STUDYDADDY
Get Homework Help
From Expert Tutor
Get Help

Electron Commer Res (2013) 13:243–256
DOI 10.1007/s10660-013-9121-4

Threat modeling of a mobile device management system for secure smart work

**Keunwoo Rhee · Dongho Won · Sang-Woon Jang ·
Sooyoung Chae · Sangwoo Park**

Published online: 11 May 2013
© Springer Science+Business Media New York 2013

Abstract To enhance the security of mobile devices, enterprises are developing and adopting mobile device management systems. However, if a mobile device management system is exploited, mobile devices and the data they contain will be compromised. Therefore, it is important to perform extensive threat modeling to develop realistic and meaningful security requirements and functionalities. In this paper, we analyze some current threat modeling methodologies, propose a new threat modeling methodology and present all possible threats against a mobile device management system by analyzing and identifying threat agents, assets, and adverse actions. This work will be used for developing security requirements such as a protection profile and design a secure system.

Keywords Mobile device management system · Threat modeling · Security requirement · Smartphone · Tablet PC

K. Rhee (✉) · S.-W. Jang · S. Chae · S. Park
The Attached Institute of ETRI, P.O. Box 1, Yuseong-gu, Daejeon 305-600, Korea
e-mail: kwrhee@ensec.re.kr

S.-W. Jang
e-mail: jsw@ensec.re.kr

S. Chae
e-mail: sychae@ensec.re.kr

S. Park
e-mail: psw@ensec.re.kr

D. Won
College of Information and Communication Engineering, Sungkyunkwan University, 2066,
Seobu-ro, Jangan-gu, Suwon, Gyeonggi-do 440-746, Korea
e-mail: dhwon@security.re.kr

1 Introduction

Recently, the use of smartphones and tablet PCs in business has increased as a result of their mobility, but the spread of mobile devices increases the risk of information leakage from their loss or misuse. Therefore, many enterprises are adopting mobile device management (MDM) systems to enhance the security of both company- and employee-owned mobile devices.

However, if developers do not consider all possible threats against an MDM system, it will not provide sufficient security to prevent all threats and could compromise the mobile devices.

Therefore, this paper defines all possible threats. This is the basis of developing security requirements, such as a protection profile in the Common Criteria [4]. In addition, knowledge of potential threats is crucial to the design of security functions.

There are a number of studies related to formal threat modeling methodologies for complex systems such as MDM [5, 7, 9–12, 19, 20, 22, 23, 27, 28, 30, 33]. According to previous research [20, 30], a threat modeling process consists of the following steps: (1) characterization of the system and analysis of the technical background; (2) identification of assets; and (3) definition of threats.

ISO/IEC TR 13335-1 [15] and ISO/IEC 15408 (Common Criteria) [4] illustrate why threat agents, assets, and vulnerabilities should be identified to define threats. According to ISO/IEC 15408, a threat consists of an adverse action performed by a threat agent on an asset [4]. In other words, the identification of threat agents, assets, and adverse actions that exploit vulnerabilities is the key to defining a threat. Therefore, we propose a threat modeling methodology for an MDM system by integrating and extending [20, 30], ISO/IEC TR 13335-1, and ISO/IEC 15408. The proposed threat modeling methodology has five steps: (1) characterization of the system and analysis of the technical background; (2) identification of threat agents; (3) identification of assets and their values; (4) identification of vulnerabilities and adverse actions; and (5) definition of threats. Figure 1 describes the revised relationships between the components of a threat.

The remainder of this paper is organized as follows. Section 2 provides a detailed understanding of an MDM system, and Sect. 3 identifies the threat components—threat agents, assets, and adverse actions. Based on these components, Sect. 4 then defines all possible threats to an MDM system. Finally, Sect. 5 discusses the significance and applicability of this paper.

2 Mobile device management system

The first step in threat modeling is to completely understand the system in question. This entails defining its usage and understanding every component and its interconnections [4].

An MDM system manages smartphones and tablet PCs remotely by monitoring their status and controlling their functions. Table 1 lists a number of the principal monitoring, controlling, and managing functions of an MDM system [1, 6, 17, 34].

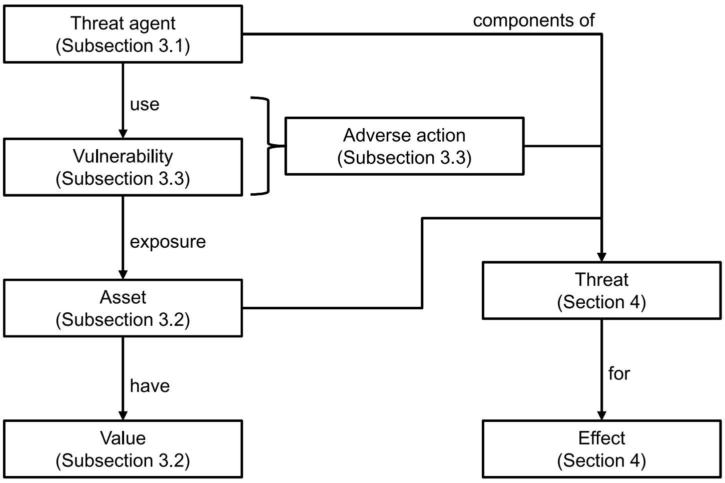

Fig. 1 Revised relationships between the components of a threat

Table 1 Functions of an MDM system

Function	Description
Application	Install and uninstall enterprise applications
Management	Execute and stop enterprise and non-enterprise applications
	Update enterprise and non-enterprise applications
	Prevent uninstallation of enterprise applications
	Remove non-enterprise applications
	Install certificate
Device Management	Enable and disable camera, screen capture, Bluetooth, Wi-Fi, GPS, microphone, synchronization, etc.
	Control access point
Device inventory	Check assigned IP address, SIM state, OS information, application ID/name/version, Bluetooth status, Wi-Fi status, GPS status, phone number, IMEI, hardware resource information, data roaming setting, device type, etc.
Security	Remote device lock and unlock
Management	Remote device data wipe
	Remote device reset
	Push and remove configuration data
	Set password and password policies (combination, length, history, failure count, etc.)
	Encrypt and decrypt data
	Configure account (Exchange ActiveSync, e-mail, VPN, etc.)

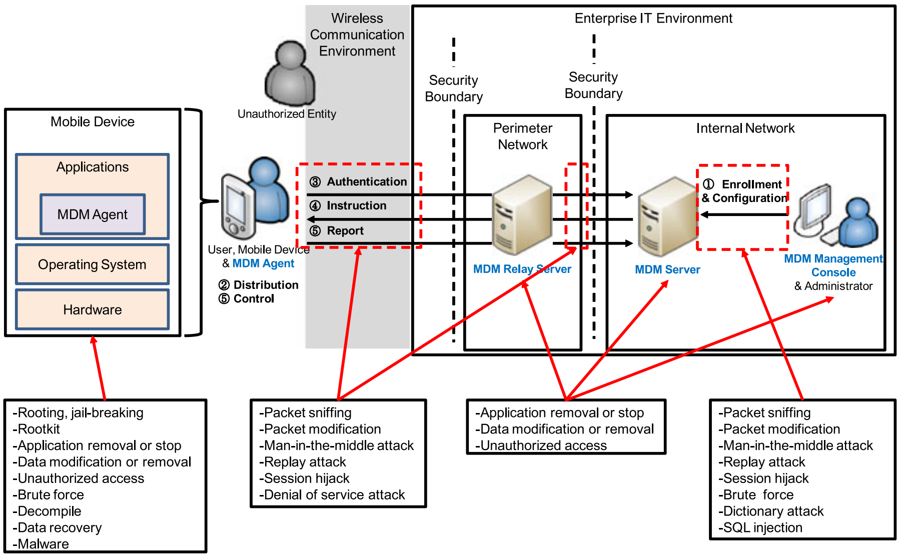

Fig. 2 Architecture of an MDM system and possible attacks

As shown in Fig. 2, there are four essential components to an MDM system:

MDM agent An MDM agent collects mobile device status data and sends them to the MDM server. It also applies policies received from the MDM server to the mobile device and transmits the result back to the server. The MDM agent is installed on the mobile device in the form of an application.

MDM server An MDM server manages the data of registered mobile devices and users and distributes the mobile device management policy and application.

MDM management console An MDM management console is an application that allows the administrator to login to the MDM server to manage the system.

MDM relay server An MDM relay server relays and controls the flow of information between entities that cannot directly communicate because of security issues or their physical layout.

Interactions between the above four components consist of the following five steps:

Step 1. Enrollment/configuration The mobile device data and user data of the organization are registered in the MDM system and the policy to be applied to each mobile device is configured.

Step 2. Distribution The MDM agent is distributed and installed on the mobile devices. The MDM agent can be distributed through an application store/market or in-house.

Step 3. Authentication When an MDM agent is run after installation, certain mobile device data (e.g. IMEI, IP/MAC address, phone number, etc.) are sent to the MDM server to verify whether they match the data registered in the system.

Step 4. Instruction The MDM server sends each MDM agent the mobile device control policy, and commands such as 'remote wipe', according to the mobile device status data and the individual user.

Step 5. Control/report The MDM agent controls the functions of the mobile device according to the mobile device control policy/command and reports the results to the MDM server.

3 Threat agents, assets, and adverse actions

In this section, we identify threat agents, assets, and adverse actions for the system analyzed in Sect. 2. As these are the threat components, it is very important to completely identify them in order to define potential threats.

3.1 Threat agents

A threat agent is an entity that can adversely act on assets [4]. Generally, we consider only unauthorized entities to be threat agents, although mobile device users and system administrators can also be threat agents. In addition, natural events such as flood, earthquake, and fire can also be a threat agent. In an MDM system, there are four kinds of threat agent:

Administrator If administrators are not trained, they can unintentionally threaten the MDM system. However, administrators are generally well trained and attentive to the operation of the system. Since administrators manage the system, they have enough resource and opportunities to attack the system. Generally, we think that administrators are trustable. But, sometimes, bribed or dissatisfied administrators may become malicious.

User Users access to a mobile device, the MDM agent, and business applications. Therefore, they have enough resources and opportunities to attack the system. Generally, a common user is not an expert to attack the system. However, a user such as an IT engineer can analyze and attack the system with a high level understanding. He/she may act maliciously when they want to access privileges that are not assigned to them.

Unauthorized entity Unauthorized entities are generally hackers, competitors, and their malware. Therefore, they are experts to attack the system. They are malicious and have enough resources. In addition, the finder of a lost device can be an unauthorized entity. He/she is also malicious. But he/she is not an expert and doesn't have enough resources. He/she has few opportunities to attack the system since he/she is not an owner or manager of the system.

Table 2 Threat agents

Threat agent	Expertise	Resource	Opportunity	Motivation
Administrator	High	Enough	Many	Malicious or non-malicious
User	High or low	Enough	Many	Malicious or non-malicious
Unauthorized entity	High or low	Enough or not enough	Few	Malicious
Nature	–	Enough	–	–

Nature Threats posed by nature include earthquakes, floods, fires, and so on. It has very powerful resources to extensively damage the system. However, it has no expertise or motivation. The opportunity of the nature is no measurable.

Table 2 gives a detailed analysis of these threat agents in terms of their expertise, resource, opportunity, and motivation aspects.

In order to define realistic and meaningful threats, we make two assumptions:

Assumption 1 The authorized administrator of the system can be trusted and is well trained, because no system is secure against an authorized administrator launching an attack.

Assumption 2 The MDM relay server, the MDM server, and the MDM management console are located in a physically secure location, and thus cannot be damaged by earthquakes, floods, fires, etc.

With these two assumptions, we can reduce the threat agents to users (T1) and unauthorized entities (T2).

3.2 Assets

Assets are entities that have a value, however subjective, placed upon them. This value is defined as the commercial value, but the value of business assets can range from very high to very low. For example, a customer's private information in a businessman's mobile device has a very high commercial value, but an introductory brochure will have a low commercial value. Therefore, we redefine the value as the principles to be protected. There are four classical principles—Confidentiality, Integrity, Availability, and Authenticity, which together are known as CIAA.

In order to allow identification, we extend all possible assets from access points. As shown in Fig. 2, the access points are the components of the MDM system and the information flow between the components. Figure 3 shows the identified assets according to the location and asset type. In order to identify realistic and meaningful assets, the server platform and hardware are excluded from the list of assets.

The identified assets can be categorized as business data (e.g. confidential downloaded or produced business data), status of mobile device (e.g. IMEI, phone number, IP address, etc.), system functional data (e.g. policy/instruction/report for man-

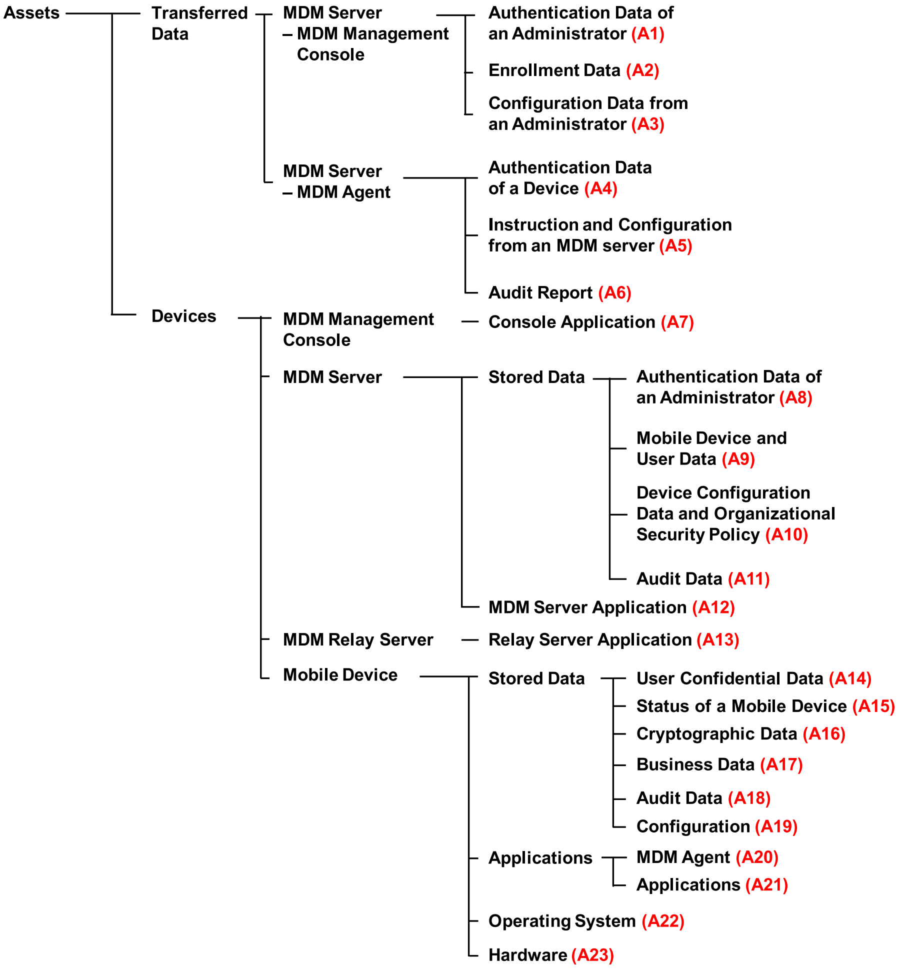
Assets
Transferred Data
MDM Server – MDM Management Console
Authentication Data of an Administrator (A1)
Enrollment Data (A2)
Configuration Data from an Administrator (A3)
MDM Server – MDM Agent
Authentication Data of a Device (A4)
Instruction and Configuration from an MDM server (A5)
Audit Report (A6)
Devices
MDM Management Console
Console Application (A7)
MDM Server
Stored Data
Authentication Data of an Administrator (A8)
Mobile Device and User Data (A9)
Device Configuration Data and Organizational Security Policy (A10)
Audit Data (A11)
MDM Server Application (A12)
MDM Relay Server
Relay Server Application (A13)
Mobile Device
Stored Data
User Confidential Data (A14)
Status of a Mobile Device (A15)
Cryptographic Data (A16)
Business Data (A17)
Audit Data (A18)
Configuration (A19)
Applications
MDM Agent (A20)
Applications (A21)
Operating System (A22)
Hardware (A23)

Fig. 3 Breakdown of assets by location and type

agement, profile for access to MDM server, etc.), system confidential data (e.g. encryption/decryption key, session key, etc.), user/administrator confidential data (e.g. E-mail/VPN/Wi-Fi account, password/pin/locking pattern of mobile device, administrator's ID/password, etc.), software (e.g. enterprise applications, MDM system applications, OS of mobile device, etc.), and H/W modules (e.g. camera, Wi-Fi, external memory, USB port, etc.)

Business data such as a marketing strategy and system confidential data such as an encryption key are confidential. Status of mobile device affects the MDM server's instruction or configuration to the MDM agent. Therefore, the integrity and availability of status of mobile device are important. But the status of mobile device is not confidential. System functional data affects the operation of an MDM agent. Therefore, integrity and availability should be protected. In addition, authenticity of the system functional data should be guaranteed since system functional data such as an instruc-

Table 3 Assets and their value

Category	Asset	Value
Business data	A17	Confidentiality
Status of mobile device	A2	Integrity
	A15	Integrity, Availability
System functional data	A3, A4	Integrity, Authenticity
	A5, A6	Integrity, Availability, Authenticity
	A9–11, A18, A19	Integrity, Availability
System confidential data	A16	Confidentiality
User/administrator confidential data	A1	Confidentiality, Integrity, Availability
	A8, A14	Confidentiality, Integrity, Availability, Authenticity
Software	A7, A12, A13, A20–22	Integrity, Availability
H/W modules	A23	Integrity

tion can be delivered from a fake MDM server. User or administrator confidential data such as ID and password are confidential. In addition, their integrity, availability, and authenticity should be protected since an attacker tries to modify or remove or reuse them in order to disguise as a legitimate user or an administrator. Finally, availability and integrity of software and availability of hardware should be protected for the correct operation of the MDM system.

Table 3 explains the assets to be protected and their value.

3.3 Adverse actions

An adverse action performed by a threat agent on an asset exploits system vulnerabilities, such as poor architecture design and development, and inadequate security policies, plans, and procedures. Generally, adverse actions combine a number of attack types, such as packet sniffing, SQL injection, password dictionary attack, and malware [2, 3, 14, 16, 29, 31].

Possible vulnerabilities and attacks can be grouped according to the target. Figure 2 shows the possible vulnerabilities and attacks [8, 18, 21, 24–26, 29, 35–42].

These vulnerabilities and attacks do not completely cover all possible adverse actions. There are various network, host, application, and web vulnerabilities [19]. However, these vulnerabilities and attacks can be categorized using more generalized terminology. Table 4 shows the generalized adverse actions and related assets.

4 Threats

Threats can be identified by defining the relationship between threat agents, assets, and adverse actions. In other words, it is a kind of ‘subject (threat agent)—verb

Table 4 Adverse actions and assets

Attacks	Description	Asset
Reuse (M1)	Unauthorized reuse of captured traffic or stored data	A1, A3–6, A8, A14
Disclose (M2)	Unauthorized disclosure of captured traffic or stored confidential data	A1, A8, A14, A16, A17
Modify (M3)	Modification of authentication data, configuration data, audit report	A1–15, A18–22
Repudiate (M4)	Blocking of communication	A5, A6
Analyze (M5)	Cracking a poor security mechanism	A8, A14, A16
Remove (M6)	Destruction of application or configuration data	A7–15, A18–21
Stop (M7)	Stop the service or process	A7, A12, A13, A20, A21
Bypass (M8)	Bypass of system security functions	A23
Install (M9)	Installation of an unauthorized application or malware	A22
Execute (M10)	Execution of an unauthorized application or malware	A22

(attack)—object (asset)’ structure. However, this structure does not sufficiently explain the effect of threats. Therefore, we analyze the effects of the defined threats and describe threats with their effects.

In general, threats can be classified into six categories based on their effect [20]. These are spoofing (S), tampering (T), repudiation (R), information disclosure (I), denial of service (D), and elevation of privileges (E).

Table 5 shows the defined threats with their effects. The threats are categorized by their assets, effects, and attacks. In Table 5, ‘/’ means ‘OR’. For example, an unauthorized user (T2) reuses (M1) authentication data of an administrator (A1) to obtain an administrator’s authority (S). To reuse authentication data of an administrator such as administrator’s ID and password, a threat agent uses packet sniffing and launches a replay attack. Therefore, the authenticity of the asset is violated. Figure 4 illustrates this example by the relationships described in Fig. 1.

5 Conclusion

In this paper, we established a threat model for an MDM system. By characterizing the system, identifying threat agents, assets, and adverse actions, and defining the threats and their effects, we gained a deep understanding of the MDM system in order to prepare for threats. This work will be used to develop security requirements [13] and design a secure system [32, 43]. In addition, we can establish another threat model for an emerging system using this threat modeling methodology.

Table 5 Threats

Threat level	Description	Threat-Attack-Asset-Effect
Spoofing (admin)	A threat agent performs adverse action on the transferred or stored data to obtain an administrator's authority level	(T1/T2)-(M1/M3)-(A1/A8)-S, (T1/T2)-M6-A8-S
Spoofing (user/device)	A threat agent performs adverse action on the transferred or stored data to obtain the authority of a legitimate user or device	(T1/T2)-(M1/M3)-(A4/A14)-S, (T1/T2)-M3-A2-S, (T1/T2)-(M3/M6)-A9-S
Illegal access	A threat agent performs adverse action on the stored data to access a mobile device or an MDM server as a legitimate user or administrator	T2-(M3/M6)-A14-S, T2-M5-(A8/A14)-S
Elevation of privileges	A threat agent performs adverse action on the transferred or stored data to gain privileges that are not assigned to the threat agent	(T1/T2)-(M1/M3)-(A3/A5/A6)-E, (T1/T2)-M3-A2-E, (T1/T2)-(M3/M6)-A10-E, (T1/T2)-M3-(A15/A18)-E, (T1/T2)-(M3/M6)-A19-E
Bypass	A threat agent performs adverse action on a locked hardware module in order to use a mobile device	(T1/T2)-M8-A23-E
Denial of service	A threat agent performs adverse action on the transferred or stored data to induce incorrect operation	(T1/T2)-(M1/M3)-(A3/A5)-D, (T1/T2)-M6-(A8/A9)-D, (T1/T2)-(M3/M6)-A10-D, (T1/T2)-(M6/M7)-(A7/A12/A13)-D, (T1/T2)-M6-A14
Bad records	A threat agent performs adverse action on the transferred or stored data to interfere with investigations	(T1/T2)-M1-A6-D, (T1/T2)-(M3/M6)-A11-D
Incapacitation (MDM agent)	A threat agent performs adverse action on an MDM agent to interfere with its operation	(T1/T2)-(M6/M7)-A20-D
Incapacitation (application)	A threat agent performs adverse action on an application, such as an anti-virus or business application, in order to interfere with its operation	(T1/T2)-(M6/M7)-A21-D
Disclosure	A threat agent performs adverse action on the data to leak confidential information such as the administrator's ID/password, encryption/decryption key, and so on	(T1/T2)-M2-(A1/A8/A14/A17)-I, (T1/T2)-(M2/M5)-A16-I
Repudiation	A threat agent performs adverse action on the transferred or stored data to retain former privileges	(T1/T2)-M4-(A5/A6)-R, (T1/T2)-M6-(A15/A18/A19)-R
Tampering	A threat agent performs adverse action on applications and the operating system of a mobile device to mount an attack	(T1/T2)-M3-(A7/A12/A13/A20/A21/A22)-T
Malware	A threat agent performs adverse action on the operating system of a mobile device to install or execute malware	(T1/T2)-(M9/M10)-A22-T

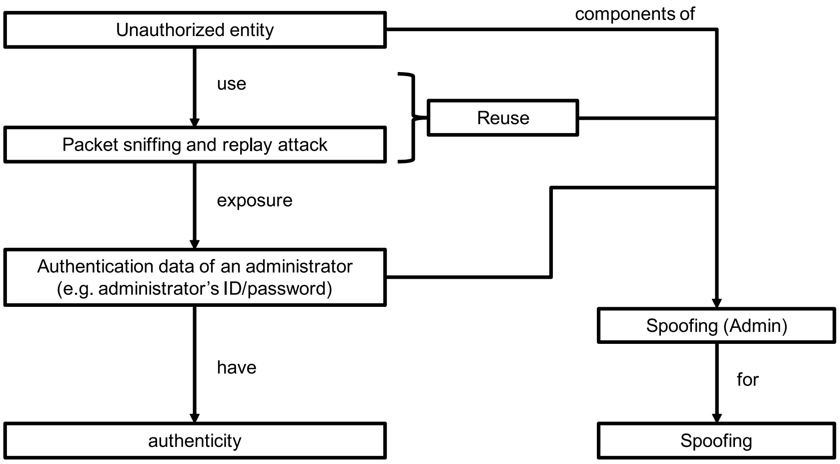
Unauthorized entity
components of
use
Reuse
Packet sniffing and replay attack
exposure
Authentication data of an administrator
(e.g. administrator's ID/password)
Spoofing (Admin)
have
for
authenticity
Spoofing

Fig. 4 Relationships between the components of an example threat

Acknowledgements This paper is based on Keunwoo Rhee's Ph. D. dissertation written at Sungkyunkwan University, Previous versions circulated under the title, "A Study on the Security Evaluation of a Mobile Device Management System."

References

1. Apple Inc. (2010). iPhone in business mobile device management. http://images.apple.com/iphone/business/docs/iPhone_MDM.pdf. Accessed 29 May 2012.
2. Bickford, J., O'Hare, R., Baliga, A., Ganapathy, V., & Iftode, L. (2010). Rootkits on smartphones: attacks, implications and opportunities. In *Proceedings of 11th workshop on mobile computing systems and applications (HotMobile'10)* (pp. 49–54).
3. Bruns, J. (2009). Mobile application security on android. Black Hat 2009. http://www.blackhat.com/presentations/bh-usa-09/BURNS/BHUSA09-Burns-AndroidSurgery-PAPER.pdf. Accessed 29 May 2012.
4. CCMB (2009). Common criteria for information technology security evaluation. Part 1: Introduction and general model. Version 3.1, Revision 3, Final, CCMB-2009-07-001.
5. Chen, Y., Boehm, B., & Sheppard, L. (2007). Value driven security threat modeling based on attack path analysis. In *Proceedings of the 40th Hawaii international conference on system sciences (HICSS'07)* (pp. 280a).
6. Cisco Systems, Inc. (2012). Global IT survey highlights enthusiasm over tablets in the enterprise, shows customization, collaboration and virtualization as key features. http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=658006. Accessed 29 May 2012.
7. CVSS (2012). Forum of incident response and security teams. http://www.first.org/cvss/cvss-guide.html. Accessed 29 May 2012.
8. C-skills blog (2012). http://c-skills.blogspot.com. Accessed 29 May 2012.
9. Demchenko, Y., Gommans, L., Laat, C. D., & Oudenaarde, B. (2005). Web services and grid security vulnerabilities and threats analysis and model. In *Proceedings of the 6th IEEE/ACM international workshop on grid computing* (pp. 262–267).
10. Goldberg, Y. (2012). Practical threat analysis for the software industry. http://www.ptatechnologies.com. Accessed 29 May 2012.
11. Hasan, R., Myagmar, S., Lee, A. J., & Yurcik, W. (2005). Toward a threat model for storage systems. In *Proceedings of the 2005 ACM workshop on storage security and survivability (StorageSS'05)* (pp. 94–102).

12. Håvaldsrud, T., Ligaarden, O., Myrseth, P., Refsdal, A., Stølen, K., & Ølnes, J. (2010). Experiences from using a UML-based method for trust analysis in an industrial project on electronic procurement. *Electronic Commerce Research*, *10*(3–4), 441–467.
13. Herrmann, P., & Herrmann, G. (2006). Security requirement analysis of business processes. *Electronic Commerce Research*, *6*(3–4), 305–335.
14. Hogben, G., & Dekker, M. (2010). Smartphone: Information security risks, opportunities and recommendations for users. European Network and Information Security Agency. http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport. Accessed 29 May 2012.
15. International Organization for Standardization (2004). ISO/IEC TR 13335-1: information technology—security techniques—management of information and communications technology security—Part 1: Concepts and models for information and communications technology security management. http://www.iso.org/iso/iso_catalogue_tc/catalogue_detail.htm?csnumber=39066. Accessed 29 May 2012.
16. Jeon, W., Kim, J., Lee, Y., & Won, D. (2011). A practical analysis of smartphone security. In M. J. Smith & G. Salvendy (Eds.), *Lecture notes in computer science* (Vol. 6771, pp. 311–320). Berlin: Springer.
17. Layland, R., Wexler, J., Datoo, A., George, A., Rege, O., Marshall, J., Herrema, J., & Duckering, B. (2011). The 2011 mobile device management challenge—defusing mobile anarchy in the enterprise. Network World and Robin Layland present. http://solutioncenters.networkworld.com/mobile_management_challenge. Accessed 29 May 2012.
18. Lee, K. (2011). *A study on the design of secure multi function printer conforming to the Korea evaluation and certification scheme*. Suwon: Sungkyunkwan University
19. Meier, J. D., Mackman, A., Dunner, M., Vasireddy, S., Murukan, A., Meier, J. D., Mackman, A., Dunner, M., Vasireddy, S., & Murukan, A. (2003). *Improving web application security: threats and countermeasures*. Microsoft Press. http://msdn.microsoft.com/en-us/library/ff649874.aspx. Accessed 20 July 2012.
20. Myagmar, S., Lee, A. J., & Yurcik, W. (2005). Threat modeling as a basis for security requirements. In *Proceedings of the symposium on requirements engineering for information security (SREIS'05)*.
21. National Vulnerability Database (2012). CVE-2011-1149. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1149. Accessed 29 May 2012.
22. Ni, J., Li, Z., Gao, Z., & Sun, J. (2007). Threat analysis and prevention for grid and web security. In *Proceedings of the 8th ACIS international conference on software engineering, artificial intelligence, networking, and Parallel/Distributed computing (SNPD 2007)* (pp. 526–531).
23. Oladimeji, E. A., Suppakkul, S., & Chung, L. (2006). Security threat modeling and analysis: a goal-oriented approach. In *Proceedings of the 10th IASTED international conference on software engineering and applications (SEA 2006)*.
24. OWASP (2012). Man-in-the-middle attack. http://www.owasp.org/index.php/Man-in-the-middle_attack. Accessed 29 May 2012.
25. OWASP (2012). Session hijacking attack. http://www.owasp.org/index.php/Session_hijacking_attack. Accessed 29 May 2012.
26. OWASP (2012). SQL injection. http://www.owasp.org/index.php/SQL_Injection. Accessed 29 May 2012.
27. Pauli, J., & Xu, D. (2005). Threat-driven architectural design of secure information systems. In *Proceedings of the 7th international conference on enterprise information systems (ICEEIS 2005)*.
28. Prasad, N. R. (2007). Threat model framework and methodology for personal networks (PNs). In *Proceedings of the 2nd international conference on communication systems software and middleware (COMSWARE 2007)* (pp. 1–6).
29. Schmidt, A. D., Schmidt, H. G., Batyuk, L., Clausen, J. H., Camtepe, S. A., & Albayrak, S. (2009). Smartphone malware evolution revisited: android next target? In *Proceedings of the 4th international conference on malicious and unwanted software* (pp. 1–7).
30. Stango, A., Prasad, N. R., & Kyriazanos, D. M. (2009). A threat analysis methodology for security evaluation and enhancement planning. In *Proceedings of 2009 third international conference on emerging security information, systems and technologies (SECURWARE 2009)* (pp. 262–267).
31. Stouffer, K. A. (2004). System protection profile-industrial control systems version 1.0. National Institute of Standards and Technology. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=822602. Accessed 29 May 2012.

32. Swamynathan, G., & Almeroth, K. (2010). The design of a reliable reputation system. *Electronic Commerce Research*, *10*(3–4), 239–270.
33. Swiderski, F., & Snyder, W. (2004). *Threat modeling, redmond*. Washington: Microsoft Press.
34. Sybase, Inc. (2011). Afaria: a technical overview. http://m.sybase.com/files/White_Papers/Afaira-Techinical-WP.pdf. Accessed 29 May 2012.
35. Tegrak Kernel (2012). http://pspmaster.tistory.com. Accessed 29 May 2012.
36. Wang, Z., & Stavrou, A. (2010). Exploiting smart-phone USB connectivity for fun and profit. In *Proceedings of the 26th annual computer security applications conference (ACSAC'10)* (pp. 357–366).
37. Wikipedia (2012). Brute-force attack. http://en.wikipedia.org/wiki/Brute-force_attack. Accessed 29 May 2012.
38. Wikipedia (2012). Dictionary attack. http://en.wikipedia.org/wiki/Dictionary_attack. Accessed 29 May 2012.
39. Wikipedia (2012). iOS jailbreaking. http://en.wikipedia.org/wiki/IOS_jailbreaking. Accessed 29 May 2012.
40. Wikipedia (2012). Replay attack. http://en.wikipedia.org/wiki/Replay_attack. Accessed 29 May 2012.
41. Wikipedia (2012). Rooting (Android OS). http://en.wikipedia.org/wiki/Rooting_(Android_OS). Accessed 29 May 2012.
42. You, D., & Noh, B. (2011). Android platform base Linux kernel rootkit. In *Proceedings of 2011 6th international conference on malicious and unwanted software* (pp. 79–87).
43. Zarmpou, T., Saprikis, V., Markos, A., & Vlachopoulou, M. (2012). Modeling users' acceptance of mobile services. *Electronic Commerce Research*, *12*(2), 225–248.

Keunwoo Rhee received B.S. degree in Information and Communication Engineering, M.S. degree in Computer Engineering, and Ph.D. in Electrical and Computer Engineering from Sungkyunkwan University in 2004, 2006, and 2012, respectively. He joined The Attached Institute of ETRI in 2008, and is currently a member of engineering staff of The Attached Institute of ETRI. His interests are cryptography, information security, information assurance, and security evaluation.

Dongho Won received M.S. and Ph.D. degrees in Electronic Engineering from Sungkyunkwan University in 1978 and 1988, respectively. After working at ETRI from 1978 to 1980, he joined Sungkyunkwan University in 1982, and is currently a Professor of the College of Information and Communication Engineering. His interests are cryptology and information security.

Sang-Woon Jang received B.S. degree in Mathematics and M. S. degree in Information Security Engineering from Korea University in 2002 and 2004, respectively. He joined The Attached Institute of ETRI in 2004, and is currently a senior member of engineering staff of The Attached Institute of ETRI. His interests are cryptography, information security, information assurance, and security evaluation.

Sooyoung Chae received Ph.D. degree in Information Security(Network System Security) from Korea University in 2008. He joined The Attached Institute of ETRI in 2001, and is currently a principal member of engineering staff of The Attached Institute of ETRI. His interests are cryptography, information security, information assurance, and security evaluation. Recently advised on Cloud computing security is interested.

Sangwoo Park received B.S. degree, M.S. degree and Ph.D. in Mathematics from Korea University in 1989, 1991 and 2003, respectively. He joined The Attached Institute of ETRI in 2000, and is currently a principal member of engineering staff of The Attached Institute of ETRI. His interests are cryptography, cyber security, and security evaluation.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

STUDYDADDY

Get Homework Help
From Expert Tutor

Get Help