Wireless Security: Past, Present and Future

Senior lect. Răzvan Daniel ZOTA, PhD.
Economy Informatics Department, Academy of Economic Studies Bucharest, zota@ase.ro

Very often, wireless security has been seen with strange eyes because it seems somehow counterintuitive that someone can deploy and use a secure network which has no physical access barriers. Despite of that, millions of wireless LANs based on the IEEE 802.11 standard are already in use all over the world. The past was not so happy for the security wireless protocols developed, but the present and the perspective future will make a brighter world for wireless security. This article reveals the past, present and the future of security in the wireless networking.
Keywords: *Wireless Networking, Security, 802.11 Standard, Network security, WEP, EAP, TLS, TKIP.*

1 Introduction

The first wireless security solution for 802.11-based networks, *Wired Equivalent Privacy (WEP)*, received a great deal of coverage due to various technical failures in the protocol. However, users were rapidly adopting wireless networks because of the freedom and mobility they provide. Standards bodies and industry organizations are spending a great deal of time and money on developing and deploying next-generation solutions that address growing wireless network security problems.

The 802.11i IEEE draft standard provides next-generation authentication, authorization, and encryption capabilities. The WiFi Alliance, a wireless industry organization, has jumped the gun and created the WiFi Protected Access (WPA) standard, a subset of the 802.11i draft. These new standards are more complicated than their predecessors but are more scalable and secure than existing wireless networks. They also dramatically raise the bar for attackers and administrators. The new standards will employ a phased adoption process because of the large installed base of 802.11 devices. Proper migration to 802.11i and mitigating the legacy wireless risks will be abumpy road. However, the end result will provide users a secure base for mobile computing needs.

2. The threats of wireless access

To understand the 802.11i protocol and the advantages it offers over existing wireless security mechanisms, we must understand potential attackers and their threats. Knowledge of the real threats against wireless networks will help us place the complex landscape of security mechanisms in context. Depending on your environment and the assets you need to protect, the risks posed by various attackers might vary.

2.1. Targeted attackers

The vision of IT professionals about attackers (or hackers), is often the image of a malicious individual dedicated to breaking into a trusted network. They think of an attacker with a grudge, sitting in a dark dorm room, working late into the night doing stealthy scans, creating custom exploits, and quietly compromising their infrastructure. They think of someone who has nothing better to do than full-time attacking. A dedicated attacker who targets a specific enterprise is an IT pro's worst nightmare, but an unlikely one. Similarly, a targeted wireless attacker also is very unlikely. For an attacker to explicitly target a network, there must be a valuable enough asset for the attacker to pursue. For most home and small office networks, the payoff for breaking into a wireless network is simply too small for an attacker to expend the effort. However, if your enterprise contains valuable trade-secret, financial, or personal information, then the threat of a targeted attacker, even though it's remote, is likely to warrant a more secure solu-

tion than what the legacy WEP mechanism provides.

2.2. Opportunity attackers

Very probably, someone will attack a wireless network because it is a target of opportunity; one that has no functional level of security and that an attacker easily can compromise. Attacker misuses vary wildly on targets of opportunity. Some attackers pursue internal assets on the network, but generally it seems that most attacks simply attempt to gain Internet access. While this type of misuse is technically an attack, the asset's value is low. Using open wireless Internet access points to check email and read news sites is a way of life for some people, so many could argue whether this really is an "attack." However, if users access the open network to launch attacks against external resources and using the wireless network to hide their identities, for example, the case is much more clear-cut. Nonetheless, when a "user" accesses assets without permission, by most definitions, this type of "use" is an attack.

For attackers pursuing more valuable assets such as financial data and trade secrets, targets of opportunity are not a viable way of achieving their goals. Randomly attacking local targets on an open wireless network is not a high-yield activity for dedicated attackers. Typical home or small-office networks have few valuable assets (credit card numbers, personal information, and so on) worth pursuing, assuming the hosts on the network are vulnerable to attack in the first place. Spending an hour hunting for a single credit card number simply is not worth most motivated attackers' time. Large enterprise environments are not likely to be targets of opportunity because they have rudimentary wireless security mechanisms in place.

2.3. The attackers from inside

Often there is another type of attacker which is usually called "accidental." Employees within an enterprise potentially can subvert wireless network security better than targeted attackers. These employees' actions can punch through most defenses, and they underscore the need for wireless network internal auditing. For example, an employee might have difficulty with an existing enterprise wireless network: the network may be difficult to use or provide sub-par coverage in certain areas of a building. To overcome these difficulties, the employee could install a personal desktop wireless access point. While this solution is effective for the employee, it is not acceptable from an IT security standpoint. This rogue access point is outside the IT staff 's control and might not adhere to enterprise security standards. Worse, the access point is an uncontrolled hole into a core network. Rogue access points are difficult to prevent with the current wireless security standards, but 802.11i, in conjunction with a properly engineered wired network, minimizes their vulnerabilities. Similarly, employees can leave their wireless interfaces connected to wireless networks when they dock their workstations using wired network docking stations, thereby providing uncontrolled dual-homed hosts. 802.11i and a properly engineered wired network could mitigate this threat.

3. A summary of wireless security

Very often wireless networks are cited for their lack of physical security. Unlike a wired network, an attacker could be in an unsecured location such as a parking lot or a passing car. Many assume that this level of uncontrolled physical access is a wireless network's worst liability. This is true to an extent. To compromise a wireless network, an attacker must be near enough to interact with the network infrastructure. For high-speed data networks based on 802.11b, the attacker must be within several miles of the targeted wireless network. An attacker in Bucharest cannot attack a wireless network in Sibiu, for example. This requirement for physical proximity limits the potential attacker pools for any given network. Combined with the requirement for physical proximity is the wireless network's explosive growth. The data sets about the explosive growth of wireless, such as those available from NetStumbler (www.netstumbler.com), reflect a large growth in many areas of the world. If the network administrator's concern is to prevent

unauthorized users from accessing the Internet, then using legacy WEP encryption and authentication will raise the bar high enough to stop this kind of access. However, if your enterprise requires security against targeted attackers, then 802.11i will likely be a better solution.

4. Wireless network responses

In order to defend against targeted attackers, wireless networks need a robust and layered protection mechanism. The original 802.11 security protocol (WEP), is insufficient because it is vulnerable to various cryptographic attacks that reveal the shared key used to encrypt and authenticate data. In the last years various publicly available tools have automated these attacks, including Airsnort (http://airsnort.shmoo.com) and WEPCrack (http://wepcrack.sourceforge.net). The WEP protocol also uses a static key that requires manual rotation; this is not practical for even a relatively small number of wireless clients. Finally, WEP's authentication only verifies the client machine, not the actual user accessing the machine.

It is clear that it is a need for a new solution to address these issues and pose a barier counter the possible attacks. The 802.11i IEEE working group's goal is to create a new standard for wireless security. The result is an IEEE draft, which consists of three major parts: *Temporal Key Integrity Protocol (TKIP)* and counter mode cipher block chaining with message authentication codes *(counter mode CBC-MAC)* provide link-layer data confidentiality and integrity while 802.1x provides port-based wireless client access control.

4.1. TKIP

The TKIP protocol is an immediate replacement for WEP. It fixes the well-known problems with WEP, including small initialization vectors (IV) and short encryption keys. TKIP uses RC4, the same symmetric encryption algorithm as WEP, so you can upgrade existing hardware to support the standard. TKIP is not an ideal solution, and all existing applications might not support it, but once it's final it will provide increased security for the millions of 802.11 devices already deployed.

The 802.11i uses TKIP as a stepping-stone to more robust solutions later. TKIP uses 48-bit vectors, which limit existing cryptographic attacks against WEP. Currently, the 24-bit IV WEP uses lets cryptanalysis attackers recover the shared encryption key. Extending the IV to 48-bits limits the scope of this attack. TKIP also utilizes a longer encryption key than WEP's. Forty-bit keys are relatively weak even when properly implemented, but WEP's flaws make its standard 40-bit key weaker than 40 bits, leading to brute-force attacks. The 128-bit WEP addressed this short-key problem but it was never part of an IEEE standard. Each 802.11 vendor implemented 128-bit WEP on its own, and these unique implementations caused problems for heterogeneous environments in which interoperability was an issue.

By using longer keys and implementation standards, TKIP addresses WEP's short-key problem. TKIP uses per-packet keying: a shared base key, a client's MAC address, and a packet's sequence number create a unique key for each packet. Attackers can launch a cryptographic attack against WEP by capturing data for an extended period of time. The attackers then examine the data for patterns that ultimately will disclose the key. TKIP's per-packet keying makes cryptographic attacks impractical by eliminating the threat of attacks based on harvesting large amounts of data encrypted by the same key. TKIP periodically rotates the broadcast key to avoid data-harvesting problems similar to those just discussed. The broadcast key is used for broadcast traffic and 802.1x authentication and it must be rotated for confidentiality of the authentication process. TKIP uses a message integrity code (MIC) to fix problems with undetected WEP modification attacks.

An attacker could store the WEP integrity check value (ICV), change encrypted packets, and update the ICV without knowing the WEP key. This ICV security breakdown prevents remote stations from detecting the modification. MIC uses a cryptographically protected one-way hash in the payload, en-

suring packet-tampering detection immediately upon decryption. TKIP is part of the existing WPA industry standard, and the WiFi alliance is leveraging its built-in upgradeability to convince vendors to deploy TKIP as well as WEP in the near term.

4.2. CBC-MAC

Beside TKIP, another protection mechanism *(Counter mode with CBC–MAC Protocol or CCMP)* has little resemblance to the initial WEP. Wireless network confidentiality, integrity, and authentication were CCMP's design criteria. CCMP uses the 128-bit advanced encryption standard (AES) for data protection rather than RC4; while RC4 is not inherently flawed, AES is the new strong symmetric encryption standard. Hardware vendors are creating robust AES encryption-processing hardware that can handle AES as effectively as today's RC4 encryption hardware. CCMP uses a 48-bit IV to seed the initial key derivation process as well as seed the MIC used in CCMP packets. CCMP encrypts data in 128-bit chunks using cipher block chaining (CBC) mode and provides data integrity checks via a MAC.

The CCMP protocol, like any new cryptographic protocol, has not withstood the test of time and determined attackers, even though it should be the flagship wireless encryption mechanism. If 802.11 networks hope to provide a trustworthy networking platform, CCMP must instill confi- dence in the hearts of network engineers and users. The IEEE 802.11i committee has worked diligently to ensure this happens. CCMP is a required component of any 802.11i implementation. It is set to be part of the second-generation WPA industry standard.

4.3. 802.11x

The IEEE 802.1x protocol is a port-based authentication protocol for Ethernet networks. It protects networks from unauthorized use in open environments (such as in a university campus) where any active network wall port is a hole into the network's infrastructure. 802.1x lets the port stay "hot" but requires authentication before a user receives full network access. This physical port concept now extends to wireless networks. While there are no wall ports, a user must authenticate before being granted full access.

802.1x authentication occurs when a client first joins a network. Then, periodically, authentication recurs to verify the client has not been subverted or spoofed. 802.1x has the added benefit in a wireless network of not inducing a per-packet overhead. This lightweight implementation is important because it does not adversely affect the relatively low throughput of wireless networks. With 802.1x, authentication occurs after an association forms because a wireless client must be able to transmit authentication information to an access point, which requires an association. The catch is that even though the association exists, the access point only lets the client send authentication information. The access point forwards the authentication information to a back-end server via Remote Authentication Dial-In User Service (RADIUS) for verification.

Once the authentication process completes, the authentication server sends a message to the access point that the client has been authenticated and network access should be granted. The response might contain authorization information that the access point can use to enforce local access policies. In 802.11i, the response packet also contains cryptographic keys sent to the client to seed the link-level encryption mechanism.

The 802.1x protocol uses *Extensible Authentication Protocol (EAP)* to handle authentication requests. EAP was originally developed for Point-to-Point Protocol (PPP) connections to provide a more flexible framework for authenticating users. Rather than specifying a fixed authentication mechanism, EAP provides an extensible platform for vendors to implement their own authentication mechanisms. This extensible mechanism "future proofs" 802.1x from vulnerabilities and from changes in authentication processes and implementations. If a security problem were to be discovered in an existing authentication mechanism, the mechanism could be swapped out for a more robust one. Because EAP provides such a flexible and extendable authentication framework, it became part of

802.1x to extend the protocol's longevity. Several common EAP methods have been defined in various Internet Engineering Task Force (IETF) drafts or other industry documents. EAPMD5 is a password-based mechanism for client authentication; while not exceptionally secure, it is easy to implement.

EAP-TLS creates a Transport Layer Security (TLS) session within the EAP authentication process. This is quite an advance over a password authentication mechanism, but it requires users to have certificates installed prior to using the wireless network. This means a complete PKI infrastructure must be in place to use EAP-TLS at the enterprise level. EAP-TTLS and PEAP (Protected EAP) create a secure authentication mechanism in a TLS tunnel. TTLS is TLS authentication in the tunnel, and PEAP lets any other EAP method be used in the tunnel. These allow for secure transport of authentication credentials without the explicit use of a complete PKI installation. Researchers at the University of Maryland have found flaws in 802.1x ("An Initial Security Analysis of the IEEE 802.1x Standard," www.missl.cs.umd.edu/wireless/1x.pdf). These flaws can be mitigated if the 802.1x authentication is performed within an encrypted channel. For this reason, clients are still required to have an initial shared secret with the wireless infrastructure to ensure the initial authentication process's security. Like WEP, the shared key requires some out-of-band distribution mechanism and must be protected from outsiders.

The security community also is examining current EAP methods. Over the next years, churn will be likely in various EAP methods as researchers discover vulnerabilities and address them in later protocol revisions. While TKIP and CCMP are still largely unimplemented by most vendors, 802.1x client support is already integrated into Windows XP and Mac OS X. There is also available an open-source implementation called Open1x which runs on Linux and FreeBSD (www.open1x.org). Access points from vendors such as Cisco and Avaya that understand 802.1x authentication are being shipped from 2003.

5. The future looks brighter

The original 802.11 security mechanisms enabled wireless networking to become a big business industry. However, as attackers have matured, we've come to rely on networks, and we've discovered flaws in the core wireless security protocols. The 802.11i protocol is an attempt to turn wireless networking into a trusted medium for users of all types: TKIP provides enhanced security for existing infrastructure, CCMP is a fresh start for data integrity and confidentiality on the network, and 802.1x is a fully extensible and robust authentication mechanism that allows infrastructures to authenticate users, not just wireless hosts.

Also, in 2004, the Wi-Fi Alliance introduced *Wi-Fi Protected Access 2 (WPA2™),* the second generation of WPA security. Like WPA, WPA2 provides enterprise and home Wi-Fi users with a high level of assurance that their data will remain protected and that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard ratified in June 2004. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is eligible for FIPS (Federal Information Processing Standards) 140-2 compliance. Launched in September 2004 by the Wi-Fi Alliance, WPA2 is the certified interoperable version of the full IEEE 802.11i specification which was ratified in June 2004.

Like WPA, WPA2 supports IEEE 802.1X/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES). AES satisfies U.S. government security requirements. It has been adopted as an official government standard by the U.S. Department of Commerce and the National Institute of Standards and Technology (NIST). Organizations that require the AES encryption avail-

able in WPA2 should be aware that upgrading to it may require new hardware.

References

1. AirDefense, *Wireless LAN Security: What Hackers Know That You Don't*, Whitepaper, www.airdefense.net, 2005
2. AirMagnet, Inc., *The Top Seven Security Problems of 802.11 Wireless*, Whitepaper, www.airmagnet.com, 2004
3. Convery S., *General Design Considerations for Secure Networks,* Cisco Press, January 2004
4. Intel Corporation, *Intel Building Blocks for Wireless LAN Security*, Whitepaper, http://developer.intel.com, 2003
5. Potter B., *Wireless Security's Future*, IEEE Security & Privacy Magazine, July-August 2003
6. Preston G., *Next-Gen Nets Need Next-Gen Security*, http://networkingpipeline.bitpipe.com/, 12 November 2004
7. *Wi-Fi Alliance, Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise,* Whitepaper, March 2005.