The cyber crime threat on mobile devices

Chris Mitchell
Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK
www.chrismitchell.net

Abstract

This paper is concerned with highlighting recent and emerging cyber crime threats to mobile devices. The main classes of threat are briefly reviewed, and the history of attacks against mobile systems is summarised. Two case studies of attacks against general-purpose systems not normally thought of as security-sensitive are given, and conclusions are drawn.

1 Introduction – mobile devices

A wide range of mobile devices are in use today, including (smart) phones, media players, tablets, and notebook PCs. These devices are typically network-connected for most of the time they are switched on. This poses a well-known, albeit not well-understood, threat from cyber criminals.

Apart from the 'obvious' mobile devices, a growing number of everyday objects are also 'always/often connected', including road vehicles of all kinds (cars, lorries, etc.), RFID tags embedded in all sorts of devices, chip-based payment cards, including proximity-based cards, electronic key fobs, and public transport vehicles. Of course, these are just the *mobile* devices – many everyday fixed objects are also rapidly becoming Internet connected, including 'smart' buildings, e.g. shops, restaurants, homes, and workplaces, and installations within buildings, such as domestic appliances and factory machinery.

Of course, traditional mobile devices (such as phones, PCs, etc.) have been the main focus of security and privacy concerns. Whilst there are very major issues for such systems, perhaps other devices pose an even greater threat. It may well be that the possibilities for crime (and countermeasures) involving such everyday devices have not been properly thought through, and this issue forms the main focus of this paper.

The remainder of this paper is structured as follows. The main cyber (and hence cyber crime) threats to mobile devices are reviewed. We then look at how these threats apply to some of the less well-studied classes of mobile device, and the news is not always good. One reason for problems in all categories of mobile devices and systems is that systems have evolved piecemeal, and there is no overall security architecture. As with all IT products, the pressure to release the latest innovation always takes precedence over the need for security. Moreover threats arise from 'accidental' functionality; systems are interconnected because we 'might as well', without thought about the possible consequences.

2 The cyber security landscape

2.1 Threats

Cyber threats to mobile devices can be divided into two main classes. **Communications-based** threats include access network impersonation, mobile device impersonation, and man-in-the-middle attacks (both active and passive). **System-based** threats include software vulnerabilities, side channel attacks, and social engineering attacks (including malicious applications).

The cyber criminal may have many different motives for performing an attack on a mobile device, including hardware theft, information theft, or simply denial of service or sabotage. It is difficult to enumerate all the ways a criminal might seek to gain from an attack; indeed, it is hard to determine where criminality ends and terrorism begins. As a result, it would seem prudent to consider all possible security issues when trying to address cyber crime.

The security measures we can deploy to address possible threats can be divided into two broad sets. In a network we can deploy authentication (of network to device, and device to network), and secure channel establishment. Within a system we can employ a range of techniques, including: secure software design (to reduce the need to patch vulnerabilities), attack surface reduction (to reduce the impact of vulnerabilities), secure hardware/firmware design (to make finding side channel attacks difficult), careful user interface design (to reduce the risk of user error), and user education regarding threats.

Unfortunately, systems designers and manufacturers do not always do a good job of deploying the necessary security measures. With respect to mobile network security, security measures have been applied only very patchily. The industry has often worked in the 'deploy first and then make secure later' mode. Additionally, 'quick and dirty' solutions have been deployed which have often proved inadequate. Certainly there are many well-known vulnerabilities in our mobile networking infrastructure which have yet to be fixed, often because of the huge cost of retrofitting security. In terms of system security, the picture is no better. The first mobile virus was reported back in 2004 [5], and more recently huge numbers of vulnerabilities have been reported in smart phone systems (see below).

2.2 Network security

Some currently deployed network access protocols offer very limited security. For example, authentication of the 'access network' to the device is sometimes non-existent, e.g. as in GSM and IEEE 802.11 Wi-Fi. Existing security measures aim at controlling access to the network to protect the investment of the network owners, rather than the serious threat to end nodes posed by unauthenticated access points.

The effects of such a lack of network authentication have been widely documented in print and on the Internet[1]. This situation has given rise to a series of public domain implementations of 'fake network' attacks on GSM and IEEE 802.11, as well as attacks arising from compromised access points, where the compromise might arise from software or hardware attack. There are a host of examples of fake network software, including AirJack[2] and airsnarf[3]. For example, Airsnarf is a rogue

[1] http://en.wikipedia.org/wiki/Snarfing
[2] http://sourceforge.net/projects/airjack/

wireless access point utility designed to demonstrate how a rogue access point can steal usernames and passwords from public wireless hotspots. A graphic description of how airsnarf could be used to compromise user security is provided on Kewney's blog[4].

Pair-wise device authentication can also be vulnerable; for example the original Bluetooth pairing scheme was rather weak[5]. In general, as a result of the lack of comprehensive and integrated security solutions for mobile connected devices, there is an ever-growing risk of widespread malware attacks, as devices become more 'smart' and flexible. This is all happening in an environment in which malware attacks on mobile devices continue to become more numerous and serious (see below).

Apart from poor security fundamentals, privacy is also a major issue. Device tracking is a particular problem. In any network protocol, addresses of some sort are exchanged between devices, and, at least at some level of the protocol hierarchy, these addresses need to be exchanged in cleartext. If the address of the mobile device is fixed, then this offers a simple way of tracking the location of that device, and by implication, its owner. Of course, work is ongoing to address this problem for a wide variety of protocols, including for mobile networks.

It is not only the protocols used in networks that have proved vulnerable. A range of attacks have been devised against the cryptographic algorithms that underpin these security protocols. For example, WEP (the first suite of algorithms for Wi-Fi) was quickly broken [4], and the replacement suite (WPA) has also been attacked [12] (although WPA2 appears to be robust). A wide range of attacks have been demonstrated against GSM cryptography [1]; this is not so surprising – after all, GSM is 25 years old. However, this is not all ancient history – a very recent announcement from Ruhr University Bochum shows that satellite phones are not immune from simple crypto attacks [3]. These attacks do not arise because of the lack of robust cryptographic technology – it is often about cost pressures trumping security requirements.

2.3 System security

System security problems with mobile devices have been known for some time. For example, the Register reported back in February 2007[6] that, according to McAfee, 3G malware attacks in mobile networks had reached a new high. Informa had reported[7] that 83% of mobile operators were hit by mobile device infections in 2006, and the number of reported security incidents in 2006 was more than five times as high as in 2005. Even five years ago, 200 strains of mobile malware had been discovered.

Since then the situation has got much worse, as more recent reports show. For example:

---

[3] http://airsnarf.shmoo.com/
[4] http://www.newswireless.net
[5] http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/
[6] http://www.theregister.co.uk/2007/02/12/mobile_malware/
[7] http://www.techshout.com/mobile-phones/2007/15/83-percent-of-global-mobile-operators-have-been-hit-by-mobile-device-viruses-reveals-mcafee-report/

- Bloomberg reported[8] in April 2011 that, according to Kaspersky, the 'Android mobile-phone platform faces soaring software attacks and has little control over ... applications. Applications loaded with malicious software are infiltrating the Google operating system at a faster rate than with personal computers at the same stage in development. [Kaspersky] identified 70 different types of malware in March, [an increase] from just two categories in September'.
- Wyatt, in 'The Lookout Blog', reported in May 2011[9] that 'multiple applications available in the official Android Market were found to contain malware that can compromise a significant amount of personal data. Likely created by the same developers who brought DroidDream to market back in March, 26 applications were found to be infected with a stripped down version of DroidDream [called] 'DroidDreamLight'. At this point we believe between 30,000 and 120,000 users have been affected by DroidDreamLight'.
- A Sophos report from November 2009[10] reports on a range of iPhone malware.

2.4 Is this as bad as it gets?

So far we have looked at the traditional notion of mobile systems. These are relatively closed systems, sometimes carefully designed from a security perspective. What's the worst that can happen in such a case? We would expect to see loss of hardware (possibly with a relatively small impact), and loss of user data; clearly such attacks are not good, but the overall impact on society is probably limited. Indeed, organisations can limit the damage by protecting their back-end servers.

However, there is a far more serious emerging threat scenario involving the much larger world of everyday devices with embedded IT functionality and connectivity. We now have always-connected mobile systems which are often thought of as not having major security requirements; they are typically designed without concern about, or knowledge of, security threats. However potentially very serious threats apply: valuable hardware is at risk, and there are even major safety implications.

3 The problem

It is reasonable to ask why we have these serious security problems. Of course the picture is complicated, but the following factors appear to play a major role.

- Perhaps most significantly, there is huge business pressure to market products first and worry about security and the risks of cyber crime second.
- Technology gets used in ways unanticipated by designers (as exemplified by the growth in SMS, and the use of the Internet Protocol in almost every kind of network), which means that initial threat analyses no longer hold.
- Retrofitting security is typically very difficult; indeed, it is sometimes impossible in practice.
- Available 'retrofit' security technology is not used (examples of such 'failed' technology abound).

[8] http://www.bloomberg.com/news/2011-04-21/google-s-android-system-faces-more-app-attacks-in-new-security-frontier-.html
[9] http://blog.mylookout.com/blog/2011/05/30/security-alert-droiddreamlight-new-malware-from-the-developers-of-droiddream/
[10] http://nakedsecurity.sophos.com/2009/11/23/lightning-strikes-iphone-malware-malicious/

- Improving security and privacy rarely has a big pay-off to the user (individual or corporate) – except perhaps **after the event**, i.e. after a major cyber crime event.

There are also conflicting pressures on suppliers of products. Two major security and privacy requirements are the need for *high robustness*, because of the criticality of IT, and the need for *privacy protection*, not least because of emerging legal frameworks and user demands. These requirements often conflict directly with business, technological and social forces, which are inevitably a lot more powerful than security and privacy requirements. Major economic, technological and social factors include increasing *complexity*, arising from inevitable technological drift and which directly threatens robustness, the increased use of third parties (*outsourcing*) which makes privacy and security assurance very hard to achieve, and the use of *intelligence* (sophisticated IT) everywhere, not least to improve flexibility which also directly threatens robustness.

4 Case studies

We briefly examine two case studies of major security issues which have been found in classes of system which are not normally thought of as security products.

4.1 Case study I – remote keyless entry (RKE) systems

Over the last half dozen years, Paar and his collaborators at the Ruhr University of Bochum have looked at attacks on a variety of real world hardware systems. One system they studied extensively is based on a cipher called KeeLoq. KeeLoq is widely used in remote keyless entry (RKE) systems, as employed for garage door openers and car door systems.

Their work [6], [11] reveals a variety of worrying facts. The KeeLoq cipher itself is not terribly strong. However, much more serious is the fact that the design of the key management system is such that all devices for a single system share the same key. Compromising this key (which can be achieved through the analysis of a single consumer device) breaks the entire system. This means that cloned keys could be simply and cheaply manufactured – the possibilities for large scale criminality are clear.

The RKE/KeeLoq attacks were completed a couple of years ago. More recently the Bochum team have successfully attacked a range of other real-world systems, including:

- FPGA security systems, designed to protect the confidentiality and integrity of software [10]; and
- personal wireless systems (including electronic passports, contactless payment cards and RFID systems) [7], [8].

The sad lesson from their work would appear to be that almost every real world system they have looked at contains very major vulnerabilities. Life may very well be sweet for the future cyber criminal.

4.2 Case study II – cars

In the second case study we consider recent work of a group of researchers at the University of California at San Diego and the University of Washington (two major papers on this work were published in 2010 and 2011, [2], [9]). They have performed a detailed study of cyber attacks on cars.

Their attacks have been made possible by the recent evolution of IT in cars. A modern car contains networks of communicating devices (computers/ECUs). These networks control most aspects of a car's operation, including its brakes (and anti-lock mechanisms), gears, throttle, and engine management. Functionality often also includes external connectivity, e.g. including mobile telephony.

This gives rise to a large and varied attack surface, including the following elements. In the US, the mandatory Onboard Diagnostics Unit (OBD-II) port provides direct access to the vehicle's internal network. User-upgradeable systems (e.g. audio players) are routinely connected to internal networks. Wireless devices (e.g. Bluetooth) are also connected to internal networks. Finally, and most seriously, remote telematics systems (for safety, diagnostics, and anti-theft) provide continuous connectivity via mobile phone networks.

The team performed experiments using two cars purchased specifically for purpose. They observed that the car's internal CAN bus has little security – any compromised component can impersonate any other component. There are many other security issues.

They demonstrated remote attacks on a car via a broad range of attack vectors, including: mechanic's tools, CD players, Bluetooth and mobile telephony. To perform a mobile phone based remote attack, they reverse-engineered the telematics protocol and used a buffer overflow vulnerability in the car gateway to take over the car telematics unit. This attacks works completely 'blind', i.e. without listening to responses from vehicle. Building on this attack they demonstrated the ability to compromise internal vehicle systems, and thereby systematically control the car's engine, brakes, lights, instruments, radio, and locks. The attack could be exploited for theft and surveillance.

Why are such serious attacks feasible (and arguably even easy)? Part of the problem is simply the way the supply chain works. Manufacturers integrate components provided by third party suppliers, and do not even have access to details of how the security functions in the components operate. That is, they cannot assess the level of security provided, even if they wanted to. This is compounded by the fact that users may add third party systems (e.g. audio players) with serious security ramifications, yet systems are low cost consumer items. Finally, suppliers are subject to serious cost pressures and do not even understand the nature of the cyber threats, since security is not their field of expertise.

5 The way forward

How can we start to address these issues? Perhaps the most serious problem is that we are adding communications functionality, and so serious cyber crime vulnerabilities, and internal inter-connectivity to systems without thinking through the security issues. Manufacturers and users are encountering major security (and cyber crime) problems they have no previous exposure to. There is a serious danger is that the sorry cycle of security problems with PCs will endlessly repeat itself with new classes of product.

It seems likely that the situation will get worse before it gets better. This is the usual pattern with new technology that allows ubiquitous connectivity. For example, first generation mobile phone networks had no security functionality, and so a major crime problem arose. Similarly, once the

Internet became widely used, PCs and servers were (and still are) subject to many attacks. This pattern is now repeating itself with smart phones, and, more worryingly, looks set to arise with many other consumer products.

Possibly even more worryingly, no-one in academia (as far as I know) has worked on understanding the security properties of public transport systems such as planes and trains (which are increasingly network connected). However, exactly the same issues as arise for cars may well apply in this domain. That is, it is far from clear whether these systems been designed to counter the kind of adversarial threat mode encountered on the Internet.

How can we start to address these problems? Well, this paper is intended to try to raise awareness of the threat. Producers of systems need to be aware of two main things: security is a problem that cannot be ignored, and getting security right is non-trivial. Perhaps most importantly, security is not just a question of randomly adding some cryptographic functionality.

The good news is that getting security right does not need to be expensive. For example:

- eliminating unnecessary functionality (reducing the attack surface) can solve many problems;
- following good software engineering practices can minimise the risk of buffer overflow vulnerabilities;
- robust crypto and sound security protocols are widely available and standardised.

What can consumers/end users do? Sadly, we must be prepared to pay just a little more for devices which make life harder for cyber criminals. We must put pressure on manufacturers to make more secure products, and on governments to legislate and regulate, where appropriate. At this point it is also tempting to demand that users be less easily duped. However, ultimately, users need to be protected; it seems unreasonable to expect users to become security experts.

Perhaps our best hope in the long run is that governments and regulatory bodies will act. We rely on regulation to ensure that cars, airliners and trains are safe. These regulators need to take on board the new mobile threat – this is a very serious issue! However, a closed 'conformance mentality' by manufacturers is not always a good thing, and standards alone will not solve all the problems. Anecdotal evidence suggests that FIPS 140 (a US standard for Hardware Security Modules (HSMs)) has had a limited effect on overall HSM security. The focus has been on compliance (and addressing issues covered by the standard) possibly at the expense of worrying about security in general. Perhaps FIPS 140 does not focus on the most important issues, but instead on those easiest to standardise.

6 Concluding remarks

There are ways in which disasters can be avoided. However, there do not seem to be any urgent general efforts to fix the problems, although individual manufacturers may be taking significant steps. Certainly, in the past, manufacturers and network operators have been left to clear up the mess they have created. This may be fair, but what happens in the mean time to the victims of cyber crime? Perhaps more general action is required, e.g. from government and regulators?

It is clear that making connected systems secure is non-trivial. It requires specialist expertise and a long-term commitment to adopting state of the art product development practices. However, the technology already exists. What is required is a willingness to address the problem, and also to invest in the expertise required to fix problems before they arise.

References

[1] E. Barkan, E. Biham, and N. Keller, 'Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication'. *Journal of Cryptology* **21(3)** (2008) 392-429.

[2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, 'Comprehensive Experimental Analyses of Automotive Attack Surfaces'. In: D. Wagner (ed.), *Proceedings of USENIX Security 2011*, USENIX (2011).

[3] B. Driessen, 'Eavesdropping on satellite telecommunication systems'. Draft of February 8th 2012.

[4] S. R. Fluhrer, I. Mantin, and A. Shamir, 'Weaknesses in the Key Scheduling Algorithm of RC4'. In: *Proc. Selected Areas in Cryptography 2001*, Springer (2001) pp.1-24.

[5] M. Hypponen, 'Malware goes mobile'. *Scientific American* (November 2006) 70-77.

[6] M. Kasper, T. Kasper, A. Moradi, and C. Paar, 'Breaking KeeLoq in a Flash: On Extracting Keys at Lightning Speed'. In: *Proc. AFRICACRYPT 2009*, Springer (2009) pp.403-420.

[7] T. Kasper, D. Oswald, and C. Paar, 'Wireless security threats: Eavesdropping and detecting of active RFIDs and remote controls in the wild'. In: *Proc. 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2011)*.

[8] T. Kasper, D. Oswald, and C. Paar, 'Security of wireless embedded devices in the real world'. In: N. Pohlmann, H. Reimer and W. Schneider (eds.), *Securing electronic busibness processes*, Vieweg (2011), pp.1-16.

[9] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, 'Experimental Security Analysis of a Modern Automobile'. In: *Proc. IEEE Symposium on Security and Privacy 2010*, IEEE (2010) pp.447-462.

[10] A. Moradi, A. Barenghi, T. Kasper, and C. Paar, 'On the vulnerability of FPGA bitstream encryption against power analysis attacks: extracting keys from xilinx Virtex-II FPGAs'. In: *ACM Conference on Computer and Communications Security 2011*, ACM (2011) pp.111-124.

[11] C. Paar, T. Eisenbarth, M. Kasper, T. Kasper, A. Moradi, 'KeeLoq and Side-Channel Analysis – Evolution of an Attack'. In *Proc. FDTC 2009*, IEEE (2009) pp.65-69.

[12] E. Tews and M. Beck, 'Practical attacks against WEP and WPA'. In: *Proc. ACM WISEC 2009*, ACM (2009) pp.79-86.