SECURITY FEATURES IN WIRELESS NETWORKS

Miriampally, V.R.
Department of Electrical Engineering
Adama Science & Technology University
Ethiopia
miriampally@gmail.com

ABSTRACT

The authentication procedure to be used by the network to identify and authenticate the subscriber is generally known as security function. It makes it possible to protect the radio link from unauthorized calls there off. After introducing the kinds of security services typically required for network security such as confidentiality, data integrity, message authentication, non repudiation, uniqueness, user authentication, user authorization, service availability, and intrusion detection, in this paper we briefly introduce the range of cryptographic algorithms. We then consider IP network security in particular. Here we mainly focus on security in wireless networks, including WLAN security and GSM security; we explore the interactions of Mobile IP with security protocols like IPsec and AAA protocols.

Keywords: WLAN security, GSM security & Mobile IP security

1. INTRODUCTION

Security and QoS are two-thirds of a triumvirate, the third part of which is mobility. They are the major network-level areas of technical challenge that wireless IP must successfully handle to succeed. Of the triumvirate, security and QoS are more similar to each other than to mobility. Whereas mobility is for the most part an interesting problem only in the wireless case, security and QoS are among the most important areas of work and development for IP, whether wired or wireless. In both cases, there are challenging and interesting problems in the wired side, with additional challenges when wireless is considered.

One reason why security is so challenging is that it is a negative problem (Salzer & Kassohoek, 2003). In many other problems in the wireless IP world, the objectives are to achieve something that can be verified with reasonable effort. For example, it is easy to verify that the objectives of a protocol like Mobile IP are met, when packets get forwarded to the correct locations of mobile hosts (MHs). However, it is difficult to verify that a network is secure, because we would need to test it against a variety of different attacks. Even then, vulnerabilities might not be spotted, only to be revealed by yet another type of attack that the designer has not considered. Furthermore, in many other cases, a natural feedback mechanism exists when something fails the user can be expected to complain. However, if security fails, the person or persons with knowledge of the failure are typically the attackers, who would often not have an incentive to report the security failure.

We consider only network security here. Thus, we examine only security issues related to communicating over a network. This includes security issues related to communicating over a wired or wireless data link, but not machine security. Machine security includes proper and careful design of operating system software and machine hardware to avoid security holes that can be exploited by malicious users. It also includes physical security, such as keeping machines in secure locked areas, and proper care of laptops in places like airports where some thieves target laptops and personal digital assistants (PDAs). A practical system designed with security in mind would need to consider machine security and network security, as well as carefully designed procedures for the human operators (e.g., to avoid a malicious user stealing unauthorized operator’s key and accessing the system).Security does not come for free. It must be provided for, at the cost of such things as bandwidth, power consumption, and delays. There are trade-offs involved, depending on the levels of security required for different situations. These trade-offs are better understood for wire line networks than wireless networks, given that wire line networks have been around for longer. When wireless links are involved, constraints like limited bandwidth, power, and processing capability may become the optimal parameters for tradeoff.

In some cases, wireless-specific algorithms and protocols may be beneficial. For example, wireless transport layer security (WTLS) is a version of transport layer security (TLS) optimized for the wireless environment, allowing less computationally intensive algorithms to be used at the wireless terminal and lower bandwidth overhead and faster handshakes, at the cost of a lower level of security (Dierk & Allen, 1999). The introduction of specialized protocols like WTLS for wireless access, however, introduces another challenge. It places a burden on servers unless there is a translation gateway that shields the servers from having to understand all the specialized protocols. The WAP gateway is an example of one such gateway that has WTLS/TLS translation among its features (Wapforum.org). One of the most important features that wireless access enables is mobility. To support mobility everywhere, the network must augment its routing, QoS, security, and other features.

First, user authentication for network access when a subscriber accesses the network over a wireless link (even in a home network) is important, since the terminals are not permanently attached by wire to any given location. Second, when the subscriber is roaming, a number of challenges arise:

- How to work with mobility protocols to support seamless provisioning of security services while roaming and for inter administrative domain mobility, and
- How to coordinate between the visited and home network in authentication, authorization, and accounting (AAA), as well as providing other security mechanisms.

2. WLAN SECURITY

When 802.11 WLANs were first designed, it was noted that they should have the same level of security as typical LANs like Ethernet LANs. Ethernet does not encrypt traffic, but because Ethernet machines are connected to one another by cables, it is harder to tap into the LAN than for a WLAN (where an attacker need not physically connect any hardware to the LAN to eavesdrop). Therefore, the wired equivalent privacy (WEP) scheme was proposed. WEP is a weak, 40-bit secret key (symmetric) encryption scheme that was not designed to be super-strong, but to raise the difficulty of eavesdropping WLAN traffic to an equivalent level as with a wired LAN. Additionally, an integrity check value (ICV) is computed on the plain text and appended to the plaintext before WEP encryption. Figure 1 shows WEP encryption; since it is a symmetric scheme, decryption is straightforward, given the secret key.

For WEP encryption, the plaintext is bitwise exclusive-ORed (in exclusive-OR is a binary operation often abbreviated as XOR, where the output is 0 if the two input bits are the same and 1 otherwise) with the output of the WEP pseudorandom number generator to produce the cipher text. Thus, the cipher text can be decrypted only if the output of the WEP pseudorandom number generator is known. The idea is that only the intended receiver would know the two inputs to the WEP pseudorandom number generator that the transmitter uses. These two inputs are a secret key and initialization vector (IV). How does the receiver know these values, The802.11 standard assumes, but does not specify, the existence of an external key distribution mechanism that distributes the secret key to a set of authorized mobile stations. The IV, on the other hand, is not distributed beforehand. Furthermore, it may be changed by the transmitter as often as with the transmission of every 802.11packet. However, the current IV value is always appended in plaintext to every802.11 packet, so the intended receiver only needs to know the secret key beforehand. Note that this also means that the other stations to which the same secret key has been distributed can also decrypt the packets for the receiving station. This is not necessarily cause for alarm, since WEP is only meant to provide privacy equivalent to that of a WLAN. Furthermore, the set of authorized mobile stations with the same secret key can be thought of as analogous to stations on an Ethernet LAN, which can hear all the traffic on the same LAN.

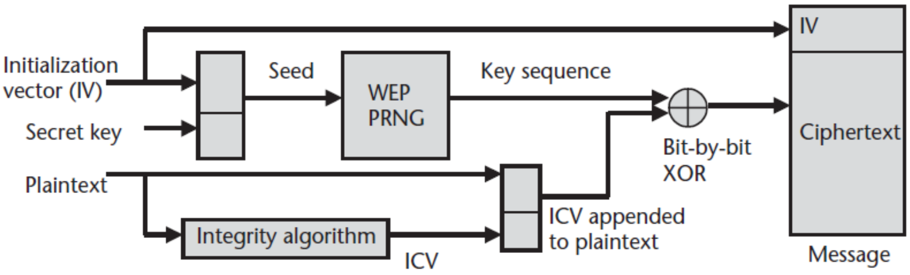

Figure 1: WEP encryption.

Nevertheless, the various weaknesses of WEP have been highly publicized (Cam-Wignet, 2003).As a result, an enhanced version of WEP, sometimes known as WEP2, has been developed, that uses 104-bit keys instead of 40-bit keys. Meanwhile, the IEEE came up with 802.11i, for enhancing WLAN security. 802.11i introduces a new security framework for the 802.11 family that incorporates 802.1x (for integration into the AAA infrastructure and thus providing network access control for roaming mobile stations), as well as stronger encryption algorithms. These new encryption algorithms include advanced encryption standard (AES).The 802.11i standard closes many of the holes found with WEP. Meanwhile, some organizations that are more security-conscious have opted for network-layer solutions to complement the security mechanisms provided at the link layer by 802.11. These solutions include the use of IPsec(security framework for IP-layer security services). In a wireless context, though, there are issues that arise from the use of both IPsec and Mobile IP together, and these will be discussed in the coming sections.

2.1 GSM Security

In GSM, as with any other wireless system, user authentication is very important because users are mobile and often change their points of attachment to the network. The authentication forms the basis for ensuring that only authorized users obtain service from the network, and only for the services for which they are authorized. The other major security service that GSM provides is confidentiality, to prevent attackers from listening to mobile phone conversations.

Confidentiality is mostly provided by encryption, with one significant exception that we will explain. The authentication and encryption mechanisms used in GSM are not independent. Instead, the key used for the ciphering (encryption) is computed as part of the authentication process. So we examine authentication first. There are two kinds of authentication that are needed. First, because the phones are small, light, and portable, they can be easily misplaced and fall into the hands of unauthorized users. Thus, the human user of the phone must be authenticated with the phone through a password that is typically arranged in conjunction with the service provider upon signing up for service. More precisely, the authentication is with the SIM card, if you replace your SIM card in your phone with another, you need to know the password for the other SIM card. The human user only has access to all the features of the phone (including making and receiving calls) after successful authentication with the SIM card. Note that this authentication is only local on the phone; nothing goes over the air in this process.

Thus, a second kind of authentication is needed, in which the GSM network authenticates the subscriber for service. More precisely, the GSM network actually authenticates the SIM card in a process that does not involve the human user, and that happens multiple times, regularly, when a mobile phone is on. To those who might wonder why the human user is not directly authenticated with the network, but indirectly through the SIM, we point out the analogy of the ubiquitous lock-and-key system used to safeguard most people’s houses. The key is analogous to the SIM card, and the lock to the authentication procedure with the GSM network. The lock authenticates the key, not the human! Anybody with the right key can open the lock. What is to prevent somebody from stealing the keys and using them, the person has to know the right house in which to use the keys.

Knowing the right house is like knowing the password in the user authentication to the SIM card. Authentication of the SIM by the network is done through a challenge/response mechanism. The SIM and the authentication center (AuC) in the mobile Station (MS’s) home network share a key, K_i, which must never be revealed to third parties. K_i and a random number are used by the AuC as input to an algorithm, A3, to generate a value, signed response (SRES). The network sends the SIM a challenge, namely the random number. It expects that only the SIM with K_i can use A3 to generate the correct SRES for the input pair of K_i and the random number. Thus, the response sent back to the network is the SRES the SIM computes. The network compares the two values, and if they match, the SIM is authenticated. GSM authentication is illustrated in Figure 2 (note that this is a conceptual view of GSM authentication, because we have been referring to “the network” as a single entity, whereas actually two network elements are involved; a more complete picture of GSM authentication is given in Figure 3).

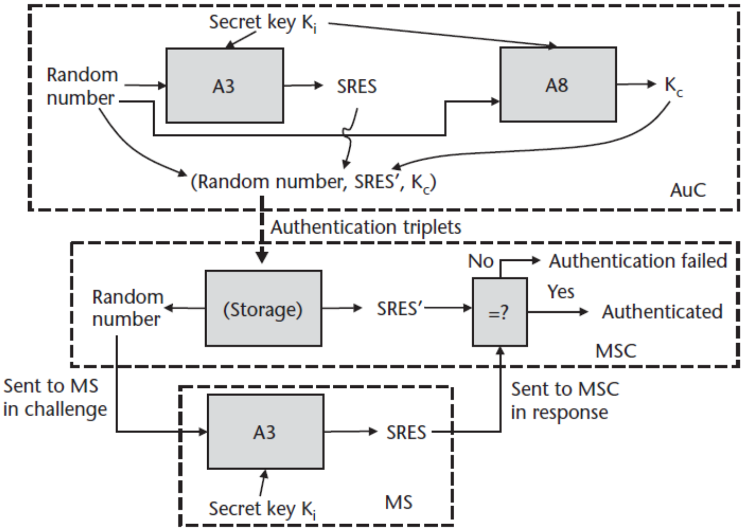

Figure 2GSM authentication (conceptual).

Most of the time, user traffic is encrypted for privacy. However, the ciphering(encryption) can be turned on only after authentication completes. This is because the key used by GSM encryption, K_c, is computed during authentication. Therefore, GSM cannot provide privacy for the control signaling that initiates authentication. The main concern is that the MH needs to identify itself at this time. In particular, the network needs to obtain the MH's (international mobile subscriber identity) IMSI from the MH.

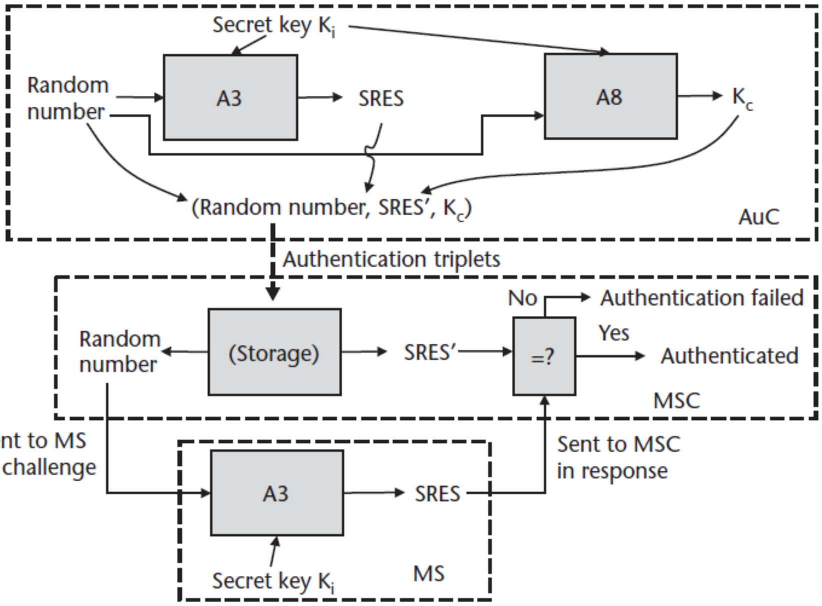

Figure 3: GSM authentication.

The problem is that sending the IMSI regularly over the air unencrypted opens the door to theft of the IMSI and other privacy issues. GSM uses an ingenious work around; instead of sending the IMSI over the air each time the MH needs to identify itself to the network, it usually sends what is known as a temporary mobile station identifier (TMSI). The link between TMSI and IMSI is known by the serving mobile switching center (MSC), and GSM provides for a way to pass this knowledge to the next serving MSC, upon handoff to a new MSC. Thus, the sending of the IMSI itself over the air in plaintext is minimized.

Network could be the AuC doing all this, but typically it is the serving MSC, so the signaling does not have to take a long time going between the AuC in the home network to the MS in a foreign network, when it is roaming. But the AuC cannot reveal the K_i to any MSC. Thus, the solution is for the AuC to pre-compute authentication triplets comprising of (random number, associated SRES computed with that random number and K_i, resulting K_c), and to send these triplets to the MSC in batches. Thus the MSC only once in a while would contact the AuC to refresh the triplets. Figure 3 shows the more complete picture of GSM authentication that includes the authentication triplets. Finally, we turn to confidentiality in GSM. As we mentioned, K_c is derived during authentication. The same two inputs, K_i and the random number, are sent to a different algorithm (A8, instead of A3) to generate K_c. The encryption scheme used is a secret key scheme. Two new keys, S1 and S2, are generated for each frame, using the A5 algorithm. The inputs to A5 are the frame number and K_c, so S1 and S2 will change from frame to frame. S1 is used to XOR the traffic from the network to the MS, while S2 is used to XOR the traffic from the MS to the network.

2.2 Security and Mobile IP

Mobile IP provides basic support for authentication, but not confidentiality or data integrity. This is because authentication is more of a challenge where there is mobility than in networks without mobility. How does a HA know if the registration message it is receiving from a foreign network is really from one of the MHs it serves meanwhile, the need for confidentiality and data integrity are not necessarily increased in mobility situations. Therefore, confidentiality and data integrity are presumed to be handled by other IP protocols. Since Mobile IP does not make assumptions about the security of the wireless link, it has to assume that transmissions can be heard by attackers (eavesdropping).Therefore, replay attacks may be possible, and so the authentication schemes must be protected against replay attacks. What are the entities that are need to have security associations with each other, at a minimum; the MH must be able to authenticate each other's messages.

Otherwise, if the HA does not authenticate the registration message from the MH, any node could claim to be the MH and maliciously register an arbitrary IP address as the MH's COA. Similarly, if the registration response from the HA is not authenticated, an attacker could intercept and destroy the MH's registration message, and state falsely that the home agent (HA) has updated its binding for the MH to the latest care-of address(COA), by sending an unauthenticated registration reply to the MH.

Therefore, Mobile IP makes it mandatory for both registration messages and registration replies to be authenticated. This is done by including the mobile-home authentication extension in the messages. (Mobile IP uses a general method of allowing miscellaneous, optional information to be attached to Mobile IP messages, while extensions are self-contained sequences of information, including an extension type code and length.) The mobile-home authentication extension contains a 4-byte SPI that, together with the home IP address of the MH, uniquely identifies an MH-HA security association. The default authentication algorithm is HMAC-MD5 [2].Additionally, there may also be security associations between the MH and foreign agent (FA), and between the FA and HA. Two optional authentication extensions, the mobile foreign authentication extension and the foreign-home authentication extension, are optionally attached to Mobile IP registration messages and replies. These would only make sense when an FA is used—thus, they are not used when a collocated COA is being used. Although these two are optional, they must be used when the MH and FA, or FA and HA, respectively, share a security association.

Note that of the three authentication extensions, the Mobile-Home and Mobile-Foreign Authentication Extensions (if used) are added by the MH in registration requests, whereas the Foreign-Home Authentication Extension (if used) is added by the FA in the registration request, when it forwards the registration message from the MH.

2.2.1 Mobile IP and AAA

We note that the original Mobile IP security model, as just described, assumes that the MH is able to actually send Mobile IP registration messages, and respond to them, soon after entering the foreign network. This implies that the foreign network has given the MH sufficient access to its network to be able to do the registration. More specifically, if co-located COAs are used, this means the MH is able to obtain an IP address in the foreign network, and if FAs are used, this means that the FA is receiving and processing Mobile IP registration messages from the MH. How valid is this assumption, in many cases, for mobility within an organization (more specifically, where the points of attachments used are all part of the same network administrative domain), it is valid. For example, if the points of attachment are WLAN access points (Aps), all APs and MHs belonging to that organization may use the same WEP key. However, it turns out that the assumption is not valid in many practical situations. In many practical situations, an MH may move into areas that are part of a different network administrative domain than its home network administrative domain. This may be the case if the MH is part of an organization that is so large that it wants to have multiple administrative domains (e.g., one per office location or per business unit), or if the MH simply moves into a network belonging to a different organization. In these cases, the MH may have trouble obtaining connectivity to perform Mobile IP registration (Krawczyk et al, 2014).

A good analogy offered by Perkins is that the designers of Mobile IP assumed connectivity would be provided as a courtesy service to visitors, in the same way that free electricity is provided to visitors to charge their laptops (Perkins, 2000). However, this turns out not to be the case. I think this connectivity is more like library borrowing privileges not casually given to visitors! And there are good reasons for treating connectivity like library borrowing privileges rather than for treating it like electricity. Network resources are a valuable commodity, like library books use of network resources may not infrequently affect network performance for other, more legitimate users. This is rarely the case for electricity. Often, in these cases of movement between administrative domains, the network prevents foreign or unknown terminals from having access. Two main classes of access control are

(1) Access control schemes that work at the link layer and
(2) Access control schemes that work at the network layer.

An example of a link-layer access control scheme is the use of WEP, where the user has to know the WEP key to be able to establish a wireless link. Another example is a WLAN authorization scheme that only allows establishment of link-layer connectivity with an AP if the MH has a MAC address that is in a database. With these schemes, link-layer access is denied to unauthorized network outsiders, so an MH would be unable to send any IP packets, not to mention Mobile IP registration messages. An example of a network-layer access control scheme, on the other hand, might be to allow wireless links to be established, but to place an access router behind the wireless link, on the network side, that controls further access to network resources. The access router may allow limited access only to an AAA server and not to other network services.

After the exchanges with the AAA server, the access router then opens up access to the relevant set of network services as appropriate. Whether access control is of the link-layer or network-layer variety, the obvious solution is for AAA servers in the foreign network to communicate with AAA servers in the home network. This is because the foreign network AAA server probably does not have information about the MH, while the home network server should have such information. A typical arrangement is that the operators of the two networks have agreed to allow subscribers from each other's networks to access an agreed-upon set of services. This set of services may be small, perhaps just basic IP connectivity with best effort service, or it may also include other services like preferential queuing services in routers. In any case, the AAA server in the foreign network communicates with the AAA server in the home network so the AAA server in the home network can authenticate that the MH is indeed one of the home network's subscribers. Furthermore, since subscribers may not all have the same authorization for services, the server can authorize the MH for the appropriate set of services. Lastly, accounting can be performed so that network usage can be monitored and the subscriber billed appropriately.

A common and popular protocol for AAA is remote authentication dial-in user service (RADIUS) (Rigney, 2000). A more modern protocol for AAA is DIAMETER (Calhoun, 2003). Whatever the AAA protocol used, the next is how to get it to work with Mobile IP. The first option that might come to mind is to use AAA first, thus providing connectivity, and then to do Mobile IP registration, thus providing proper routing for the home IP address. However, this slows down the handoff process. Already, with Mobile IP alone, there can be serious handoff latency problems, and adding the latency from the AAA communications will cause more user unhappiness. Therefore, the currently in-favor model is to combine the AAA and Mobile IP signaling by piggybacking Mobile IP registration messages on AAA messages, as shown in Figure 4. This helps with latency, because only one round-trip is made between the two networks, rather than two, in the case that AAA is first completed before Mobile IP begins. This comparison is illustrated in Figures 5 and 6.

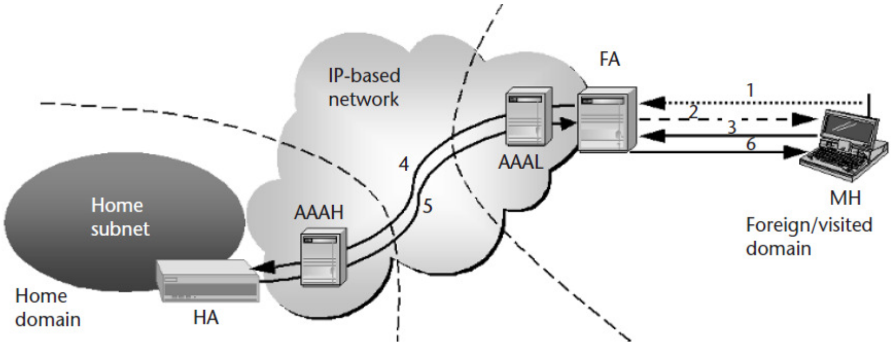

Figure 4: Mobile IP with AAA.

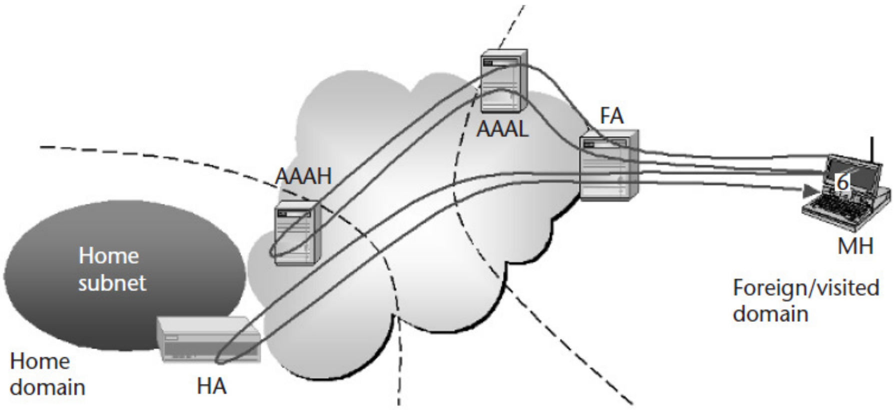

Figure 5: Two round-trips add latency to registration process.

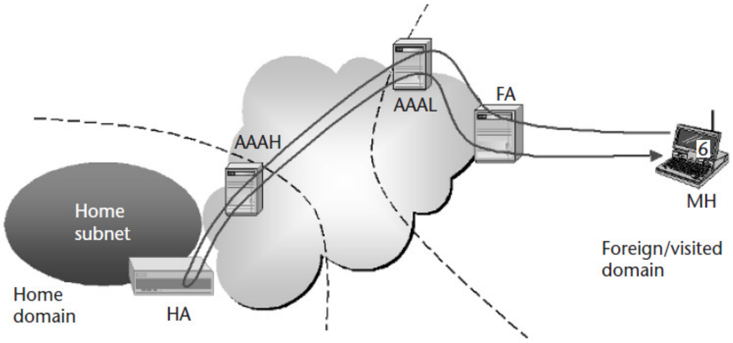

Figure 6: One round-trip reduces latency impact of AAA.

2.2.2 Mobile IP and IPSec

We have seen how the use of Mobile IP may result in problems with the use of Resource Reservation Protocol (RSVP) for QoS purposes, because RSVP was designed with the implicit assumption that the IP addresses of the end hosts do not change during the time that RSVP is used. Similarly, because an IP destination address is one of the three parameters that identify an IPSec security association, we might reasonably expect that the simultaneous use of Mobile IP and IPSec results in the same kinds of problems. Actually, in many cases, this may not be an issue, such as when IPSec is not used end to end but between two fixed gateways, which is the case in many (virtual private network) VPN applications. However, in some applications it may become an issue, such as when one end of the IPSec tunnel is at an MH, as would be the case in the wireless band-aid application we introduced in Table 1.Some proposed solutions suggest modifications of IPSec or Mobile IP to make them work together. For example, it has been suggested that the Mobile IP tunnel should be modified to be IPSec tunnels bearing either an encrypted security payload(ESP) or authentication header(AH) (or both), instead of being IP-in-IP tunnels (Binkley & McHugh, 1999).

Table 1 Example applications and needs

Applications	Needs
VPN	Create a virtual network over a shared IP network like internet, where all the traffic must be confidential.
Wireless link band-aid	Add an artificial ‘skin layer’ of protection for all IP packets over a vulnerable wireless link.

Another approach introduces the concept of a wireless security gateway that intercepts all packets on the wired side headed for the HA (Barton, 2002). Thus, regular IPSec packets are inserted into, and removed from, the Mobile IP tunnel. Thus, there is dual encapsulation between the HA and FA. The IP addresses on both sides remain unchanged whether the MH is at home or roaming; in particular ,it is the IP address of the security gateway interface that faces the HA on one side, and the home IP address of the MH on the other side (since the IPSec tunnel is outside the Mobile IP tunnel).

3. CONCLUSION

We discussed about security in this paper. After introducing the kinds of security services typically required for network security (confidentiality, data integrity, message authentication, non-repudiation, uniqueness, user authentication, user authorization, service availability, and intrusion detection), we briefly introduce the range of cryptographic algorithms, such as DES, at our disposal. We then consider IP network security in particular, touching upon requirements and briefly introducing IPSec. More time is spent on security in wireless networks, including WLAN security and GSM security. We explore the interactions of Mobile IP with security protocols like IPSec and AAA protocols.

REFERENCES

1. Saltzer, J. H., and M. F. Kaashoek, "Topics in the Engineering of Computer Systems," classnotes for Computer Systems Engineering course at MIT, 2003.
2. Krawczyk, K., M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication,"RFC 2104, February 1997.
3. Dierks, T., and C. Allen, "The TLS Protocol Version 1.0," RFC 2246, January 1999.
4. http://www.openmobilealliance.org/; formerly http://www.wapforum.org.
5. Cam-Winget, N., et al., "Security Flaws in 802.11 Data Link Protocols," *Communications of the ACM, Special Issue on Wireless Networking Security,* Vol. 46, Issue 5, May 2003,pp. 35–39.
6. Perkins, C., "Mobile IP Joins Forces with AAA," *IEEE Personal Communications Magazine,* August 2000, pp. 59–61.
7. Rigney, C., et al., "Remote Authentication Dial in User Service (RADIUS)," RFC 2865,June 2000.
8. Calhoun, P., et al., "Diameter Base Protocol," RFC 3588, September 2003.
9. Binkley, J., and J. McHugh, *Secure Mobile Networking Final Report*, June 1999;http://www.cs.pdx.edu/research/SMN/final.ps.
10. Barton, M., et al., "Integration of IP Mobility and Security for Secure Wireless Communications," *ICC 2002,* New York, June 2002.