HIDDEN LAYER AUTHENTICATION USING SMART CARD FOR WEP BASED WLANS

GIANNIS PIKRAMMENOS, GHASSAN SARKIS, JOHN SOLDATOS, VASILIOS ANAGNOSTOPOULOS

National Technical University of Athens,

Electrical Engineering and Computer Science Dpt.

GR 15753, Athens, Greece. *e-mail: gpik@telecom.ntua.gr*

Key words: Smart Card, WLAN, Security, WEP, IV, IVT, authentication.

Abstract: WEP has been criticized for vulnerabilities of the offered security services. Several factors contribute to this effect, as the wireless nature of IEEE 802.11 standards, the solid architecture of the deployed LAN components as well as the inflexible security algorithm of WEP. Secrecy is dependent on the synchronization of the peer encrypting processes and their proper authentication. By implanting a hidden layer to the architectural structure of the system, the complexity of the system is elevated. Such an implant could be a Smart Card containing secrets related to encryption and authentication of multiple components. The on demand introduction of Smart Card in the hosting system enables the pre-synchronization of the systems secrets as and two-way authentication.

1. INTRODUCTION

Layering principles are widely applied in IT world in order to classify the functional responsibilities and to monitor the operational characteristics of each layer mechanism. A well known layering application is the IEEE networking protocol stack with WLAN (IEEE 802.11) [1] as an example. Security layering is also widely accepted, separating accessibility to clusters

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35691-4_52

D. Gritzalis et al. (eds.), *Security and Privacy in the Age of Uncertainty*

depending on the privileges of the attached users. The file system structure of a Smart Card fits within this area.

Hidden layers of information processing are common in Neural Networks as well as in telecommunications' routing. These layers are intermediate layers of the processing procedure that are not directly noticeable from the user. Their lack to adapt to variable operational conditions could be bypassed by enabling real-time structural update, elevating in this way its complexity [2] and scrambling the picture to attackers.

The idea presented here is to introduce Smart Cards as a hidden layer as a secure storage area and an authentication gateway. Embedded processing capabilities of Smart Cards allow for the encryption and manipulation of information, making feasible the update of the contents without any degradation to the achieved secrecy, integrity and confidentiality level [3]. This hidden layer shall interwork with diverse layer protocols, computational environments and functional entities vertically as well as horizontally.

2. SMART CARD BASED HIDDEN LAYER

Wired Equivalent Privacy (WEP) is the security element which has been bundled to 802.11 directly and serves to provide confidentiality and authentication services to 802.11 networks. WEP uses the RC4 algorithm with 40 bit or 128 bit (symmetric) encryption keys to encrypt data at the link-layer (MAC layer). There are two fundamental flaws found in WEP security [4], [5]. The first (more mathematically proven than practically) is the way RC4 algorithm uses key scheduling and random number generation. The second lays in the way WEP handled the RC4 keys for encrypting the 802.11 payloads. Specifically, there is a problem with Initialization Vector (IV) being transmitted in the clear along with the cyphertext for the purposes of rapid decryption at the receiving end, and that it is repeated more or less frequently, depending on the amount of traffic.

The problem with key scheduling based on the random generation mechanism could be solved by centrally dictating the IV sequences. This would require a storage area where bundles of such sequences could be stored temporarily for immediate application in a table. The insecure transmission of these IVs over the air could be bypassed if initial values could be securely provided to the remote wireless terminal so as to be aware that it shares a secret with the AP without being obliged to transmit it. The integration of a Smart Card into the wireless terminal could be the solution to both problems. The transmitted information that represents IVs could be replaced by pointers to actual IVs stored in a table (Initial Vector Table - IVT) that is common between the two peers. Third parties could not then

access the actual information in the clear and could possibly be discouraged from statistically revealing it by frequently updating the IVT contents with new values. The update could be realized downward (from the AP to the wireless terminal) once the connection is secured. It is preferable to involve another security mechanism for this transaction (different from the one under discussion) so as to disengage the control data from the controlled channel. IVTs could be transmitted in bursts or continually as and in one piece or concatenated, so as to elevate system's complexity and to moderate the traffic overhead imposed to the data transmission because of security information exchange.

Smart Cards could be a perfect place for the IVT information storage, as it is an autonomous, secure computational system that could interact with the host device at the wireless terminal under the supervision of the authorized person (the card holder). This scheme allows for a layered security mechanism that enhances the operation of the present WEP mechanisms with minor modifications while at the same time it increases the system complexity by incorporating multiple authentication dependencies. Keys for the encryption are produced under the co-operation of multiple mechanisms based on systems that work in different locations (Smart Card and Smart Card Authentication Server – SCAS).

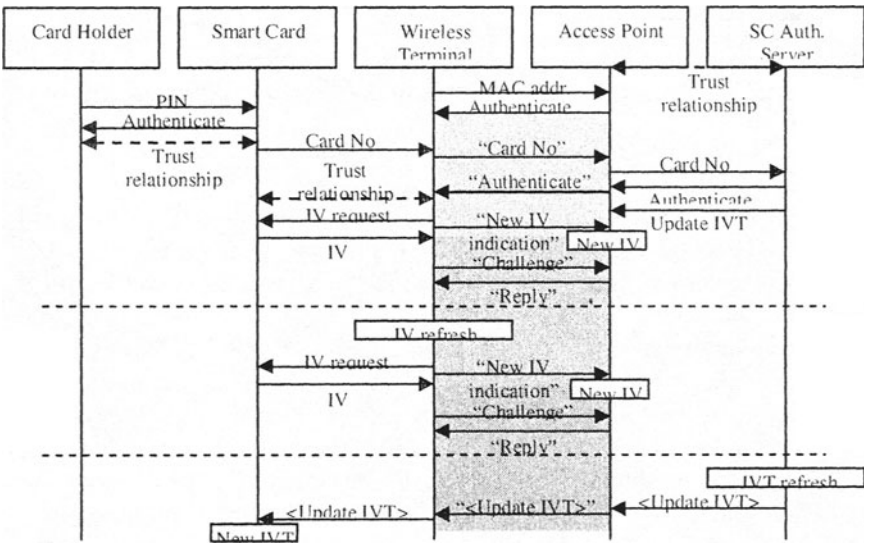

Figure 1 Authentication dependencies and security levels applied – light grey: plain WEP encryption, dark grey: enhanced encryption with dynamic IV update.

Until the enhanced method develops a key to encrypt the air channel (darker gray areas), the encryption mechanism is based on the classical WEP operation (light grey). The exchange of the pointers identifying the actual

(kept secret) key value is hardening attackers' efforts to resolve and link keys to an attack attempt, while the co-operation of remote systems favors the involved parties synchronization and the monitoring of critical information exchange. Figure 2 depicts the architecture of the system with the enhanced security mechanism regarding the functional interworking among the components as well as the roles assignment regarding authentication. Note that potential multiple usage of the Smart Card for different applications allows for its interworking with higher layer mechanism to produce analogous security functions. In such a case, the User could be authenticated indirectly by the Smart Card or directly interworking with higher layer mechanisms. Resuming, a Smart Card could guarantee user's authority on the system operation (as the card holder), wireless terminal encryption logic secrecy and possibly higher layer encryption logic secrecy as well.

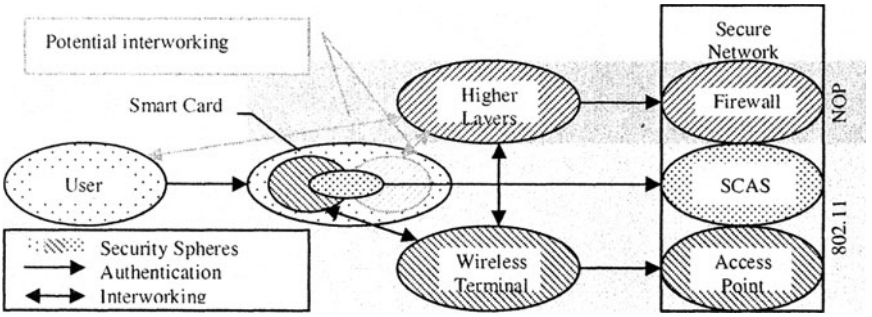

Figure 2 Architecture of a Smart Card enhanced WLAN system.

The modifications to the WEP mechanism in order to incorporate Smart Cards as IVT storage medium, as described in the previous, include:

- The adoption of an Initial Vector Table (IVT) logic that is not embedded but referenced,
- The introduction of a register that would point to IVT for the actual value of the WEP key to be fetched, being transmitted over the air in clear instead of the real value,
- A fetching mechanism that would apply interworking between Smart Card (referenced storage area) and MAC embedded WEP mechanism,
- The introduction of a Smart Card hosting device in the configuration of the wireless terminal,
- The introduction of a dedicated server (SCAS) that would validate Smart Cards in operational wireless systems and update them with IV values.

3. CONCLUSIONS

The added value offered by Smart Cards to the security mechanism of wireless systems as IEEE 802.11 is that it introduces a hidden layer that incorporates secrecy intelligence. This secret layer, that alters the operational model of the WLAN, is able to interwork with all the involved functional components as an authentication mediator. As such, secrecy is raised and the proper secrets are revealed only to the authorized procedures. This extra layer is not straightforwardly detected and this adds complexity to the system along with the capability to dynamically update the functionality of the encryption mechanism by refreshing with new keys dictated by a central repository monitoring their usage.

This paper proposes a new architecture in comparison with those proposed in [6], the hidden layer authentication based on removable media as Smart Cards. It is preferable method over fast packet keying [7] because it decomposes the information of the station from the secret information. Upper layer authentication [8] is supported through the smart card as well, as explained in the previous. Finally, Hidden Field Equations [9] proposal is cordial to the spirit of the presented proposal, strengthening its basis.

4. REFERENCES

[1] IEEE Std 802-2001, "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture," IEEE Computer Society, LAN/MAN Standards Committee, 8 March 2002

[2] "Rapid Re-keying WEP recommended practice to improve WLAN Security", Nancy Cam-Winget (Atheros), Jesse Walker (Intel Corp), Bernard Aboba (Microsoft Corp), Joe Kubler (Intermec Corp), August 2001, http://www.drizzle.com/~aboba/IEEE/1

[3] "JAVA CARD MANAGEMENT SPECIFICATION," Java Card Management (JCM) Task Force, Version 1.0b, 06 October 2000.

[4] "WEPCrack is an open source tool for breaking 802.11 WEP secret keys" http://wepcrack.sourceforge.net/

[5] Fluhrer S., Mantin I., Shamir A., "Weaknesses in the key scheduling algorithm of RC4", Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.

[6] "An IEEE 802.11 Wireless LAN Security White Paper", Jason S. King, October 22, 2001, http://www.llnl.gov/asci/discom/ucrl-id-147478.html

[7] "WEP Fix using RC4 Fast Packet Keying", RSA Security Inc, http://www.rsasecurity.com/rsalabs/technotes/wep-fix.html

[8] "Wireless LAN upper layer authentication and key negotiation", Håkan Andersson, RSA Laboratories, January 17, 2002, http://www.rsasecurity.com/rsalabs/technotes/wlanweb.doc

[9] "Security of Hidden Field Equations (HFE)", Nicolas T. Courtois, RSA'2001, San Francisco, April 10th 2001