out across the UK and more subscribers connect to the 4G network using compatible Smartphones then the threat scenarios will become more established.

---

105 Interview with Tom Schroeder, Senior Specialist, Enterprise Mobility Solutions, Symantec. Held with Goode Intelligence, 6 March 2013.
9. INVESTIGATION AND SECURITY ANALYSIS INTO MOBILE APP MARKET SECURITY

Overview

This section investigates measures that have been implemented to secure mobile app store services.

App stores are the main delivery mechanism for mobile apps.

App stores are divided into official, those that are approved and usually run by the mobile operating system vendor, and unofficial, everything else.

The two most popular mobile app stores are provided by Apple and Google and are tied to iOS and Android Smartphone operating systems respectively.

Apple iOS users cannot use an app store from a competing mobile platform. A developer creating a native iOS app must distribute this app through the official app store. The same lock-in to the operating system vendor’s app store is seen for Blackberry OS, BlackBerry World app store, and Windows Phone 8, Windows Phone app store.

This differs from Android where an Android developer is not tied to Google Play. They can distribute their app through a wide variety of distribution channels including unofficial app stores, e.g. Amazon Android app store, file sharing sites, e.g. BitTorrent, and even by sideloading an app from a connected desktop. Android really is an open platform.

In general, according to Adaptive Mobile’s Cathal McDaid “app store security ranges from good to poor”. Goode Intelligence believes that out of the top two mobile app stores Apple operates at the good end, Google Play is somewhere in the middle (but edging up towards good all of the time) and the unofficial Android app stores are at the poor end of the spectrum.

Official App Stores

The official app stores are run and managed by the major Smartphone operating system vendors. They have all implemented security measures to protect the integrity of the app distribution process. The main driver in adopting security measures within official app stores is to prevent malicious code from being distributed to smart mobile devices including Smartphones.

In its ‘Emerging Cyber Threat Report 2013’, Georgia Tech University106 Professor Traynor, assistant professor with Georgia Tech’s School of Computer Science states that, “largely, it [security within app stores] appears that the mechanisms in place appear to be working.”

Study into the implications of Smartphone operating system security

The following sections will investigate the state of security measures for the main Smartphone operating systems app official app stores starting with an analysis of the Apple app store.

**Apple App store**

Apple prides itself on the security of its app store. Every app that is submitted by an Apple iOS developer to the app store is reviewed.

The review process includes checking for Malware and to determine if it is a fake or rogue app.

A fake or rogue app is a pirated version of an app that may be offering a premium (paid for) version of an app for free. Fake and rogue apps have been known to carry malicious code.

As a result of these protection mechanisms there has been no recorded instance of malware that has been uploaded or distributed via the Apple app store.

**BlackBerry World**

In addition to BlackBerry's own security mechanisms for BlackBerry World the Canadian Smartphone manufacturer has enlisted the help of a security vendor, Trend Micro, to ensure the reputation of its mobile apps.

BlackBerry is concentrating on anti-fraud and reputation management to distinguish its app store offering within the market. According to a BlackBerry spokesperson BlackBerry aims to be compliant with the upcoming EU Data Protection legislation that is planned to become law during 2014.

BlackBerry World is starting to use a new service supplied by Trend Micro that acts as an app store reputation service. Trend’s mobile app reputation service was initially developed for the Android platform but has been modified to work for BlackBerry OS apps. The reputation service scores apps on a reputational basis according to three defined levels:

- Malicious
- Privacy
- Resource Utilisation (battery, memory and network utilisation)

It then rates the app on a 1-10 basis, where 10 is a high risk and 1 is classified as a low risk. Every app is scanned using this service and BlackBerry has the ability to reject the app if the score is high. The reputational scoring will also be available to BlackBerry OS users. They can use the scoring to judge whether an app should be downloaded or not.
Study into the implications of Smartphone operating system security

**Google Play**

Google’s app store (initially Market and now Play) has seen its fair share of malware but is not the main distributor of Android malware in the world. Unofficial Android app stores are considered to be the main distribution vector for Android malware.

Google has been proactive in attempting to curb the spread of malware from Play by introducing two main security components, Bouncer and the Kill Switch ‘app revocation’ function.

It still falls short of Apple’s app checking service and relies on technology to scan apps that have been already uploaded rather than create tighter processes for preventing criminals writing rogue apps that may contain malicious code.

**Bouncer**

Google announced during February 2011 news of its mobile malware analysis and checking service, codenamed “Bouncer”.

Google not yet revealed exactly how Bouncer works but security researchers have identified certain characteristics of the service including checking if an app attempts to harvest contact information from a phone and monitoring the SMS service in case an app tries to send unauthorised PSMS messages.

According to Google, Bouncer has been responsible for a 40 percent drop in the number of malicious apps in its app store.\(^{107}\)

Despite Bouncer’s appearance security vendors operating in the anti-virus market say that malware is still evident within Play. Security researchers have claimed to have circumvented Bouncer by placing malware in the Google Play app store.

It is certainly a move in the right direction and Google should be applauded for its efforts.

**Kill Switch**

Google operates a ‘revocation’-based security model for dealing with MM and other Apps that break the terms and conditions of Android Market. It is called the ‘REMOVE_ASSET’ or ‘Kill Switch’ function and is invoked by Google when an application breaks the terms and conditions of Google Marketplace.

Google has had this facility since 2008 and reportedly first used this facility in June 2010.

This function enables Google, and other Android Appstore service providers, to control potentially malicious applications that have been uploaded to the Appstore by removing them from the store and then removing them from devices that they can invoke the remote kill function on.

\(^{107}\) A look at Google Bouncer by TrendLabs: http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-at-google-bouncer/
Study into the implications of Smartphone operating system security

Google invoked this function in March 2011 when 58 MM-infected Apps were found on Android Market. It was claimed that around 260,000 Android devices had downloaded the MM and Google invoked the Kill Switch in an attempt to remove it. In blog posting on its Google Mobile Blog, the company announced:

“We are pushing an Android Market security update to all affected devices that undoes the exploits to prevent the attacker(s) from accessing any more information from affected devices. If your device has been affected, you will receive an email from android-market-support@google.com over the next 72 hours. You will also receive a notification on your device that “Android Market Security Tool March 2011” has been installed. You may also receive notification(s) on your device that an Application has been removed. You are not required to take any action from there; the update will automatically undo the exploit. Within 24 hours of the exploit being undone, you will receive a second email.”

Third-party Android App stores

Third-party Android app stores operate around the world and in some regions, Russia, Taiwan and China in particular; they are more popular than the official Google Play app store.

Third-party Android app stores are operated by a variety of organisation that includes mobile device manufacturers, MNOs and independent organisations including Amazon (both an ecommerce retailer and an Android handset manufacturer with its Kindle Fire).

The Wireless Industry Partnership (WIP) has a list of third-party Android app stores that is an excellent reference point and highlights what a vibrant market this is.

Popular Chinese-based Android app stores include:

- AppChina
- GoMarket

For many unofficial Android app stores there is a lack of control mechanism and security checks. These include:

- Weak registration checks including non-existent identity checks
- No DRM
- No App signing
- Weak submission rules
- No MM detection
- No App revocation (including use of the “Kill Switch”)
- Allowing Fake and Repackaged Apps to be submitted
- No policy for illegitimate or illegal content
- Allowing hard-core adult content (there are even specialist app stores for this)

There has been recent activity that may suggest that some of the more commercially successful and legitimate third-party Android app stores may be improving their processes and security mechanisms.

In February 2013 the Russian-based security vendor, Kaspersky Labs, announced plans that they were to protect an Android app store, Yandex.Store, using Kaspersky’s integrated antivirus engine. All submitted Android apps will be scanned using Kaspersky’s antivirus technology to prevent malware from entering the store.

---

10. INVESTIGATION AND SECURITY ANALYSIS INTO SIDELOADING MOBILE APPS

Overview

Following on from the discussion on app store security it is time to discuss the specific security risks of sideloading mobile apps – mainly an Android issue.

Sideloading mobile apps is defined as when a user can install a mobile app without using the official platform app store or app market.

The ability to install mobile apps from outside of the ‘official’ platform app stores is only officially supported on one Smartphone operating system, Google’s Android.

It can be achieved through ‘unofficial’ means on other devices when a user decides to Jailbreak their device. For instance, Jailbreaking an iOS device and allowing a user to install mobile apps from other sources outside of Apples official app store, e.g. through Jailbreak app stores such as Cydia. As we have seen Jailbreaking breaks the official iOS security model and creates increased levels of risk for the user, including the risk of being infected by malware.

For this study this section shall analyse the impact on sideloading mobile apps on Android Smartphones.

Android Sideloading

What is it?

Android sideloading is installing mobile apps outside of Google’s official mobile app store, Google Play.

Android has an option within the operating system settings that allows the installation of apps from any source.

There is a setting, usually found in the ‘security’ option of the ‘settings’ option, named ‘Unknown sources – Allow installation of non-Market apps’. Android Smartphones out of the box will have this option turned off. As a representative of O2 informed us “by default this is set to off, but a customer can turn it on.”

Once a user goes to this option and clicks on it to turn the option on then they will have the functionality to load and install mobile apps from virtually any source. From unofficial app stores, from file sharing sites including ‘BitTorrent’ and by copying over the Android app by connecting a Smartphone to a desktop computer. In some regions of the world you can purchase CD-ROMS that contain hundreds of Android apps (.APK files) that can then be copied to a Smartphone via a desktop computer.
Study into the implications of Smartphone operating system security

The majority of Android apps will be delivered to Smartphones via Google Play but some app developers may want to bypass this route just because they can. In mid-March 2013 reports were seen in the industry press that Facebook had prompted its Android users to download an update to a new version of its Apps without using Google’s official Play app store. As an article in The Verge stated “if Facebook can skip Google Play to update its app, what’s stopping a malicious developer from circumventing Google Play’s built-in virus scanner?”

**Why is it allowed?**

To answer this question on why Google has decided to support a much more open app delivery model we must go back to the start of Android. Apple iOS was already deployed on millions of iPhones and the Apple app store market was exploding, attracting thousands of app developers and hundreds of household names. Google had a challenge to catch up with Apple. Without a thriving mobile app ecosystem then there was a real possibility that Android would lose vital market share to Apple. Therefore Google made the strategic decision to be as open as possible, publishing Android as open source software and opening up the app delivery mechanism to anybody that wanted to operate what was becoming a booming market. It also allows organisations within the Android ecosystem to offer a branded app store experience.

Online retailers like Amazon can produce their own branded Android Smartphones and Tablets that are tightly integrated into their own retail ecosystem. Amazon’s own app store would not be possible without having an option to sideload apps from outside of Google’s own app market.

The decision to support an open app delivery business model is driven by Google’s commercial and business strategy and reflects the open license model.

However, the business advantages come at a security cost.

**The risks**

One of the major strengths of the mobile app delivery model is that by having a centralised market or distribution centre you can assert policy and control mechanisms on it. For instance, an app store owner can develop rules for how apps are written and then delivered to the central store. They can also scan uploaded apps to ensure that they are efficient and free of any malicious code. By allowing a user to install an app from any source you break this model and as a result greatly increase security risk.

There has been evidence of malware in Google Play but this is a small percentage of the total Android malware examples that have been detected. Google has strengthened security in its app market with the introduction of malware detection and removal tools. Google continues to strengthen its app store security mechanisms. Users do not have the same

---

110 Facebook nags Android users with updates outside of Play Store. The Verge, 15 March 2013
Study into the implications of Smartphone operating system security

levels of assurance in the majority of the unofficial app stores and file sharing websites that Android users can go to acquire mobile apps.

There is no doubt that this weakens the Android security model and it is currently the single biggest reason why malware is able to infect Android Smartphones.

**Should Sideload be stopped?**

If sideloading apps pose a serious security risk to Android Smartphone users than why is it still allowed.

There have been calls from the security industry to block sideloading and by default UK MNOs will turn-off the sideloading option in Android Smartphones that they ship.

The European Network and Information Security Agency (ENISA) in a report published in 2011 recommends that “the Smartphone should either be blocked from using untrusted app stores or, for expert users, present clear warnings about installing from untrusted sources”.

However, there may consequences to the Android ecosystem that may affect its openness if Google was to decide to remove the sideloading option from the operating system in future releases. Electronic commerce retailers such as Amazon are reliant on sideloading support to allow its Android-powered Kindle smart devices to download apps from Amazon’s own curated app store.

---

APPENDICES

Appendix A: Apple iOS Devices and Operating Systems

The following table, table A1 details Apple iOS devices and operating systems.

Table A1: Apple iOS devices and operating systems

<table>
<thead>
<tr>
<th>Model</th>
<th>Launch Operating System</th>
<th>Highest Supported Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone</td>
<td>iPhone OS 1.0</td>
<td>iPhone OS 3.1.3</td>
</tr>
<tr>
<td>iPhone 3G</td>
<td>iPhone OS 2.0</td>
<td>iOS 4.2.1</td>
</tr>
<tr>
<td>iPhone 3GS</td>
<td>iPhone OS 3.0</td>
<td>iOS 6.1</td>
</tr>
<tr>
<td>iPhone 4</td>
<td>iOS 4.0 (GSM) and iOS 4.2.5 (CDMA)</td>
<td>iOS 6.1.1</td>
</tr>
<tr>
<td>iPhone 4S</td>
<td>iOS 5.0</td>
<td>iOS 6.1.1</td>
</tr>
<tr>
<td>iPhone 5</td>
<td>iOS 6.0</td>
<td>iOS 6.1</td>
</tr>
<tr>
<td>iPod Touch 1st generation</td>
<td>iPhone OS 1.1</td>
<td>iPhone OS 3.1.3</td>
</tr>
<tr>
<td>iPod Touch 2nd generation</td>
<td>iPhone OS 2.1.1 and OS 3.1.1</td>
<td>iOS 4.2.1</td>
</tr>
<tr>
<td>iPod Touch 3rd generation</td>
<td>iPhone OS 3.1.1</td>
<td>iOS 5.1.1</td>
</tr>
<tr>
<td>iPod Touch 4th generation</td>
<td>iOS 4.1</td>
<td>iOS 6.1</td>
</tr>
<tr>
<td>iPod Touch 5th generation</td>
<td>iOS 6.0</td>
<td>iOS 6.1</td>
</tr>
<tr>
<td>iPad</td>
<td>iPhone OS 3.2</td>
<td>iOS 5.1.1</td>
</tr>
<tr>
<td>iPad 2</td>
<td>iOS 4.3</td>
<td>iOS 6.1</td>
</tr>
<tr>
<td>iPad 3</td>
<td>iOS 5.1</td>
<td>iOS 6.1</td>
</tr>
<tr>
<td>iPad 4</td>
<td>iOS 6.0</td>
<td>iOS 6.1</td>
</tr>
<tr>
<td>iPad mini</td>
<td>iOS 6.0</td>
<td>iOS 6.1</td>
</tr>
<tr>
<td>Apple TV 2nd generation</td>
<td>iOS 4.1 (Apple TV 4.0)</td>
<td>iOS 6.0 (Apple TV 5.1)</td>
</tr>
<tr>
<td>Apple TV 3rd generation</td>
<td>iOS 5.1 (Apple TV 5.0)</td>
<td>iOS 6.0 (Apple TV 5.1)</td>
</tr>
</tbody>
</table>
Study into the implications of Smartphone operating system security

Appendix B: Apple iOS Version History

The following table, table A2 details Apple iOS version history.

Table A2: Apple iOS version history

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Release date</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone OS 1.x</td>
<td>1.0</td>
<td>29 June 2007</td>
</tr>
<tr>
<td>iPhone OS 1.x</td>
<td>1.0.1</td>
<td>31 July 2007</td>
</tr>
<tr>
<td>iPhone OS 1.x</td>
<td>1.0.2</td>
<td>21 July 2007</td>
</tr>
<tr>
<td>iPhone OS 1.x</td>
<td>1.1</td>
<td>14 September 2007</td>
</tr>
<tr>
<td>iPhone OS 1.x</td>
<td>1.1.1</td>
<td>27 September 2007</td>
</tr>
<tr>
<td>iPhone OS 1.x</td>
<td>1.1.2</td>
<td>12 November 2007</td>
</tr>
<tr>
<td>iPhone OS 1.x</td>
<td>1.1.3</td>
<td>15 January 2008</td>
</tr>
<tr>
<td>iPhone OS 1.x</td>
<td>1.1.4</td>
<td>26 February 2008</td>
</tr>
<tr>
<td>iPhone OS 1.x</td>
<td>1.1.5</td>
<td>15 July 2008</td>
</tr>
<tr>
<td>iPhone OS 2.x</td>
<td>2.0</td>
<td>11 July 2008</td>
</tr>
<tr>
<td>iPhone OS 2.x</td>
<td>2.0.1</td>
<td>4 August 2008</td>
</tr>
<tr>
<td>iPhone OS 2.x</td>
<td>2.0.2</td>
<td>18 August 2008</td>
</tr>
<tr>
<td>iPhone OS 2.x</td>
<td>2.1</td>
<td>9 September 2008</td>
</tr>
<tr>
<td>iPhone OS 2.x</td>
<td>2.2</td>
<td>21 November 2008</td>
</tr>
<tr>
<td>iPhone OS 2.x</td>
<td>2.2.1</td>
<td>27 January 2009</td>
</tr>
<tr>
<td>iPhone OS 3.x</td>
<td>3.0</td>
<td>17 June 2009</td>
</tr>
<tr>
<td>iPhone OS 3.x</td>
<td>3.0.1</td>
<td>31 July 2009</td>
</tr>
<tr>
<td>iPhone OS 3.x</td>
<td>3.1</td>
<td>9 September 2009</td>
</tr>
<tr>
<td>iPhone OS 3.x</td>
<td>3.1.2</td>
<td>8 October 2009</td>
</tr>
<tr>
<td>iPhone OS 3.x</td>
<td>3.1.3</td>
<td>2 February 2010</td>
</tr>
<tr>
<td>iPhone OS 3.x</td>
<td>3.2</td>
<td>3 April 2010</td>
</tr>
<tr>
<td>iPhone OS 3.x</td>
<td>3.2.1</td>
<td>15 July 2010</td>
</tr>
<tr>
<td>iPhone OS 3.x</td>
<td>3.2.2</td>
<td>11 August 2010</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.0</td>
<td>21 June 2010</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.0.1</td>
<td>15 June 2010</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.0.2</td>
<td>11 August 2010</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.1</td>
<td>8 September 2010</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.2</td>
<td>November 2010</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.2.1</td>
<td>22 November 2010</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.2.5</td>
<td>7 February 2011</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.2.6</td>
<td>10 February 2011</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.2.7</td>
<td>14 April 2011</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.2.8</td>
<td>4 May 2011</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.2.9</td>
<td>15 July 2011</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.2.10</td>
<td>25 July 2011</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.3</td>
<td>9 March 2011</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.3.1</td>
<td>25 March 2011</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.3.2</td>
<td>14 April 2011</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.3.3</td>
<td>4 May 2011</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.3.4</td>
<td>15 July 2011</td>
</tr>
<tr>
<td>iOS 4.x</td>
<td>4.3.5</td>
<td>25 July 2011</td>
</tr>
</tbody>
</table>
Study into the implications of Smartphone operating system security

<table>
<thead>
<tr>
<th>iOS Version</th>
<th>Version</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS 5.x</td>
<td>5.0</td>
<td>12 October 2011</td>
</tr>
<tr>
<td>iOS 5.x</td>
<td>5.1</td>
<td>7 March 2012</td>
</tr>
<tr>
<td>iOS 5.x</td>
<td>5.1.1</td>
<td>7 May 2012</td>
</tr>
<tr>
<td>iOS 6.x</td>
<td>6.0</td>
<td>19 September 2012</td>
</tr>
<tr>
<td>iOS 6.x</td>
<td>6.0.1</td>
<td>1 November 2012</td>
</tr>
<tr>
<td>iOS 6.x</td>
<td>6.0.2</td>
<td>18 December 2012</td>
</tr>
<tr>
<td>iOS 6.x</td>
<td>6.1</td>
<td>28 January 2013</td>
</tr>
<tr>
<td>iOS 6.x</td>
<td>6.1.1</td>
<td>6 February 2013</td>
</tr>
<tr>
<td>iOS 6.x</td>
<td>6.1.2</td>
<td>19 February 2013</td>
</tr>
<tr>
<td>iOS 6.x</td>
<td>6.1.3</td>
<td>19 March 2013</td>
</tr>
</tbody>
</table>
Appendix C: Apple iOS Wireless Software Update Process

To update iOS software wirelessly the device owner currently follows these steps:

1. Plug the device into a power source.
2. Go to the Software Update option in Settings to allow iOS to automatically check for available updates (see A3 below).

Figure A3: Wireless Software Update option for iOS 5 and later device

3. If a software update is available then the device owner can choose the Download option to download the update.
4. Once the download has successfully completed, the software update needs to be installed. By choosing the Install option (see figure A4 below) the installation process is initiated and the software update is installed.

Figure A4: Wireless Software update installation option for iOS 5 and later device
Appendix D: Apple iOS iTunes Software Update Process

To update iOS software via Apple iTunes the device owner currently follows these steps:

1. It is recommended that the latest version of iTunes is used to manage a connected software update.
2. With the iOS device connected to the personal computer running iTunes, the device owner can check for updates. If updates are available they can download and install them. See figures A5 and A6 for details.

Figure A5: iTunes Software update “Check for Update” option for iOS devices

![iTunes Software update “Check for Update” option for iOS devices](source: Apple)

Figure A6: iTunes Software update “Download” option for iOS devices

![iTunes Software update “Download” option for iOS devices](source: Apple)
Appendix E: Google Android version history

The following table, **Table A7**, details Google Android version history.

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Release date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android 1.0</td>
<td>1.0</td>
<td>23 September 2008</td>
</tr>
<tr>
<td>Android 1.1</td>
<td>1.1</td>
<td>9 February 2009</td>
</tr>
<tr>
<td>Android 1.5 Cupcake</td>
<td>1.5</td>
<td>30 April 2009</td>
</tr>
<tr>
<td>Android 1.6 Donut</td>
<td>1.6</td>
<td>15 September 2009</td>
</tr>
<tr>
<td>Android 2 Eclair</td>
<td>2.0</td>
<td>26 October 2009</td>
</tr>
<tr>
<td>Android 2 Eclair</td>
<td>2.0.1</td>
<td>3 December 2009</td>
</tr>
<tr>
<td>Android 2 Eclair</td>
<td>2.1</td>
<td>12 January 2010</td>
</tr>
<tr>
<td>Android 2.2 Froyo</td>
<td>2.2</td>
<td>20 May 2010</td>
</tr>
<tr>
<td>Android 2.2 Froyo</td>
<td>2.2.1</td>
<td>18 January 2011</td>
</tr>
<tr>
<td>Android 2.2 Froyo</td>
<td>2.2.2</td>
<td>22 January 2011</td>
</tr>
<tr>
<td>Android 2.2 Froyo</td>
<td>2.2.3</td>
<td>21 November 2011</td>
</tr>
<tr>
<td>Android 2.3 Gingerbread</td>
<td>2.3</td>
<td>6 December 2010</td>
</tr>
<tr>
<td>Android 2.3 Gingerbread</td>
<td>2.3.1</td>
<td>December 2010</td>
</tr>
<tr>
<td>Android 2.3 Gingerbread</td>
<td>2.3.2</td>
<td>January 2011</td>
</tr>
<tr>
<td>Android 3.0 Honeycomb</td>
<td>3.0</td>
<td>22 February 2011</td>
</tr>
<tr>
<td>Android 3.1 Honeycomb</td>
<td>3.1</td>
<td>10 May 2011</td>
</tr>
<tr>
<td>Android 3.2 Honeycomb</td>
<td>3.2</td>
<td>15 July 2011</td>
</tr>
<tr>
<td>Android 3.2 Honeycomb</td>
<td>3.2.1</td>
<td>20 September 2011</td>
</tr>
<tr>
<td>Android 3.2 Honeycomb</td>
<td>3.2.2</td>
<td>30 August 2011</td>
</tr>
<tr>
<td>Android 3.2 Honeycomb</td>
<td>3.2.3</td>
<td>Unknown</td>
</tr>
<tr>
<td>Android 3.2 Honeycomb</td>
<td>3.2.4</td>
<td>December 2011</td>
</tr>
<tr>
<td>Android 3.2 Honeycomb</td>
<td>3.2.5</td>
<td>January 2012</td>
</tr>
<tr>
<td>Android 3.2 Honeycomb</td>
<td>3.2.6</td>
<td>February 2012</td>
</tr>
<tr>
<td>Android 4.0 Ice Cream Sandwich</td>
<td>4.0</td>
<td>19 October 2011</td>
</tr>
<tr>
<td>Android 4.0 Ice Cream Sandwich</td>
<td>4.0.1</td>
<td>21 October 2011</td>
</tr>
<tr>
<td>Android 4.0 Ice Cream Sandwich</td>
<td>4.0.2</td>
<td>28 November 2012</td>
</tr>
<tr>
<td>Android 4.0 Ice Cream Sandwich</td>
<td>4.0.3</td>
<td>16 December 2011</td>
</tr>
<tr>
<td>Android 4.0 Ice Cream Sandwich</td>
<td>4.0.4</td>
<td>29 March 2012</td>
</tr>
<tr>
<td>Android 4.1 Jelly Bean</td>
<td>4.1</td>
<td>9 July 2012</td>
</tr>
<tr>
<td>Android 4.1 Jelly Bean</td>
<td>4.1.1</td>
<td>23 July 2012</td>
</tr>
<tr>
<td>Android 4.1 Jelly Bean</td>
<td>4.1.2</td>
<td>9 October 2012</td>
</tr>
<tr>
<td>Android 4.1 Jelly Bean</td>
<td>4.2</td>
<td>13 November 2012</td>
</tr>
<tr>
<td>Android 4.1 Jelly Bean</td>
<td>4.2.1</td>
<td>27 November 2012</td>
</tr>
<tr>
<td>Android 4.1 Jelly Bean</td>
<td>4.2.2</td>
<td>11 February 2013</td>
</tr>
</tbody>
</table>
Appendix F: A guide to mobile operating systems

Types of mobile operating systems – mobile models

In the main, there are three main types of mobile operating system:

1. Manufacturer-built proprietary operating systems where the operating system developer (the owner) is also the hardware manufacturer. This includes:
   a. Apple iOS
   b. BlackBerry OS

2. Third-party proprietary operating systems where the operating system developer (the owner) will license its operating system, usually for a fee, to third-party hardware manufacturers (Original Equipment Manufacturers or OEMs). In this method, similar to Microsoft’s personal computer operating system (Windows) model, the devices will have a consistent appearance and behaviour. There is little scope for customisation of the operating system by the OEMs. This includes:
   a. Microsoft Windows Phone (Mobile)

3. Free and open source operating systems where the operating system developer (owner) will release the operating system via the open source license method. Open source operating systems are developed by a company, a group of companies or a community of developers. Customisation of the operating system is usually allowed to a certain degree (within the parameters of the license agreement). This includes:
   a. Google Android
   b. Symbian

ROM and Mobile Operating Systems

In the case of mobile devices, Read-Only Memory (ROM) refers to the internal storage of the device that contains the firmware/operating system. Modification of the firmware/operating system contained in ROM is usually only allowed under special circumstances and is protected.

These special circumstances include updating the firmware/operating system as part of the operating system software update and patching process.

Unauthorised changes to the firmware/operating system can happen and is called flashing, rooting or jailbreaking a device.

Sources of Smartphone operating systems

There are different types of firmware/operating system applicable to mobile devices. The type that a consumer may find in their Smartphone and other smart mobile devices depends on the operating system and the device that they are using. They include:

- **True Stock ROM/Firmware**: This is where you have the firmware/operating system in a default form. There is little or no modification and this usually refers to situations
where the operating system and the device are built by the same company, e.g. Apple, BlackBerry and Google-branded Android devices

- **MNO or Manufacturer branded Stock ROM/Firmware:** This type is when the Stock ROM/Firmware is enhanced by a MNO or a device manufacturer (OEM). Changes can be interface enhancements, custom User Interface (UI), modifications made to work in certain regions and on certain mobile networks and restrictions to limit the use of a device within a specific region or MNO. The majority of Android devices are considered to be branded Stock ROM.

- **Custom ROM/Firmware:** These are usually at the ‘unofficial’ end of the mobile industry where independent developers will take the basic ROM/Firmware and customise it. Custom ROMs are more common on the more open mobile operating systems, including Android.
Appendix G: Goode Intelligence research methodology and assumptions

Goode Intelligence (GI) aims to create research and analysis that is independent, unbiased, accurate, reliable and actionable. To help GI achieve these goals, a research and analysis methodology has been developed that uses a combination of industry best practice and tried and tested research and analysis techniques. It is complimented by the experience of the GI research and analysis team of developing products that are readable, intelligent and useable.

The GI research and analysis methodology uses a combination of quantitative and qualitative techniques in evaluation. The GI research and analysis methodology is being constantly monitored and fine-tuned to ensure that the information that is published is independent, unbiased, accurate, reliable and actionable.

Bound into this research methodology are Quality Assurance (QA) methods whereby all stages are reviewed, either internally or externally. Where it is internally reviewed, a Principle or Senior Analyst will ‘peer’ review each stage before it is accepted.

GI follows a three-stage methodology for research projects that is outlined in the graphic below.

---

Scope

The scope stage is managed by GI with strategic input from the client. The end result is a formal, signed-off, project scope. The scope is a working document that forms the framework for the project. Both the project sponsor and GI sign-off the project scope document. The scoping exercise has these major benefits:

1. To identify high-level project objectives, key deliverables, project resources and timeline.
Study into the implications of Smartphone operating system security

2. To enable GI to accurately deliver a project in accordance with the requirements of the project sponsor.

3. As a benchmark to enable the project sponsor to measure the success of the project.

Research

The second project stage is the research stage, carried out by GI with regular reporting back to the client.

GI’s research methodology is based on gathering information from two main sources; recorded and observable data:

Recorded Data

Available from a combination of GI’s internal analyst database and external published sources that include premium subscription, research tools.

Observable Data

Includes interviews with key personnel within organisations that GI has close relationships with and whom Ofcom has recommended.

Analysis and Report Generation

The analysis and report generation stage will be carried out by GI.

This stage will comprise of three main parts:

1. Analyse collected data
2. Produce the Research report
3. Deliver report and presentation to Ofcom with Q&A session

Validation and QA

Validation is a critical part of GI’s research and analysis methodology. Before each report is published GI validates the information using peer review to ensure that the analysis and hypothesis is accurate.

The major QA tools employed in this methodology are:

- Defined project scope that both Goode Intelligence and the client approve and sign off
- Project checkpoints at milestones where peer review is deployed
- Document proof-reading at draft and final stages
Study into the implications of Smartphone operating system security

- Regular project updates to the client including weekly status meetings
- Draft report review meeting with the client to receive feedback on draft report
- End of project meeting to measure using project scope to measure that Goode Intelligence has delivered the project in accordance to the client’s requirements
Appendix H: About Goode Intelligence

Goode Intelligence is the leading research, analysis and consultancy organisation for the mobile security industry; providing services to global technology and telecommunications organisations."

Founded in 2007 by Alan Goode and headquartered in London, Goode Intelligence helps technology providers, regulators, investors and IT purchasers make strategic business decisions based on quality research, insight and consulting.

Goode Intelligence works with a cross-section of clients, from global brands that are ranked on the FTSE/Fortune 100 to start-up technology companies.

For more information about our work and services please contact us via email – enquiry@goodeintelligence.com.