A Private Mode for Mobile Users

John Baluch
College of Electrical Engineering, The University of Akron
jbb30@zips.uakron.edu

Professor Stephen Wicker
School of Electrical and Computer Engineering, Cornell University

July 30, 2010

Abstract

Privacy concerns about mobile devices have become an increasingly important issue ever since the mobile platform has become a source for political, economic and social expression [4]. It is a surveillance technology [4] through the use of phone calls, text messages, applications and web use. This paper introduces the differences between the content and context of telephony and the legislature that defines them for cellular devices. The social impacts of such surveillance are then discussed to show that users can be manipulated to a desired end, and how this impacts political behavior. Previous research shows that a Private Overlay can be used to give mobile users control over their personal information by using a Public Key Authority. It concludes with a new method for implementing a Private Overlay, without the previous hurdles.

1 Introduction

Cellular devices have become an every-day phenomena for most people. Communication through conversation, text messaging and email have penetrated daily life and has become an important part of society. The content and the context of digital telephony should be understood to best appreciate the privacy implications that are current with cell phones. Then, a discussion to show the cellular platform in light of a surveillance technology will be given to establish the need of a private overlay.

2 Content versus Context

Legislature on message content was first addressed in 1928 by Olmstead v. United States. The court determined that wiretap was not search and seizure, since nothing was 'searched' or 'seized', but heard. The decision was reversed in 1967 when a man had been wiretapped during the use of a pay phone (Katz v. United States). The Supreme Court ruled that tapping phone calls from a booth required a warrant, and that the Fourth Amendment "protects people, not places". [4]

The distinction between content and context should not be confused, as context has not had such luck in recieving protection under law. The best way to understand them is in terms of postal mail. The message inside of an envelope is considered the content, i.e. what the writter wishes to convey. Information written on the envelope – sender and reciever addresses, are considered the context.

In 1976 a man was convicted for bootlegging (United States v. Miller). "Investigators obtained, without a warrant, copies of Mr. Miller's deposit slips and checks" [4]. Mr. Miller appealed, arguing that a warrant should have been obtained before his bank records were taken. The court disagreed, stating that there was no "expectation of privacy... since the checks are not confidential commuications" (Justice Lewis Powell). The information was given up freely to the bank and shared amongst its employees in a regular manor. [4]

2.1 Passive/Active Surveillance

2.1.1 Passive

Passive surveillance is a multidimensional problem that "has its impact through the cellular user community's awareness for the potential of surveillance"[4]. It affects many aspects of the cellular platform, but one will be focused on more specifically – the hindering of political speech. The mobile device has become an increasingly important channel for expressing political opinion. For example, in 2004 the cell phone organized mass action against political corruption in Ukraine, known as the "Orange Revolution". [4]

In Kenya, 2008, reports that the Kenyan presidential election was rigged by current president Mwai Kibaki quickly sparked a texting campaign. The texting prompted demonstrations that quickly turned to racial hatred, but was calmed by authorities. The cellular service providers "gave the Kenyan government a list of some seventeen hundred individuals who had allegedly used texting to promote mob violence"[4].

The previous example brings out an important thought – that users may know that they are always being watched, but never know when. In *Discipline and Punish*, Michel Foucault discusses the effects of constant surveillance. Those who are watched have an instinctive discipline within them and become docile. Applied to the revolt in Kenya, if another rigged election were to occur, then many people may not feel safe enough to express their opinion.

2.1.2 Active

Subscriber information is used to sort individuals into categories by the service provider and by third party companies. This profiling is done for the purpose of manipulating information flow in a way that guides users to make a desired choice. The technique is called "framing" and "is so important to decision making that individuals have been shown to come to differing conclusions depending on how the relevant information has been presented" [4].

Advertising uses the same concept, placing people within a conceptual framework and using personal information to fine tune the frame to draw them to a specific product. This ability is amplified when marketers can see customer response, as it is with the cellular platform. Although many may be fine with targeted advertising, arguing that they are pleased with their decisions, the issue lies with the limited selection of choices – that a users choices has been pre-selected and the ability to explore has been limited.[4]

3 Mobile Private Mode

Cellular devices should provide users with an optional mode to which personal data can be controlled. By establishing a private overlay, this information can be kept out of the hands of third parties and can insure the user that they are not under constant surveillance. Such an overlay should be:

Simple enough that any non-technnical user could control.

Sohpisticated so that adversaries could not tamper, clone and illegally distribute.

Anonymous to ensure the users privacy.

3.1 Previous Work

The first concept of a private overlay was provided in a paper written by Professors Stephen Wicker of Cornell University [4]. His approach (in brief) implements a private mode by means of a *Trusted Platform Module* (TPM), a physical chip that acts as a cryptographic vault. In addition, a *Public Key Infrastructire and Certification Authority* (PKI) would be required to distribute a public encryption key and a private decryption key. The mode suggested works on the basis that only the equipment needs to be located and not the named subscriber.

It is assumed that the user already posses a mobile device which has the capabilities to execute a private mode. The network authorizes subscribers to use the mode by sending out an identical certification message to all users on a regular basis, which is encrypted using that subscriber's public encryption key.

If the private mode is activated, the device generates a *Random Equipment Tag* (RET) and combines it with the certification message to create a *Privacy Enabling Registration* (PEC). The PEC is sent to the service provider to prove that the request is from a valid user (i.e. a paying customer).

The purpose of the RET is to separate the user from the mobile phone. It acts as a device tag which replaces the phone number and is known only to the subscriber and the network, however the tag is anonymous to the network.

3.2 Approach

The previous approach used a physical piece of hardware for which a private overlay could operate on. It required that users interested in a private mode acquire a device that can operate within the overlay, whether through purchase of a new phone with a TPM, or to have it installed. It has been assumed that the chip does not compromise any mobile devices of their size or their structure, however in the event that a device manufacturer has no incentive to implement a TPM in every device, or it is not feasable in some models, then a software version may be more suitable.

The *Trusted Computing Group* (TCG) approved a means more suitable for mobile devices, dubbed the *Mobile Trusted Module* (MTM), an offspring of the TPM. The advantage of the MTM is that it can be implemented via a software version with similar, and very different, security measures of a physical TPM.

A user may purchase the rights to use a private mode through a port for which the service provider administers, such as an online application store or an outlet. Once purchased, the MTM is downloaded and installed just as a system update would. During setup, a PKI is established and a Random Product Key is generated and stored with the MTM. The product key is never associated with the account, but can be validated by the network.

Upon first-time activation, the network requests a Remote Attestation of the device to ensure device and code integrity. When prompted, the MTM makes an image of the hardware and software present and sends it to the network to prove that the device has not been tampered with.

If the device passes inspection, the service provider asks for a *Privacy Enabling Combination* (PEC), which consists of the product key and a *Random Equipment Tag* (RET), and is encrypted using the public encryption key. The PEC acts as a unique combination which cannot be traced back to the user, but proves that the sender is a valid user. The RET is a random number which identifies only the device and is used as if it were a phone number. There is never any connection between the RET and the actual phone numebr or account, but if the user wanted to be reached, the RET would need to be given to other individuals by the user.

3.3 Protection

The architecture that has been laid out in the current approach has been designed to make cloning, mass-distribution, and theft too difficult for adversaries to deem beneficial. Indeed, there are many ways in which malicious users may exploit the systems weaknesses and thus this section does not claim to be an exhaustive list of attacks.

3.3.1 Signal Interception

There are two opportunities for an attacker to steal information from a transmitted signal: during download (if applicable), and when the PEC is sent to the utility.

Assuming that the product is downloaded and not bought within a physical store, the information may be intercepted and altered before entering the mobile phone. At this point, the product key may be extracted and duplicated for multiple devices. Also, the MTM may have its settings and features changed or disabled.

However, since every device must generate its own RET, another device's RET will not register correctly with the duplicated product key, and will

thus be denied service. If an MTM's RET generator is disabled, or a valid PEC is implemented into another phone's memory, then the private mode could be duplicated. Luckily, every session requires a remote attestation with the service provider, which will catch any changes that have been made to the MTM code.

3.3.2 Replicated Memory

One of the largest issues with software is that it can be copied, changed, and illegally distributed. Such things could be done to the private overlay, application and all of its keys and codes to another, identitcal device. This in turn would allow a consecutive device to use the same private mode.

However, many users would have the same PEC and thus the same RET. If multiple devices have the same RET and are running simultaneously, then they will also be registered in multiple locations and can be detected by the service provider. Since RETs also act as a private phone number, every device using a replicated overlay would also recieve the same calls.

3.3.3 Stolen Device

With phones getting smaller by the year, it is common that they become lost or stolen. In the hands of the wrong user, private information and services may be easily accessed, especially the private mode since the device is separated from the user identity. The use of a *Personal Identification Number* (PIN) may be created by the subscriber, stored under the RTS, and used upon accessing the application. If the PIN is known only by the owner, then an antagonist cannot easily use such a mode.

4 MTM: How it works

Mobile Trusted Module is a new security element that has its origins from the TPM (both are newly approved TCG applications), but differs significatly in a few ways. MTM can be introduced as a functionality of a device with several instances running at once. This allows manufacturers to deploy it as if it were an add-on to other security measures.
A funcional version of MTM is possible because of the concept of secure boot. Upon powering the device, the boot sequence is measured, *including* the MTM. If the sequence enters a non-approved state, the sequence terminates and the boot fails.

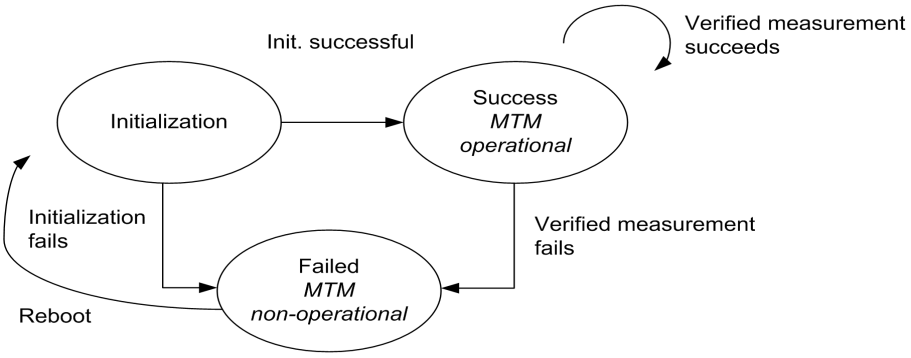

Figure 1: Secure boot operation [1]

Secure boot must pass through two discrete states - the *Engine Resst* and *Engine Root-of-Trust Initialization* before launching the MTM. The first ensures that nothing is running prior to the MTM first setting up. The second produces preconditions that are defined by "Roots of Trust" [1] which define the context that the MTM is set up. A *Root of Trust for Enforcement* (RTE) states platform-specific mechanisms which must be present to ensure the integrity of the MTM and the code which it runs. For a more detailed explanation on how the Mobile Trusted Module works, see reference [1].

5 Future Work

This research emcompasses only one way in which a private overlay may be implemented. Future researchers should implement a virtual MTM and its respective privacy applications onto a mobile phone. A way in which the MTM could be installed as an update in the device without returning it to the manufacturer should be a goal. The system's weaknesses should also be exploited to test the effectivness of its security measures, and whether they could be improved upon.

6 Acknowledgements

We gratefuly thank Professor Stephen Wicker for his support, and Jesus Noland, Nathan Karst, Radamẽs Mererro and DaNae Grubbs for their contributions. This research is on behalf of the Team for Research in Ubiquitous

Secure Technologies (TRUST) and funded by the NSF.

7 Biography

John Baluch will be a Junior Electrical Engineer at the University of Akron. He works on obtaining his certificate in Project Management outside of school in order to give himself a better understanding of how engineering and business work together in industry, and their limitations. He is a member of NSPE, OSPE and of the Akron local chapter of IEEE. Upon graduation, John plans to adventure in an engineering career to gain valuble experiences and has hopes to later attend graduate school.

References

[1] Ekberg, Jan-Erik, and Markku Kylänpää. *Mobile Trusted Module (MTM) - an introduction.* Tech. no. NRC-TR-2007-015. Nokia Research Center, 14 Nov. 2007. Web. 30 June 2010.

[2] Barkuus, Louise, and Anind Dey. *Location-Based Services for Mobile Telephony: a Study of Users Privacy Concerns.* Tech. no. IRB-TR-03-024. Intel Research Berkely, July 2003. Web. 30 June 2010.

[3] Schmidt, Andreas U., Nicolai Kuntze, and Michael Kasper. *On the Deployment of Mobile Trusted Modules.* Tech. Fraunhofer Institute for Secure Information Technology SIT. Web. 25 June 2010.

[4] S. B. Wicker, Surveillance Architectures: Digital Telephony and the Question of Privacy, Communications of the ACM, to appear.

[5] Pfitzmann, Andreas, Birgit Pfitzmann, Matthias Schunter, and Michael Waidner. *Trusting Mobile User Devices and Security Modules.* Publication no. 0018-9162/97. IEEE, 1997. IEEE Xplore. IEEE. Web.

[6] S. B. Wicker and D. E. Schrader, Privacy-Aware Design Principles For Information Networks Proceedings of the IEEE, to appear.

[7] Ghosh, Anup K., and Tara M. Swaminatha. *SOFTWARE SECURITY AND PRIVACY RISKS IN MOBILE E-COMMERCE.* Publication. 2nd ed. Vol. 44. ACM, 2001. Print. Communications of the ACM.

[8] Palen, Leysia, Marilyn Salzman, and Ed Youngs. *Going Wireless: Behavior & Practice of New Mobile Phone Users.* Publication no. 1-58113-222-0/00/0012. ACM, 26 Dec. 2000. Web. 25 June 2010.

[9] Trusted Computing Group (TCG). *TCG Mobile Trusted Module Specification.* Rep. TCG, 26 June 2008. Web. 30 June 2010.