Global Information Assurance Certification Paper

AN ALTERNATIVE PACKET AUTHENTICATION/FILTERING METHODOLOGY

Greg G. Darroca
MBUS511

Purpose

This paper intends to review an alternative methodology in packet authentication/filtering. The Link Layer Packet Authentication (LLPA) is an IP packet filtering process which occurs within and no higher than the OSI Link Layer (Layer 2). Proposed by a trio of network/systems security researchers (Professors Geoffrey Xie and Cynthia Irvine, Mr. Cary Colwell) from the Computer Science Department, Naval Postgraduate School, the LLPA is designed to be efficient in high speed authentication[1] and offers the flexibility and extensibility of software based cryptography. LLPA boast two innovative features: Dynamic multiple key management with short lifetime for each key, and a fixed length authentication trailer (AT) attached to each packet. These innovative features combine to potentially provide high speed authentication, and theoretically be highly resistant to Denial-of-Service (DoS) attacks, man-in-the-middle attacks, and any other hacking techniques that occur above the Link Layer.

Background

The IT industry appears to have focused implementation of virtual private network (VPN) remote client-to-host secure session towards the Security Architecture for the Internet Protocol (IPsec). IPsec separates packet security application into two categories: authentication and data confidentiality. Both categories rely solely on providing the security mechanism in the header. In an IP-based network like the Internet, this seems like a good match. Although present router technology forwards packets at gigabit per second speeds, the hardware-based implementation of IPsec VPN still suffers in throughput performance due to the penalties imposed by the cryptographic process[2] occurring in the Network Layer that is IP. This performance penalty leaves IPsec VPN vulnerable to DoS attacks, where the slow VPN authentication gateway can be overwhelmed with incoming invalid packets. However, manufacturers reduce the latency by encoding the cryptographic algorithm in hardware, thus improving throughput. Unfortunately, hardware encoding of cryptographic algorithm leaves the implementation inflexible[3], therefore more expensive to update/upgrade. The symmetrical[4] nature of its secure session

[1] Performance is comparable to hardware-base authentication.
[2] Encryption and decryption of header data using proprietary algorithm.
[3] Cannot be reprogrammed for update as easily as software-based implementation, but software implementation is more vulnerable to DoS than hardware implementation.
[4] Shared secret key. Remote client and gateway host uses one key for the authentication

keying presents another vulnerability in that the intruder only has to discover one key to compromise the whole session. Thus, leaving the session participants exposed to hacking techniques in the upper OSI layers afterwards.

Link Layer Packet Authentication

The LLPA model consists of remote users, a public network such as the Internet, a Packet Authenticator Gateway (PAG), and a secure area/domain associated with the PAG. The PAG is the AT processor, detaching it from the main packet body, and sorting and executing its fields in accordance with the authentication process. The AT is a fixed length, 32-byte segment that is attached to the tail of the IP packet. It is made up of:

- 16 bytes to hold the digital signature, referred to as Message Authentication Code (MAC)
- 1 byte for the version field
- 1 byte for the option field
- 2 bytes to hold the "option" data
- 2 bytes to hold the "Start of protected segment" marker
- 2 bytes to hold the "Length of protected segment" data
- 4 bytes to hold the sequence number
- 4 bytes to hold the key index

Note: For the sake of brevity, only the MAC, sequence number and key index fields will be discussed in the description of LLPA's operation.

The MAC is produced using a symmetric key and the IP packet[5] as the input into the MAC algorithm. Instead of using just one key for the session, LLPA proposes to utilize multiple symmetric keys, each key being applied for a period of time (e.g., 1 minute, 2 minutes, 30 seconds, etc.) throughout the session. Each key is utilized no longer than its cryptoperiod[6]. The advantage gained then is that it increases the complexity to compromise the session for an intruder. That is, the intruder must now "crack" multiple keys in order to make sense of the session. Even if an intruder is successful with a key, this success will only compromise a short segment of the session. Additional protection is derived by not transmitting the key itself with the trailer-IP. Instead, a key index associated with a symmetric key is used. The sequence number ensures that no two packets have identical MAC even if both have identical protected segment. This is further protection from the man-in-the-middle attack.

---

process.

[5] The protected segment. The user may choose to either narrow or expand the protected segment. The smaller the protected segment, the less processing (and time) the PAG must expend in authenticating the packet.

[6] The anticipated period it takes for an intruder to discover the key.

Since multiple symmetric keys are required, LLPA provisions for a key distribution/management segment of the authentication process called the Key Distribution Center (KDC). The KDC could be a separate hardware component from or an integrated part of the PAG. The decision is a matter of requirement, cost or personal choice. The KDC generates the tables of symmetric keys for each session. These "prefetch" keys are then distributed to the remote user and the PAG upon receipt of a request for a session. The session key table is refreshed as necessary.

Operation

The remote user initiates the session with a request to the KDC. The KDC responds with a "prefetch" table of keys being transmitted securely to the remote user and the PAG concerned. The remote user and the PAG then synchronize in order to match sequence and key indexes. The remote user proceeds with the session by transmitting IP packets with attached ATs. The PAG processes the packets by detaching the AT from the IP packet; extracts the key index to determine the correct symmetric key; computes a MAC with the indicated key and the IP packet body; and compares the results with the MAC carried within the AT. All of this is executed within the Link Layer and without parsing the IP header. Thus an additional reduction in latency is gained by not elevating the authentication process to the Network Layer. The fixed length format also adds to the efficiency and high speed of the process, copying from the successful application of fixed length cell switching in Asynchronous Transmission Mode (ATM) technology. If there is a match with the MACs, the IP packet is forwarded into the secure domain for further processing. If a match is not achieved, the packet is simply dropped. Due to the fixed format, the authentication elements can be encoded into hardware, and gain the necessary high speed authentication processing that should make LLPA highly resistant to DoS attacks. Lastly, LLPA does not suffer from the security weaknesses of the IP and of those protocols above it.

Conclusion

Conceptually, LLPA offers promising speed and security advantages over header based implementation of secure IP communication. Its dynamic multiple key management and authentication trailer model is innovative, and proffers lower cost, flexible security architecture at performance comparable to hardware-based authentication. The "trailer" methodology allows LLPA to be fully compatible with existing network and Internet protocols. However, LLPA does suffer shortcomings. Its most glaring weakness is the time and vulnerability cost users must bear during the set-up phase[7]. This is no different

[7] User-host authentication to the KDC and key table distribution.

from other login/authentication process of other security protocols except that it may take longer and require more cryptographic resources to adequately protect the key table distribution. Associated with this is the equally important matter of synchronizing the key tables between user(s) and host(s). LLPA suggests a "key window"[8] as a possible solution, but also allows the user to determine its own schema. Then there is the matter of intervening network/Internet routers fragmenting LLPA packets based on path maximum transmission unit (PMTU) settings along the way. Since the MAC is partly based on the packet body, the fragmentation will cause the MAC to be invalid; therefore the associated packets are rejected at the PAG. LLPA advocates the use of path MTU discovery or other similar mechanism to prevent fragmentation.

Reference:

1. Bellovin, S. M. (1989). "Security Problems in the TCP/IP Protocol Suite.". URL: http://rootshell.com/beta/documentation.html

2. Chapman, D. B. (1992). "Network (In)Security Through IP Packet Filtering." . URL: http://rootshell.com/beta/documentation.html

3. Fratto, M. (1998). "IPSec-Compliant VPN Solutions: Virtualizing Your Network." Network Computing.
URL: http://www.networkcomputing.com/914/914r1.html

4. Fuller, E. R. (2000). "Denial of Service Attack." (April 6). URL: http://www.sans.org/infosecFAXQ/dos.htm

5. Moskowitz, R. (1998). "What Is A Virtual Private Network?" Network Computing.
URL: http://www.networkcomputing.com/905/905colmoskowitz.html

6. Stallings, W. (1999). Cryptography and Network Security: Principles and Practice. Upper Saddle, New Jersey, Prentice Hall.

7. Townsley, W., A. Valencia, et al. (1999). "RFC2661: Layer Two Tunneling Protocol "L2TP".".
URL: http://www.ietf.org/rfc/rfc2661.txt?number=2661

8. Wright, G. R. and W. R. Stevens (1995). TCP/IP Illustrated, The Implementation. Reading, MA.

9. Wright, G. R. and W. R. Stevens (1995). TCP/IP Illustrated, The Protocols.

[8] A sliding window of 3 keys: previous key, present key and next key.

Reading, MA, Addison-Wesley.

10. Xie, G. B., C. Irvine, et al. (1999). “A Protocol for High Speed Packet Authentication.” (June 7).

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event