History and implementation of IEEE 802 security architecture

Meareg Abreha

Department of Computer Science, Addis Ababa University,

Addis Ababa, Ethiopia

mearegab@gmail.com

Abstract

Security is a dynamic trend that demands continuous innovation as advancement in computing serves both those who want security and those others who want to breach. Through the years, security on the IEEE 802 has passed through various generations of evolution. Each security implementation has been a stepping stone to the next better architecture. Dozens of security techniques were invented and while many of them were filtered out to be replaced by better ones, others still persist with little or no modification.

This paper discusses the characteristics and pitfalls of previous security mechanisms that led to the continuous evolution of the IEEE 802 security architecture and implementations in brief, but in a phased manner. Emphasis has been given to a select of security architectures that suitably qualify the measurement parameters used in this paper such as access control and confidentiality.

Keywords: IEEE 802, IEEE 802 security, IEEE security, network security, security architecture

1. Introduction

Nowadays security is a must have feature, not a luxury, for any networking standard that wants to be taken seriously. Security implementation on IEEE 802 started back in the 1990s barely as proof of concept of number theory's application in computer security. Soon enough, it became clear that security was a tough issue and techniques, before implementation, needed thorough analysis and revision from experts. We can visualize security easily in terms of authentication or access control in one facet and confidentiality along data integrity on the other. The reason these parameters serve as gauges of security architecture is because they provide the possible means to control entities, such as clients and resources, in a given network.

The wired network standard, Ethernet, has pioneered in an implementation of an access control mechanism and was later ported to the wireless standards with some modifications.

Confidentiality was not much of an issue with the wired technologies for obvious but non-scalable reasons. Closed medium in wired networks plays a security role as much of the information exchange and client information is hidden away from attackers unless they have direct access to routes. It was only with the rise of wireless technologies that confidentiality started to become a serious matter. User information was floating in the air which was an open invitation to attackers. This has led to a series of cryptographic techniques development for ciphering data exchange between users. Data integrity on the other hand is a task that depends on the success of the above security facets. Thus, if there is better confidentiality and authentication then achieving data integrity is much easier.

2. Access Control and Authentication

Access control is important in networks where resources need to be managed effectively and even when privacy is needed. In networks with access control, users who want to access resources first need authenticate themselves and, also, level of resource access can be subject to their authorization status.

Extensible Authentication Protocol (EAP) [5] is a point-to-point protocol [6] based standard authentication mechanism for the 802.1x [3]. IEEE 802.1x is a standard for port-based Network Access Control, originally developed for IEEE 802.3 (Ethernet), now provides an authentication mechanism to devices wishing to attach to a LAN or Wireless LAN [4]. This port-based network access control uses the physical characteristics of the switched LAN infrastructure to authenticate devices attached to a LAN port. Access to the port can be denied if the authentication process fails.

IEEE 802.1x contains three components: Authenticator, Supplicant and also an Authentication server [5]. Authenticator Port Access Entity (PAE) enforces authentication before allowing access to services accessible using that port. The authenticator's port-based access control defines two types of logical ports that access the wired LAN by means of a single physical LAN port: One is the Uncontrolled Port, which allows an uncontrolled exchange between the authenticator (the wireless AP) and other networking devices on the wired network regardless of any wireless client's authorization state. The other is Controlled Port, and allows data to be sent between a wireless client and the wired network only if the wireless client is authorized by 802.1x.

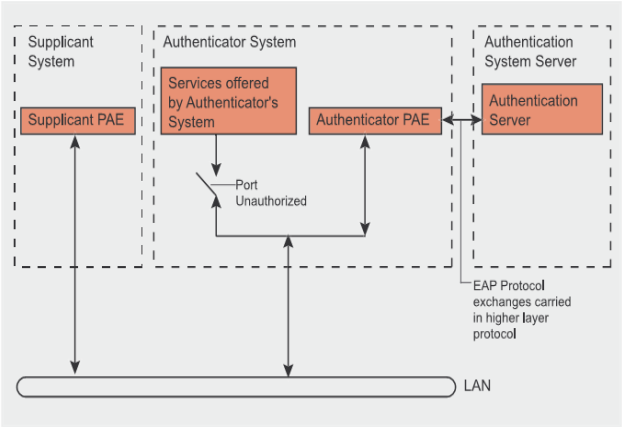

Figure 2.1 IEEE 802.1x model from the IEEE 802.1x specification [12]

In wireless LANs because multiple wireless clients contend for access to the same frequency channel and send data using the same channel, an extension to the basic IEEE 802.1x protocol is required to allow a wireless AP to identify the secured traffic of a particular wireless client.

To adapt EAP messages to be sent over Ethernet or wireless LAN segments, the IEEE 802.1x standard defines EAP-Over-LAN (EAPOL), a standard encapsulation method for EAP messages [21].

Even though 802.1x does not specify what kind of back-end authentication server must be present, but Remote Authentication Dial-In User Service (RADIUS) [**7**] is the de-facto back-end authentication server used in 802.1x.

The 802.11i standard of the WLANs uses the 802.1x/EAP mechanism to authenticate users when used in enterprise mode (when an authentication server is available). Mutual authentication is supported with hierarchy of keys generation and exchange between users [19].

The IEEE 802.15.1 (Bluetooth) standard uses a challenge-response scheme as an authentication mechanism where a specific implementation is dependent on the application used [22]. Even though the IEEE 802.15.4 doesn't specify a specific authentication implementation, in Zigbee (an upper layers extension on top of the base standard) a trust center/coordinator uses a shared network key request mechanism to nodes before it allows them to join the network [23].

IEEE 802.16 (WiMAX) performs RSA based authentication function using X.509 digital certificates or uses an EAP based authentication mechanism [24]. In IEEE 802.20, a standard for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility, implements an EAP based authentication through its Basic EAP Support Protocol in its Services Sublayer [27].

The IEEE 802.21, a standard for optimization of handover between heterogeneous IEEE 802 networks, establishes Message Independent Handover (MIH) Security Association through TLS, (D)TLS handshake or EAP execution over the MIH protocol [28]. The IEEE 802.22, a

standard for using white spaces in the television frequency spectrum, implements an EAP-TLS or EAP-TTLS as an authentication mechanism using X.509 digital certificate profiles based on RSA or Elliptic Curve Cryptography (ECC) [29].

3. Data Confidentiality and Integrity

Though data confidentiality is not as famous as in the wireless, the wired (Ethernet) network too also has some implementations. The IEEE 802.1AE standard defines a Layer 2 security protocol called Medium Access Control Security (MACSec) that provides point-to-point security on Ethernet links between nodes for securing wired LANs.

Before the 2010 revision of the IEEE 802.1x, there was no mechanism to help ensure the confidentiality or integrity of the traffic sent after authentication. Thus, attackers with physical access to the authenticated port could tamper traffic and other conventional protection mechanisms such as MAC address filtering that can by passed easily by spoofing techniques.

But fortunately the 2010 revision modified IEEE 802.1x to provide data confidentiality to wired LANs, besides authentication, by integrating the MACsec protocol of the IEEE 802.1AE standard with EAP Over LAN and IEEE 802.1AR (Secure Device Identity, DevID) [25] to support service identification [8].

Data confidentiality has been tightly related to the wireless technologies for the reason of medium vulnerability as stated in the introduction. Confidentiality and data integrity has been first introduced to IEEE 802.11 (Wi-Fi) with the use of the RC4 algorithm [9] incorporated as a cryptographic technique in the IEEE 802.11 1999 standard [1].

In 1999 the IEEE 802.11 standard included the first Wireless LAN security protocol called Wired Equivalent Privacy (WEP). WEP played the role of security protocol for WLANs till 2001 when its weaknesses started to be revealed. Using RC4 algorithm for encryption and data integrity was the main source of WEP's weaknesses [10]. WEP does not prevent forgery of frames or replay attacks, uses weak RC4 keys and reuses Initialization Vectors (IV) which made data decryption possible with cryptanalytic methods or data modification without knowing encryption key and lack of key management [11, 12, 13].

The IEEE Task Group I of the 802.11 was formed to replace the original privacy mechanism, the WEP algorithm, provided by the initial 802.11 standard with an enhanced security as well as support to legacy protocols for backward compatibility [2, 14]. The IEEE 802.11i is based on IEEE 802.11 standard with security enhancement in the MAC layer [15].

The final draft was ratified on the 24th of June, 2004 as 802.11i [19] and was included in the 2007 amendment of the IEEE 802.11.

Wi-Fi Protected Access (WPA) is an interim protocol security of the 802.11i which was designed to temporarily serve as a transitional protocol replacing WEP as it addresses all known vulnerabilities issues of WEP. Major changes over WEP include that it uses an enhanced encryption scheme, Temporal Key Integrity Protocol (TKIP) and also incorporates the 802.1x/EAP authentication. TKIP, still uses RC4 though, removes the predictability of keys by using a key hierarchy and key management methodology, by leveraging the 802.1x\EAP framework. Data integrity is ensured through Message Integrity Check (MIC) or also known as Michael [18].

The final IEEE security protocol which fully satisfies the 802.11i requirements is called Wi-Fi Protected Access Version 2 (WPA2). The predecessor, WPA, nevertheless it avoided several of the WEP's weaknesses; it has been subject to various attacks [15, 16, 17]. WPA2 unlike WPA includes specification for IBSS (Independent Basic Service Set), pre-authentication, and Advanced Encryption Standard's (AES) [26] implementation of Counter Mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) protocol (CCMP) instead of TKIP.

In 2009, the 802.11w standard, an amendment to 802.11i, for protecting management frames was ratified. This security standard aims at avoiding Denial-of-Service (DoS) caused by spoofed disconnect attacks. Management frames' spoofing was possible as they were sent in plain texts which open doors for spoofed de-authentication and disassociation or authentication or association requests in existing connection [20].

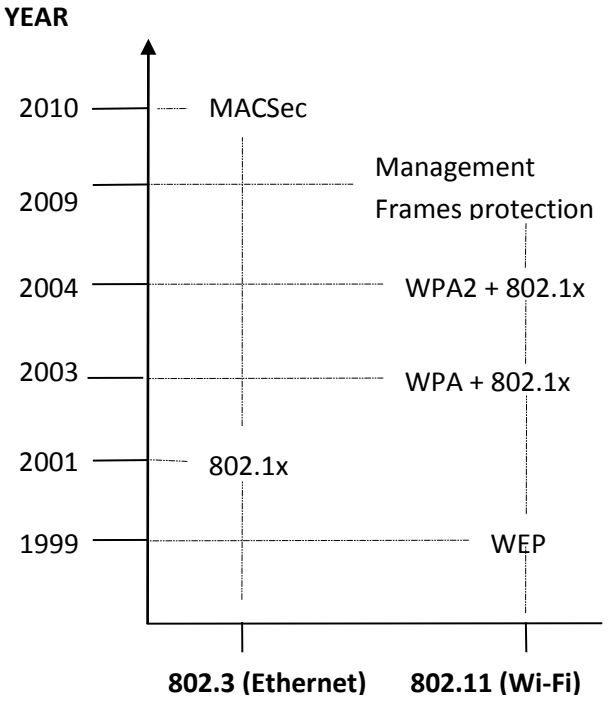

Figure 3.1 Timeline of security amendments in the Ethernet and Wi-Fi standards

The IEEE 802.15.1 Bluetooth standard generates a symmetric encryption key from an authentication key generated earlier and uses it to user data symmetric encryption. It has three

modes of encryption settings. These are *no encryption:* where communication is in plain text or *point-to-point only encryption:* which signifies no broadcast messages are encrypted and *point-to-point and broadcast encryption:* where all messages are encrypted [22].

IEEE 802.15.4, a standard for Low-Rate Wireless Personal Area Networks, defines in a frame by frame basis the Security Level field for deciding the varying degrees of optional protection levels that can be provided and supports up to 128 bits symmetric keys based encryption [23].

Privacy, in IEEE 802.16 standard has two component protocols: an encapsulation protocol to secure data across the fixed Broadband Wireless Access network and a key management protocol to provide secure distribution of keying data from the Base Station to the Server Station. It supports data encryption with Data Encryption Standard (DES) or AES in modes such as CBC and also message authentication functions such as HMAC or CMAC are supported [24].

In IEEE 802.20 standard, AES is used for encrypting and decrypting Radio Link Protocol packets. Message integrity is achieved through AES CMAC function [27].

In the 802.21 standard, Media Independent Handover (MIH) messages can be protected by TKIP or CCMP mechanisms if they are transported over layer 2 or by IPSec if they are transported over the IP layer and implements the HMAC-SHA1-96 algorithm for message authenticity [28].

Protection mechanisms in the IEEE 802.22, a standard for Wireless Regional Area Networks (WRANs), are divided into two security sublayers that target non-cognitive as well as cognitive functionality of the system and the interactions between the two [29]. In sublayer 1 Encapsulation Protocol defines a set of supported cryptographic suites for securing packet data over the air. AES in GCM (Galois Counter Mode), the only data encryption and authentication algorithm supported in IEEE 802.22 is applied to MAC PDU payload when required by the selected ciphersuite. The function of the security sublayer 2 at the cognitive plane is to provide protection for the incumbents as well as protection to the IEEE 802.22 systems against DoS attacks of various types targeted at the cognitive functions of the IEEE 802.22 systems.

4. Conclusion

In the early days, the first generation of IEEE 802 Security began with simple implementation of cryptographic techniques such as RC4. But advancements in computing power and the availability of tools to exploit weaknesses of techniques posed practical attacks and pushed

stakeholders to revise techniques. The second which is also known as current generation of security protocols included implementation of stronger cryptographic techniques such as DES and AES with various modes of operations.

Although security is improved, the power of computing, as Moore's law estimates, is increasing dramatically. Besides the trend in computing power, cloud computing is also changing the way service is provided. Even though such changes equip clients with tremendous computing and storage powers, they come with greater security challenges. Thus, the next generation of security architectures should focus on scaling the current architectures for cloud systems while introducing stronger and efficient cryptographic techniques.

References

[1] IEEE LAN/MAN Standards Committee. "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." IEEE Std 802.11-1999 (1999, IEEE Computer Society, LAN/MAN Standards Committee)

[2] Benton, Kevin. "The evolution of 802.11 wireless security." *University of Nevada, Las Vegas, Informatics-Spring* (2010).

[3] IEEE LAN/MAN Standards Committee."IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control." IEEE Std 802.1x-2001, June 2001.

[4] IEEE LAN/MAN Standards Committee. "IEEE Std 802.1x™-2004 (Revision of IEEE Std 802-1x-2001)." IEEE Standard for Local and Metropolitan Area Networks, Port-Based Network Access Control, (Dec. 13, 2004, IEEE Computer Society, LAN/MAN Standards Committee).

[5] Aboba, Bernard, L. Blunk, J. Vollbrecht, James Carlson, and Henrik Levkowetz. "RFC 3748-Extensible authentication protocol (EAP)." *Network Working Group* (2004)

[6] Simpson, William. "The point-to-point protocol (PPP) for the transmission of multi-protocol datagrams over point-to-point links." (1992).

[7] Aboba, Bernard, and P. Calhoun. "RFC 3579-RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)." *Internet Society, September* (2003).

[8] IEEE LAN/MAN Standards Committee. "IEEE Std 802.1x-2010 (Revision of IEEE Std 802-1x-2004)." IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control, (Feb. 2010, IEEE Computer Society, LAN/MAN Standards Committee).

[9] Stallings, William. "The RC4 Stream Encryption Algorithm." (2005).

[10] Borisov, Nikita, Ian Goldberg, and David Wagner. "Intercepting mobile communications: the insecurity of 802.11." In *Proceedings of the 7th annual international conference on Mobile computing and networking*, pp. 180-189. ACM, 2001.

[11] Gutjahr, Alexander, and A. Ludwigs. "Wired Equivalent Privacy (WEP) Functionality, Weak Points, Attacks." *Freiburg University. Available From:http://www.data.ks.unifreiburg.de/download/praxisseminarWS*9

[12] Lehembre, Guillaume. "Wi-Fi security–WEP." *WPA and WPA2* (2005): 2-15.

[13] Fluhrer Scott, Itsik Mantin, and Adi Shamir. "Weaknesses in the key scheduling algorithm of RC4." In Selected areas in cryptography, pp. 1-24. Springer Berlin Heidelberg, 2001

[14] Al Naamany, Ahmed M., Ali Al Shidhani, and Hadj Bourdoucen. "IEEE 802.11 wireless LAN security overview." *International Journal of Computer Science and Network Security* 6, no. 5B (2006): 138-186.

[15] Ozasa, Yuko. "A study on the Tews-Weinmann-Pyshkin attack against WEP." *IEICE Technical Report* 2007 (2007): 17-21.

[16] Tews, Erik, and Martin Beck. "Practical attacks against WEP and WPA." In *Proceedings of the second ACM conference on Wireless network security*, pp. 79-86. ACM, 2009.

[17] Ahmad, Md Sohail. "Wpa too!." *DEF CON* 18 (2010).

[18] Stanley, Dorothy, Jesse Walker, and Bernard Aboba. "Extensible authentication protocol (EAP) method requirements for wireless LANs." Request for Comments 4017 (2005).

[19] IEEE Computer Society LAN MAN Standards Committee. "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements, ANSI." *IEEE Std* 802.11i, 2004.

[20] Ahmad, Md Sohail, and Shashank Tadakamadla. "Short paper: security evaluation of IEEE 802.11w specification." In *Proceedings of the fourth ACM conference on Wireless network security*, pp. 53-58. ACM, 2011.

[21] Stanley, Dorothy, Jesse Walker, and Bernard Aboba. "Extensible authentication protocol (EAP) method requirements for wireless LANs." *Request for Comments* 4017 (2005).

[22] IEEE LAN/MAN Standards Committee. "Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)". IEEE Std 802.15.1-2005 (2005)

[23] IEEE LAN/MAN Standards Committee. "IEEE Std.802.15.4: IEEE Standard for Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks." IEEE Std 802.15.4-2003 (2003)

[24] IEEE LAN/MAN Standards Committee. "IEEE Standard for Air Interface for Broadband Wireless Access Systems." IEEE Std 802.1-2012(Revision of IEEE Std 802.16-2009) (2012).

[25] IEEE Standards Association. "IEEE 802.1 AR Secure Device Identifier." (2009).

[26] Daemen, Joan, and Vincent Rijmen. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.

[27] IEEE, "IEEE STD 802.20-2008: Standard for Local and Metropolitan Area Networks: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility-Physical and Media Access Control Layer Specification", IEEE-SA Standards Board, 2008.

[28] IEEE LAN/MAN Standards Committee. "IEEE Standard for Local and metropolitan area networks-Part 21: Media Independent Handover Services Amendment 1: Security Extensions to Media Independent Handover Services and Protocol." IEEE Std. 802.21a™-2012, May 2012.

[29] IEEE Standards Association. "Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands." *IEEE Std* (2011): 802-22.