CHALLENGES IN MOBILE SECURITY

PANG Jian Hao Jeffrey, CHUA Chee Leong, CHAN Guan Huat, LIM Seh Leng

ABSTRACT

In recent years, mobile devices have been used increasingly in organisations to improve productivity with the Ministry of Defence looking to leverage this trend to enhance its operational efficiency. However, the use of mobile devices also opens up new areas of vulnerability for potential adversaries to target.

This article shares the security challenges that arise from the use of mobile technology and how DSTA is adopting a systematic approach in overcoming and securing the mobile cyber space. The article further discusses some design considerations for mobile solutions and shares emerging technologies in mobile malware analysis and detection.

Keywords: mobile, security, threats, malware

INTRODUCTION

The widespread use of mobile devices, such as smartphones and tablets, brings users much convenience and ease of use by allowing them to be connected to the Internet anytime and anywhere. The Ministry of Defence (MINDEF) has also adopted mobile devices in various areas such as email processing on-the-go and enabling soldiers to access e-learning materials on their own time in order to enhance productivity

However, with the diversity of mobile devices and the variety of security threats that can affect them, there is no one-size-fits-all solution to mobile security. Organisations should hence take a holistic approach to securing enterprise mobility to support business needs, including security policies formulation, device and configuration management for multiple devices and user education on mobile security.

This article reviews the challenges in achieving mobile security and presents DSTA's approach in securing the mobile cyber space. The article further presents some emerging methods for predictive malware detection to migitate application-based attacks.

MOBILE THREATS AND CHALLENGES

Mobile threats can largely be divided into several categories such as physical, network-based, system-based and application-based threats.

Physical Threats

One challenge faced in mobile security is the loss or theft of a mobile device. Compared to desktop computers, mobile devices are highly portable and lightweight. Hence, there is a greater likelihood of them getting lost or stolen.

Gaining physical access to a device would allow an attacker to perform malicious actions such as flashing it with a malicious system image that is connected to a computer to install malicious software or conduct data extraction. Hence, it is important not to leave devices unattended. In addition, device authentication and encryption need to be enforced to protect mobile devices against unauthorised access.

Network-based Threats

Mobile devices use common wireless network interfaces such as Wi-Fi and Bluetooth for connectivity. Each of these interfaces has its own inherent vulnerabilities and is susceptible

to wireless eavedropping attempts using readily available tools like Wifite or Aircrack-ng Suite. Users should thus only connect to trusted networks using WPA2[1] or better network security protocols.

System-based Threats

Manufacturers can sometimes introduce vulnerabilities into their devices unintentionally. For instance, the SwiftKey keyboard in Samsung Android devices was found to be vulnerable to eavesdropping attempts. Security updates were subsequently released to fix the issue (SwiftKey, 2015). Similarly, there exist critical vulnerabilities in Apple devices' iPhone Operating System (iOS). One example is the "No iOS Zone" vulnerability that automatically connects any iOS devices within range to a fabricated network and repeatedly crashes the device to deny its use (Amit, 2015). This vulnerability was eventually fixed in a later version of the iOS. These incidences highlight the need to perform timely updates of mobile devices to mitigate system issues.

Application-based Threats

Similar to system vulnerabilities, third-party applications on mobile devices may also be out-of-date. Some application developers do not release software updates in a timely manner or may have dropped support for older OS versions. Even if software updates are available, users may not update applications on their mobile devices promptly. Using outdated software increases the risk that an attacker may exploit vulnerabilities associated with these software.

Malicious applications, also known as malware, can perform malicious operations when installed on a device such as stealing data, downloading other malware, sending premium rate messages or even remotely controlling a device (see Figure 1). These actions can result in financial losses and other forms of tangible or intangible losses to an individual or organisation. Hence, it is important to detect and prevent malware from infecting mobile devices.

Attackers usually use social engineering techniques to trick users into installing these malicious applications. It can be in the form of a link in a message, a shortened hyperlink or a repackaged application that masquerades as a legitimate application. It is therefore essential that controls be enforced on the download and installation of applications.

Most anti-virus vendors offer mobile versions of their desktop anti-virus software. The core technique used in these mobile solutions is based on the traditional signature-based detection techniques. By analysing known malware samples and developing specific signatures for detection, this approach helps detect known malicious applications. Although signature-based approach can be effective in containing known malware, it fails to detect new, unknown or evolving variants due to a lack of signature for such malware. Mobile malware has stayed ahead by using transformation and obfuscation techniques to evade detection. For example, polymorphic and metamorphic malware have the ability to modify their code as they propagate so that signature-based detection techniques are unable to pick up on their virus signatures. As such, a new approach for malware analysis and detection is needed to ensure mobile security.

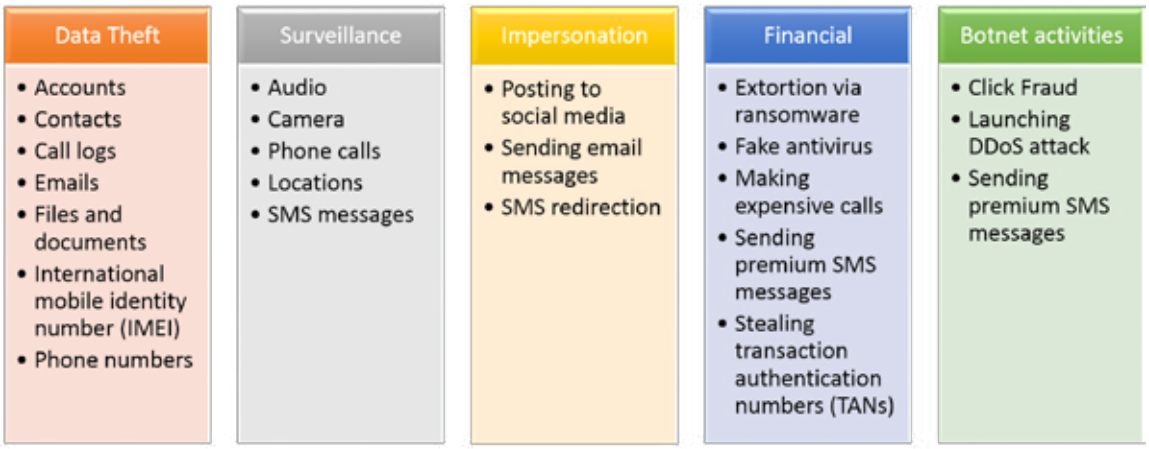

Figure 1. Figure denoting different kinds of malware activities

SYSTEMATIC APPROACH TOWARDS MOBILE SECURITY

DSTA adopts a systematic approach in assessing the mobile threats discussed in the previous section. This approach consists of five key elements – understanding, protection, detection, response and education (see Figure 2). This section discusses the use of this approach with reference to application-based threats.

Protection

Protection is a key component of mobile security and covers two main aspects. The first aspect is to prevent unwanted threats from entering or affecting the mobile system.

For example, having understood that malware can exist in the form of an application package or file, incoming network traffic can be scanned at a network proxy or gateway to check for malicious payload before forwarding it to the device. Applications and OS-es of devices are also updated timely to patch any vulnerabilities.

Figure 2. Figure denoting the different elements in mobile security

Understanding

Active monitoring of cyber space keeps the organisation informed of new threats that can affect security. When such threats are discovered, they are studied and assessed for any impact to existing systems. Their mitigation measures will also be identified. For example, when a malware attack is discovered, understanding critical information such as attack vectors, malicious indicators and impact, can help organisations derive an appropriate countermeasure. In cases where a solution is not readily available or is still being developed, these mitigation measures will be applied in the interim.

The other aspect of protection is to protect sensitive data from being leaked to unauthorised destinations. This can be achieved by securing the network channel using virtual private network and blocking outgoing traffic to unauthorised destinations using customised firewall rules.

As most mobile devices transmit data through the wireless network, it is possible for an attacker to analyse the network and steal critical data while it is in transit. Therefore, DSTA has implemented an encryption solution that entails storing the encryption key on the user's smartcard. This prevents unauthorised personnel from being able to read the content of the encrypted data without the user's smartcard.

Detection

In an application-based threat, malware is one of the key tools used by attackers to perform malicious activities on a mobile device. The harm caused by malware and malicious activities can be reduced through early detection. The classic defence method against malware is the use of anti-virus. However, malicious software writers have become more sophisticated, often using mechanisms to change or obfuscate their codes to foil detection by classic security defences. As such, a new approach of employing a combination of static and dynamic analysis, as well as machine learning techniques is proposed to achieve comprehensive results.

Another detection methodology is to monitor and pick up anomalous system activities and behaviours. Once an anomaly is detected, alerts are triggered to the user and backend reporting system. These alerts may provide information on the malicious activities and can be correlated with other security data to provide cyber defence engineers with useful information to detect and respond to threats quickly.

Response

Incident response is an important element in any security framework. When an incident occurs, the incident response team will need to step in to contain it and conduct technical investigation. The prevention or mitigation method is then reviewed to prevent similar incidents from occurring.

In an application-based attack, the application used is analysed to understand its behaviour and other critical information required to assess its impact and derive appropriate countermeasures.

Education

Although many users may be aware that mobile devices are actively targeted by malware, most still do not believe that they will fall victim to these attacks. Thus, it is important to educate users on the safe practices for mobile device usage and keep them updated on new forms of attacks.

DESIGN CONSIDERATIONS OF MOBILE SOLUTION

DSTA's design and development of mobile solutions gave rise to some challenges and provided many learning points for the organisation.

Capability and Scalability

To empower mobile users with the capability to process classified information on the move, DSTA designed and developed a two factor authentication[2] (2FA) solution for mobile devices using smartcard technology. The solution consists of four components – the smartcard reader hardware, driver, smartcard middleware and client application. The client applicaton requires the smartcard middleware and the driver to communicate with the smartcard and the reader respectively. To log in, the 2FA solution requires the user to present a tangible asset that only he or she has, such as a smartcard, as well as enter a piece of information that only he or she knows, such as a PIN.

One of the challenges is in sourcing for a smartcard reader and interface that can work with mobile devices. Smartcard readers used for desktops are not suitable for mobile devices due to interface or driver incompatibility. Furthermore, the software driver and middleware need to be customised in order to work with certain hardware and mobile OS. Moreover, as peripheral interfaces for mobile devices are changed every few years, the smartcard solution may have to be modified or even redeveloped often.

DSTA overcame this issue by adopting a systems engineering approach in which each component of the mobile smartcard solution was designed to be modular and developed on an open standard smartcard application interface, making the solution flexible in adapting to changes in the mobile world. With this modular design, subsequent development of the mobile smartcard solution requires less development work. Throughout the years, many peripheral interface options for smartcard readers were explored, developed and delivered for use in MINDEF. These include Secure Digital Input Output, Compact Flash, Bluetooth and USB interfaces (see Figure 3).

Hardware Limitations

While the processor speed of mobile devices has gone up significantly over the last few years, the devices themselves are still limited in terms of memory size, network connection and physical interfaces. These can be limiting factors in solution design. For example, the mobile security solution needs to be optimised for power efficiency as mobile devices tend to have shorter battery life. Network data transfer also has to be minimised as data transfer over mobile network can incur high costs to users.

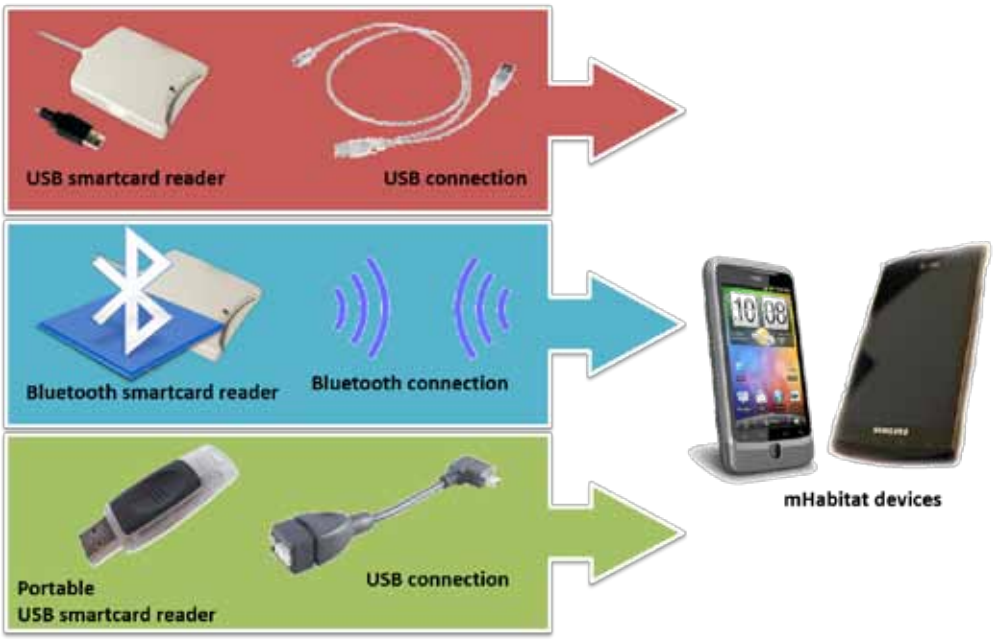

Figure 3: Illustration of different smartcard interfaces

In addition, the number of available interface ports on a device may be a design consideration. Most mobile devices have only one interface port that is also intended for charging. If a solution requires the use of an interface port for a long period of time, the device will not be able to charge. Therefore, the number of interface ports needs to be considered when selecting a suitable device.

Usability and Security

A traditional approach to enhance security is to fully harden a device. This involves locking down the device, restricting users from downloading applications, mandating strong authentication to access the mobile device and limiting connectivity, among other security measures. While this results in a secured device, it may no longer be user-friendly enough to meet the original intent as a technology enabler.

As such, DSTA adopts a design strategy that takes into account the usability and security of the mobile security solution. To achieve this, a threat risk assessment is performed before designing any solution to identify the critical areas that must be secured and analyse how this may affect usability. Any residual risk and proposed mitigation methods are discussed with stakeholders to reach a common understanding and agreement. This ensures that both security and usability are optimised while satisifying user requirements.

EMERGING MOBILE MALWARE DETECTION TECHNOLOGY

This section discusses some emerging approaches for analysing and detecting mobile malware and how they can be integrated into the larger defence infrastructure. Many research institutes have studied these approaches which can be largely categorised into static analysis, dynamic analysis and machine learning.

Static Analysis

Static analysis is the analysis of an application that is performed without actually executing the program. By performing a static analysis, an analyst can deduce the behaviours of an application. Other useful information such as required permissions, resources used and embedded strings can also be discovered. Additionally, information such as header files and database information can be extracted for analysis. For example, the RiskRanker project statically identified applications with different security risks. It detected properties such as encrypted code execution, dynamic code loading and various suspicious actions (Grace, Zhou, Zhang, Zuo, & Jiang, 2012).

Although static analysis incurs less performance overhead, its effectiveness can largely be limited by techniques such as code obfuscation, encrypted code and dynamic loading of code during runtime.

Dynamic Analysis

Dynamic analysis is the analysis of an application that is performed by executing a program on a real or virtual environment to observe its behaviours at runtime. These behaviours include system calls at runtime, file accesses and network information which are difficult to analyse solely with static analysis. A commonly used approach is the sandbox concept whereby an inspected application is being executed in an emulator or virtual environment for behaviour monitoring. For example, the DroidScope project provided an open source implementation of a customised Android OS. This implementation is capable of collecting an application's behavioural information at different layers of the platform (Lok & Heng, 2012).

The information collected from these application sandboxes allows one to understand the behavioural characteristics of an application and provides insights that may be useful to combat new and unknown malware.

Machine Learning

Machine learning is a popular technique used in financial and marketing industries to predict trends and user behaviour patterns. By analysing a large amount of real world data, machine learning algorithms are able to correlate patterns and trends to make predictions or classify observations. Machine learning-based malware detection allows organisations to classify an application as being either malicious or benign.

Static or dynamic analysis can be used to collect the data required for machine learning. The former was used in the Drebin project which outperformed nine out of ten selected anti-virus software with a detection rate of more than 93% (Arp, Spreitzenbarth, Hübner, Gascon, & Rieck, 2014). The results show that these emerging techniques can be useful tools for protection against application-based threats.

Proposed Integrated Malware Detection System

DSTA is continously experimenting and exploring solutions to enhance cybersecurity. One such solution is the adoption of an integrated system approach in malware detection (see Figure 4). This integrated system aims to combine and assess the results from several backend detection engines that leverage different detection techniques to derive a final assessment of targeted applications. As no single technique is completely robust and foolproof, a combination of the mobile malware detection approaches can be integrated to complement signature-based detection.

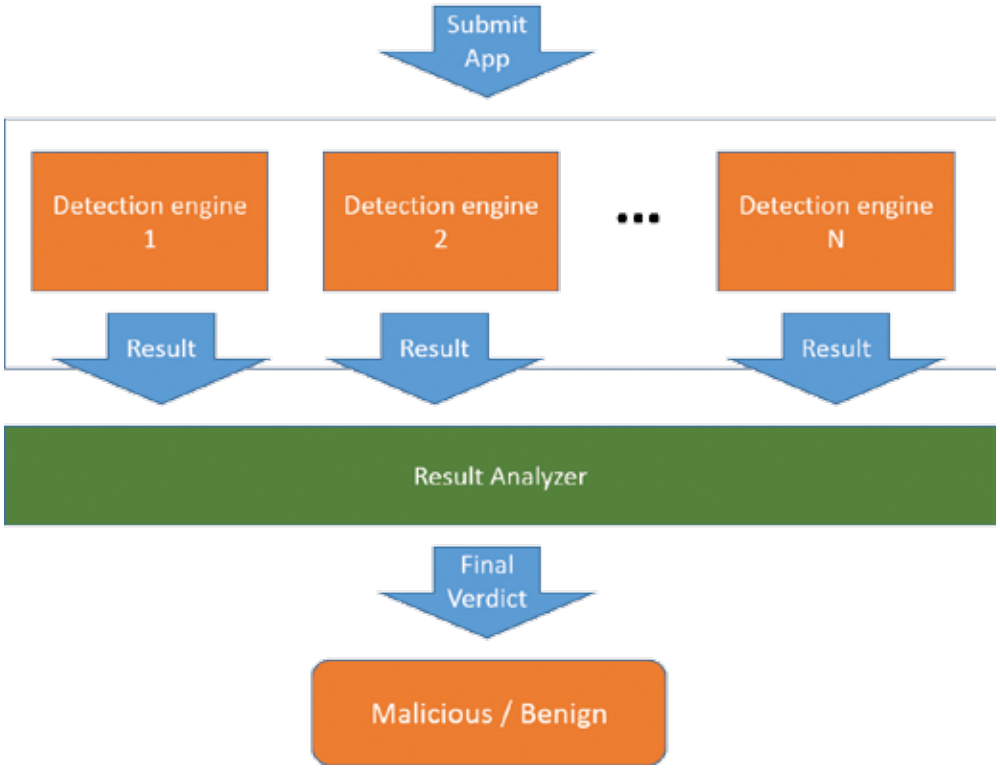

Figure 4. Illustration of proposed Integrated malware detection system

The positive research findings from the use of emerging technologies have led to the commercialisation of some research projects. However, most commercial-off-the-shelf (COTS) solutions are only available with cloud-based offerings which may not be suitable for use in the defence industry due to security concerns. On the other hand, an on-premise system requires updates and the timeliness of such updates needs to be assessed. Other considerations include the technical feasibility of integrating various COTS systems as COTS products might not provide interoperable interfaces for integration. Thus, various assessment need to be done to evaluate these products before they can be used. Despite these various considerations, this integrated system shows potential in detecting new and unknown malware that cannot be picked up by signature-based detection techniques.

CONCLUSION

This paper has highlighted the various threats faced in mobile computing and provides a comprehensive framework in securing the mobile cyber space. Mobility is a critical area of IT infrastructure that needs to be protected. To stay ahead of sophisticated cyber threats on mobile devices, the approaches presented in this article provide a systematic framework to protect mobile devices against different categories of threats. Some emerging techniques for malware detection are also highlighted. With this framework, a more secure mobile infrastructure can be delivered to MINDEF to further enhance military enterprise functions and operations.

REFERENCES

Amit, Y. (2015, April 22). *"No iOS zone" – a new vulnerability allows DoS attacks on iOS devices*. Retrieved from https://www.skycure.com/blog/ios-shield-allows-dos-attacks-on-ios-devices/

Arp, D., Spreitzenbarth, M., Hübner, M., Gascon, H., & Rieck, K. (2014). Drebin: effective and explainable detection of Android malware in your pocket. *Network and Distributed System Security Symposium, San Diego, California*. Retrieved from http://www.internetsociety.org/sites/default/files/11_3_1.pdf

Grace, M., Zhou, Y., Zhang, Q., Zou, S., & Jiang, X. (2012). RiskRanker: scalable and accurate zero-day Android malware detection. *International Conference on Mobile Systems, Applications, and Services, Lake District, United Kingdom*, 281-294. doi: 10.1145/2307636.2307663

Lok, K. Y., & Heng, Y. (2012). DroidScope: seamlessly reconstructing the OS and Dalvik semantic views for dynamic Android malware analysis. *USENIX Security Symposium 2012, Bellevue, Washington*. Retrieved from https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final107.pdf

SwiftKey. (2015, June 17). *An update on the Samsung keyboard security vulnerability*. Retrieved from http://swiftkey.com/en/blog/samsung-keyboard-security-vulnerability-swiftkey/

ENDNOTES

[1] Wi-Fi Protected Access II (WPA2) is a security protocol for wireless networks that implements the National Institute of Standards and Technology FIPS 140-2 compliant AES encryption algorithm and 802.1x-based authentication.

[2] Two-factor authentication (also known as 2FA) is a technology used to prove a user's identity by requiring the user to provide a combination of two components. These components may be something that the user possesses (e.g. the user's smartcard), and something that the user knows (e.g. a PIN).

BIOGRAPHY

PANG Jian Hao Jeffrey is an Engineer (Cybersecurity) who is currently involved in the development of cybersecurity solutions on mobile devices for DSTA, the Ministry of Defence (MINDEF) and the Singapore Armed Forces (SAF). Jeffrey graduated with a Bachelor of Engineering (Computer Science) degree with Honours from Nanyang Technological University (NTU) in 2012.

CHUA Chee Leong is a Development Manager (Cybersecurity) managing the development of cybersecurity solutions to detect and prevent cyber threats on mobile devices. Chee Leong graduated with a Bachelor of Engineering (Electrical and Electronic Engineering) degree from NTU in 1998. He further obtained a Master of Engineering (Electrical and Electronic Engineering) degree from NTU in 2000.

CHAN Guan Huat is a Development Manager (Cybersecurity) designing, developing and implementing cybersecurity solutions on mobile devices. Guan Huat graduated with a Bachelor of Engineering (Electrical and Electronic Engineering) degree from NTU in 2002.

LIM Seh Leng is a Development Programme Manager (Cybersecurity) who currently leads the development of secure mobility solutions for DSTA, MINDEF and the SAF. Seh Leng graduated with a Bachelor of Engineering (Electrical Engineering) degree with Honours from the National University of Singapore in 1994.