IEEE 802.11i WLAN Security Protocol Based On Genetic Software Engineering Model

Weifeng Gao *, Xiaoxi Zheng, Bin Lu

School of Computer Science, WuYi University, Jiangmen, 529020, China

Keywords: WLAN Security, IEEE 802.11i, RSN, Genetic Software Engineering (GSE).

Abstract. Wireless local area networks (WLANs) based on the IEEE 802.11 standards are one of today's fastest growing technologies in businesses, schools, and homes, for good reasons. As WLAN deployments increase, so does the challenge to provide these networks with security. Security risks can originate either due to technical lapse in the security mechanisms or due to defects in software implementations. Standard Bodies and researchers have mainly used UML state machines to address the implementation issues. In this paper we propose the use of GSE methodology to analyse the incompleteness and uncertainties in specifications. The IEEE 802.11i security protocol is used as an example to compare the effectiveness of the GSE and UML models. The GSE methodology was found to be more effective in identifying ambiguities in specifications and inconsistencies between the specification and the state machines.

Introduction

The first wireless security solution for 802.11-based networks, the Wired Equivalent Privacy(WEP), received a great deal of coverage due to various technical failures in the protocol [1].Standards bodies and industry organizations are spending more time and money on developing and deploying next-generation solutions that address growing wireless network security problems. The IEEE 802.11i standard proposes a Robust Security Network (RSN) with much-improved authentication, authorization, and encryption capabilities. The Wi-Fi Alliance, a wireless industry organization, has created the Wi-Fi Protected Access (WPA) standard, a subset of the 802.11i.

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 [2]. Proper migration to 802.11i and mitigating the legacy wireless risks will be a bumpy road. However, the end result will provide users a secure base for mobile distributed processing needs.

The 802.11i Security

The IEEE 802.11i standard defines two classes of security framework for IEEE 802.11 WLANs: RSN and pre-RSN as shown in Fig. 1. A station is called RSN-capable equipment if it is capable of creating RSN associations (RSNA). Otherwise, it is called pre-RSN equipment. The network that only allows RSNA with RSN-capable equipment's is called a RSN security framework. The major difference between RSNA and pre-RSNA is the 4-way handshake. If the 4-way handshake is not included in the authentication/association procedures, stations are said to use pre-RSNA [3].

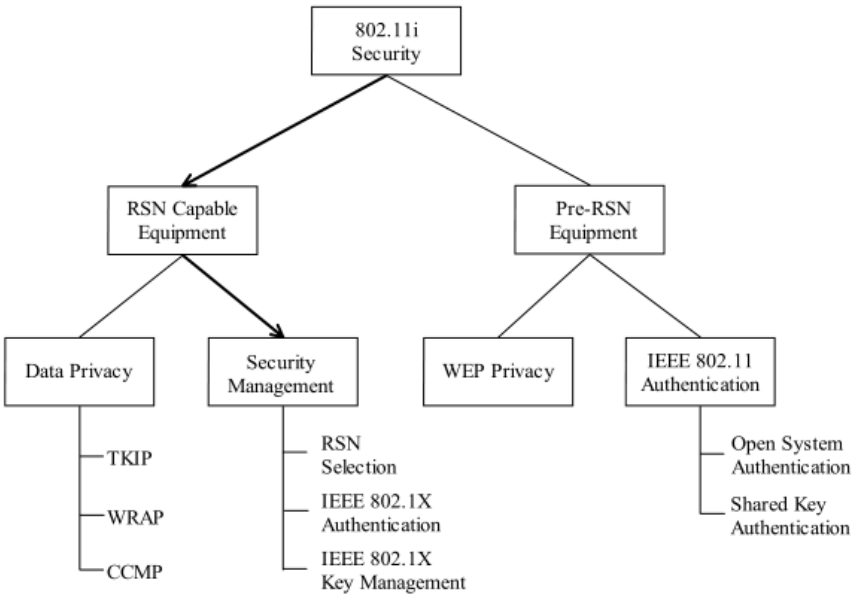

Figure 1. The 802.11i Security Framework

In addition to enhancing the security in pre-RSN, the RSN security defines key management procedures for IEEE 802.11 networks. It also enhances the authentication and encryption in pre-RSN. The enhanced features of RSN are as follows:

Authentication Enhancement: IEEE 802.11i utilizes IEEE 802.1X for its authentication and key management services. It incorporates two components into the IEEE 802.11 architecture IEEE 802.1X Port and Authentication Server (AS). IEEE 802.1X port represents the association between two peers. There is a one-to-one mapping between IEEE 802.1X Port and association.

Key Management and Establishment: Two ways to support key distribution are introduced in IEEE 802.11i: manual key management and automatic key management. Manual key management requires the administrator to manually configure the key. The automatic key management is available only in RSNA. It relies on IEEE 802.1X to support key management services [4].

Encryption Enhancement: In order to enhance confidentiality, two advanced cryptographic algorithms are developed: Counter-Mode/CBC-MAC Protocol (CCMP) and Temporal Key Integrity Protocol (TKIP). In RSN, CCMP is mandatory. TKIP is optional and is recommended only to patch pre-RSN equipment.

Modeling

In the process of modeling the RSN, we first model the WLAN environment using the Structure and Composition Trees. Thereafter, the requirements translation is accomplished followed by the development of the requirements behaviour trees (RBTs).

WLAN Structure. The behavior of a system takes place on a network structure. This structure can be defined using the analogous of behavior trees called structure trees. The structure tree is used in our analysis to demonstrate the connection structure of two STAs in an ESS. The model shows how the connecting STAs coordinate with other components in the system.

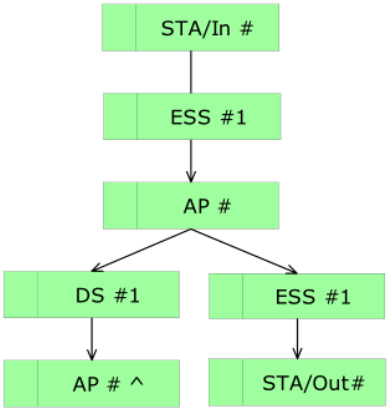

Figure 2. Connection Structure

Fig.2 shows the connection structure of the Extended Service Set (ESS). An STA in an ESS can either directly connect to another STA via a single AP or it can connect via a number of Aps through the Distribution System (DS). The recursion symbol (^) used in the AP# component notify that there can be several reversions before an STA connects to another STA [5].

WLAN Composition. The composition tree identifies the hierarchy of all components in the RSN, their characterizations, classifications, multiplicity, and their compositional properties.

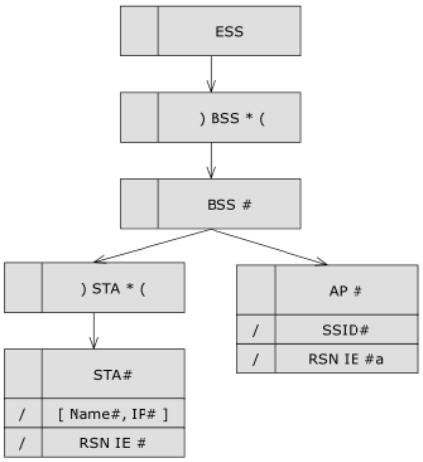

Figure 3. ESS Composition

Fig.3 shows the composition of an ESS. An ESS consists of one or more Basic Service Sets (BSS). The BSS is made of one AP and several STAs. An AP advertises the SSID of the associated ESS and its RSN capabilities using the RSN Information Element (IE). Similarly, the STAs have their own identifiers and IP addresses. The STAs also advertise their RSN capabilities in their RSN IE.

The next step in GSE modeling is requirements analysis. Firstly, the requirements are assembled from the standard and translated. Thereafter, the RBTs are built. The RBTs are then integrated to derive at the Design Behavior Tree (DBT). Finally, the DBT is used to derive at the other GSE models for the analysis of the RSN. Detailed records of requirements translation, integration and defect identification can be found in [6].

Discussion

The wireless attacks listed in the Table 1 are issues arising from the various uncertainties and inconsistencies in the specifications. The following discussions provide an insight of the defects and their consequences.

In Clause 8.4.1 permitting an STA to guess SSIDs can lead to malicious associations with illegitimate APs. Furthermore during the initial stages of an RSNA both the supplicant and the authenticator operate independently [7]. Therefore, in a situation where the supplicant or the authenticator is allowed to make presumptions can lead to revelation of vital information to undisclosed entities allowing malicious associations or Identity-Theft. In case of a re-association request by a roaming STA we first transit the STA into DISCONNECTED state before it is made to associate with the new AP. This case makes the RSN more reliable so that session-hijack attacks can be avoided.

If an AP is not RSN capable, STAs should not be permitted to associate with that AP. In Clause 8.4.2, we force the AP to DISCONNECT from the STA in order to avoid any malicious associations ensuring strong RSN security policy.

During the CONNECTING stages of the AP and STA as described in Clause 8.4.3, there is no common shared secret. Therefore there is a possibility a Man-In-The-Middle scenario can reveal the credentials of a legitimate STA causing malicious associations. Therefore, STAs, which are unable to meet the RSN requirements of an AP at the first instance, are DISCONNECTED immediately without permitting them to retry or guess information relevant to dot11 association.

Table 1. Possible Attacks on the RSN

IEEE Clause	Req. No.	Possible Attacks	Solutions
8.4.1	1	Identity Theft	APs are not allowed to advertise their SSIDs
	1	Identity Theft	STAs are not allowed to guess SSIDs
	2	Malicious Association	Re-association starts from DISCONNECTED state
	2	Malicious Association	Pre-authentication is achieved via the DS, hence STA is at AQUIRED state
	3	Man-In-Middle	Authenticator port is controlled
8.4.2	3	Malicious Association	STA is deliberately reverted back to DISCONNECTED State
8.4.3	5	Malicious Association	STA is DISCONNECTED if RSN requirements are not met
	5	Man-In-Middle	AP goes to DISCONNECTED state if it does not choose to associate?
8.4.6	8	Man-In-Middle	EAP messages are protected by filtering (integrity?)
	8	Man-In-Middle	STA DISCONNECTED if it is unable to prove its identity to the AS

In Clause 8.4.6 when both STA and AP become AUTHENTICATED they share a common secret. Until this point the integrity of the messages exchanged between the STA and the AP are dubious [8]. An adversary sitting in the vicinity of an RSN can construct an attack scenario if the participating STAs are allowed to revert to intermediate states in case of an uncertainty. Therefore, it is not recommended to revert an STA into AQUIRED state if AUTHENTICATION fails at any stage.

Conclusion

Inconsistencies between requirements and design models are a common problem faced by software engineers. Although the IEEE standards carry more technical details of the protocol, the fact is that the software engineers who implement the system have little or no domain knowledge in relevant fields. Most domain experts tend to project their mental replica on design models, assuming to be understood by everyone. This not only leads to confusion but also makes problem resolution impossible without proper fallback to specifications.

The systematic analysis performed in this study using the GSE methodology has identified a number of ambiguities and defects in specifications. We have shown that issues in software

specifications can lead to serious security breaches. Feasible improvements are also recommended to remedy those issues and a number of GSE models have been developed to represent the improved RSN environment. Although, we have not analyzed the system to the lowest levels, the details provided here are sufficient enough for a software developer to produce a system with strong RSN policies.

The discrepancy in the requirements and the UML state machines shown in the standard have led to several inconsistencies. Many of the identified incompleteness issues and ambiguities in the standard's requirements arise from semi-tacit and tacit knowledge not being specified. This leads to a software engineer acquiring considerable domain expertise in order to design and implement the RSN. Therefore, detailed and accurate specifications are essential to enable software engineers implement standards without software flaws.

The GSE models have highlighted a number of incompleteness and inconsistency issues, which were not identified by the UML models. The GSE models derived are simple, easy to understand and provide systematic tracking to the original specifications.

References

[1] Borisov, N. Goldberg, I. Wagner, D. "Intercepting Mobile Communications: The Insecurity of 802.11", ACM SOGMOBILE, Vol. 7, Jan. 2001, pp. 180-188.

[2] Mead, N.R. McGraw, G. "Wireless Security Future", IEEE Security & Privacy, July/Aug. 2003, pp. 68-72.

[3] Dromey, R.G. From Requirements to Design: formalizing the key steps, Proc. 1st International Conference on Software Engineering and formal methods, Sep. 2003,Brisbane, Australia, pp. 2-11.

[4] IEEE Std. 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999.

[5] Stubblefield, A. Ioannidis, J, Rubin, A.D. A key recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)", ACM Transactions on Information and System Security, Vol. 7, No. 2, May 2004, pp. 319-332.

[6] IEEE Std. 802.1X-2001, "Local and Metropolitan Area Networks – Port-Based Network Access Control", June 2001.

[7] Wi-Fi Alliance. "Wi-Fi Protected Access (WPA)", Version 2.0, April 2003.

[8] Wi-Fi Alliance. "Securing Wi-Fi Wireless Networks with today technologies", February, 2003