ISSN-2230-9659

Wireless Security Threats and Risk Mitigation

Kailash Aseri
M.Tech. (Cs) Scholar, Manav Bharti University,
Solan (H.P.)

ABSTRACT:-

Computer Security generically classifies security threats in nine categories ranging from errors and omissions to threats to personal privacy. All of these represent potential threats in wireless networks as well. However, the more immediate concerns for wireless communications are device theft, denial of service, malicious hackers, malicious code, theft of service, and industrial and foreign espionage. Theft is likely to occur with wireless devices because of their portability. Authorized and unauthorized users of the system may commit fraud and theft; however, authorized users are more likely to carry out such acts. Since users of a system may know what resources a system has and the system's security flaws, it is easier for them to commit fraud and theft. Malicious hackers, sometimes called crackers, are individuals who break into a system without authorization, usually for personal gain or to do harm. Malicious hackers are generally individuals from outside of an agency or organization (although users within an agency or organization can be a threat as well). Such hackers may gain access to the wireless network access point by eavesdropping on wireless device communications. Malicious code involves viruses, worms, Trojan horses, logic bombs, or other unwanted software that is designed to damage files or bring down a system. Theft of service occurs when an unauthorized user gains access to the network and consumes network resources.

ISSN-2230-9659

INTRODUCTION

Industrial and foreign espionage involves gathering proprietary data from corporations or intelligence information from governments through eavesdropping. In wireless networks, the espionage threat stems from the relative ease with which eavesdropping can occur on radio transmissions. Attacks resulting from these threats, if successful, place an agency's systems—and, more importantly, its data—at risk. Ensuring confidentiality, integrity, authenticity, and availability are the prime objectives of all government security policies and practices. information must be protected from unauthorized, unanticipated, or unintentional modification. Security requirements include the following:

- **Authenticity**—A third party must be able to verify that the content of a message has not been changed in transit.
- **Nonrepudiation**—The origin or the receipt of a specific message must be verifiable by a third party.
- **Accountability**—The actions of an entity must be traceable uniquely to that entity.

Network availability is "the property of being accessible and usable upon demand by an authorized entity."

Risks in wireless networks are equal to the sum of the risk of operating a wired network (as in operating a network in general) plus the new risks introduced by weaknesses in wireless protocols. To mitigate these risks, agencies need to adopt security measures and practices that help bring their risks to a manageable level. They need, for example, to perform security assessments prior to implementation to etermine the specific threats and vulnerabilities that wireless networks will introduce in their environments. In performing the assessment, they should consider existing security policies, known threats and vulnerabilities, legislation and regulations, safety, reliability, system performance, the life-cycle costs of security measures, and technical requirements. Once the risk assessment is complete, the agency can begin planning and implementing the measures that it will put in place to safeguard its systems and lower its security risks to a manageable level. The agency should periodically reassess the policies and measures that it puts in place because computer technologies and malicious threats are continually changing. To date, the list below includes some of the more salient threats and vulnerabilities of wireless systems:

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.

ISSN-2230-9659

- Malicious entities may gain unauthorized access to an agency's computer or voice (IP telephony)
- Network through wireless connections, potentially bypassing any firewall protections.
- Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- Denial of service (DoS) attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.
- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their physical movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Viruses or other malicious code may corrupt data on a wireless device and be subsequently introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other agencies for the purposes of launching attacks and concealing their activity.
- Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.
- Malicious entities may use a third party, untrusted wireless network services to gain access to an agency's network resources.
- Internal attacks may be possible via ad hoc transmissions.

ISSN-2230-9659

- As with wired networks, agency officials need to be aware of liability issues for the loss of sensitive information or for any attacks launched from a compromised network.

EMERGING WIRELESS TECHNOLOGIES

Originally, handheld devices had limited functionality because of size and power requirements. However, the technology is improving, and handheld devices are becoming more feature-rich and portable. More significantly, the various wireless devices and their respective technologies are merging. The mobile phone, for instance, has increased functionality that now allows it to serve as a PDA as well as a phone. Smart phones are merging mobile phone and PDA technologies to provide normal voice service and email, text messaging, paging, Web access, and voice recognition. Next-generation mobile phones, already on the market, are quickly incorporating PDA, IR, wireless Internet, e-mail, and global positioning system (GPS) capabilities.

Manufacturers are combining standards as well, with the goal to provide a device capable of delivering multiple services. Other developments that will soon be on the market include global system for mobile communications-based (GSM-based) technologies such as General Packet Radio Service (GPRS), Local Multipoint Distribution Services (LMDS), Enhanced Data GSM Environment (EDGE), and Universal Mobile Telecommunications Service (UMTS). These technologies will provide high data transmission rates and greater networking capabilities. However, each new development will present its own security risks, and government agencies must address these risks to ensure that critical assets remain protected.

ISSN-2230-9659

EM Band Designation	Frequency Range	Wireless Device/Application
VLF: Very Low Frequency	9 kHz–30 kHz	
MF: Medium Frequency	300 kHz–3 MHz	AM radio stations (535 kHz–1 MHz)
HF: High Frequency	3 MHz – 30 MHz	
VHF: Very High Frequency	30 MHz–300 MHz	FM radio stations VHF television stations 7–13, NTSC Standard (174 MHz–220 MHz) Garage door openers (~40 MHz) Standard cordless telephones (40 MHz–50 MHz) Alarm Systems (~40 MHz) Paging Systems (50 MHz–300 MHz)
UHF: Ultra High Frequency	300 MHz–3 GHz	Paging systems (300 MHz–500 MHz) 1G mobile telephones (824 MHz–829 MHz) 2G mobile telephone (800 MHz–900 MHz) Global System for Mobile Communication (GSM) Enhanced Data Rates for Global Evolution (EDGE) (800/900/1800/1900 MHz bands) 3G Mobile telephones (international standard) (1,755 MHz–2200 MHz) Bluetooth devices (2.4-2.4835 GHz) Home RF (2.4 GHz ISM Band) WLAN (2.4, 5 GHz)
SHF: Super High Frequency	3 GHz–30 GHz	Applications in the short range, point-to-point communications including remote control systems, PDAs, etc. WLAN (5.8 GHz). Local Multipoint Distribution Services (LMDS), a fixed wireless technology that operates in the 28 GHz band and offers line-of-sight coverage over distances up to 3 to 5 kilometers.
EHF: Extremely High Frequency	30 GHz–300 GHz	Satellite communications
IR: Infrared	300 GHz	Remote controls for home audio-visual components IR links for peripheral devices PDA and cellular telephone IR links

BIBLIOGRAPHY

1. NIST Special Publication 46, *Security for Telecommuting and Broadband Communications*, National Institute for Standards and Technology.

2. Norton, P., and Stockman, M. *Peter Norton's Network Security Fundamentals*. 2000.

3. Wack, J., Cutler, K., and Pole, J. NIST Special Publication 41*, Guidelines on Firewalls and Firewall Policy,* January 2002.

4. Gast, M. *802.11 Wireless Networks: The Definitive Guide Creating and Administering Wireless Networks*, O'Reilley Publishing, April 2002.

5. Arbaugh, W.A., Shankar, N., and Wan, Y.C. "Your 802.11 Wireless Network Has No Clothes." March 30, 2001.

6. Basgall, M. "Experimental Break-Ins Reveal Vulnerability in Internet, Unix Computer Security."http://www.dukenews.duke.edu/research/encrypt.html, January 1999.

7. Cam-Winget, N., and Walker, J. "An Analysis of AES in OCB Mode." May 2001.

ISSN-2230-9659

8. Ismadi, A., and Sukaimi, Y.B. *Smart Card: An Alternative to Password Authentication*. SANS, May 26, 2001.

9. Lucent Technologies. *ORINOCO Manager Suite Users Guide*. November 2000.

10. Menezes, A. “Comparing the Security of ECC and RSA.” January 2000.

11. Cagliostro, C. *Security and Smart Cards*. www.scia.org, 2001.

12. Cardwell, A., and Woollard, S. “Clinic: What are the biggest security risks associated with wireless technology? What do I need to consider if my organization wants to introduce this kind of technology to my corporate LAN?” www.itsecurity.com, 2001.

13. Ewalt, D. M. “RSA Patches Hold in Wireless LANs: The fix addresses problems with the Wireless Equivalent Privacy protocol, which encrypts communication over 802.11b wireless networks.” *Information Week,* (www.informationweek.com), December 2001.

14. Leyden, J. “Tool Dumbs Down Wireless Hacking.” *The Register,* www.theregister.co.uk, August 2001.

15. Marek, S. “Identifying the Weakest Link.” *Wireless Internet Magazine* www.wirelessinternetmag.com, November/December 2001.