Addressing the Weak Link Between Layer 2 and Layer 3 in the Internet Architecture

Hayriye Altunbasak, Sven Krasser,
Henry Owen
School of Electrical and
Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia 30332–0250
Email: {hayriye, sven, owen}@ece.gatech.edu

Joachim Sokol, Jochen Grimminger,
Hans-Peter Huth
Siemens AG, Germany
Email: {joachim.sokol, jochen.grimminger,
hans-peter.huth}@siemens.com

Abstract— **In the data link control layer, a Medium Access Control (MAC) address is utilized to uniquely identify each node of a network. With the rapid expansion and evolution of the Internet, the methodology of addressing in the data link layer and mapping between network and data link layers has become inadequate to provide secure services in networks. Since the current protocols used in networks do not provide a secure binding between the Internet Protocol (IP) and MAC addresses, they create a weak link between network and data link layers in Local Area Networks (LANs). In this paper, we examine the security concerns in the data link layer as well as the IP and MAC address binding problem in LANs.**

I. Introduction

The expansion and evolution of the Internet has introduced new challenges and revealed some of its shortcomings. This, in turn, has motivated researchers to propose new architectures and protocols to improve the Internet Protocol (IP). Some researchers focus on new naming and addressing protocols, whereas others focus on new architectures for a heterogeneous network environment. The former requires changes in host software and is easier to deploy. However, it may not address all the issues in the current Internet. The latter requires changes in the Internet infrastructure, which makes it harder to deploy. Recently, there have been discussions on IP addressing and its functions as well. IP addresses are used to identify hosts in network layer. In addition to an IP address, each node in a local network is identified with its physical machine address, which is the Medium Access Control (MAC) address. While the IP address identifies the location of the host, the MAC address uniquely identifies the host/machine. Hence, there must be a mapping between IP and MAC addresses in local area networks (LANs). This mapping is accomplished by the Address Resolution Protocol (ARP). However, the mapping does not bind the IP and MAC addresses securely. Moreover, even though the MAC address of each network interface card in a network is supposed to be globally unique, it can easily be changed enabling MAC cloning. In this paper, we discuss this weak link between the network and the data link layers as well as describe possible approaches to solve this problem. Our intent is to foster discussions in this area. In addition, we focus on the Layer 2-3 link in IP over Ethernet networks. However, most of the discussion applies to other types of networks as well.

A. Addressing at Layer 2 and Layer 3

Each host connected to an IP/Ethernet LAN is associated with two addresses: a MAC address and an IP address. The MAC address is a globally unique data link layer (Layer 2) address stored in the network card at the host. The Ethernet protocol requires a MAC address independent of the upper layer protocols to build Ethernet frames. Each Ethernet frame consists of a header (containing the source and destination MAC addresses), data, and cyclic redundancy check sections. The host IP address is used by the network layer (Layer 3) protocol Internet Protocol (IP). Each host on a network has a unique IP address. An Ethernet frame is constructed from an IP packet delivered to the data link layer. However, the data link layer requires the source and destination MAC addresses, which are not included in the IP packet. The IP packet contains the source and destination IP addresses, and each host knows its MAC address.

B. The Address Resolution Protocol (ARP)

In a LAN, the Address Resolution Protocol (ARP) is used to map IP addresses to MAC addresses. In order to find out the MAC address of the destination, the source broadcasts an ARP Request packet to the network. Each host on the network examines the ARP packet and checks if the IP address in the ARP Request message matches its IP address. If it does, the host sends an ARP Reply with its MAC address. Each host also keeps a cache of ARP Replies for IP-MAC associations.

ARP is a simple stateless network layer protocol. It does not implement any security measures to bind IP and MAC addresses. ARP is generally not used to resolve IPs that are not on the same LAN. A host realizes this by comparing the network parts of its and its destination's IP addresses. Then, it crafts a frame with the corresponding router as the destination. This means the router's IP has to be resolved. Each host machine also maintains an ARP cache to convert MAC addresses to IP addresses. An ARP cache may contain both dynamic and static entries. Dynamic entries in the cache are added and removed automatically over some time, whereas static entries remain in the cache until the computer is restarted. Note that this simple protocol does not include any type of authentication, leading to major insecurity. For instance, the ARP Poisoning attack exploits gratuitous ARP (ARP Reply sent without an ARP Request) messages. Because ARP maps an IP address to a physical machine address recognizable in local networks, it is an important part of the Layer 2 and Layer 3 link.

C. The Dynamic Host Configuration Protocol (DHCP)

IP addresses assigned to hosts in networks may be static or dynamic. Temporary IP address assignments are done by Dynamic Host Configuration Protocol (DHCP) servers from a pool of IP addresses. This temporary IP address is called a dynamic IP address and allocated for a period of time. In addition to an IP address, DHCP provides further configuration information such as subnetwork mask, default gateway, and DNS server etc. DHCP is an inherently insecure protocol. Since DHCP provides dynamic bindings for MAC and IP addresses, it is a critical part of the Layer 2 and Layer 3 link, as well.

In this paper, we summarize some of the issues regarding the Layer 2 and Layer 3 link. This is followed by a short discussion of the IEEE P802.1AE Standard for Local and Metropolitan Area Networks: Media Access Control Security (Draft) and other related solutions to address security and naming issues in networks. We also discuss some possible approaches to address the weak link between Layer 2 and Layer 3. Finally, we present some concluding remarks.

II. Problems with Linking Layer 2 and Layer 3

In LANs, ARP and DHCP are the protocols used to map and bind a physical host to an IP address, respectively. However, these protocols are inherently not secure and create an overhead in local networks. In this section, we present a summary of the issues caused by the weak link between Layer 2 and Layer 3 in LANs.

A. ARP Overview

ARP is a simple and trusting protocol. A networked device trusts ARP Requests and Reply messages without ensuring that they come from the correct devices. ARP does not provide any authentication methods to verify that the sending or responding device is really who it says it is. ARP is a Layer 3 protocol. However, it is based on broadcast messages on the LAN.

An ARP message is included in the data field of a Layer 2 frame. The Ethernet Type field of the frame is set to 0x0806 to indicate an ARP message. In addition, a host may send a gratuitous ARP when it is initializing its IP stack. This gratuitous ARP is an ARP Request message to check for a duplicate IP address. In this gratuitous ARP, the host asks for the Layer 2 address of its own IP address.

B. ARP Problems

ARP introduces a security risk in local networks since ARP messages can easily be spoofed. For example, an attacker can sniff other hosts' frames by performing a man-in-the-middle or MAC flooding attack. An attacker can send a forged ARP Reply message to a host in the local network to re-direct frames going to a wireless access point or a router to a rogue network device. This is a classic man-in-the-middle attack.

In a MAC flooding attack, the attacker sends spoofed ARP Replies to a switch to overflow the switch's Content-Addressable Memory (CAM) table, which stores MAC addresses, switch port numbers, and Virtual Local Area Network (VLAN) information at switches. Depending on the switch settings, some switches go into broadcast mode in case of an overflow allowing sniffing.

Other possible attacks in Layer2 utilizing ARP are port stealing, broadcasting, Denial of Service (DoS), MAC cloning, and hijacking attacks [1], [2], [3], [4].

One of the recommended actions against ARP attacks is to employ static ARP entries. Static ARP entries are permanent entries in ARP caches. This technique prevents most of the attacks. However, it is impractical. Administrators must create new entries on every machine on the network every time a new host is connected, or when a Network Interface Card (NIC) is replaced. Furthermore, it does not allow the use of some Dynamic Host Configuration Protocol (DHCP) configurations. Lastly, it does not solve the secure binding issue of IP and MAC addresses.

We observe three core problems related to ARP that cause the weak link between Layer 2 and Layer 3 and create an overhead. First, there is no secure binding of IP and MAC addresses. As a result, there are several possible ARP attacks in LANs. In fact, this is not the fault of ARP but the naming architecture. ARP is a protocol designed to work with the existing naming architecture used in Layer 2 and Layer 3 on networks. The naming architecture may be considered as the main cause of these issues. Ideally, a host should not have its identity tied to simply a MAC address. Instead, there should be a trust mechanism to identify hosts and tie their identities to end-point identifiers used by upper layer protocols.

Second, the format used in ARP does not allow for more than one resolution to be done in the same packet [5]. ARP was designed that way for simplicity. However, ARP and the existing naming structure do not directly allow multihoming features. Here, we refer to end-host multihoming where the host has several network interfaces. Any new naming architecture should address multihoming, mobility, and device identification issues as well.

Third, ARP introduces an overhead by constantly mapping IP and MAC addresses. On IP over Ethernet networks, after a device identifies itself with a MAC address and establishes its IP address, one may use only the IP address to address the device. MAC addresses are used to identify network devices in local networks. However, after devices establish IP/subnet addresses, it is satisfactory to have only the IP address of a destination device to send IP packets to that device. In that case, there is no need for an ARP cache. Switches still need to maintain tables for IP addresses and corresponding port numbers. In LANs, ARP is used to map this IP address to a MAC address to use in an Ethernet frame. Each machine on a local network examines the destination MAC address of an Ethernet frame to check if the frame is addressed to itself. A more efficient protocol should be able to use only one of the addresses after an initial setup. A network device may identify itself when it is first connected to a subnetwork to establish a network address and may use that address after that point without constant mappings. This type of protocol requires changes in Layer 2 architecture. Moreover, an authentication method should be used to verify the owner of an address. Again, a new naming architecture may solve this overhead while including some security features.

C. DHCP Overview

In LANs, the Dynamic Host Configuration Protocol (DHCP) is used to dynamically allocate IP addresses to computers for a time period. To obtain configuration information from a DHCP server, a DHCP client first sends a DHCPDISCOVER packet, which is a broadcast message in the local subnetwork. Each DHCP server responds with a DHCPOFFER message if it has some unused IP addresses available. The client may receive multiple offers. It then chooses one of the offers to accept and sends a DHCPREQUEST broadcast message destined to a specified server. After receiving the DHCPREQUEST, only the selected server commits the allocated address in its repository and responds with a DHCPACK message. When the DHCP client receives the DHCPACK message, it checks if the IP address is in use by sending an ARP message. If the address is not used, the client begins using the configuration information provided by the server.

D. DHCP Problems

DHCP servers can be easily attacked if no security is implemented. For instance, in the DHCP starvation attack, the attacker requests all of the available DHCP addresses. This results in a DoS attack on the network. The attacker can also use a rogue DHCP server to provide addresses to clients. The attacker can point the users to a different default gateway with the DHCP responses. The new default gateway can be a machine maintained by the attacker. This enables the attacker to look through the packets before he or she forwards them to the actual default gateway. Authentication of the DHCP messages is required to prevent this type of attack.

Security issues involving rogue DHCP clients are also related to the weak link Layer 2 and Layer 3 in networks. An attacker acting as a DHCP client may cause a DoS attack by generating a large number of DHCPDISCOVER messages to request IP addresses, spoofing a different MAC address for each message. The attacker (the rogue client) responds to the resulting DHCPOFFERs to quickly exhaust available IP addresses at the DHCP servers. Even though it is possible to use ARP Request and PING messages to query the addresses used in the network, the rogue client may listen to these messages and answer them. Some DHCP servers use a list of specific MAC addresses to restrict clients. However, since DHCP clients broadcast their MAC addresses to request service, these MAC addresses can easily be spoofed by an attacker for a later use. An attacker may use a DoS attack to prevent a target/victim machine from accessing the network. The attacker then renews the IP lease of the victim's machine so that the attacker can use the victim's IP address. In addition, it is possible to gain service on a network by listening a valid MAC address and then spoofing it [6]. There are other methods that exploit DHCP service. In this section, our focus was on the DHCP attacks related to the IP and MAC address binding problem.

We have two main observations about the DHCP security issues related to the weak link between Layer 2 and Layer 3 in networks. First, when DHCP servers lease IP addresses to clients, they do not enforce a secure binding between IP and MAC addresses which may be used to verify the authenticity of any frame/packet later on the networks. Second, when clients/machines are identified by MAC addresses, it does not ensure if the clients are who they claim to be.

In order to solve security problems in DHCP, RFC 3118 has been released by the Internet Engineering Task Force's (IETF) DHCP working group. This RFC describes token-based and delayed authentication methods for authentication of DHCP messages [7]. In the token-based authentication method, servers and clients exchange passwords or tokens in plain text over the wire. This method does not provide strong security for DHCP.

The delayed authentication method utilizes a shared symmetric key to mutually authorize a DHCP client and a DHCP server. In the delayed authentication method, the key is not sent over the wire. In addition, it uses a nonce or the time in the DHCP packets to prevent replay attacks. The client and the server agree on a secret ID (SID) that references the shared secret key without sending it over the wire. This secret key is used to hash DHCP packets.

In addition to these methods, Glazer, Hussey, and Shea have proposed a Certificate-Based DHCP Authentication (CBDA) method [8]. In both delayed authentication and CBDA, authentication information is sent in each DHCP packet as an option. CBDA implements the core components of delayed authentication. However, CBDA utilizes X.509 certificates or certificate chains with a common signer in the option field of the DHCPDISCOVER and DHCPOFFER packets. In CBDA, in the DHCPREQUEST and DHCPACK packets, only the signed hashes of the packets are sent in the options.

Another authentication method worth mentioning is the DHCP Authentication via Kerberos V [9]. This authentication method authenticates only the client. Furthermore, it involves communication with a Kerberos server in addition to the DHCP server communication.

These DHCP authentication methods still have some issues. For instance, delayed authentication requires that shared cryptographic keys are previously distributed to the clients and servers. Another issue of delayed authentication is key flexibility. When a client changes networks, it requires a different key to access the new DHCP server. Since different networks require different keys, this method introduces the issue of managing multiple shared secret keys. The authentication method via Kerberos only identifies the client and does not prevent rogue servers. Furthermore, it introduces an additional complexity using a Kerberos server. CBDA has some issues as well. In practice, DHCP packets are kept small. However, certificates are large and may cause problems if long certificate chains are used. There are also trust issues present in any certificate chaining protocol [8]. Moreover, the certificate revocation policy may be very complicated to set up. Finally, as long as there is no authentication method used in Layer 2 frames, one can use a DoS attack to prevent a victim from accessing the network temporarily and spoof its IP and MAC addresses. There is still a need to incorporate an authentication method with DHCP that binds IP and MAC addresses in the network at any point.

III. Addressing the Weak Layer 2-3 Link

A. MAC Security

Recently, the 802.1AE Media Access Control (MAC) Security Task Group has been formed in order to secure bridged Local or Metropolitan Area Networks [10]. This study also tries to bind Layer 2 and Layer 3 addresses by introducing security in Layer 2. The IEEE P802.1AE Standard for Local and Metropolitan Area Networks (LAN/MANs): Media Access Control (MAC) Security is still in draft form. The draft defines MAC security (MACsec) entities in end stations and bridges that provide connectionless user data confidentiality, frame data integrity, and data origin authenticity [11].

MACsec includes a Security TAG (SecTAG) in the frames after a header. The goal of the standard is to facilitate secure communication over publicly accessible LAN/MAN media for which security has not already been defined. In addition, it utilizes the IEEE Standard 802.1X, already widespread and supported by multiple vendors.

However, the standard's scope does not include key management and the establishment of secure associations [10], [11]. This draft notes that the security transform should be applied to both data and control frames to provide protection against ARP attacks. In addition, MACsec provides point to point integrity, but not global integrity [11]. For instance, a legitimate user may perform ARP spoofing.

B. IP Version 6 (IPv6)

In IPv6, an autoconfiguration option is defined to tie IP and MAC addresses. In IPv6 during the address autoconfiguration, a tentative link-local address is derived using the link-local prefix and 64-bit interface identifier. Depending on the type of the interface, the way interface identifier generated is different. For instance, for Ethernet, an IEEE EUI-64 (Extended Unique Identifier-64) address is generated using the MAC address (48 bits). The MAC address is divided in the middle and FFFE is inserted to generate 64 bit interface ID. This process can be considered as a type of Layer 2-3 binding.

C. The Host Identity Protocol (HIP)

Another study with a somewhat similar concept is the Host Identity Protocol (HIP). HIP maps an end-point identity to a host identity. In today's Internet, an IP address reflects the point of attachment of the host to the network. However, IP addresses are also used to identify hosts. This binds the location of a host on a network to its identity. If a host changes its location and thus its point of attachment to the network, it has to change its IP address and hence its identity. Other hosts trying to communicate cannot reach the host because its identity changed. One previous attempt to solve this problem is the Mobile IP framework.

The current IP-based naming architecture imposes security problems. IP addresses can easily be spoofed, and attackers can assume the identity of a victim by stealing its IP address. The current approach to solve this is the use of certificates by trusted authorities in conjunction with application layer encryption. HIP tries to solve these problems by decoupling the host identity from its network address and introducing a new name-space [12]. Instead of using the IP address as identifier, hosts are identified by their Host Identifier (HI) [13]. The HI is also the host's public key. Since the size of an HI might vary depending on the cryptographic algorithm used, a 128 bit long hashed version of it, the Host Identity Tag (HIT) is used to represent the HI at a protocol level. A third representation of the HI is the 32 bit long local scope identifier (LSI). It is designed to be able to replace IP addresses in the IP version 4 application programming interface. Transport protocols bind to the HIT or LSI rather than to an IP address. This enables the host to change its point of attachment to the network without terminating any ongoing transport connections. An HI or HIT is returned by a directory service together with one or multiple IP addresses at which the host might be reached. The HI (since it is a public key) is used to assure the authenticity of the host. This assumes that the returned HI has not been tampered with, e.g. by means of a secure directory service.

In the HIP architecture, while IP addresses continue to act as locators, the HIs take the role of end-point identifiers [12]. Note that HIP maps HIs to IP addresses. In the HIP architecture, the Host Identity Layer between Layer 3 and Layer 4 translates HIs to IP addresses and ARP translates IP addresses to link layer addresses. HIP solves the security problem related to identification of the hosts/end-points by incorporating a public key into the identities. This provides end-to-end security.

However, HIP does not address all sorts of possible Layer 2 attacks. ARP spoofing can still be used to mislead packets since ARP works at a lower level unprotected by HIP. Nonetheless, due to the encryption facilities of HIP, man-in-the-middle attacks are prevented. One disadvantage of HIP is that it requires changes at the end hosts and a revised, secure directory system. The concepts used in HIP may be extended to between Layer 2 and Layer 3 to securely identify a network device and bind MAC and IP addresses.

D. Cryptographically Generated Addresses (CGAs)

Cryptographically Generated Addresses (CGAs), which is a new naming architecture proposed for IPv6 addresses, also utilizes a Public Key Infrastructure (PKI) to identify address owners. In this addressing method, some IP address bits are created from a cryptographic hash of the address owner's public key. The owner signs messages with its private key to assert ownership of the address. One of the advantages of CGA is that it does not require a trusted authority [14]. Note that both CGA and HIP identifies hosts with public/private key pairs. However, while HIP utilizes a hash of the public key as the primary identifier for IP nodes and is a new protocol layer between Layer 4 and Layer 3, CGA uses the IP layer addressing structure to bootstrap security [14]. The approach used in CGA may be extended to Layer 2 to identify hosts as well.

E. Solving the Layer 2/Layer 3 Binding Problem

We believe that there are two possible approaches to address the weak Layer 2-3 link: a cryptographic method, which binds IP and MAC addresses using DHCP or a trusted server, and a new naming architecture. A cryptographic MAC-IP binding method may address the weak Layer 2-3 link. In this approach, during the authentication of a host at a DHCP server, the DHCP server or a trusted party may ensure authenticity of the Layer 2 frames by setting up security parameters in the local network. For instance, the DHCP server may distribute a key to bind IP and MAC addresses at each host. This key may be used to generate a message integrity check/hash value for each Layer 2 frame. These hashes must be protected against replay attacks as well. The key used to verify authenticity of Layer 2 frames must be delivered to the host securely by the DHCP/trusted server. If a trusted server is used to generate security parameters such as the key, then that server should communicate with the DHCP server as well. However, involvement of a third party introduces an additional complexity and traffic load to the network. Moreover, this approach with or without involvement of a third party requires changes in switch/bridge software. In the case of static IP addresses, machines may prove their identity and inform their IP addresses to a trusted server. This trusted server may provide security parameters to these machines. Another way to bind IP and MAC addresses cryptographically is to create secure associations/channels between end-points in link layer. This is similar to MACsec. This type of solution should provide global integrity to prevent ARP spoofing by the legitimate hosts. Layer 2 frames carrying ARP messages must be authenticated as well. Finally, this approach does not eliminate the overhead created by MAC and IP mappings using ARP.

The second approach, a new naming architecture, may solve the issues in networks in a more feasible fashion. But, in practice, it is harder to implement. A new naming architecture that uses cryptographic identities for network devices may secure identities and separate identities from locations totally. This eliminates the need of location and identity bindings. HIP is such an architecture. Since HIP provides a cryptographic identification for end-points/hosts, it solves the secure identification problems. However, HIP is designed to work between Layer 3 and Layer 4. This type of identification should be carried into Layer 2 as well. For instance, a public/private key pair may be used to identify machines instead of MAC addresses. MAC addresses could be a hash of a public key at Layer 2 (similar to HITs/HIs in HIP). An advanced ARP mechanism could use such a property to give hosts the ability to prove that they are the legitimate users. Then again, public/private key computations are too expensive to utilize in Layer 2 authentications since Layer 2 frames need to be processed fast. Instead, public/private keys may be used to establish symmetric keys to authenticate Layer 2 frames. HIP requires the host that desires to initiate a connection to solve a puzzle in order to complicate denial of service attacks. The idea is to increase the resource needs for hosts involved in starting a denial of service attack. A related approach could be used to prevent ARP flooding attacks. In addition, data confidentiality may be provided by upper layers to decrease computational requirements at Layer 2. The only necessity in Layer 2 is the authentication of the frames. CGA is another example for such an architecture. CGA utilizes PKI to identify address owners. In CGA, a cryptographic hash of the IP address owner's public key is used to generate IP addresses. The address owner signs messages with its private key. This public/private key pairs may be utilized to identify machines by extending CGA into Layer 2. Again, PKI is computationally expensive to be directly utilized in Layer 2 authentications. Moreover, if such an approach is utilized in Layer 2, every HIT/CGA and related public key information must be registered in a directory server and must be available to Layer 2 switches/bridges. Again, this requires changes in switch/bridge software. Furthermore, generating a public/private key pair for every device/machine that is globally unique is a challenge. Finally, note that all these approaches should address multihoming, mobility and device identification issues as well.

IV. Conclusions

In this paper, we presented issues caused by the weak link between network and data link layers in local networks. Current protocols used in networks do not provide a secure binding between the Internet Protocol (IP) and MAC addresses. We summarize some of the issues regarding the Layer 2 and Layer 3 link and discuss related solutions to address security and naming issues in networks. We also present possible approaches to address the weak link between Layer 2 and Layer 3.

One of the approaches mentioned uses a DHCP server to create security parameters for Layer 2 on local networks. A DHCP server or a trusted party may be utilized to distribute security parameters to authenticate Layer 2 frames. We believe that encryption for data confidentiality can be handled by upper layers to minimize computational load in Layer 2.

Another approach mentioned is to use a new naming architecture. We observe CGA and HIP naming architectures in the literature utilizing PKI. Extension of these approaches may solve/eliminate MAC-IP binding issues. However, since public/private key computations are not feasible in Layer 2 authentications, these methods may not be directly used. In addition, generating a globally unique public/private key for every host/machine is not a reasonable approach. Moreover, it is still a question whether a globally unique public/private key pair is needed for every machine/host in a network instead of a locally unique public/private key pair. Finally, multihoming, mobility and device identification issues should be addressed by these approaches.

Future work should focus on examining possible approaches in detail and investigating the best approaches to address the weak link between Layer 2 and Layer 3.

References

[1] Connie Howard, *Layer 2 – The Weakest Link: Security Considerations at the Data Link Layer*. Available at http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac222/about_cisco_ packet_feature09186a0080142deb.html.

[2] Ryan Spangler, *Packet Sniffing on Layer 2 Switched Local Area Networks*, December 2003. Available at http://www.packetwatch.net/documents/papers/layer2sniffing.pdf.

[3] A. Ornaghi, M. Valleri, *Man in the middle attacks Demos*, Blackhat 2003. Available at http://www.blackhat.com/presentations/bh-usa-03/bh-usa-03-ornaghi-valleri.pdf.

[4] S. Convery, *Hacking Layer 2: Fun with Ethernet Switches*, Blackhat 2002. Available at http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-converyswitches.pdf.

[5] David C. Plummer, *An Ethernet Address Resolution Protocol*, RFC826, November 1982.

[6] Maththew P. Harvey, *Dynamic Host Configuration Protocol: Security Implications and Possible Safeguards*, February 2004. Available at http://www.giac.org/practical/GSEC/Matthew_Harvey_GSEC.pdf.

[7] Ralph Droms, William Arbaugh, *Authentication for DHCP Messages*, RFC3118, March 2003.

[8] Glenn Glazer, Cora Hussey, and Roy Shea, *Certificate-Based Authentication for DHCP*, March 2003. Available at http://www.cs.ucla.edu/ chussey/proj/dhcp_cert/cbda.pdf.

[9] Hornstein at al., *DHCP Authentication via Kerberos V*, November 2000. Internet Draft, The Internet Society.

[10] *IEEE 802.1AE*, Media Access Control (MAC) Security. Available at http://www.ieee802.org/1/pages/802.1ae.html

[11] *IEEE P802.1AE/D1.2 Draft*, Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security. Available at http://www.ieee802.org/1/files/private/ae-drafts/d1/802-1ae-d1-2.pdf.

[12] Pekka Nikander, *Applying Host Identity Protocol to the Internet Addressing Architecture*, Proceedings of The 2004 International Symposium on Applications and the Internet, SAINT2004, Tokyo, Japan, January 26-30, 2004.

[13] R. Moskowitz, P. Nikander, P. Jokela, T. Henderson, *Host Identity Protocol*, February 2004. Available at http://hip4inter.net/drafts.php/draft-moskowitz-hip-09.txt.

[14] Tuomas Aura, *Cryptographically Generated Addresses (CGA)*, Internet Draft, April 2004. Available at http://ietfreport.isoc.org/ids/draft-ietf-send-cga-06.txt.