Data Link Layer-Security Issues

A Annapurna,
M. Tech,
Assistant Professor, CSE Department
Vardhaman College of Engineering
Hyderabad,India
e-mai:purna.1201@gmail.com

Sheena Mohammed,
M.Tech,
Assistant Professor, CSE Department
Vardhaman College of Engineering
Hyderabad,India
e-mail:sheenamd786@gmail.com

D.Madhuri,
M.S
Assistant Professor, CSE Department
Vardhaman College of Engineering
Hyderabad,India
e-mail:madhuriqa123@gmail.com

Abstract-Security issues in the data link layer are not properly explained while network security problems in other layers of OSI model are studied and addressed. In this paper, we propose a new security inter-layering structure to secure data link layer in Internet protocol over Ethernet networks. In the data link layer, we have proposed to use secure namespaces instead of Media Access Control(MAC) to identify network devices, which provides a mean to bind data link layer with other layers of OSI model very securely. Present network structure provides a link to link security and the key establishment protocol to generate security parameters in this layer.

Keyword- MAC, OSI, IEEE802.1

I. INTRODUCTION

Data link layer is one of the layers in OSI model which deals with raw data transmission from data link layer to network layer. Data transmitted over the network is done through fragmenting the data into small packets. The function of data link layer is to provide service to network layer.

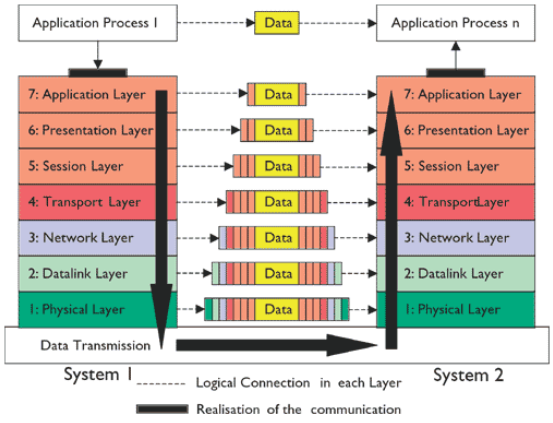

Figure 1. OSI Model

Security issues in this layer of local area networks have started long term overdue in standard groups and in the literature. Security in wireless networks have been greatly improved by IEEE 802.11i standards. Confidentiality, integrity and authenticity attacks exist in both wired and wireless networks. Security issues in wired LANS need to be addressed to improve security in both networks. In this paper, we propose a new data link layer security architecture with a key establishment protocol that may be incorporated into MAC security. In LANs, we observe that several security threats are caused by the insecure addressing in the data link layer and the weak link between the network and data link layers. Layers lack the ability to inform other layers whether any security measures are utilized or security weaknesses exist. In this paper, we examine the data link

layer security in IP over Ethernet networks. We propose to utilize secure namespaces instead of MAC addresses to identify network devices in the data link layer. We introduce a new security inter-layering concept to provide security in this layer. It is followed by describing proposed data link layer architecture. In this MAC address namespace of data link layer is not enough to provide security services in local area networks.MAC addresses are utilised to identify hosts and machines in the data link layer. While MAC addresses of each interface card is to be globally unique. IP addresses must identify hosts in the network layer and mappings should be done between IP and MAC addresses in Ethernet bases local area networks.ARP is not a secure protocol to do the above criteria. Third, a negotiation in the data link may not be detected by upper layers where security implementations exist in the network. Our model consists of many layers.

II. PROBLEM

Data link layer communication is very weak link in terms of security. Security should be addressed at different layers of the model. This is the only problem that mainly affects the data link layer. Each layer offers security services to another layer and itself independent of other layer. Security may provide sufficient level of guarantee against weaknesses present in other layers. This generates computational overhead and usage of bandwidth is more in network.

At lower layers it is very difficult o keep track of security in transport layer as security associations, may have data analysis may be required. We should be capable to create a flexible security mechanism to ensure data securely while transmission.

So, we had proposed a new security inter-layering concept to inform each layer regarding the security protocols and features in other layers.

It allows the usage of namespaces in various layers in networks. A lower layer may choose to utilize different namespaces depending on the applications. This inter layering is utilised to create secure bindings among namespaces. Security in each layer should be different and dependent on functionalities of layers.

This concept is easily adapted to future architectures or namespaces it is not a specific architecture limited to certain layer or network architecture.

III. SOLUTION TO DATA LINK LAYER SECURITY ISSUES:

Security in LANS can be accomplished with data link layer architecture. Essential requirements for secure LANs are that network devices should allow data traffic from and to authorised hosts. To do this, network devices should have the capability to verify integrity of messages and origin of the data at this layer.

Data link layer may use a secure namespace from other layers instead of MAC addresses, thus avoids overhead that a new secure namespace for the data link layer will create and also prevents occurring possible weakness

We use different terms in this new inter-layering architecture, they are: hosts, machines refer to end points in a local network.

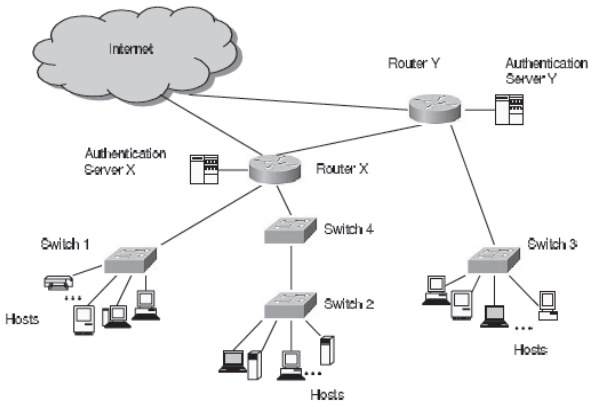

Figure 2. An illustration of the network architecture.

Architecture of data link layer:

In this proposed architecture, we utilise the IEEE802.1 concepts for access control and also a key hierarchy is used for wired and wireless networks.

The architecture has three important components: authentication servers, authenticators and the hosts.

Authentication Servers:

We use these servers to establish realms and security parameters in these local networks. These servers are integrated into routers. Authentication servers records and manages the data link layer identifiers in its realms. Hosts discuss security parameters and their data link layer identifiers with authentication servers during key establishment protocol. Authentication servers and hosts use key establishment protocol to perform

mutual authentication, to generate session keys. Authentication servers assign IP addresses to hosts in their realms at the end of the key establishment protocol; we can assign same IP address to several hosts with different L2ID. The server utilizes a distributed database maintaining the list of ID's and IP addresses for network access.

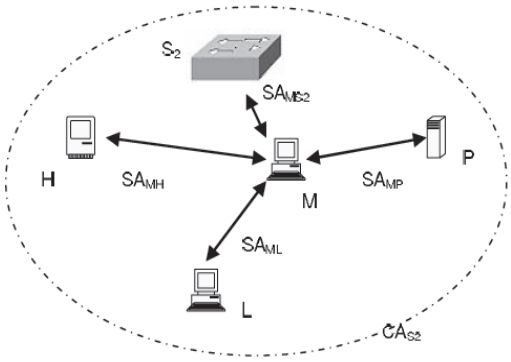

Figure 3. An illustration of the security

Authenticators:

Authenticators are the data link layer devices which act as gateways between hosts and authentication servers. In the architecture, authenticators function as access points. These are the layer 2 devices, such as switches where these switches function as authenticators. Authenticators communicate with authentication servers to receive their L2Ids to establish security parameters. Each authenticator controls a connectivity association; it consists of an authenticator and a number of hosts. A host with several data link layer connections can participate in more than a connectivity association.

A secure protocol is used by authenticators and hosts in the realm of authentication servers. Every connection association is supported by security associations.

Authenticators with direct links create SA's with each other.

Hosts:

In the proposed data link layer security architecture, hosts are identified by L2ID's. A host utilizes key establishment protocol to negotiate its L2Ids and learn its IP address from authentication server. At the end of key establishment protocol, before host can send any data frame, it is necessary to create SAs in its CA. Host utilises four way hand shake protocol, and establishes security association protocols. After host completes hand shake protocol it becomes a member of CA and creates an SA with data link layer devices that is connected. A host tries to communicate with destination host finds the location and the identity of destination host via a method. Hosts that participate in different CAs communicate via authenticators.

Key Management:

In this architecture, there are four different types of communication that require confidentiality, data authentication and protection that require mechanisms such as

- Authentication servers to/from authenticators,
- Authenticators to/from hosts, hosts to/from hosts, and
- Authenticators to/from authenticators.

IV. CONCLUSION

Our objective is to secure the data link layer and bind the upper layer of OSI model with data link layer , we also focus on preventing specific attacks, such as misbinding attacks. We should emphasize that identity binding is essential in our architecture to authenticate messages. We prevent these misbindings by including identities under signatures.

In this, we introduced new data link layer security architecture with security inter-layering in IP over Ethernet networks. We proposed secure identities such as public keys to secure the link between data link layer and network layer.

We proposed network structure providing link-to-link security with security connections. We described a method to establish the secure associations and addressed the key management. We proposed a key establishment protocol to discuss data link layer identifiers, security parameters and authenticate hosts and servers. We also utilise the four-way hand shake protocol and the key hierarchy of 802.11i standard to consistent with wireless networks addressing security issues between wireless networks and wired networks.

The proposed architecture separates identities and locations supporting mobility. It modifies other internetworking layers as well. It requires the network layer to incorporate identifiers in IP packets. This architecture requires all layers of the devices, such as bridges to own data link layer identifiers.

V. REFERENCES

[1] Networks: Media Access Control (MAC) Security, January 2006,IEEE P802.1AE Standard for Local and Metropolitan AreaIEEE Working Draft, D5.1. Available:"IEEE 802.1AE-Media Access Control (MAC) Security," July.

[2] C. Howard, "Layer 2 – The weakest link: Security Considerations at the Data Link Layer," PACKET, vol. 15

[3] H. Altunbasak, S. Krasser, H. L. Owen, J. Grimminger, H.-P.Huth, and J. Sokol, "Securing Layer 2 in Local Area Networks," in ICN, vol. 2, Reunion, France, April 2005, pp. 699–706.

[4] H. Altunbasak, S. Krasser, H. Owen, J. Sokol, J. Grimminger, and H.-P. Huth, "Addressing the weak link between Layer 2 and Layer 3 in the Internet architecture," in Proc. of the 29th Annual IEEE Conference on Local Computer Networks (LCN), Tampa, Florida, November 2004.

[5] IEEE Std 802.11i, Amendment to IEEE Std 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) SecurityEnhancements, June 2004.

[6] T. Karygiannis and L. Owens, Wireless Network Security 802.11, Bluetooth and Handheld Devices, November 2002.

[7] D. C. Plummer, "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware," IETF RFC 826, November 1982.

[8] 8. S. Kent and R. Atkinson, IP Authentication Header, Nov.1998, RFC 2402. Available http://www.ietf.org/rfc/rfc2402.txt.Stephen Kent and Randall Atkinson, IP Encapsulating Security Payload (ESP), Nov. 1998, RFC 2406 Available: http://www.ietf.org/rfc/rfc2406.txt. "NISCC vulnerability advisory IPSEC - 004033," May 2005.

[9] P. Nikander, J. Laganier, and F. Dupont, "A Non-Routable IPv6 Prefix for Keyed Hash Identifiers (KHI)," Network.

[10] Donald E. Eastlake, "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name system," IETF RFC 3110, May 2001. Available: http://www.ietf.org/rfc/rfc3110.txt.

[11] IEEE 802.1X-2001 IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control(EAPOL), 2001.

[12] R. Moskowitz, P. Nikander, P. Jokela, and T. R. Henderson, "Host Identity Protocol," Internet draft, March 2006.

[13] www.ieee802.org/1/files/private/ae-drafts/d5/802-1ae-d5-

[14] http://www.ieee802.org/1/pages/802.1ae.html

[15] http://csrc.nist.gov/publications/nistpubs/800-48/NIST SP 800-48.pdf

[16] http://www.niscc.gov.uk/niscc/docs/al-20050509-00386.html?lang=en

[17] http://tools.ietf.org/wg/ipv6/draft-laganieripv6-khi-00.txt

[18] http://www.ietf.org/internetdrafts/draft-ietf-hip-base-05.txt