American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)

ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

© Global Society of Scientific Research and Researchers

http://asrjetsjournal.org/

Wireless and Mobile Computing Security Challenges and Their Possible Solutions

Dr. Mohammad Othman Nassar*

Assistant professor at Amman Arab University, Amman-Jordan

Email: moanassar@yahoo.com

Abstract

Mobile device security has become more critical as businesses begin to rely on these devices for everyday processes. Securing information from unauthorized access is a major problem for any network, especially in the wireless networks. This paper will discuss the main security challenges concerning the mobile devices such as tablet and cell phones which run a mobile Operating System (OS). More specifically, these are Android (Google), iOS (Apple), or BlackBerry OS (RIM). Major solutions to the security challenges will also presented and discussed in this paper.

Keywords: Mobile; Security; smartphones; Android; IOS; Blackberry; Vulnerability; security challenges; solutions.

1- **Introduction**:

Security in wireless networks is even greater problem compared to wired networks, since radio signals travels through the open atmosphere which makes it vulnerable to be hacked and traced, also most wireless applications are dependent on public-shared infrastructure where you have much less control of, and knowledge about, the security discipline employed. In 2010, McAfee labs reported a 46% increase in mobile phone security, and more than 55,000 new mobile malware strains are being found every day at the labs [1].

Figure 1 shows the Security Architecture for Mobile WAP-based Devices. The number of mobile devices is increasing very fast, in 2011; device activations have risen 250% and app downloads from Google's “Play” market have topped 11 billion and counting [4]. On average, only 10% of the approximately 86 million devices in use today are secured [3].

----

* Corresponding author.

E-mail address: moanassar@yahoo.com.

Vulnerability occurs when three elements intersect, including a system weakness or flaw, attacker access to the flaw, and attacker competence to exploit the flaw [2].

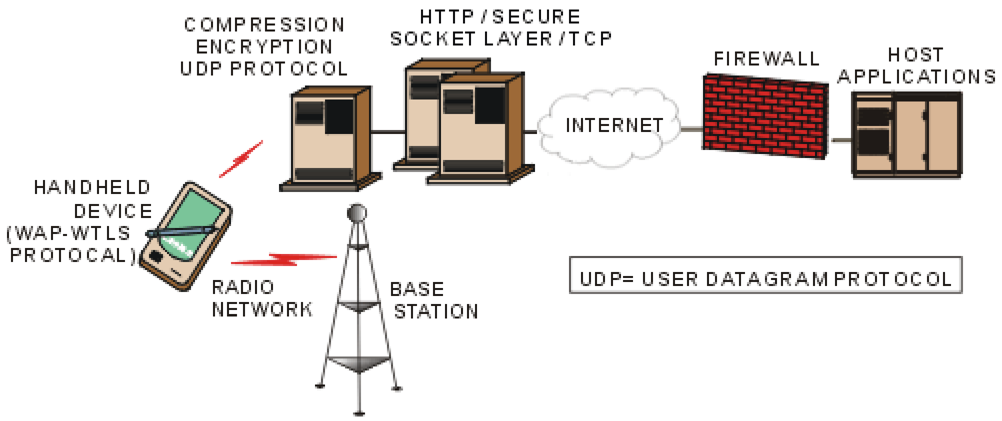

Figure 1: A Schematic of Security Architecture for Mobile WAP-based Devices

2. Mobile Networks vulnerabilities and Mobile Applications Threats

The goal of this step is to identify vulnerabilities to the system using the information gathered so far. A threat is the adversary’s goal, or what an adversary might try to do to a sys-tem [6]. Vulnerability is a weakness in security system. This section will present a set of vulnerabilities related to Mobile Networks:

2.1 Lack of centralized management in mobile networks:

The absence of management makes the detection of attacks difficult because it is not easy to monitor the traffic in a highly dynamic and large scale network.

2.2 Resource availability:

Resource availability is a major issue in mobile networks and it must be guaranteed.

2.3 Scalability:

scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

2.4 Cooperativeness:

Routing algorithm usually assume that nodes are cooperative and non-mailicious. This will allow the attacker to become an important routing agent and disrupt network operation.

2.5 Dynamic topology:

The dynamic topology nature of mobile networks may disturb the trust relationship among nodes.

3. Mobile Applications Threats

Threats to mobile applications can be classified into six categories:

1. Data loss due security vulnerabilities

2. Unauthorized data collection

3. Data exposure to other applications

4. Data exposures on the device

5. Data exposures over the network

6. Private data collection

4. Standards to evaluate the security of mobile network

We choose to use the well-known security aspects of Confidentiality, Integrity, Avail-ability, and Authentication (CIAA) as a starting point to evaluate the security of mobile network, this method is dynamically extensible to new threats, Also CIAA is valid over different time periods and different systems [7].

4.1 Availability:

Availability means the assets are accessible to authorized parties at appropriate times.

4.2 Confidentiality:

Confidentiality ensures that computer-related assets are accessed only by authorized parties [5].

4.3 Integrity:

Integrity means that assets can be modified only by authorized parties or only in authorized way.

4.1 Authentication:

Authentication enables a node to ensure the identity of peer node it is communicating with.

4.4 Nonrepudiation:

Nonrepudiation ensures that sender and receiver of a message cannot deny that they have ever sent or received such a message.

4.4 Anonymity:

Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

5. Security Attacks

Understanding the possible attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. This section will summarize the various possible attacks related to mobile devices:

5.1 Eavesdropping:

Data interception can occur when an attacker is eavesdropping on communications originating from or being sent to a mobile device. Electronic eavesdropping is possible through various techniques, such as (1) man-in-the-middle attacks,(2) WiFi sniffing etc [3].

5.2 Black hole Attack

The attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it [9].

5.3 Wormhole Attack:

The attacker receives packets at one point in the network then “tunnels” them to another point in the network, and then replays them into the network from that point.

5.4 Malware:

Malware is often disguised as a game, utility, or other useful third-party software application to initiate a wide range of attacks and spread itself onto other devices.

5.5 Byzantine attack:

A set of intermediate nodes that working alone within network carry out attacks such as creating routing loops

5.6 Phishing:

Phishing [3] is a scam that frequently uses e-mail or pop-up messages to deceive people into disclosing sensitive information.

5.7 Rushing attack:

Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route [8].

5.8 Replay attack:

An attacker retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously [9].

5.9 Router Protocol Poisoning:

In this attack an intruder causes the disruption by poisoning the routing protocol. Securing these attacks is important because the routing protocol forms the basis of network operations, and any corruption of the protocol may lead to significant consequences. These attacks on the Mobile Ad Hoc Networks can lead to looping, congestion, sub optimal routing and partitioning [14].

5.10 Flooding:

The attcker nodes inject false packets into the network [15].

5.11 Sinkhole:

The node tries to attract the data to itself from all neighboring nodes.

5.12 Spoofing:

Attackers may create fraudulent websites to “spoof” legitimate sites and in some cases may use the fraudulent sites to distribute malware to mobile devices.

5.13 Jamming:

The attacker keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

5.14 Replay Attack

The attacker collects data as well as routing packets and replays them at a later moment in time

5.15 Sybil attack:

The attacker tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods.

5.16 Desynchronization attack:

The attacker repeatedly forges messages to one or both end points which request transmission of missed frames.

5.17 Zero-day exploit:

A zero-day exploit takes advantage of a security vulnerability before an update for the vulnerability is available [10].

5.18 Overwhelm attack:

The attacker overwhelm network nodes, causing network to forward large volumes of traffic to a base station.

5.1 Denial of service attack:

Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network [15].

5.19 Gray-hole attack:

This attack leads to dropping of messages.

5.1 Man-in-the-middle attack:

An attacker sites between the sender and receiver and sniffs any information being sent between two nodes.

5.20 Fabrication:

This attack includes the generating false routing messages [5].

5.21 Traffic Monitoring:

Monitoring traffic to launch further attacks.

5.22 Traffic Analysis:

Monitoring the traffic o gain information on which nodes communicate with each other and how much data is processed.

6. Security Controls for Mobile Devices

6.1 Enable user authentication:

Devices can be configured to require passwords or PINs to gain access [16].

6.2 Enable two-factor authentication:

For sensitive transactions Two-factor authentication can be used when conducting sensitive transactions on mobile devices. Authentication protects host [17] by preventing agent pretending as host. This is achieved through shared key for encryption messages or privacy.

6.3 Verify the authenticity of downloaded applications:

Procedures can be implemented for assessing the digital signatures of downloaded applications to ensure that they have not been tampered with [11].

6.4 Install antimalware capability:

Antimalware protection can be installed to protect against malicious applications, viruses, spyware, infected secure digital cards, and malwarebased attacks.

6.5 Install a firewall:

A personal firewall can protect against unauthorized connections by intercepting both incoming and outgoing connection attempts and blocking or permitting them based on a list of rules [11].

6.6 Receive prompt security updates:

Software updates can be automatically transferred from the manufacturer or carrier directly to a mobile device.

6.7 Remotely disable lost or stolen devices:

Remote disabling [12] is a feature for lost or stolen devices that either locks the device or completely erases its contents remotely.

6.8 Enable encryption for data stored on device or memory card:

Enable encryption for data stored on device or memory card can protect the information on mobile devices.

6.9 Adopt centralized security management:

Centralized security management [13] can ensure an organization’s mobile devices are compliant with its security policies.

6.10 Implement a virtual private network (VPN):

A VPN [13] can provide a secure communications channel for sensitive data transferred across multiple, public networks during remote access.

6.11 Use public key infrastructure (PKI) support:

PKI issued a digital certificates can be used to digitally sign and encrypt emails.

6.12 Install an enterprise firewall:

A firewall can be configured to isolate all unapproved traffic to and from wireless devices.

6.13 Monitor and control devices:

Devices can be monitored and controlled for messaging, data leakage, inappropriate use, and to prevent applications from being installed.

6.14 Enable, obtain, and analyze device log files for compliance Log files:

Log files can be reviewed to detect suspicious activity and ensure compliance.

7. Conclusions and Recommendations

There appears to be a distinct lack of literature regarding mobile security, this paper is an attempt to covers the available Wireless & Mobile Computing Security challenges and their possible solutions. The shift to mobile is a major transition from the PC era, requiring enterprise IT to consider a new approach to securing corporate data and minimizing risk. Securing enterprise content on mobile requires IT to adopt new management tools and security strategies given the differences in the way mobile operates compared to PCs. However, those organizations that take a mobile first approach and address new requirements will enjoy the benefits that result, which include marked competitive differentiation and heightened innovation.

References

[1] N. Leavitt, "Mobile security: Finally a serious problem," Computer, vol. 6, no. 44, pp. 11-14, 2011.

[2] “The Three Tenents of Cyber Security,” n.d.. [Online]. Available: http://www.spi.dod.mil/tenets.htm. [Accessed 1 January 2012].

[3] T. Blitz, "Decoding mobile device security," Security, vol. 5, no. 42, pp. 46-47, 2005.

[4] Google Mobile Blog, “Android and Security,” 2 February 2012. [Online]. Available: http://googlemobile.blogspot.com/2012/02/android-andsecurity.html. [Accessed 1 January 2012].

[5] S. Desilva, and R. V. Boppana, “Mitigating Malicious Control Packet Floods in Ad Hoc Networks,” Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[6] Swiderski, F., and Snyde, W.: Threat Modeling. Microsoft Press, (2004).

[7] Myagmar, S., and Yurcik, W.: Why Johnny Can Hack: The Mismatch Between Vulnerabili-ties and Security Protection Standards. IEEE International Symposium on Secure Software Engineering (ISSSE), McLean, March (2006).

[8] C. Perkins and E Royer, “Ad Hoc On-Demand Distance Vector Routing,” 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., 1999.

[9] D. Johnson and D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[10] GAO-12-757,” INFORMATION SECURITY: Better Implementation of Controls for Mobile Devices Should Be Encouraged”,2012,[Online]. Available : http://www.gao.gov/648519.pdf

[11] ” McAfee Labs 2012 Threats Predictions ”, [Online].Available:http://blogs.mcafee.com/consumer/mcafee-labs- 2012-threats-predictions.

[12] Sophos, “Security Threat Report,” 2010. [Online].Available: http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf

[13] ”Security solutions available and proposed”,2012.[Online] Available: http://www.zdnet.com/search?q=security+solutions+available+and+proposed.

[14] P. Papadimitratos and Z. Haas, “Secure Routing for Mobile Ad Hoc Networks,” Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, 2002, pp. 27-31.

[15] P. Michiardi and R. Molva, “Prevention of Denial of Service Attacks and Selfishness in Mobile Ad Hoc Networks,” Research Report RR-02-063, Institute Eurecom, 2002.

[16]] S. Buchegger and J. Boudec, “Nodes Bearing Grudges: Towards Routing Security, Fairness and Robustness in Mobile Ad Hoc Networks,” Proceedings of 10th Euromicro Workshop on Parallel, Distributed and Networkbased Processing, Canary Islands, 2002, pp. 403-410.

[17] S. Funfrocken, “Protecting Mobile Web-Commerce Agents with Smartcards,” Proceedings of the 1st International Symposium on Agent Systems and Applications, Palm Springs, California, 1999, pp. 90-102.