Global Information Assurance Certification Paper

An Overview of Link Security – Protocols and Standards

Wen-Pai Lu

February 18, 2004

GSEC Practical Assignment Version 1.4b

GIAC Security Essential Certification (GSEC)

Table of Content

List of Figure

Abstract

The use of new technologies creates new security challenges in the enterprise infrastructure. The advent of wireless networking and the use of optical networks in the Metro Ethernet services combined with long haul networks have dramatically changed the landscape of enterprise networks. Traditional methods, such as perimeter security, applications security, etc., of protecting infrastructure may not be adequate. New security threats are discovered when these new technologies are introduced. Protecting enterprise infrastructure can no longer remain at layer 3 and above. The link security has become more important in the enterprise infrastructure security.

This paper will first present a list of potential new threats in the link layer and also discuss the need for link security. Then, the past and the current development of link security technologies and standards are presented. From the MAC address filtering method to the more complex wireless LAN security and the most recent MAC security standard the newly created IEEE standard working group developed, each method only addresses certain parts of the protection needed. After the overview of these technologies, a short presentation will explore the steps the enterprise may take to align the link security with their overall security strategy in order to strengthen the enterprise security architecture.

Introduction

New technologies are constantly introduced into the enterprise infrastructure. Access to the enterprise networks is not limited to the wired connection at your desktop or remote access through dial-up connection. Wireless LAN connection in the office as well as other wireless access through hot spots wireless LAN services and cellular data networks such as CDMA 1x (Code Division Multiple Access 1xRTT), GPRS (General Packet Radio Service) and EDGE (Enhanced Data Rates for Global Evolution) are becoming a common method to access the corporate infrastructure. Inside the enterprise networks, traditional dedicated links for inter-office connections have been replaced by metropolitan optical shared network services such as PON (Passive Optical Network), Metro Ethernet and Transparent LAN services. Carriers are finding ways to increase their network capacity without incurring additional operational expenses for enterprise LAN-to-LAN interconnections.

Inside the corporation, networks are easily accessible, not just from your desktop, but also from the network ports in conference rooms, customer presentation areas, as well as in the cafeterias. Network connectivity is everywhere inside the corporate campus and buildings so as to offer convenience for employees to increase their productivity. New technology such as IP telephony is deployed in the enterprise infrastructure in order to realize a truly voice, data and video

integration. These new technologies are implemented for improving the collaboration and communication among employees. Accompanying these new technologies, some latest devices such as IP telephones are used. The IP telephones are simply mini-PCs sitting on the desktop and they could handle more than just voice conversation.

The connection to the outside world provides an easy path to access resources on the Internet. Getting the software that allows users to look at the traffic passing by the link is just a click away. With the open network most enterprise is deploying and the easily available tools for monitoring network traffic, the level of threats will definitely increase. In addition, the trend of outsourcing resources in the enterprises is increasing. Corporations are hiring more and more contractors to handle their non-core businesses. The access to the corporate resources by these contractors is no different from regular employees. The contractor access to the corporate resources is basically restricted at the application layer. Thus, protecting corporate intellectual property and resources may require a different approach from the traditional practices. Link security is becoming the gap where most enterprises have ignored.

In this paper, we will first outline the security challenges in the enterprises today. Many of these security threats are exposed at a much lower layer such as at link layer where traditional security approach has missed. The next section will present a list of security threats occurred at link layer, and the needs for providing link security. Then, the rationales for requiring the protection at link layer as compared to other layers will be presented. After reviewing the link security, the paper will present a survey of past and present technologies and standards that address link security. This survey illustrates the history of developing such technologies, and the goal for the future ones. Finally, the paper will conclude with a proposal that discusses the steps the enterprise should take in order to develop its strategy that will lead to a more secure enterprise network.

Overview of Link Security

Security Challenges

In recent publications, more internal threats have been reported as compared to outsider attacks. Of the total attacks, over 70% are internal. Preventing internal attacks are becoming one of the urgent objectives in securing enterprise infrastructures. In addition, the popularity of deploying wireless LAN in the enterprises in the last couple of years, and the reports on wireless LAN vulnerabilities have placed more efforts in securing wireless LAN access. However, almost none or very little attention is focused on data protection strategy in the enterprise wired network.

As mentioned earlier, the availability of network ports in the corporations and the use of outsourcing resources post huge potential threats to the corporation. The threats increase several folds when new technologies such as IP telephony are deployed without knowing much about the security threats that may be exist in these new technologies. Since tools that can sniff the network from any place inside the enterprise infrastructure are easily available on the Internet, protecting corporate assets at the application layers will be inadequate.

The use of VLANs (Virtual LANs) in a corporation to partition users to different networks and separating their traffic is getting popular. For better security in each VLAN, granular security control and protection on every VLAN is needed. Although technology is available in restricting port access at the link level by the MAC addresses, this traditional approach is very labor intensive. The labor intensive efforts and the high operational expenses have prevented many network managers from deploying it in the enterprise infrastructure.

Many attacks to the enterprise networks exploit the vulnerabilities at the communication protocols level. These protocols are primarily at the network and higher layers[2]. In such, most attention in addressing these network threats are on the IP and higher layers, such as TCP, UDP and other application protocols. Focus on the data link protection has traditionally been ignored because the number of attacks is small and the impact is still very minimum. However, it does not mean that the attacks at the link layer do not exist. Many hackers and intruders are finding new ways to attack the corporate infrastructure, and these vulnerabilities may be their next targets.

Security threats in the Link Layer

Before discussing about the link layer protections, it is imperative to understand their potential threats. Understanding these threats in the data link layer would be the first step in developing a link security strategy.

First of all, sniffing the network traffic is not a difficult task as Sniffer and many other tools [1] can be easily obtained from the Internet. With these tools, intruders can obtain highly confidential information. Secondly, by capturing the passing traffic, an intruder can easily impersonate another user using her station IP address and user information to access authorized systems as well as resources. Similarly, an intruder can intercept the traffic and perform man-in-the middle attacks. Although the network may install an authentication mechanism to control the permission of users to access the network, the intruder can still sniff the link between the users and the network, and capture all information being exchanged between them.

The open network ports in the corporate public area, such as lobby, cafeteria, and open conference room is one of the vulnerabilities many enterprises start to

[2] It means OSI layer 3 and above.

address. Although the threat can be significantly reduced by blocking the network ports located in the public area, this will defeat the purpose of allowing employees to work from anywhere in the corporate building. Since there is no integrity control over the network, an intruder can capture the data traversing over the link, change the content and insert the data into the network. Detecting the unauthorized modification of packet will be difficult. Also, an intruder can easily inject unauthorized frames, such as worms or virus, into the network that could cause the disruption of the network services. As the network does not provide any verification on the packets entering the network, it would be hard to account for the sabotage.

The needs for Link Security

In today's enterprise environment, as we have discussed earlier, multiple types of networks are deployed in the corporate infrastructure – Ethernet, wireless, WAN over shared network, metro wireless and wired network, and many other more. As more and more of these types of network deployed in the enterprise infrastructure, protecting information traveling across these networks is a challenge. Since these networks may be in different domains controlled by different discrete authorities, ensuring end-to-end security may not be easy. Each authority of the network segment may have different security policy and control mechanisms.

Even in the enterprise network, more and more MAC[3] technologies may be deployed. For example, Ethernet (IEEE 802.3) and wireless LAN (IEEE 802.11) are getting popular in many corporate infrastructures. Different MAC technologies, such as WPAN (wireless personal area network, 802.15), WWAN (wireless wide area network, 802.16), and WMAN (wireless metropolitan area network, 802.20) are being developed in the IEEE 802 standard committee. These network technologies may be deployed by a service provider or the enterprises themselves in the enterprise network in the near future as standards are ratified and products become available.

In addition, link layer access is the first line of defense in the enterprise. Permission to use the network should be controlled at the link layer. Authorizing legitimate users is equally as critical as identifying the resources to be protected. Although VLANs is used in separating user traffic, protecting data traffic on the VLANs is also needed. Without the protections at the link layer, the corporate network could be exposed to the intruder attacks.

Why Link Security?

Clearly we have witnessed strong evidences that the needs for link security are growing. While protecting corporate data traffic can be accomplished at different layers in the OSI reference model, why should we focus on the data layer? In

[3] MAC – Media Access Control, an IEEE layer 2 protocol.

this section, we will explore why link layer is critical in the overall enterprise security blueprint since some of these protections cannot be adequately supported at the higher layers.

Traditionally, many protection mechanisms are performed at the application layers afforded by the application software, servers and part of the Internet (SSL for web access). In some cases, layer 3 or transport layer protection is the norm, such as IPSec or TLS. However, many protocols used in the enterprise are not securable via layer 3. Such protocols include but are not limited to NetBEUI, Spanning tree, ARP (Address Resolution Protocol) and DHCP (Dynamic Host Configuration Protocol). The intruder can exploit this vulnerability and attack the network to cause destruction or paralyze the corporate network services. For example, changing the spanning tree topology could cause an unstable condition or create a loop environment, which could completely paralyze corporate infrastructure.

On the other hand, security at the link layer (OSI layer 2) provides a lighter implementation. There are fewer protocol elements in the layer 2 as compared to the layer 3. The complexity of protecting upper layer protocols will result in operational headache and increase operational expenses.

As corporations begin to promote collaboration and communications among employees as well as the distribution of corporate meetings to global audiences, the use of multicast technology is getting popular in the enterprise. There are several challenges in providing multicast security at layer 3 and above. First of all, multicast key and its distribution are an issue at layer 3. Distributing the multicast key in a secure manner, updating and revoking multicast key may not be easy. With the layer 2, the use of the key between two nodes can also be applied to both unicast and multicast. Moreover, the data sent over the link layer will be less replicated than at layer 3. The connection is also more reliable and receiver is smaller at layer 2 as compared to layer 3.

The Link Security Technologies and Standards

In this section, an overview of the past and current technologies and standards for the link security will be presented. As the enterprise needs evolve and the nature of the enterprise infrastructure changes, the technologies and standards developed at different periods of time presented the solutions addressed to the requirements for those needs. Nevertheless, each development is not isolated and each one can be linked to the previous efforts.

MAC Address Filtering

The link security technology was developed at around the same time when LAN technology was being deployed in the enterprise network. It happened in the late

80s whereby two major LAN networks were being used, namely Ethernet (10 Mbps) and Token Ring. The earlier LAN equipment vendors, such as Cabletron, 3Com, Cisco etc. had provided port security in their switch products. Each port of the switch is manually configured with the filter that allowed only one or a group of MAC stations for using that port. The purpose was to prevent other MAC stations from connecting to that port, thus ensuring only authorized stations could be connected to the corporate network.

Although the use of MAC address filtering may work in preventing unauthorized stations in accessing the network, the labor intensive configuration does not scale well for large networks deployment. The complexity of managing networks and the inflexibility of user mobility is one of the major reasons why very few enterprise networks utilize this technology. The technology, if deployed, is usually implemented in the highly secure and well protected environment such as in the data centers.

Standards for Interoperable LAN Security (SILS) – IEEE 802.10

The concerns for LAN security increased when the use of LAN became popular in the late 80s. Although MAC filtering technique solved the problem of controlling unauthorized access, the lack of automatic control mechanism prevented wide spread deployment. Moreover, no additional control was enforced after the user's access was authorized. In 1988, a new group within IEEE 802 standard committee was formed to address security concerns in local area networks. The Standards for Interoperable LAN Security or simply called SILS working group was formed. This working group was assigned as the IEEE 802.10. The purpose of this working group, as the name implied, was to develop an interoperable security standard for local area networks, such as Ethernet, Token Passing and Token Ring. The working group primarily developed standards and specifications for security at layer 2. In order to support the security services required at layer 2 such as the keys used for encryption and decryption, they also developed the key management protocol, which was a layer 7 protocol that could communicate with layer 2 protocols.

Several implicit characteristics of LANs can potentially create vulnerabilities in the LAN environment. First of all, the address space of the LAN is flat, i.e., no hierarchical structure in the LAN address. The network administrator cannot specify the addresses each segment of network needs in order to control the access of LAN resources. Although the LAN station address is unique, any station can easily impersonate other LAN address as long as the address is not used on the same segment. The source of a LAN packet cannot be authenticated. Once the data is on the network, any station on the LAN can see the packets passing by. Since any station can see the traffic, there is no guarantee that the data received by the recipient has not been modified. Thus the potential threats appeared on a LAN include: unauthorized disclosure, masquerading, unauthorized data modification and unauthorized use of

resources. In order to address these threats on a LAN, the security services required are: connectionless confidentiality, authentication, connectionless integrity and access control. Note that only the connectionless implication of both confidentiality and integrity was applied. This is because of the nature of LAN traffic characteristics.

The IEEE 802.10 [2] standard developed under SILS consists of eight parts[4]:

Part a Security Architecture Framework

Part b Secure Data Exchange (SDE) protocol

Part c Key Management Protocol

Part d Security Management, being incorporated in part a

Part e SDE on Ethernet 2.0

Part f SDE Sublayer Management

Part g SDE Security Labels

Part h SDE PICS Conformance

Due to the length of this paper, we will just focus on the description of SDE. The SDE protocol was the first one being developed and is the core of the 802.10. Readers can read other documents provided in the following link to further understand the rest of the standard: http://standards.ieee.org/getieee802/802.10.html.

Secure Data Exchange (SDE)

The Secure Data Exchange (SDE) protocol was the first work defined by the SILS working group. The protocol defined the framework on the method two stations can communicate with each other in a secure manner. The standard defined the protocol mechanism as well as the frame format. The SDE was defined as a layer 2 entity. The entity is located above the MAC sublayer in 802 LAN and MAN protocol stacks, and is part of the LLC (Logical Link Control) sublayer. Figure 1 shows the location of SDE entity in the IEEE 802 reference model.

[4] Part b, e, f, g and h were finally incorporated in IEEE Standard 802.10 in 1998.

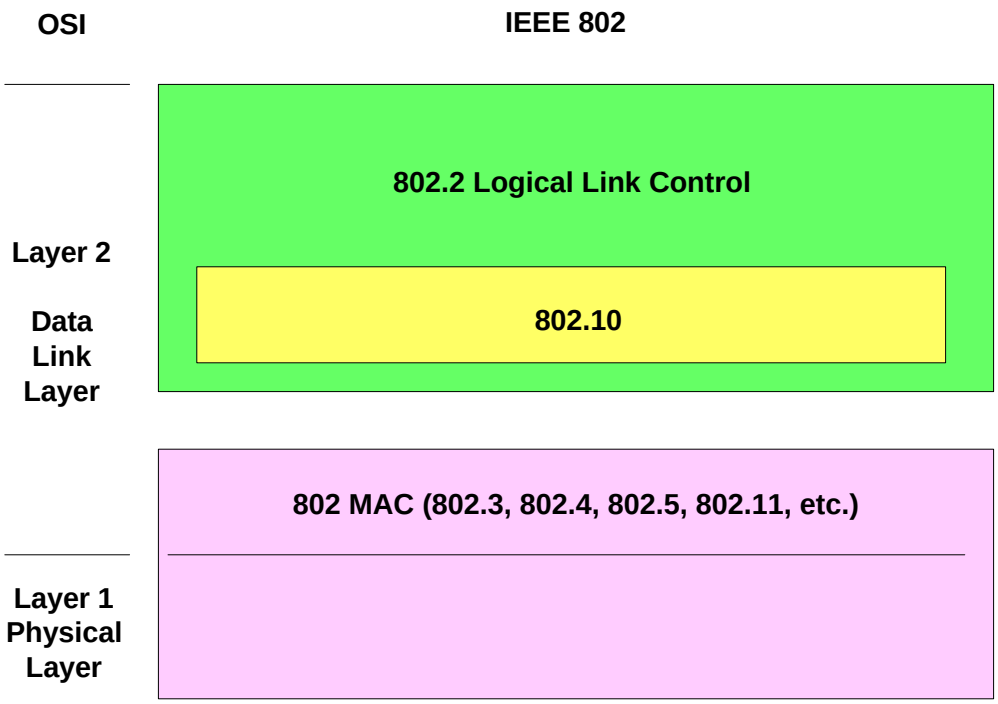

Figure 1. Location of 802.10 in the IEEE 802 Reference Model

The SDE protocol offers connectionless security services for all MAC layers[5] in the IEEE 802 family and other MAC layer protocols, such as FDDI (Fiber Distribution Data Interface). The SDE protocol specifies the provision of four security services at the data link layer: *data confidentiality, connectionless integrity, data origin authentication and access control*. Note that the four security services proposed by the SILS working group at that time were very unique. Before SILS, the ISO 7498-2 [3] defined a set of security services required at different layers of the OSI reference model. At the link layer (layer 2 of OSI reference model), the ISO 7498-2 specified that Data Confidentiality service is the only security service required at layer 2 due to the historical reason. The other three security services specified by the SILS working group were viewed by the ISO 7498-2 as the services that can be offered at upper layers. With the influence of SILS work, the ISO 7498-2 later issued an amendment [4] to specify the needs for these new services and mechanisms over LANs. Also note that among the authentication services, only data origin authentication service was needed due to the nature of LANs.

[5] At the time of the standard development, there were only 4 IEEE 802 MAC layer standards being defined, 802.3, 802.4, 802.5 and 802.6. By the time of completion of this part of the standard, 802.11 was still under development.

In the following, we will examine the protocol developed by the 802.10, which would support the abovementioned security services for addressing LAN threats. Before we start to describe its function, let us first examine the structure of the SDE PDU (Protocol Data Unit), which is shown in Figure 2. As shown in Figure 1, the SDE is above the MAC sublayer, and is within the LLC sublayer. Thus, the SDE appends additional headers to the LLC PDU (also called SDE Service Data Unit (SDU)) and passes to the MAC layer as the MAC frame data.

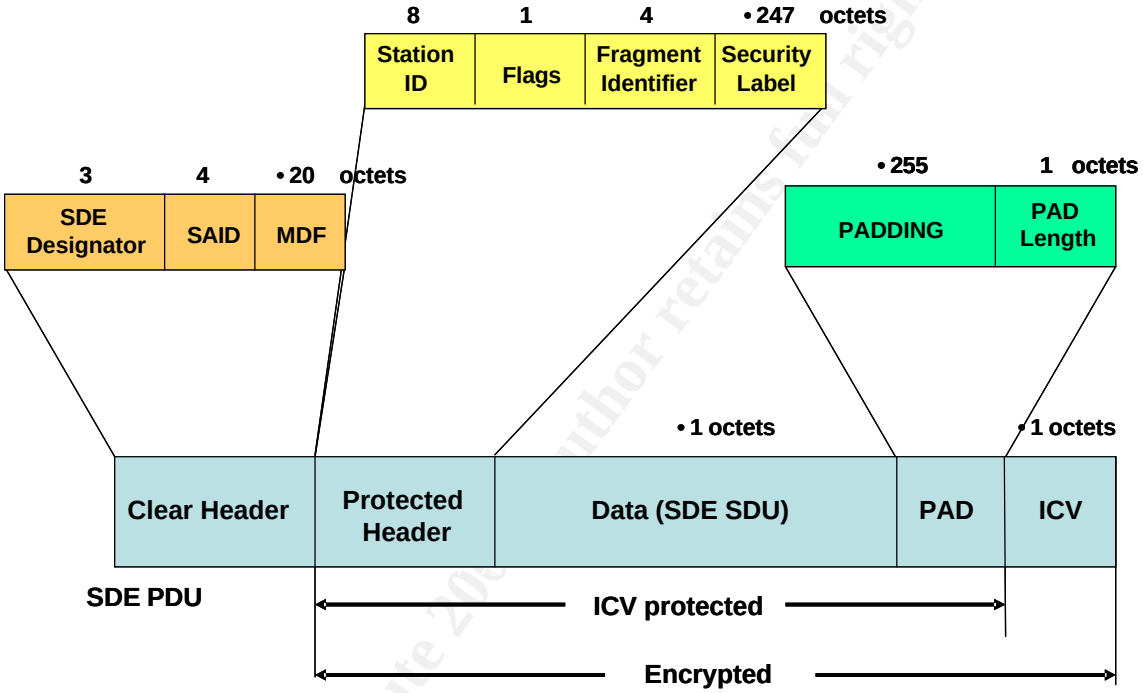

Figure 2. SDE Frame Format

The first header is a clear header. As the name implied, this header is not encrypted since the information is used to determine the type of security functions needed. Inside the clear header, there are three fields, namely SDE Designator, SAID and MDF (Management Defined Field). The use of SDE Designator is to identify SDE packets from non-SDE packets, which would allow the SDE station to process the SDE PDU as well as non-SDE PDU for interoperability purposes. The SDE Designator is identified by a reserved LSAP (Link Service Access Point).

The secure communication between two stations depends on the establishment of the security association they agreed upon. In order to obtain a security association, a key management scheme such as the one defined in IEEE 802.10c [5] can be used to negotiate for a set of agreeable key attributes and parameters. Once the security association is established, an SAID will be

created for their subsequent secure session. The agreeable keying information and its associated attributes will store in their local database called the SMIB (Security Management Information Base). The SAID is a pointer that indexes the table in this SMIB. The SAID is used for ensuring the authenticity of two communication entities. When both communication entities have the same SAID, they are then authorized to securely communicate with each other. In addition, the station ID in the Protected Header of the SDE PDU can also be used to identify the desired station for such communication. This Header is encrypted using the key negotiated during the establishment of the security association. Thus, data origin authentication service is provided. The MDF field is just a reserved space for future expansion.

Before an SDE enabled station[6] can communicate with its peer in an SILS LAN environment, the creation of security association would ensure that the station is legitimate and that they are allowed to use the LAN. This enforces the access control service. The SILS does not define a specific access control policy since the security policy is unique in each implementation environment and is outside the scope of this standard.

The confidentiality service is provided by encrypting the SDE PDU (excluding the Clear Header) using the key and its associated attributes stored in the SMIB. The standard does not mandate a specific cryptographic algorithm for encrypting the data. It is the choice of the implementer. However, the standard provides a platform to accommodate multiple types of encryption standards and algorithms.

The integrity service is given by computing the ICV (Integrity Check Value) of the SDE PDU (excluding the Clear Header). This field provides a mechanism for detecting data modification. The standard does not specify the type of algorithm in producing ICV. It is negotiable between two communicating entities and the attributes are stored in the SMIB.

In addition to the SDE protocol, SILS working group also developed other specifications such as key management protocols, security labeling, PICS (Protocol Implementation Conformance Statement) Proforma, security management and security modeling. The 802.10 standard defines a very comprehensive suite of protocols for LAN protection. Originally, each of this protocol was developed as one part of the overall standard. These parts, once finished, were then combined into one complete standard [2].

During the mid-90's, the needs for LAN protection basically did not exist in the commercial applications. Most of the security concerns were addressed in the government agencies. Thus, several products were developed for government or military use and very few commercial products were available. Later, a proposal of using the IEEE 802.10 SDE for the VLAN-like functions [6] in the switched networks was sent to the IEEE 802.1 committee and was discussed

[6] An SDE enabled station means a secure station that is protected by the SDE protocol.

during the development of VLAN standard, IEEE 802.1Q [7]. The recent developed standard, 802.1AE, which will be presented later in this paper, had recently discussed in the working group to incorporate some of the 802.10 features into this new specification.

Port Based Network Access Control – IEEE 802.1X

The IEEE 802.1X protocol was developed to provide a mechanism for authenticating and authorizing a device connected to a LAN. It is basically a replacement of the MAC address filtering technique described previously in a dynamic way. The standard generally addresses the threats of masquerading and unauthorized access to the resources. Apparently, the 802.1X [8] makes use of the existing authentication protocol, the Extensible Authentication Protocol (EAP) [9] as defined in the IETF. The EAP was written for providing authentication over PPP. The 802.1X working group took the protocol defined by EAP and tied it to the LAN physical medium like Ethernet, Token Ring, and Wireless LAN to enforce authenticity of the entity who wishes to connect to the LAN. EAP messages are encapsulated in 802 messages, which are referred to as EAPOL or EAP over LAN. Another reason for developing EAPOL is the deployment of wireless LAN in the corporation. In the following paragraph, the basic function of the 802.1X protocol will be described, followed by the application of this protocol in the LAN environment.

The 802.1X defines three basic components, supplicant, authenticator and authentication servers, which are illustrated in Figure 3. The protocol defined is based on the availability of an authentication server that provides the required authentication services and protocols. Such authentication servers can be RADIUS (Remote Authentication Dialer in User Services), Kerberos, LDAP (Lightweight Directory Access Protocol), or any other AAA (Authentication, Authorization and Accounting) servers. The supplicant is basically a workstation or PC that serves as a client, which is the device that wishes to be connected to the LAN. The authenticator is the front end device that sits on the network edge to ensure the legitimacy of the client who wishes to access the LAN. The authenticator can be a switch in the Ethernet or an access point in the wireless LAN. As a gate controlling who can access to the LAN, the authenticator helps the client to get legitimated with the authentication server. Once the authenticity of the client is validated, the client is connected. The port is then opened, and traffic packets can now be sent from the client to the LAN.

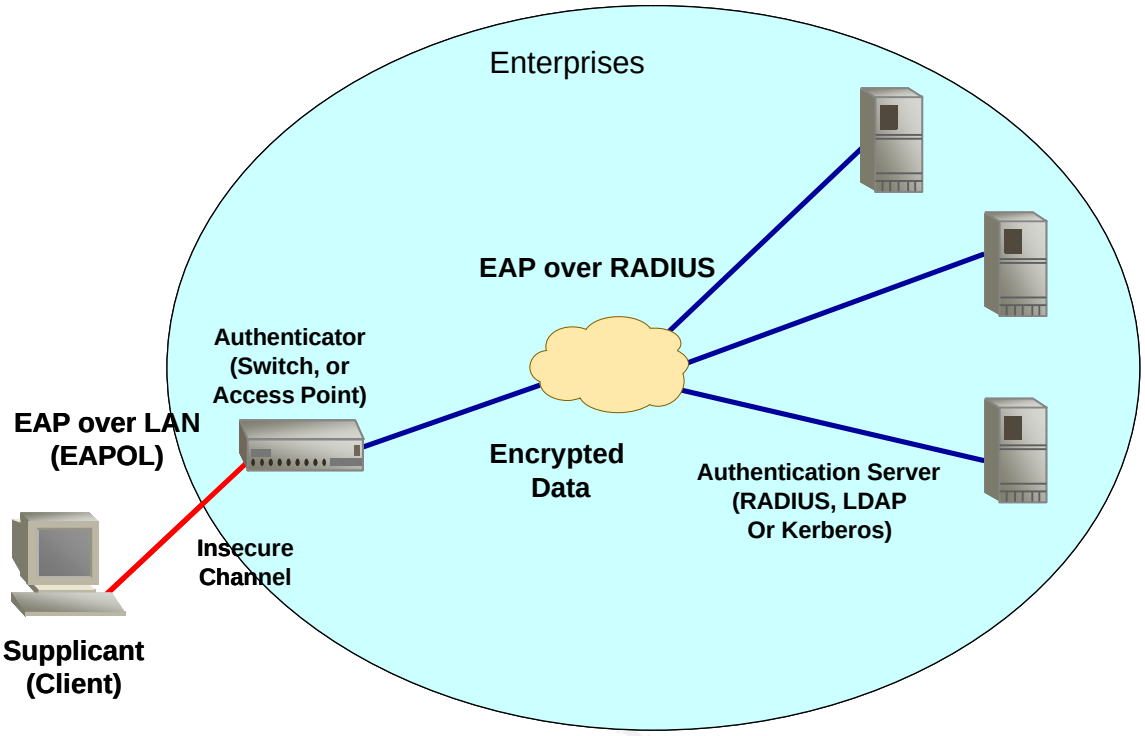

Figure 3. IEEE 802.1X Authentication Model

Looking at the packet level, the authenticator takes the Ethernet frame, strips its header and encapsulates with RADIUS header. Then it sends the new encapsulated frame to the RADIUS servers. The reverse process will strip the RADIUS header, append with Ethernet header and send to the client.

Figure 4 shows the working process of the EAP protocol in the LAN environment. As illustrated, there is an EAP over LAN (EAPOL) on the left side between the PC and the switch. There is also another EAP over higher layer protocol, such as RADIUS on the right side between the switch and the RADIUS server. Although the 802.1X does not mandate the type of authentication server used, the RADIUS server seems to be the most common one. Since a RADIUS server is applied, the protocol described on the right side of the diagram shows the RADIUS protocol. If another authentication server is used, then the associated protocol will be operated.

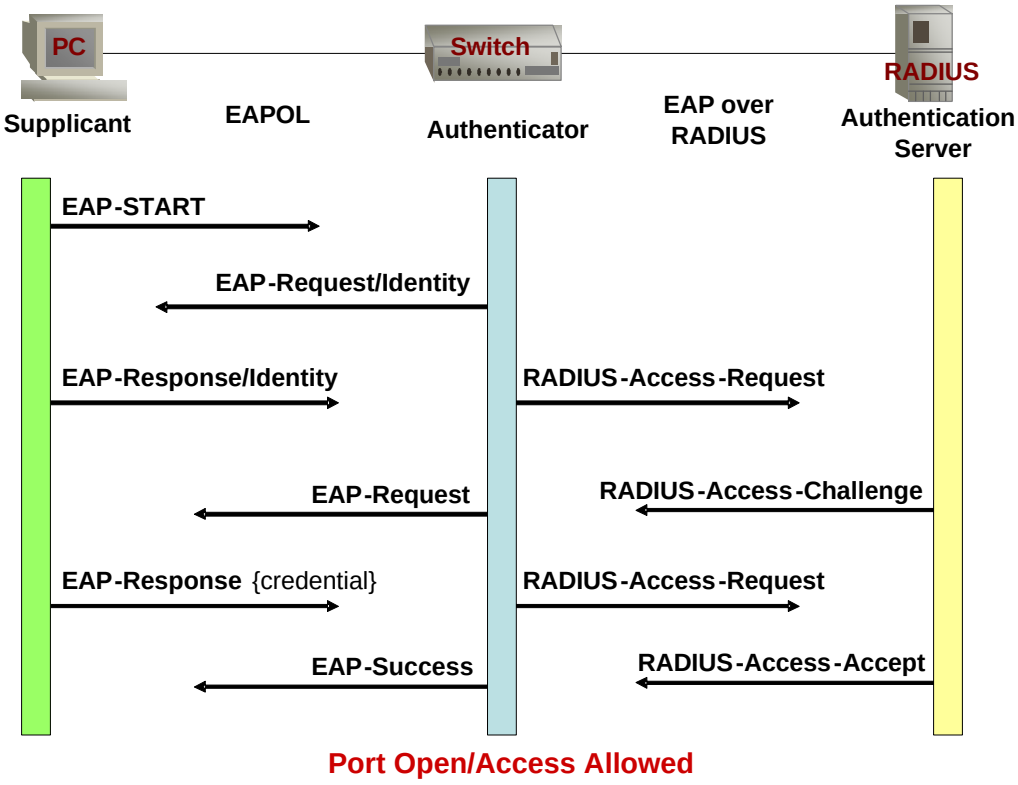

Figure 4. IEEE 802.1X EAP Authentication

First, the PC connects to the LAN and requests for an access. This starts a sequence of message exchanges in the authentication process. The switch replies with an EAP-request message and asks for identification. Next, the PC sends an EAP-response packet with its identity and the identity of the authentication server. The switch will then repackage the information the PC has provided and sends a RADIUS-Access-Request to the RADIUS server. In response to the Access-Request, the RADIUS server forwards an Access-Challenge to the switch, which in turns relays it to the PC in terms of EAP-Request message. The client will provide its credentials to the switch that is then converted to RADIUS-Access-Request later sent to the RADIUS server. The result is either an ACCEPT or a REJECT packet from the RADIUS server to the PC depending on the PC's credential. If it is accepted, then the port is opened and the subsequent traffic from the PC will be allowed. If it is rejected, however, then no more traffic can be allowed into the network from this PC.

The 802.1X provides an excellent mechanism to control the access of client devices to the network by using appropriate authentication protocols and servers. The access control is based on various authentication protocols. However, once the user is on the network, the algorithm will provide no mechanism to control

what resources within the LAN can be accessed. Additional techniques that may require such capability become necessary.

Enhanced security for WLAN – IEEE 802.11i

Since the inception of wireless LAN, its security has always been a hot topic. The IEEE 802.11, the wireless LAN, was created with protection in mind. The design of the WEP (Wired Equivalent Protection) protocol is to provide an equivalent protection as in the wired network when the 802.11b was introduced. The WEP protocol specifies the use of RC-4 cryptographic algorithm with either 40-bit or 128-bit keys. However, more recent reports [10][11] indicate that vulnerabilities were discovered in the WEP protocol. The WEP protocol addresses only the data confidentiality and integrity. The authentication and access control are provided with the use of 802.1X.

In order to address growing security concerns in the wireless LAN [12], IEEE 802.11 working group formed a new task group, TGi (Task Group i), and a new draft standard, the 802.11i [13] was developed to address the growing concerns of wireless LAN security. The draft standard specifies a Robust Security Network (RSN) to provide a number of security features to the 802.11 network. These new features particularly address the weakness in the WEP as well as the earlier version of the wireless LAN security specifications. These features include the following [13]:

- Enhanced data security and encapsulation mechanism, called CCMP (Counter-Mode/CBC-MAC Protocol) and, optionally, TKIP (Temporal Key Integrity Protocol)
- Key management algorithms
- Dynamic cryptographic key establishment
- Enhanced authentication mechanisms for both APs (Access Points) and stations

The IEEE 802.1X protocol is used extensively in the 802.11 to provide the necessary authentication and key management. An RSN (Robust Security Network) architecture relies on two components external to the 802.11 architecture as listed below.

1. The first component is an IEEE 802.1X port. 802.1X ports are present on all stations and APs. The port on a station is called a Supplicant, and the one on the AP is called an Authenticator.
2. The second component is the Authentication Server (AS). The AS is an entity that can be used to authenticate both the APs and the stations.

The 802.11i provides data origin authentication, access control, and confidentiality services to the 802.11 networks. The data origin authentication services define a method by using either CCMP or TKIP to ensure that the packets received are actually originated from the desired source. The access control service is assured based on the authentication mechanisms afforded in the 802.1X along with TKIP and CCMP. The RSN key management as well as the TKIP and CCMP protocols provide the confidentiality service. The cryptographic algorithms used to protect data traffic over the wireless link are WEP, TKIP, and CCMP. Both WEP and TKIP are based on the RC4 algorithm, while CCMP is based on the AES (Advanced Encryption Standard). Selecting an algorithm to use is negotiable between the two communicating entities.

TKIP fixes the security issues in WEP by defining a cipher suite in enhancing the WEP protocol. The enhancement comes with two major components. First, the original message is converted to a Message Integrity Check (MIC) value to ensure the authenticity of the message that prevents man-of-the-middle attacks. Second, a per-packet keying is used, which provides every frame with a new and unique WEP key that mitigates the WEP key derivation attacks. Additionally, the CCMP that uses the AES cryptographic algorithm with the CCM mode of operation provides a much stronger protection. The CCM mode combines Counter (CTR) mode for confidentiality and Cipher Block Chaining Message Authentication Code (CBC-MAC) for authentication. CCM uses the same temporal key for both CTR mode and the CBC-MAC but a new temporal key is used for every session.

In addition to the enhancement to the cryptographic algorithm, the 802.11i specifies a new key management protocol. The AKM (Automatic Key Management) operations make use of the 802.1X EAP authentication protocol as shown in Figure 4 to ensure the legitimacy of the client who wishes to access it. Once they are validated with each other, a PMK (Pairwise Master Key) will be generated both in the supplicant (client) and in the authentication server (AS). The AS will send this PMK to the authenticator (AP). At this point, both the authenticator (AP) and the supplicant (client) will begin a four-way handshake to verify each other and unblock the port for subsequent data traffic once they are agreed. This 4-way handshake is shown in Figure 5. At the same time, a new Pairwise Encryption and Integrity keys are generated that can used for the message confidentiality and authentication.

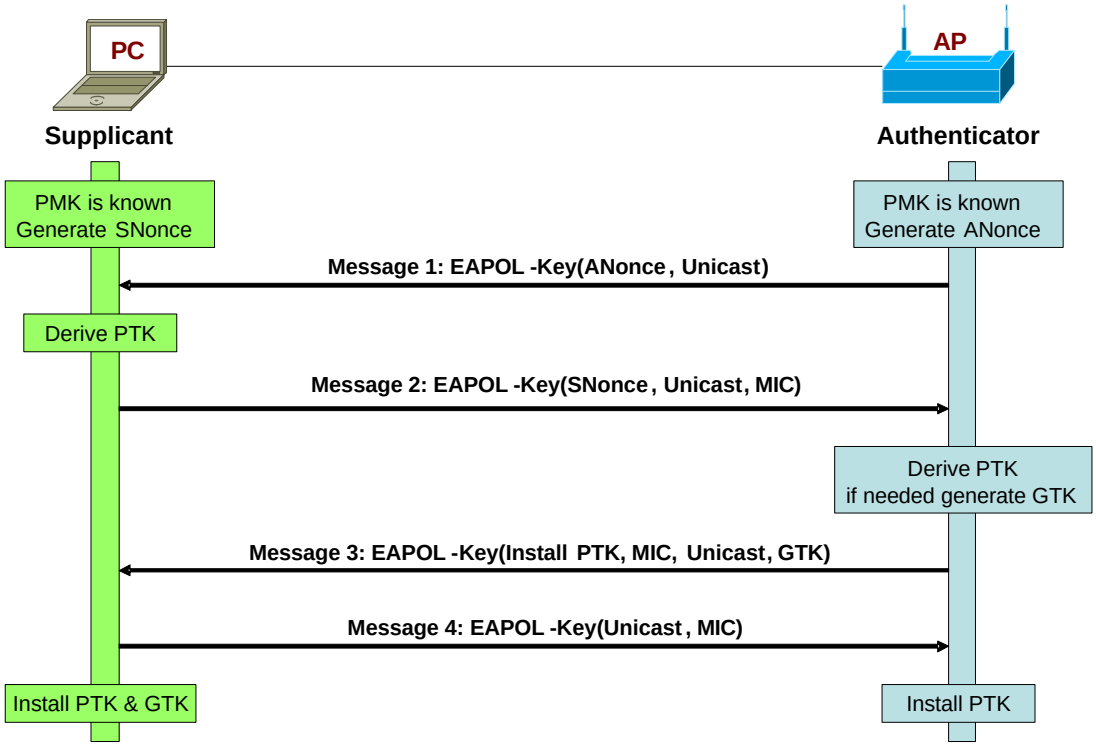

Figure 5. Establishing Pairwise and Group Keys

MAC Security – IEEE 802.1AE

The use of MAC layer protocol is no longer limited to the enterprise environment, such as Ethernet, Token Ring and wireless LAN. More working groups within IEEE 802 standard committee have been formed in the last several years. There are working groups developing specifications for wireless PAN (802.15-Personal Area Networks), wireless MAN (802.16-Broadband Wireless Access), wireless WAN (802.20-Mobile Broadband Wireless Access), and optical networks (802.17-Resilient Packet Ring). These network technologies are developed not only for the enterprises, which is traditionally the target of 802 networks, but also for the service providers. The needs for security over these MAC layer network are beyond what are offered by traditionally enterprise IT departments. For example, a service provider may provide a Resilient Packet Ring (802.17) to a multi-tenants building where multiple companies are located. These companies may be competitors themselves. The ring is connected to every node in each company, which means that the traffic will flow through each node before heading to the service provider's aggregation hub. This characteristic resembles the similar behavior in the LAN environment where all vulnerabilities can be

applied here. In addition, the service providers will have to worry about other security threats that are not applicable in the enterprise environment, such as theft of services, billing dispute, and other issues. All these security concerns especially in the service providers' space, bring up new attention in providing security services to a new set of link layer protocols.

A new working group was formed in July 2002 and approved by the IEEE 802 Executive Committee on November 15, 2002 to focus on the MAC layer security. The new group is under the 802.1 committee, and it is named as the 802.1AE Link Security working group [14]. According to the IEEE 802.1AE draft standard released on November 10, 2003, the scope is "to specify provision of connectionless user data confidentiality, frame data integrity, and data origin authenticity by media access independent protocols, and entities that operate transparently to MAC clients."[7] [15] The standard will also "facilitate secure communication over private and publicly accessible LAN/MAN media for which security has not already been defined, and allow the use of IEEE Standard 802.1X"[8] [16].

The working group looked at both 802.10 as well 802.11i to determine if the security services and protocols proposed therein are sufficient for use in any MAC layer environment. They felt that the 802.10 is too end-to-end specific, and the link-by-link is an add-on. That standard primarily addresses the protection for end-stations. The authentication mechanism provisioned by the 802.10 is not sufficient in the service providers' network. On the other hand, the 802.11i is particularly tailored to the wireless LAN, and it only addresses the authentication and data confidentiality. However, the group believed that the new protocol should leverage as much possible from both standards instead of re-inventing the wheel themselves.

The security support of the MAC services is for secure communication between two authenticated MAC entities that could be an end stations attached to LAN and a MAC bridge connected to a bridged LAN. Currently, the specification identifies the support in a MAC bridge network that the bridge can be either a regular 802.1D bridge or a VLAN aware bridge. However, the provision for key management protocol is outside the scope of this specification.

One of the key differentiators of this specification is its focus in the service provider environment. In their early studies presented at the March 2003 meeting, the primary business level requirements are to prevent theft of services, separating customers from each other and maintaining billing records. The focus on the service provider market shifts away the traditional approach in their early standard development. However, the specification defined may still apply to

[7] ANSI/IEEE Std. 802.1AE/D1:2003, Medium Access Control (MAC) Security, December 9, 2003. p.1. (December 15, 2003)
[8] IEEE 802.1 Link Security Study Group, June 2003 meeting minutes, Ottawa. p.1. (December 15, 2003)

some large enterprises since the boundary between enterprise and service providers is getting blurred. Needless to say, the security specification that the 802.1AE has developed will demonstrate the latest security solution for the current network environment. Moreover, many of the large corporate backbone networks have moved from the traditional point-to-point dedicated topology to a shared distributed network. As a result the security services provided by this specification will have some impact to the enterprises.

What should Enterprises do?

Understanding the importance of link security in the enterprise security, the steps that the enterprise IT should take must provide adequate protection not only within the corporation but also across the network boundary. With various link layer security technologies and standards, where each addresses a certain need for LAN security, the task of sorting out the best strategy will be a challenge. As we described earlier, the link security can provide the protection needs that are not available at other layers. In this section, the steps that the enterprise can take to address their security needs will be briefly described.

First of all, the enterprise should perform a detailed threat analysis of their enterprise architecture. They need to determine the security threats they are confronting and also the business requirements and needs for such protection. Understanding business value of the security will increase the effectiveness of the implementation. Then, a link security strategy should be developed within the enterprise security architecture. To be consistent with the overall security framework, the alignment of link security will help to seamlessly work with the other parts of the security, such as, infrastructure and application level security. The results of the threat analysis provide a good understanding on the types of security and controls needed at the link level. Apparently, the link level may not be just limited to the data link layer of the OSI model. It may also represent the connection between two nodes, such as from the PC to the next switch, or between two routers in the network.

Utilizing the available technologies and standards, the enterprise can address the security needs for the enterprise infrastructure. Since each technology and standard only address certain security threads in the enterprise network, designers may not get all the protection they need from the available commercial products. These products and technologies may be used at different stages of the deployment. The security architect should first develop an overall network architectural view of how protections are needed in the infrastructure. Then, each component defined in the infrastructure security architecture can be further analyzed to determine what technology would be better fitted to provide the required functions. For example, if the control of the access to the corporate network at the network edge is necessary, 802.1X can be used to authenticate users to check for their legitimacy. The key of this approach is to make sure the

technology that is deployed can be aligned with the overall strategy. To ensure such alignment, a roadmap that presents the use of current and potential future technologies shall also be developed. As new products and technologies become available, migration can be easy and seamless. Otherwise, the results will be silo. Not only is the protection not adequate, the cost of integration will also be higher.

Conclusions

Link security is playing an important role in the enterprise security architecture. As new technologies are deployed in the enterprise infrastructure such as wireless and optical, new security threats that require specific protections are different from the traditional approaches. The level of security approaches may not lie at the higher layers. As the control of link access becomes critical to the enterprise security and the vulnerabilities in the enterprises, new threats appear in the data layers. The paper outlines the security challenges the network administrator faces and present new security threats in the link layers. The rationale for provisioning link security in the enterprise infrastructure is also discussed. In the past, current and future security standards and technologies are presented. Since each addresses certain security threats at different times for specific needs, network designers and architects will require an in depth study in order to effectively apply these technologies to address their security needs. Finally, the paper concludes with a proposal of enterprise actions in addressing link security issues.

APPENDIX: ACRONYMS

AES	Advanced Encryption Standard
AKM	Automatic Key Management
AP	Access Point
ARP	Address Resolution Protocol
AS	Authentication Server
CBC-MAC	Cipher Block Chaining – Message Authentication Code
CCMP	Counter-Mode/CBC-MAC (CCM) Protocol
CDMA 1x	Code Division Multiple Access 1xRTT
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EDGE	Enhanced Data Rates for Global Evolution
FDDI	Fiber Distributed Data Interface
GPRS	General Packet Radio Services
ICV	Integrity Check Value
LDAP	Lightweight Directory Access Protocol
LLC	Logical Link Control
LSAP	Link Service Access Point
MAC	Medium Access Control
MDF	Management Defined Field
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PMK	Pairwise Master Key
PON	Passive Optical Network
RADIUS	Remote Authentication dial in user Services
RSN	Robust Security Network
SAID	Security Association Identifier
SDE	Secure Data Exchange
SDU	Service Data Unit
SILS	Standard for Interoperable LAN Security
SMIB	Security Management Information Base
TKIP	Temporal Key Integrity Protocol
VLAN	Virtual LAN
WEP	Wired Equivalent Protection
WLAN	Wireless LAN

REFERENCES

[1] Ethereal, a free network protocol analyzer for Unix and Windows. URL:http://www.ethereal.com/

[2] ANSI/IEEE Std. 802.10:1998, Standard for Interoperable LAN/MAN Security (SILS), 1998. URL:http://standards.ieee.org/getieee802/download/802.10-1998.pdf

[3] ISO 7498-2:1989, Information processing systems – Open system Interconnection – Basic Reference Model – Part 2: Security Architecture, 1989.

[4] ISO 7498-2-Amendment 1:1996, Information processing systems – Open system Interconnection – Basic Reference Model – Part 2: Security Architecture – Amendment 1: Layer Two Security Services and Mechanisms for LANs, 1996.

[5] ANSI/IEEE Std. 802.10c:1998, Supplement to 801.10-1998, Key Management (Clause 3), 1998. URL:http://standards.ieee.org/getieee802/download/802.10c-1998.pdf

[6] IEEE VLAN Standardization via 802.10, slides 29-33, September 2003. URL: http://www-users.itlabs.umn.edu/classes/Fall-2003/inet4011/lectures/lec10.ppt

[7] IEEE 802.1 – 1995 Document Register, Document no. 95-030 and 95-031. URL : http://www.ieee802.org/1/files/public/docs95a/n030.txt

[8] ANSI/IEEE Std. 802.1X:2001, Port Based Network Access Control, 2001. URL: http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

[9] Vollbrecht J., and Blunk, L., “PPP Extensible Authentication Protocol (EAP)” IETF RFC 2284, March 1998. URL:http://www.ietf.org/rfc/rfc2284.txt

[10] Stubblefield, A, Loannidis, J., and Rubin, A, “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”, AT&T Labs Technical Report TD-4ZCPZZ, Revision 2, August 21, 2001. URL:http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

[11] Borisov, N., Goldberg, I., Wagner, D., “Intercepting Mobile Communications: The Insecurity of 802.11”. URL:http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

[12] Arar, Yardena, “Beefing up 802.11b Security”, PCWorld.com, February, 2002. URL: http://www.pcworld.com/news/article/0,aid,82563,00.asp

[13] ANSI/IEEE Std. 802.11i/D7.0:2003, Medium Access Control (MAC) Security Enhancement, October, 2003.

[14] IEEE P802 Link Security Executive Committee Study Group, 2003. URL:http://grouper.ieee.org/groups/802/linksec/

[15] ANSI/IEEE Std. 802.1AE/D1:2003, Medium Access Control (MAC) Security, December 9, 2003.

[16] IEEE 802.1 Link Security Study Group, June 2003 meeting minutes, Ottawa. URL:http://www.ieee802.org/1/linksec/meetings/Jun03/InterimMtgJune2003.doc