An Experimental Study of Cross-Layer Security Protocols in Public Access Wireless Networks

Avesh K. Agarwal Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University, Raleigh, NC 27695

Abstract- **Wireless networks require strong security mechanisms due to their open medium. However, security effects system performance, and therefore impacts quality of service (QoS) of communication. To analyze the impact of security on system performance, we conduct a detailed experimental study on a wireless IP testbed with security at different layers. We study their impact on different types of data streams such as TCP and UDP with regard to authentication time and cryptographic overhead. Specifically, we experiment with the most widely used security protocols such as WEP, IPsec, 802.1x with RADIUS, and SSL. We classify security protocols into individual and hybrid policies. Then, a new metric, *relative security index*, is introduced to analyze security strength and overhead tradeoffs quantitatively. Our results demonstrate that the stronger the security, the more signaling and delay overhead; whereas, the overhead does not necessarily increase monotonically with the security strength. Also, we notice that authentication time is a more significant factor than cryptographic cost regarding their contributions towards QoS degradation in wireless networks.**

Keywords - Wireless networks, security policies, authentication time, cryptographic cost.

I. Introduction

Rapid increase in the usage of mobile devices such as laptop computers and portable devices etc. has led to the wide deployment of the wireless local area networks (WLANs) for providing ubiquitous Internet. Besides these advantages, inherent broadcast nature of wireless networks has raised several security concerns [12]. WEP [8], 802.1x [3], [7] with Extensible Authentication Protocol (EAP) [11], Remote access dial in user service (RADIUS) [6], IP security (IPsec) [4] and Secure Socket Layer (SSL) [2] are some of the widely used security protocols. Previous studies show that these protocols are prone to several attacks [8]. To overcome these problems, researchers have come up with many solutions to improve the security aspects of these protocols in recent years [9]. We observe that most of the previous research is focused on security aspects with little thought given to performance impact of security protocols on system performance.

Measurements are very important to determine the realistic view of the performance overhead associated with the security mechanisms. Therefore, to gain fundamental understanding of performance impact due to security protocols, experimental studies are carried out in the past in various network environments [10], [13]. However, these studies have explored security protocols individually without exploring the possibilities and advantages associated with integrated security services at different layers. Moreover, these studies perform experiments in few network scenarios providing less detailed real-time results. To address these issues, we setup a real-time experimental testbed, which is a miniature of existing wireless networks to ensure that our experimental results can mimic large scale wireless networks. Security protocols are classified into individual and hybrid security policies to study cross-layer integration. Moreover, we define *relative security index* to analyze security strength and overhead associated with each security policy, respectively. Authentication time and cryptographic cost are metrics evaluated under TCP and UDP traffic streams in our testbed.

The remainder of the paper has been organized as follows. In Section II, we describe our testbed architecture, network scenarios, security policies, and performance metrics. A new metric relative security index (RSI) is discussed in detail in Section III. Experimental measurements discussing about authentication time and cryptographic cost along with remarks are presented in Section IV. Section V concludes the paper.

II. Testbed Infrastructure

In order to achieve the above goals, we have designed the various experiments based on security policies, mobility scenarios and performance metrics. In following subsections, we discuss them briefly. Besides this, we also provide summary of hardware equipments and software used in our testbed.

A. Testbed Architecture

Fig. 1 shows testbed architecture. In the testbed, there are two subnets, each consisting of a router which acts as a home agent (HA) and a foreign agent (FA) connected to Cisco access points (Aironet 1200 Series) to provide wireless connectivity. Each router also acts as an IPsec gateway and a Radius server for authentication in IPsec and 802.1x security policies, respectively. Different security protocols have been configured to provide security over wireless segment of the network. An IPsec tunnel is configured between two home agents to provide security services over the wired segment of the network. All systems use RHL 9.0 kernel 2.4.20. Routers, HAs and FAs are Dell systems (Pentium IV 2.6 GHZ). Moreover, two Sharp Zaurus (Intel XScale 400 MHz with Linux Embedix), two

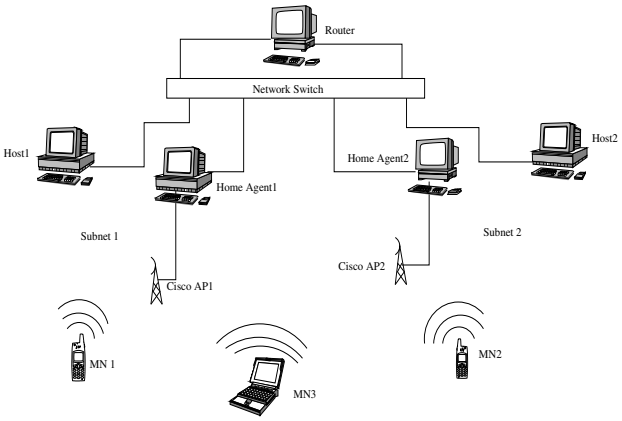


Fig. 1. Testbed Architecture

iPAQs (Intel StrongARM 206 MHZ with Familiar Linux) and a Dell Laptop (Celeron Processor 2.4GHZ with RHL 9) are used as MNs. Open source softwares such as FreeSwan for IPsec [4], Xsupplicant for 802.1x supplicant [1], FreeRadius for Radius server [6], OpenSSL for SSL [2], Mobile IP from Dynamic [5], Ethereal (packet analyzer), Netperf and ttcp (network monitoring utilities) are used for different functionalities in the testbed.

B. Network Scenarios

Network scenarios are classified into non-roaming ($\mathcal{N}$) and roaming ($\mathcal{R}$) based on user's current location, i.e., whether a user is in its home domain or foreign domain, respectively. Non-roaming scenarios, represented as $\mathcal{N}$, are defined as the scenarios when both communicating mobile users are in their home domain. Following are the details of various non-roaming scenario configured in the testbed.

- **Scenario** $N1$**:** It deals with the situation when both mobile nodes are in the same subnet in the network which is their home domain also.
- **Scenario** $N2$**:** Mobile nodes communicate with their home agent in the network that is acting as an application server providing services to mobile clients in the network. Here, a part of the communication path is wired, which is not the case in scenario N_1.
- **Scenario** $N3$**:** It is to capture the impact of security services when participating mobile nodes are in different domains in the network.

When at least one of two communicating mobile users is in a foreign domain, we refer it as roaming scenario, represented as $\mathcal{R}$. The following roaming scenarios are configured in our experimental testbed.

- **Scenario** $R1$**:** This scenario specifies when one end node, which is in a foreign domain, is communicating with the other node which is in its home domain, but two nodes are in different domains in the network. It aims to analyze the effect of security services on data streams when one node is roaming.
- **Scenario** $R2$**:** This scenario occurs when both nodes are in the same domain but one node is roaming. Therefore, current network is the foreign domain for one node, whereas it is the home domain for other node. It helps us in analyzing performance impact on data streams when roaming node is communicating with a non-roaming node in the same domain in the network.

C. Security Policies

Security policies are designed to demonstrate potential security services provided by the integration of security protocols at different layers. Each security protocol uses key management protocols, various authentication, and cryptographic mechanisms. Therefore, a variety of security policies are configured in our experiments by combining various mechanisms of security protocols. Let $\mathcal{P} = \{P_1, P_2, \ldots, P_{12}\}$ represent the set of individual and hybrid security policies configured in the network. A subset of security policies are shown in TABLE I. Next, we define individual and hybrid security policies.

TABLE I
SECURITY POLICIES

Policy	Security Polices
P_1	No Security
P_2	WEP-128 bit key
P_3	IPsec-3DES-SHA
P_4	IPsec-3DES-SHA-WEP-128
P_5	8021x-EAP-MD5
P_6	8021x-EAP-TLS
P_7	8021X-EAP-MD5-WEP-128
P_8	8021X-EAP-TLS-WEP-128
P_9	8021X-EAP-MD5-WEP-128-IPsec-3DES-MD5
P_{10}	8021X-EAP-TLS-WEP-128- IPsec-3DES-MD5
P_{11}	8021X-EAP-MD5-WEP-128-IPsec-3DES-SHA
P_{12}	8021X-EAP-TLS-WEP-128-IPsec-3DES-SHA

1) **Individual and Hybrid Security policies:** When a policy involves mechanisms in a single security protocol, it is called an *individual security policy*. "No security" means that there is no security services enabled in the network. "No Security" policy helps us in comparing the overhead associated with others in terms of authentication time and cryptographic overhead. When security policies involve mechanisms belonging to multiple security protocols at different network layers, they are called *hybrid security policies*. All policies except P_1, P_2, P_3, P_5 and P_6 which are individual policies, are the hybrid policies configured in our testbed.

D. Performance Metrics

We consider two performance metrics for determining the impact of security on system's QoS. These metrics are based on the basic security mechanism such as authentication and encryption and decryption time.

1) **Authentication Time:** We consider authentication time as the cost of authentication because time involved in an authentication phase is one of the important factors contributing towards performance impact in a network.

TABLE II

RELATIVE SECURITY INDEX

Security Policy	P_1	P_5	P_2	P_7	P_6	P_3	P_8	P_4	P_9	P_{11}	P_{10}	P_{12}
RSI	0	32	62	94	98	159	160	221	252	253	318	319
RSI (Normalized)	0	10.0	19.4	29.5	30.7	49.8	50.2	69.3	79.0	79.3	99.7	100

2) **Cryptographic Cost:** Cryptographic cost is associated with the confidentiality feature of a security policy, which is defined as the total time involved in encryption and decryption of an entire data stream during the transmission between a sender and a receiver.

III. Relative Security Index

In this section, we present a simple model to analyze the relative strength of various security policies. Every security policy provides some security features such as authentication and confidentiality in our experimental study. However, it is difficult to quantify the security strength delivered to a system or a network by a security policy based on its features. This is due to the fact that it is almost impossible to predict that when a system or a network can be compromised in the future during the configuration of a security policy. Generally, it is not easy to be fair in comparing two policies with different features. For example, assume that a security policy P_α consists of 2 features which are very strong, and another security policy P_β has of 4 features which are relatively weak. If we compare two policies with respect to the 2 features of P_α, then we can conclude that P_α provides stronger security than P_β. However, if we compare P_α and P_β with respect to the 2 features not in P_α but in P_β, we find that P_β is better than P_α. The justification of which security policy is better than the other depends upon network requirements, policies installed, and features activated in a network.

Therefore, we define *relative security index* to understand the relative strength of a security policy by using associate weights of each feature for which higher weights are assigned to a policy with more features. Let

- w_A^i be the weight associated with a mechanism i providing authentication.
- w_C^j be the weight associated with a mechanism j providing confidentiality.
- w_T^k be the weight associated with data integrity mechanism k.
- w_R^l be the weight associated with a mechanism l providing non-repudiation.
- w_M^q be the weight associated with a mechanism q providing mutual authentication.

Relative security index of a security policy is a metric which is defined as

$$RSI(P_{(\cdot)} \in \mathcal{P}) = \underbrace{w_A^i \mathcal{I}_{\mathrm{A}} + w_C^j \mathcal{I}_{\mathrm{C}} + w_T^k \mathcal{I}_{\mathrm{T}} + w_R^l \mathcal{I}_{\mathrm{R}} + w_M^q \mathcal{I}_{\mathrm{M}}}_{\text{security features}} + \underbrace{\eta \cdot C}_{\text{effect of features}} \quad (1)$$

In the above expression, $\mathcal{I}_{(\cdot)}$ is an indicator function, which equals to 1 if that particular security feature exists in the policy, otherwise zero. Consequently, the first part is the sum of the weights associated with all features provided by the security policy. The weights assigned to each protocol are shown in TABLE III. Weight assignment to these security protocols is based on several criteria such as the key length, use of digital certificates used in a particular mechanism and so on. In the second part of the RSI, which is so called *the effect of features*, η is the total number of security features provided by a security policy. For example, assume that a security policy consists of two mechanisms, and each mechanism provides authentication and confidentiality features, then the value of η of this security policy is referred to as 4. In addition, by analyzing security features of the policies, we find that a security policy with more features provides stronger security, being less vulnerable to attacks. For example, one policy has five features with very low weights 1, and the other policy has four features with very high weights 4. According to the first part in (1), the first policy has an index of $5 \cdot 1 = 5$ and the second policy has an index of $4 \cdot 4 = 16$. Without the second part, it would be concluded that the second policy is stronger. This is contradictory to our observation by using TABLE I that the policy with more features is usually stronger. Therefore, we need to consider the effect of features, that is, a security policy that has more features should be regarded as a stronger policy.

TABLE III

WEIGHTS ASSOCIATED WITH SECURITY PROTOCOLS

Security Feature	Security Mechanism	Weight
Authentication (w_A)	WEP-128 (Shared)	1
	802.1x-EAP-MD5	2
	IPsec	3
	802.1x-EAP-TLS	4
Mutual (w_M) Authentication	IPsec	1
	802.1x-EAP-TLS	2
Confidentiality (w_C)	WEP-128	1
	3DES	2
Data Integrity (w_T)	MD5 (IPsec/802.1x-EAP)	1
	SHA (IPsec)	2
Non-repudiation (w_R)	IPsec (ESP)	1
	802.1x-EAP-TLS	2

In order to signify this finding, we need to determine a value of C, which is able to ensure that regardless of the number of features and the weight of each feature, a policy with more features is always able to yield a higher security index. Assume that a security policy P_α consists of η security features and another security policy P_β consists of $(\eta - 1)$ features. Assume each feature of P_α is with weight 1 , the lowest weight assigned to any feature, yet each feature of P_β is with weight 4, the highest weight assigned to any feature. By assigning the highest weights to the features of P_β and the lowest weights to the features of P_α, we want to ensure that, by choosing a particular value of C, the total index of P_α is higher

than that of P_β. Now the total indexes of P_α and P_β, using (1), are $(\eta \times 1 + \eta \times C)$ and $((\eta - 1) \times 4 + (\eta - 1) \times C)$, respectively. So, P_α has higher weight than P_β, if the following relationship holds true,

$$\eta \times 1 + \eta \times C > (\eta - 1) \times 4 + (\eta - 1) \times C.$$

This relationship can be simplified as $C > (3\eta - 4)$. As there are at most 11 security features associated with the security policies in our experiments, we take $\eta = 11$ and obtain $C > 29$. Therefore, we choose $C = 30$ in our model. If a security policy provides the same security feature with more than one security protocol, this security feature is counted twice, and separate weights are assigned to each security protocol. For instance, the policy P_4 IPsec-3DES-SHA-WEP-128 provides authentication and confidentiality features by IPsec-3DES-SHA and WEP-128 as well. Therefore, when calculating weights for this policy, authentication and confidentiality features are counted twice each.

IV. Experimental Results

In this section, we discuss experimental results obtained for afore-mentioned security policies in various mobility scenarios. We provide experimental data for authentication time and cryptographic cost.

A. Authentication Time

Since WEP does not involve exchange of control messages, there is no authentication time involved with it. Since Mobile IP is used for enabling mobility in the testbed, authentication time for IPsec and 802.1x involves Mobile IP authentication time as well. Figs. 2 and 3 demonstrate the authentication versus RSI. Note that RSI values are demonstrated in an increasing order in the figures.

We observe from Figs. 2 and 3 that 802.1x-EAP-TLS policies cause the longest authentication time among all policies. This is due to the fact that the policy 802.1x-EAP-TLS uses digital certificate for mutual authentication, which involves exchange of several control packets. Moreover, IPsec policies generate longer authentication time than 802.1x-EAP-MD5 (without IPsec) policies because of IPsec tunnel establishment. In addition, we can see that the security policies create longer authentication time in roaming scenarios than non-roaming scenarios due to the reauthentication in a foreign network. Besides these general observations, we notice that authentication time does not increase proportionally with respect to the RSI of security policies. For example, we recognize that the policy P_3 (IPsec) induces lower authentication time than the policy P_6 (802.1x-EAP-TLS) in all scenarios although it has higher RSI value than the P_6. Although P_{10} and P_{12} cause longer authentication time than other policies but these policies consist of highest RSI values due to more than one levels of security mechanisms involved.

Based on these observations, we conclude that policies in the middle of RSI group provide the best tradeoff between security and performance overhead, and IPsec policies (P_3 and P_4) are the best among them. On the other side, P_{12} (802.1x-EAP-TLS with IPsec) is the best suitable for the network carrying very sensitive data.

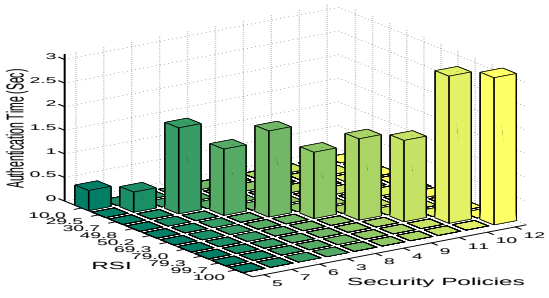


Fig. 2. Non-Roaming Scenarios: Authentication Time vs. RSI.

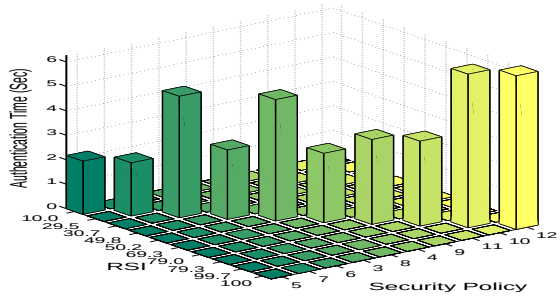
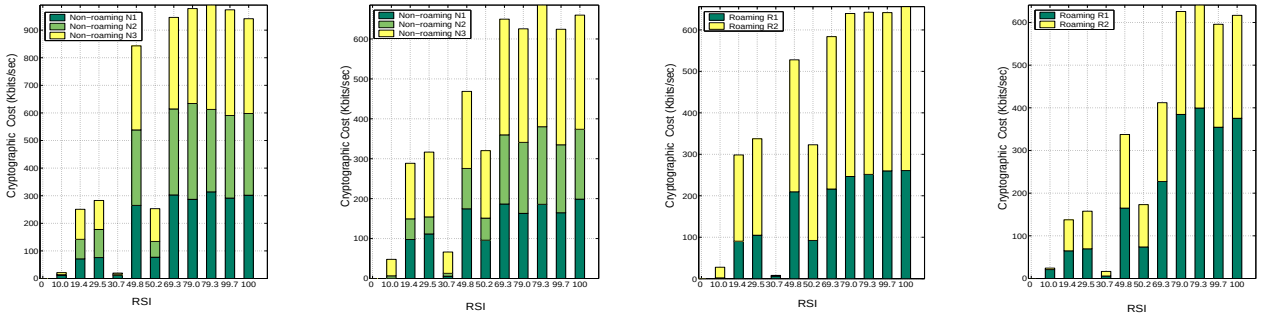


Fig. 3. Roaming Scenarios: Authentication Time vs. RSI.

B. Cryptographic Cost

Now, we discuss cryptographic cost associated with security policies in roaming and non-roaming scenarios as shown in Figs. 4. We notice from Fig. 4(a) that cryptographic costs associated with policies (P_4, P_9, P_{11}, P_{10}, P_{12}) are very close to each other, showing little variations. Generally, the policies (P_4, P_9, P_{11}, P_{10}, P_{12}) exhibit 16% higher cryptographic costs than P_3, and 366% higher than that of P_2, P_7 and P_8. Further, we observe that P_5 and P_6 exhibit negligible cryptographic costs, which is due to the fact that these policies do not consist of any encryption/decryption mechanisms associated with them. A closer look at graphs reveals that cryptographic cost increases corresponding to RSI values. However, we see that P_8 is the policy with a higher RSI value but with lower cryptographic cost. Specifically, P_8 exhibits 78% lower cryptographic cost than policies (P_4, P_9, P_{11}, P_{10}, P_{12}), and almost similar to policies P_2 and P_7. This suggests that P_8 (802.1x-EAP-TLS with WEP) provides the best tradeoff between security and performance overhead in these scenarios. We also notice the similar behavior for UDP traffic in various scenarios from Fig. 4(b). However, cryptographic costs of security policies for UDP traffic are less than that of TCP traffic. It is due to the fact that TCP requires acknowledgment for each packet, leading to the transmission of more number



(a) TCP Traffic. (b) UDP Traffic. (c) TCP Traffic. (d) UDP Traffic.

Fig. 4. Cryptographic Cost vs. RSI.

of packets through the networks than UDP. So TCP results in higher encryption and decryption processing overhead, leading to increased cryptographic cost.

Comparing the cryptographic costs from Figs. 4(c) and 4(d), we find that P_{12} (with the highest RSI value) demonstrates a about two times higher cryptographic cost than P_2, P_7, P_8, and 25% higher than P_3 for TCP traffic in R1 scenario. Whereas, P_{12} exhibits 72% higher cryptographic cost than P_2, P_7, P_8, and 24% higher than P_3 in R2 scenario during TCP. On the other side, P_{12} demonstrates about 4 times higher overhead than P_2, P_7, P_8, and 128% higher than P_3 for UDP traffic in R1 scenario. In addition, P_{12} shows 143% higher cost than P_2, P_7, P_8, and 40% higher than P_3 during UDP traffic in R2 scenario. In addition, we observe that P_9, P_{10}, P_{11} show cryptographic cost very close to P_{12} with little variations. Therefore, we notice that P_8 provides the best tradeoff in all roaming scenarios due to low overhead associated with it. However, we observe that variations between cryptographic costs of P_{12} and P_8 are small. Therefore, it suggests that P_{12} may also be a good choice in roaming scenarios.

In addition, we notice that, as hardware becomes faster in the future,, cryptographic cost (i.e., time involved in encryption/decryption) will be reduced further, and as shown in Fig. 3, authentication time in roaming scenarios is very high, it may affect mobile applications significantly as user's mobility increases. Therefore, we speculate that QoS degradation in a network may be more significant due to the authentication cost than the cryptographic cost in the future.

C. Remarks

We have observed that there is always a tradeoff between security and performance associated with a security policy, depending upon the network scenario and traffic types. We find that the cross-layer integration of security protocols may provide the strongest protection, but with more overhead. Our results demonstrate that in general, the stronger the security, the more signaling and delay overhead; whereas, the overhead does not necessarily increase monotonically with security strength. Moreover, we notice that IPsec policies provide the best tradeoff between security and performance regarding authentication time; 802.1x-EAP-TLS policy is the most suitable option for low cryptographic overhead and better security strength in many scenarios. In addition, experimental results reveal that authentication time is a more significant factor than cryptographic cost with respect to their contribution towards QoS degradation in the network.

V. Conclusions

We discussed the issue of performance overhead and security strength associated with security protocols in public access wireless networks. Specifically, we studied the cross-layer integration of various security policies with respect to authentication time and cryptographic cost in different network scenarios with TCP and UDP data traffics. We believe that combination of these real-time results can lay a very strong foundation for future wireless networks for designing new security protocols or improving the existing ones.

References

[1] 802.1x Supplicant. *http://www.open1x.org*.
[2] *OpenSSL*. *http://www.openssl.org*.
[3] IEEE 802 Standards. *http://standards.ieee.org/getieee802*.
[4] IPSEC. *http://www.freeswan.org*.
[5] Mobile IPv4. *http://dynamics.sourceforge.net*.
[6] RADIUS. *http://www.freeradius.org*.
[7] IEEE Std 802.1x-2001x: Port-Based Network Access Control. *http://www.ieee802.org/1/pages/802.1x.html*, June 2001.
[8] N. Borisov, I. Goldberg, and D. Wagner. Intercepting Mobile Communications:The Insecurity of 802.11. In *Proceedings of the Seventh Annual International Conference on Mobile Computing And Networking*, July 2001.
[9] M. D. Corner and B. D. Noble. Zero-Interaction Authentication. In *Proceedings of IEEE/ACM MOBICOM*, pages 1–11, September 2002.
[10] O. Elkeelany, M. M. Matalgah, K.P. Sheikh, M. Thaker, G. Chaudhary, D. Medhi, and J. Qaddour. Perfomance Analysis Of IPSEC Protocol: Encryption and Authentication. In *Proceedings of IEEE Communication Conference (ICC)*, pages 1164–1168, May 2002.
[11] IETF. PPP EAP TLS Authentication Protocol. *RFC 2716*, October 1999.
[12] T. Karygiannis and L. Owens. Wireless Network Security 802.11, Bluetooth and Handheld Devices. *National Institute of Technology, Special Publication*, pages 800–848, November 2002.
[13] W. Qu and S. Srinivas. IPSEC-Based Secure Wireless Virtual Private Networks. In *Proceedings of IEEE MILCOM*, pages 1107–1112, October 2002.