B-3. DEVELOPMENT OF THE AUTHENTICATION RELIABILITY AND SECURITY SYSTEM FOR WIRELESS LOCAL AREA NETWORK

Victor Gopeyenko, Sergejs Bobrovskis

ISMA University of Applied Sciences, Department of Natural Sciences and Computer Technologies,
Lomonosova 1, LV-1019, Riga, Latvia
e-mail: viktors.gopejenko@isma.lv; serg_lv@hotmail.com

Abstract. Wireless network, whether it's an ad-hoc or at an enterprise level is vulnerable due to its features of open medium, and usually due to weak authentication, authorization, encryption, monitoring and accounting mechanisms.

Various wireless vulnerability situations as well as the minimal features that are required in order to protect, monitor, account, authenticate, and authorize nodes, users, computers into the network are examined. Also, aspects of several IEEE Security Standards, which were ratified and which are still in draft are described.

Keywords: Authentication; Encryption; 802.11 standards; 802.1X framework; Extensible Authentication Protocol; Robust Secure Network; Network Access Protection; Wireless Intrusion Detection System; Wireless Intrusion Prevention System; Wired Equivalent Privacy.

General. In order to develop a modern, secure and reliable wireless authentication scheme technological process has passed various evolutionary stages. In the modern world these steps refer to legacy frameworks and security practices, which are widely spread across the universe but are unacceptable within the enterprise environment. New standards and amendments are constantly being developed to address various challenges and problems ranging from defining new areas of application for wireless communication.

Wi-Fi telecommunication systems advance resilience, capacity, productivity and potentiality of end-points (users or consumers). In the beginning the technological idea of data (frames) transmission across an open-medium didn't take into account feasible risks behind the scene. Thus, it facilitates the possibilities for malicious entities to expose information or data of interests by eliminating physical world boundaries like a wired network infrastructure.

Taking into account that fulminant globalization has become the central achievement of the 21st century, now the enterprise/organization competitive abilities depend on technological advantages used in-house, implemented security practices, customer credibility level, ease of access to information of concern, and etc.

The most common and widespread forms of communication between various devices are wired and wireless modes of data transmission. Wired communication refers to the transmission of data through a wire medium (physical data transmission), thus it's more secure by definition. Wireless communication is the transfer of information between the end-points that are not connected by an electrical conductor [1].

The role and function of wireless communication is mainly an extension to wired network, which increases productivity, responsiveness, availability, and accessibility for customers and enterprise users.

The main disadvantage on relying on wireless network is that data (packets) could be easily and clandestinely intercepted for further analysis if legitimate safeguard mechanisms and means aren't in-place for protection. In addition, wired network must not be underestimated, thus worldwide known best security practices should be also implemented.

There are several indispensable fields which must be taken into account to the extent of securing the enterprise facing wireless hazards: Ethernet (wired) and wireless protection, Security policies and procedures, Rules of conduct, Acceptable use policies, Peripheral device security, Employee's awareness program.

This article researches the security inference of wireless local area network (LAN) from the angle of developing and building a stable, reliable and secure authentication method used within highly protected enterprise environment; and come across with comprehensions crucial establishing secure communication between the entities involved. This paper explores various combinations of technologies, frameworks and best-practices used across enterprise organizations securing wireless telecommunication base on scheme AAA process (Fig.1).

Regardless of the authentication, authorization, accounting methods used within this framework, messages (frames) flying back and forth are called EAPOL messages. Three entities are involved in order to establish a proper communication and flaw of frames [1]:

1. Supplicant – the software installed on a client's computer. In our case we use the vendor proprietary software called Juniper Odyssey Access Client.
2. Authenticator – this specific device stands in-between Supplicant and Authentication Server and plays a secure proxy role. In most cases its Wi-Fi router from Juniper or Cisco vendors. In our case we use Cisco AIR-CAP3602I-E-K9, it's capable to handle and provide all requirements necessary for establishing RSN. In order to receive a more in-depth explanation concerning this product please visit Cisco website.

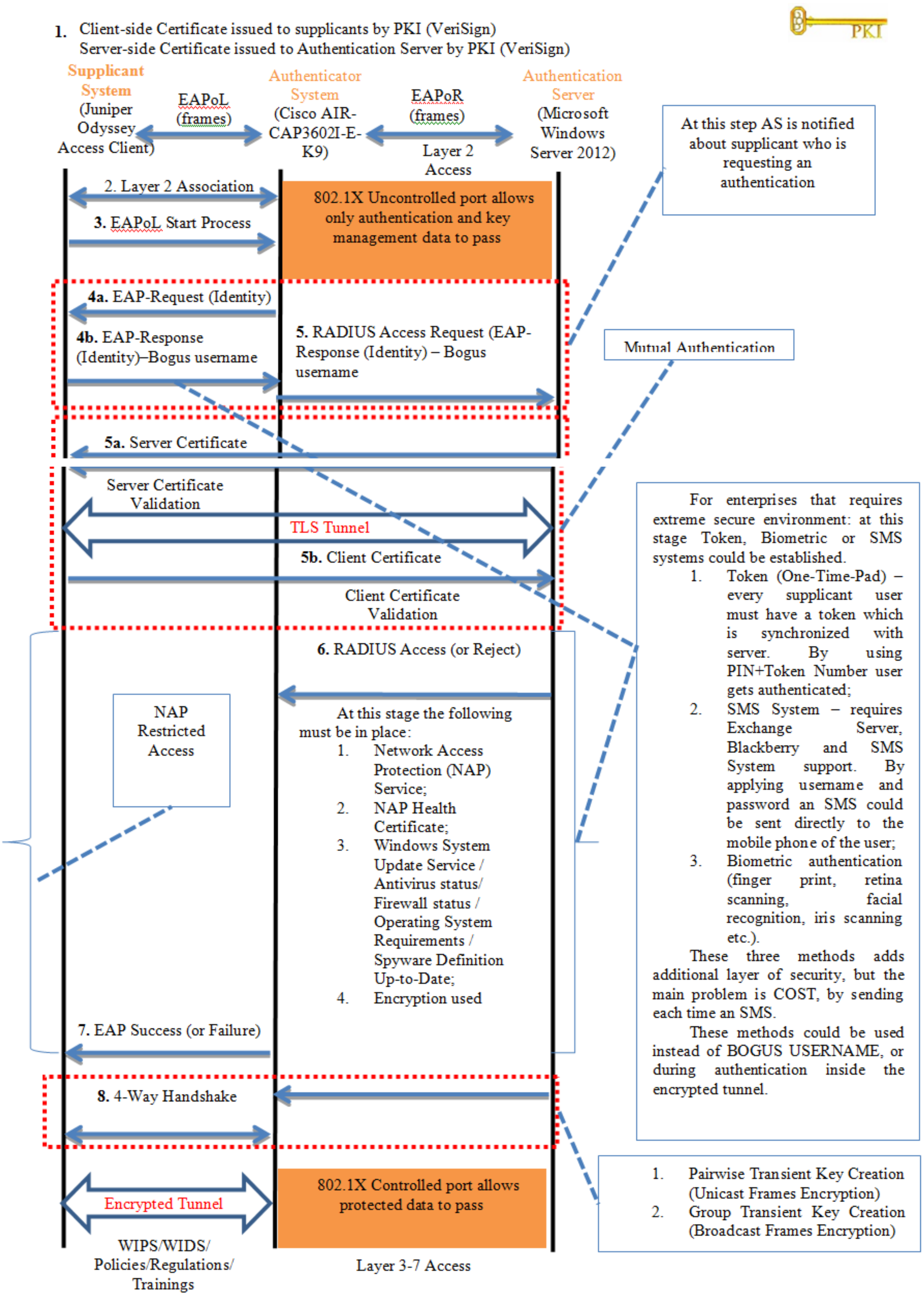
PKI
1. Client-side Certificate issued to supplicants by PKI (VeriSign)
Server-side Certificate issued to Authentication Server by PKI (VeriSign)
Supplicant System (Juniper Odyssey Access Client)
EAPoL (frames)
Authenticator System (Cisco AIR-CAP3602I-E-K9)
EAPoR (frames)
Layer 2 Access
Authentication Server (Microsoft Windows Server 2012)
At this step AS is notified about supplicant who is requesting an authentication
2. Layer 2 Association
3. EAPoL Start Process
802.1X Uncontrolled port allows only authentication and key management data to pass
4a. EAP-Request (Identity)
4b. EAP-Response (Identity)–Bogus username
5. RADIUS Access Request (EAP-Response (Identity) – Bogus username
Mutual Authentication
5a. Server Certificate
Server Certificate Validation
TLS Tunnel
5b. Client Certificate
Client Certificate Validation
6. RADIUS Access (or Reject)
NAP Restricted Access
At this stage the following must be in place:
1. Network Access Protection (NAP) Service;
2. NAP Health Certificate;
3. Windows System Update Service / Antivirus status/ Firewall status / Operating System Requirements / Spyware Definition Up-to-Date;
4. Encryption used
For enterprises that requires extreme secure environment: at this stage Token, Biometric or SMS systems could be established.
1. Token (One-Time-Pad) – every supplicant user must have a token which is synchronized with server. By using PIN+Token Number user gets authenticated;
2. SMS System – requires Exchange Server, Blackberry and SMS System support. By applying username and password an SMS could be sent directly to the mobile phone of the user;
3. Biometric authentication (finger print, retina scanning, facial recognition, iris scanning etc.).
These three methods adds additional layer of security, but the main problem is COST, by sending each time an SMS.
These methods could be used instead of BOGUS USERNAME, or during authentication inside the encrypted tunnel.
7. EAP Success (or Failure)
8. 4-Way Handshake
1. Pairwise Transient Key Creation (Unicast Frames Encryption)
2. Group Transient Key Creation (Broadcast Frames Encryption)
Encrypted Tunnel
802.1X Controlled port allows protected data to pass
WIPS/WIDS/ Policies/Regulations/ Trainings
Layer 3-7 Access

Fig.1. AAA scheme. Adapted according to Ref. [2].

3. Authentication Server – this device is responsible for actually granting or denying access for users of the network. The role could be played by only one device, like Windows Server 2012 with RADIUS support, or a combination of peripheral devices providing authentication support.

Consider that by having all services installed and enabled on one computer system you are not reducing the attack surface.

Conclusion. The realisation of intelligent wireless network communication system involves the use of 802.1X/EAP frameworks as a basis for authentication, authorisation and accounting processes. This framework gives the ability to incorporate any amount of interconnected instruments to provide confidentiality, integrity and accountability for end-users, hereby increasing customer's credibility level. The structure allows the use of legacy systems and encryption technologies, used for backward compatibility.

The structure implies the use of three entities: supplicant, authenticator, and authentication server. Choosing the best supplicant for your network access depends on technology used during AAA process. The most reliable proprietary supplicants that nowadays exist are: Juniper Networks Odyssey Access Client and Cisco Secure Services Client. The remaining entities must be based on Juniper/Cisco or Microsoft, but the price of the solution directly correlates with functionality that is implemented within. Some organizations are using a combination of Juniper, Cisco and Microsoft technologies in order to reduce the attack surface and make the network environment extremely sophisticated for malicious users.

The technological level nowadays is high. It allows to reach the same functionality implemented by using various third-party vendors and proprietary solutions. The key point is to find a balance between cost and needed functionality.

WAPs only accept authentication requests from RSN capable devices, ensuring the consistency and compliance with encryption requirements, which is WPA2/CCMP. This ensures that each MPDU is encrypted, assigned a unique key, sequenced and correctly encapsulated before entering into transmission mode across open-medium.

Employees who are willing to use laptops provided by the organization are entitled to do so. Technology used to protect internal HDD's is based on Symantec Check-Point Full Disk Encryption, which adds an additional layer of security. This software is capable of encrypting any thumb drives, CDs, DVDs and etc. which can go along with laptops. Laptops are easily stolen or lost; this allows to reduce the possibility of using internal laptops as an attack equipment.

WAPs are configured using the combination of unidirectional and bidirectional signal transmissions. This approach by maximally reducing the capability of signal interception outside the premises allows a controlling wireless transmission range. It's achievable by manipulating signal strength and direction.

During the serious international operations where absolute security is a primary concern a Faraday room (or shield) is used, totally eliminating opportunities to interconnect with wireless devices during on-going processes. Faraday cage could be implemented to create an absorption point for any signal for military, law enforcement, scientific etc. buildings, but the cost must conform to the value of object protected.

A Proverb says "the chain is only as strong as its weakest link", this also applies to security, thus before making any decision each user is authenticated and authorized to enter the building. Every user has his or her unique session during a wireless communication. An access is based on identity provided; acceptable use policy and rule of conduct are signed, this allows the system to track all traffic (frames), which is generated by a particular session. The slightest violation of acceptable use policy raises an alarm within Microsoft Operations Manager with further prosecution (in case if needed). This is a primary goal of using individual sessions.

The technological level nowadays is high and allows reaching the same functionality implemented by using various third-party vendors and proprietary solutions. The key point is to find a balance between cost and functionality needed.

References

1. Coleman D., Westcott A., Harkins B., Jackman S. – CWSP Certified Wireless Security Professional Official Study Guide – 2010, 693.p
2. 802.11 Wireless Networks, Security and Analysis, Alan Holt Chi-Yu Huang, 2010, (236.p.)