SecureMyDroid: Enforcing Security in the Mobile Devices Lifecycle

Alessandro Distefano* Antonio Grillo* Alessandro Lentini*

Giuseppe F. Italiano*

ABSTRACT

Due to the extensive growth and diffusion of mobile devices (e.g., Smartphone, PDAs, mobile phones, etc.), and to their powerful capabilities, many users are massively using mobile devices both for personal and for work-related (corporate) activities. This poses serious threats to the security of such devices. In this paper, we propose a novel approach, based on the definition of a secure lifecycle for mobile devices, in order to extend corporate security policies to such devices. We focus on a new perspective that allows us to apply strong security policies and services enforcement to mobile devices. The approach proposed leverages on a customized release of the mobile device Operating System (OS). In particular, we present a prototype (called SecureMyDroid) of a secure mobile device based on a customized release of the Google Android operating system. One of the strong features of this prototype lies in the capability of fully customizing the operating environment of mobile devices. This prevents most of the tampering that is still practicable for devices that have been personalized through the installation of customized applications such as antimalware, antivirus, etc.

Categories and Subject Descriptors

D.2.9 [**Software Engineering**]: Management - *Lifecycle.*
D.2.10 [**Software Engineering**]: Design -*Methodologies.*
K.6.1 [**Management of Computing and Information Systems**] Project and People Management- *Lifecycle, Strategic information systems planning, Systems analysis and design.*
K.6.5 [**Management of Computing and Information Systems**] Security and Protection (D.4.6) - *Invasive software (e.g., viruses, worms, Trojan horses).*

General Terms

Management, Design, Security.

Keywords

Mobile device, lifecycle management, customized mobile operating system, Android OS.

1. INTRODUCTION

The corporate usage of handheld devices, such as mobile devices, provides competitive advantages for both mobile businesses and individual users [1], and it has been rapidly growing in recent years due to wide diffusion of mobile devices. As the storage capability of mobile devices spans between internal memories, removable memories (e.g., Secure Digital, Multimedia) and SIM cards, the overall amount of sensitive personal and corporate information that can be stored in those devices can be relevant. Furthermore, some storage volumes (e.g., removable memory cards) are intrinsically less secure than other volumes (e.g., SIM cards). Hence many companies, when planning to equip their personnel with mobile devices, have to face the typical new threats related to such devices. Unfortunately, when compared to personal computers, mobile devices are lacking a number of security features (e.g., effective anti-malware solutions, intrusion detection systems), which can be fundamental in order to protect corporate and personal data as well. Furthermore, the reduced capabilities of such kind of devices impose several constraints that must be fulfilled in order to provide effective and suitable security solutions. For instance, the reduced computing capabilities of mobile devices severely limit the adoption of proactive anti-malware solutions [2] such as those based on dynamic analysis [3]. Another issue is related to the update process of mobile security solutions, which depends heavily on the availability of low-cost network connections: this may lead to a large portion of mobile anti-malware solutions being outdated and so quite ineffective against new threats. Finally, each mobile device is typically bound to its owner/user. Due to this strong bind, and to the role that mobile devices play in the current daily life, mobile devices store a great amount of personal information related to their owners/users. At the same time, it is worth noticing that mobile devices are prone to loss or theft because of their inherent nature; this results in a high potential risk for both personal and corporate data loss and theft [4].

In this paper, we focus on the new perspectives related to the security policies and services enforcement for mobile devices. In particular, we propose a novel methodological approach to protect the lifecycle of mobile devices aiming at the secure management of such devices either directly by the user or by the organization. In order to assess the feasibility and impact of our approach in a real scenario, we customized a mobile device with several security features respecting the goal of the proposed lifecycle. In particular, we realized a prototype, which we call

* Department of Computer Science, Systems and Production, University of Rome " Tor Vergata", Rome, Italy.
{distefano,grillo,lentini,italiano}@disp.uniroma2.it

SecureMyDroid, based on our own customization of a Google Android OS version and tested it on actual mobile devices.
The remainder of the paper is organized as follows. In Section 2, we review some issues related to the state of the art in mobile devices security and in particular related to insider threats. In Section 3, we introduce our approach to secure the lifecycle of mobile devices. Finally, in Section 4 we describe SecureMyDroid, our prototype based on a customized release of the Android operating system.

2. STATE OF THE ART

This section briefly introduces the current limitations in security for mobile devices. Many threats affect the security of corporate data and personal information stored on mobile devices. Currently, individuals and organizations concerned with the security risks and threats coming outside of their mobile devices (e.g., device control [5]) can use some kinds of add-on security tools or mechanisms (e.g., anti-malware solutions). The detailed description of the current solutions that are available on the market is beyond the objectives of this work. However, this type of solutions presents several major disadvantages. Among them, we cite the following:

- Often they focus just on some aspects (e.g., anti-malware solutions) among the entire set of problems.
- The current solutions have several problems related to the management and update processes that are often left to the responsibility of the final users of the device.
- They are often common applications that must be installed in the mobile devices; such kind of solutions can be quite easily circumvented.
- Often, the proposed solutions do not address the threats and risks that come from the inside of the organization (e.g., from internal users).

Due to some inherent limitations of current solutions, we propose a secure lifecycle for mobile devices which exploits secure operating systems. We remark that our approach can be combined with existing security tools in order to support and provide full and effective security services that rely on secure mobile devices and secure networks as well.
Throughout the years, security specialists have been focusing their efforts on protecting systems from outside threats (e.g., viruses, worms, hacker attacks, etc.). Unfortunately, most often vulnerabilities generated by insider threats are equally dangerous, challenging and hard to embank. For example, the CSI Computer Crime and Security Survey 2009 reports that 15% of the major security breaches are caused by insider attacks, while the Association of Certified Fraud Examiners (ACFE) establishes that the losses due to insider threats are about the 6% of the annual revenue of an organization.
Like other threats, insider threats can be related to financial risks and to data leakage. Both refer to threats and risks related to corporate assets; however the former refers to financial goods, while the latter refers to valuable information. For the scope of this work, data leakage appears to be the most interesting because of the strong relationship between mobile devices and the personal data stored in them. According to the CSI Security Survey the major risk for a corporate is due to data leakage (also referred to as data loss or data theft). Although data leakage is always a danger, often an outsider who gains such data has a relatively low perception of the value of the acquired information. On the other side, if data are stolen by an insider, the knowledge of the information and the related potential scope of the damage are much larger. The main challenges in defending an organization from insider attacks, especially in a mobile environment, are the authorization and the access control to the corporate data by privileged users.

The ideas presented in this work try to overcome the limitations in defending mobile devices from outside threats and at the same time suggests a new approach for facing effectively inside threats. Some solutions that equip the mobile device as a tool to support the business exist (e.g. iPhone [6], BlackBerry [7]). Many features implemented in our solution are similar to those already available in Apple and RIM mobile operating system. The possibility to join well known features (e.g. remote wiping) with features that are tailored on a specific business represents the main strength of SecureMyDroid.

3. MOBILE DEVICESLIFECYCLE MANAGEMENT

Generally, a product lifecycle management (PLM) [7] is a comprehensive information system that coordinates all aspects of a product from its initial design to its final disposal. PLM is well defined for a wide range of products, processes and services but its standardization in many of the security processes, and in particular in processes that involve the use of mobile devices, appears to be still missing. In particular, a private or business organization cannot take part in the whole lifecycle management of a mobile device; the lifecycle begins with an OEM (Original Equipment Manufacturer) purchase and continues until its final disposal. In this work we propose an approach for managing the mobile devices lifecycle, ranging from its purchase to its disposal. The mobile device secure lifecycle management proposed is divided into five phases:

1. Purchase Phase;
2. Set-Up Phase;
3. Usage Phase;
4. Shut-Down Phase;
5. Disposal Phase.

We assume that, in the more general setting, those phases are organized as illustrated in Figure 1.

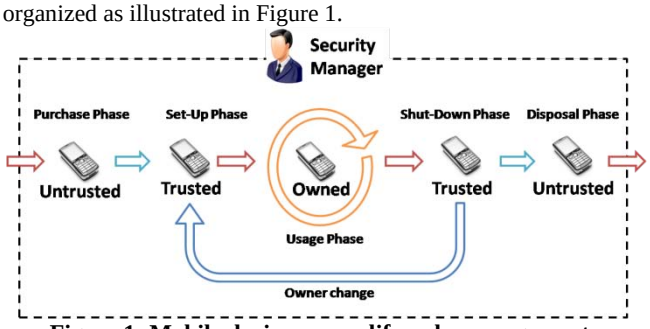

Figure 1: Mobile device secure lifecycle management.

During its lifecycle, a mobile device can be in one of three different states: *Untrusted*, *Trusted*, and *Owned*.
When the device is in the Untrusted state, neither the organization nor anyone of its employees can be considered responsible for that device. When the device is marked as Untrusted, no sensitive data must be stored on it and the device must not be connected to corporate networks. On the other side, when the device is in the Trusted state, only the organization is responsible for that device; in this state the device can store sensitive corporate data (e.g., corporate address books, corporate network profiles). While the device is in the Trusted State, no personal data must be stored in

its memories. The most complex state is the Owned state; in this state the mobile device is granted to a corporate employee, which is held responsible for that device. An Owned device can typically store both corporate and personal information; hence, any Owned device represents the preferred target for attacks to the security and privacy of the corporate assets.

3.1 Purchase Phase

During the "Purchase Phase", the organization receives a new mobile device from its supplier, and the mobile device must change its state from Untrusted to Trusted. The access to the corporate network and data is granted only for mobile devices in a Trusted State. In the simplest case, the hard reset of the device can be considered as a good starting point for this phase. The hard reset is an operation available on many mobile devices that allows restoring the device factory state; this operation erases all the installed applications and all the user data as well. Since the effectiveness of this procedure does not depend on the organization capabilities, its actual effects should be verified by manual or automatic procedures.

3.2 Set-Up Phase

The Set-Up Phase must be executed when the mobile device is supplied to a particular employee in the organization. The mobile device must be configured according to the level of the privileges of the new owner of the mobile device. The mobile device will be equipped with software applications approved or certified by the organization. It is important to remark that this is the only phase where applications are installed, in order to keep under strict control the mobile device and to try to limit possible security breaches.

3.3 Usage Phase

The central phase is the Usage Phase; this phase includes a series of supervision activities carried out while the employee is using his/her mobile device. A set of activities must be repeated, at fixed time intervals, with two main purposes: ensuring that the device has not been corrupted by any external attack and ensuring that the device has been used by its owner for the intended purposes. If the mobile device has been found to be corrupted, it must be placed in a Untrusted state and all the procedures for the recovery of damaged data and the policies for the protection from potential damages that can cause the theft of data must be implemented. The activities related to the Usage phase can be grouped into the following categories:

- **Asset Management Activities:** all the activities that focus on preserving the information asset of the organization. The periodic backup of the device memory or the integrity check of the stored information can facilitate the restore procedure even if the mobile device is lost or damaged. Sharing the public part of the updated mobile device information's within the organization (e.g., new corporate client phone or web site address) helps the information process cycle among employees;
- **Configuration Management Activities:** refer to all the activities aiming at verifying that no undesired/unwanted changes to the device configuration are applied. Examples of sensitive settings can be the call transfer function, the number of the SMS service center, the number of voicemail, etc…;
- **Application Management Activities:** this type of controls aims at monitoring that the installed applications on the mobile device cannot produce in any way threats to the corporate security and privacy. We remark that threats such as key-loggers, Trojans, worms, spywares and many other malicious software applications are already available for mobile platforms;
- **Security Management Activities:** refer to all the activities aiming at preserving the security configuration of the mobile device. Setting the device as visible to a Bluetooth discovery or increasing the priority of a specific Wi-Fi network can result in security weaknesses for a mobile device;
- **Remote Support Activities:** in order to protect the mobile device a set of functions can be remotely invoked on it. The simplest example scenario is remote wiping: when a mobile device has been lost or stolen, the organization can activate the automatic deletion of data on the mobile device; in a more complex infrastructure we can conceive the capability to grant and to remove the privileges for the access to several organization resources.

The Usage phase is complex and crucial for the entire lifecycle. In such a phase, which heavily depends on the effective device usage, it is fundamental to provide support to both ordinary (e.g., the need to install new applications) and extraordinary needs (e.g., the periodic security checks, the solution of specific issues).

3.4 Shut-Down Phase

The Shut-Down phase must be executed when the employee returns the mobile device to the organization. From the corporate perspective, in this phase it is necessary to retrieve all the useful data produced by the employee and to proceed with the transfer of responsibility on the mobile device to the company policies. From the perspective of the employee, it is necessary to provide mechanisms to recover and erase the private data stored on the phone. At the end of the data disposal operations, the device must be reset and passed from the Owned State to the Trusted State. Since the device could change its owner, before starting again the Set-Up and configuration phase, it is necessary to verify that the Shut-Down Phase was effective. Once this phase is completed, the previous owner can no longer be accounted as responsible for the device.

3.5 Disposal Phase

The last phase is the Disposal Phase; the device must be disposed of by the organization. If the mobile device is sold, it must be completely erased by either a logical or a physical point of view. If the device does not have any residual economic value, if possible, it should be physically destroyed. In both cases, the memories of all the dismissed devices must be properly reset.

4. SECUREMYDROID

In the last years, with the introduction of Open Source Mobile OSs (e.g., Android), a new perspective for mobile device customization arose: the capability to build OS images customized for specific purposes. Currently, Android is the most diffused Open Source Mobile OS with about the 6% of the market and its share it is expected to grow until 15% in 2012. Furthermore, it is expected that Netbooks will be equipped with Android as well; this can make the integration between the mobile device and the laptop corporate fleets easier for the organization. Following the guidelines illustrated by the device lifecycle presented in Section 3, we developed a prototype of the Android OS, called SecureMyDroid, specifically customized to improve security; these customized OS versions can equip the mobile device with

new and advanced functionalities (e.g., improved security mechanisms), and adapt the default capabilities (e.g., disabling the support to applications installation). Our proposal preserves the Android Security and Permission model and strengthens it against inside threats. SecureMyDroid aims at supporting the critical security control of the company such as the data loss prevention, malware defense, limitation and control of network and services access, boundary defense and so on. This approach could ensure strong guarantees in terms of trust and reliability required by a company that needs to deal with secret and sensitive data.

4.1 Main features of SecureMyDroid

SecureMyDroid is a prototype developed on a customized version of Google Android OS. It is designed to support and realize practically the secure lifecycle management of the mobile devices as proposed in this work. The basic step of this activity is to obtain, modify and compile the source code of the mobile operating system, so that the new OS image file can be deployed on the mobile device. Starting from this non-trivial result we have realized different features for improving the security management of the entire lifecycle. We sketch next some of these features.

First of all, we patched the source code of the installation manager in order to inhibit the capability to install new applications on the device. This security feature ensures both that the user cannot install new personal applications (e.g., games, entertainment) on its business device and that the device cannot be compromised by the installation of mobile malwares (e.g., virus, worms, Trojans). SecureMyDroid offers the possibility to disable the use of memory cards (e.g., secure digital cards). This countermeasure can prevent from nimbly copying or moving sensitive business data out of the device.

We strengthened the relationship between the mobile device and a specific SIM card. Whenever the device is switched on, the association with the SIM is checked; if the device recognizes that the inserted SIM does not match the expected one a dialog prompting for a special PIN is shown. The device remains inactive until the user provides the correct PIN. After a given number of unsuccessful attempts, the device can be permanently blocked.

We placed into the source code of most critical function of the mobile device (e.g., making a call, sending an SMS/MMS/e-mail, connecting to a Wi-Fi network, syncing with a computer) an event logger call. When a stated time slot elapses the collected log messages are transferred to a remote server using HTTPS connections.

SecureMyDroid can notify all the actions to an organization remote server performed by the user on the device through an HTTPS connection. At the same time, the organization can explicitly query the device through simple text messages in order to obtain specifically information such as the current GPS position, the last critical executed operations, the last contacts added to the address book..etc.

Remote wiping is another interesting feature provided by SecureMyDroid: this function enables the organization to send a remote wiping command to the mobile device. We implemented two different wiping modes: a soft mode and a hard mode. A soft wiping is carried out only on all databases containing personal information (e.g., SMS, MMS, e-mail, address book, calendar). A hard wiping implies the execution of a remove command on the mobile device shell; this completely deletes the OS and a new OS has to be installed on the mobile device to make it again operational. Remote wiping can be activated with a simple text message or can be executed when the mobile device starts with a non-authorized SIM.

Periodically, the security manager of the company can query the mobile device to receive the configuration of the customized OS. When an employee requires an upgrade of his/her customized mobile device, the security management using SecureMyDroid can backup all the data stored in the mobile device and according to the employee privileges can produce a new version of SecureMyDroid. After this, the employee can restore all the useful data on the newly customized mobile device.

When either the device is assigned to a new employee or it must to be permanently disposed, the security management may check and export the log collected on the mobile phone. Moreover, before deleting all data, if needed, he/she can activate the backup of personal information.

In summary, we have conceived and implemented the possibility that the device's operating system can be destroyed from remote and then rebuilt with a security checked image of SecureMyDroid. In additional, throughout the lifecycle of the device, the organization can implement all the online checks and changes as provided by its internal security policy. Finally, the integration of services specifically designed at the OS level (e.g., internal memory data collection, timed usage history support) helps to keep a high level of security and to protect the organization from external and internal threats related to the mobile device.

5. ACKNOWLEDGMENT

We are indebted to Fabrizio Mazzarini for his help in the implementation of SecureMyDroid.

6. REFERENCES

[1] J. Mottl, My Cellphone, My Everything..., internetnews.com, Jupitermedia Corporation, March 14, 2008, available at http://www.internetnews.com/mobility/article.php/3734366

[2] Becher, M., Freiling, F., Towards Dynamic Malware Analysis to Increase Mobile Device Security. Proceedings of SICHERHEIT 2008, 2008-04-02.

[3] Willems, C., Holz, T., and Freiling, F., Toward Automated Dynamic Malware Analysis Using CWSandbox. IEEE Security and Privacy 5, 2 (Mar. 2007), 32-39.

[4] Bowman, B., Mobile devices prone to identity theft. 2007, available at http://www.pitblado.com/lawyer_images/WFP-ArticleAUG2007.pdf.

[5] W. Jansen, V. Korolev, S. Gavrila, T. Heute, C. Séveillac, A Unified Framework for Mobile Device Security, The 2004 International Conference on Security and Management (SAM'04), June 2004.

[6] Apple Inc., iPhone in Business, April 7, 2010, available at http://www.apple.com/iphone/business/integration/

[7] Research In Motion Ltd., BlackBerry Business Solutions, April 7, 2010, http://na.blackberry.com/eng/solutions

[8] A.Sääksvuori,A. Immonen , Product Lifecycle Management, Springer, Third Ed. 2008