Australian Telecommunications Networks & Applications Conference 2004 (ATNAC2004), Sydney, Australia, December 8-10 2004

Lawful Interception based on Sniffers in Next Generation Networks

Andres Rojas and Philip Branch
{anrojas, pbranch}@swin.edu.au
Centre for Advanced Internet Architectures,
Swinburne University of Technology, Melbourne, Australia

15th October 2004

Abstract

Today, the function of Lawful Interception (LI) in IP service networks is typically performed by systems which are based on the use of traffic sniffers. These LI systems are typically used to determine when a target is attempting to use an Internet Service Provider's (ISP) services and subsequently to intercept his/her traffic for formatting and transmission to a Law Enforcement Agency (LEA). This paper evaluates whether or not these sniffer based LI systems are suitable to deployment in next generation network such as IPv6 and Mobile IPv6 networks.

Keywords:- Lawful interception, wiretapping, mobile IP, IPv6, sniffers

1 Introduction

Lawful Interception (LI) is the process whereby a Lawful Enforcement Agency (LEA) is legally allowed to intercept a target's communications for the purpose of law enforcement. Typically the process is dependent upon both the provision of a legal warrant to carry out the interception, and the technology being available to perform the interception.

Typically, telecommunications access and service providers (including ISPs) are legally obliged to provide an LI solution as part of their network/service. Failure to provide an interception capability is enough to prevent a new service's deployment[1].

Today, in IP service networks, the LI function is provided by proprietary systems that rely heavily on the use of traffic sniffers. The FBI's Carnivore/DCS1000 system[2] is a good example of a sniffer based LI tool, though many commercially available LI tools are also available [3, 4, 5].

In a typical setup, the LI system is initially configured to capture messages that identify a target's login attempt and the target's subsequent allocated IP address. The Remote Authentication Dial In User Service (RADIUS) protocol[6], which provides Authentication, Authorization and Accounting (AAA) functions is commonly used as a target protocol for capture. Once the target's IP address is known, the LI system automatically reconfigures itself to also capture all IP traffic to/from that IP address so that it can be interpreted, transformed and delivered to the LEA.

LI in IP networks is not standardized. In fact, the IETF, the body that oversees the evolution of the Internet and the standardization of it's protocols, has actively rejected the idea of including functionality intended to facilitate LI [7].

Today's Internet consists of a myriad of protocols which provide the every day functionality that we are now used to. Security, though, was designed as an "afterthought". Early protocols relied on the assumptions of correct IP addresses in IP headers, and transmission of user names and passwords in clear-text for their security [8]. Evolution has seen the adoption of ad-hoc solutions and eventually the elaboration of a generic framework for Internet security - IPsec [9].

In contrast to current networks, future network proto-

ISBN 0-646-44190-6

cols have been designed with security as one of their key requirements. For example, both IPv6 [10] and Mobile IPv6 [11] require the support for IPsec for cases where security is a concern. Another example can be found in the IETF's submission of the DIAMETER protocol [12] to support the AAA requirements for current and future networks.

This paper aims to prove that the heavy use of encryption for the exchange of AAA information means that LI systems based on sniffers in use today, which rely on the ability to capture AAA information, will not be suitable solutions for LI in future networks. Solutions to this problem are outlined.

The research area of traffic analysis and mix networks has the goal to further protect the communications of users by making receivers and senders anonymous [13, 14, 15]. An attacker, or an LI system in this case, would not be able to intercept a user's traffic. This paper does not explore the implications of this area of research on LI systems of the future. This is left as future work as it would imply that interception based on passive solutions, such as sniffers, are even more inadequate for use in future networks.

This paper does not address the issue of the interception of a user's traffic when such traffic is itself encrypted by the end users.

In section 2 we introduce how sniffer based systems are used in IPv4 service networks which use a RADIUS-based AAA infrastructure. Section 3 is an introduction to the DIAMETER protocol which will provide the AAA implementation necessary to support future networks. In section 4, we focus on the application of sniffer based LI systems to IPv6 and Mobile IPv6 networks and their interaction with AAA infrastructure, and finally, in section 5 we outline some possible solutions before concluding.

2 A Sniffer based LI system today

In this section, we describe a typical solution which is employed to provide LI functionality in an ISP's network. Commercial products are usually deployed in these situations [3, 4, 5].

Although these products can usually intercept based on information in IP traffic such as IP address, MAC address or cable modem ID, they can also intercept based on higher-layer data such as a RADIUS username, email address or instant messaging ID. In this section we examine interception based on the use of RADIUS as an authentication and authorization mechanism.

RADIUS [6] provides the communications protocol by which a user can be authenticated when trying to access a network. Typically, a dial-in user with a computer and a modem will dial into an ISP's Network Access Server (NAS) using the ISP's PSTN phone number. A user provides authentication credentials such as a username and password. The NAS, before it grants the user access to the ISP network (and consequently access to the Internet), must check that the user supplied credentials are correct. This authentication service is provided by a RADIUS server which can interact with the ISP's many NASes using the RADIUS protocol. Figure 1 shows the components of the description just given as well as an LI system based on the use of a sniffer.

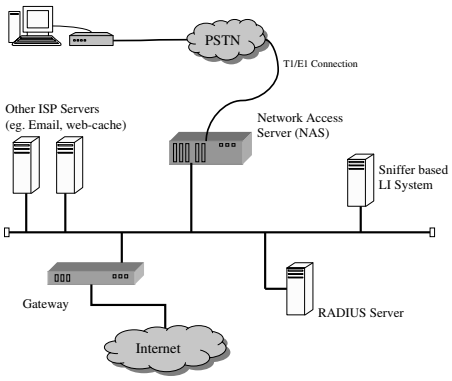

Figure 1: A typical dial-in ISP with a Sniffer based LI system

The two RADIUS messages of importance where LI is concerned are the *Access-Request* and *Access-Accept* messages. The *Access-Request* message, sent by the NAS to the RADIUS server, contains the user supplied username and password in the form of RADIUS Attributes *User-Name* and *User-Password* (though the latter is dependent on the type of authentication scheme used). The RADIUS server, acting as a centralized AAA service, will then check the user's username and password before ei-

ISBN 0-646-44190-6

ther allowing or disallowing network access. A granting of access is indicated using the *Access-Accept* RADIUS message from RADIUS server to NAS. This message also contains a RADIUS Attribute, *Framed-IP-Address*, which indicates to the NAS the IP address to assign to the user when providing the requested access.

A sniffer based LI system placed in an ISP's network, such as the one shown in 1, will capture all RADIUS messages, searching for the *Access-Request* message with a *User-Name* Attribute value corresponding to a target's username. The LI system, which is continuously capturing RADIUS traffic, then searches for an *Access-Accept* message which corresponds to the request. This correlation is achieved using a message identification field common to both messages. Once this message is captured by the LI system, it can then automatically reconfigure itself to, apart from capturing RADIUS traffic, also capture any traffic to and from the IP address reported in the *Access-Accept* message. Any user traffic is then either sent to a LEA directly or stored for subsequent delivery.

3 AAA, DIAMETER and Security

3.1 DIAMETER and Authentication, Authorization and Accounting (AAA)

Although RADIUS has been deployed for a decade or so, it does have a number of limitations. These include a lack of security when using RADIUS proxies, scalability problems in large networks and a lack of extendability when adding support for new forms of authentication.

The DIAMETER protocol has been defined by the IETF's AAA working group to be the AAA protocol of choice for the next generation of networks. It is intended to provide the AAA features to enable access to dial-in networks, mobile IP networks, roaming services, and because of it's extendability, future networks as well. In addition to this DIAMETER is designed to be backwards compatible with RADIUS.

DIAMETER is based on the provision of a base DIAMETER protocol [12] which defines the generic message formats and data types together with the generic transport, error reporting, security and accounting services. The base protocol is usually used in conjunction with a DIAMETER application which defines the specific details which are unique for that application, for example the Mobile IPv4 DIAMETER application [16] or the Network Access DIAMETER application [17]. A DIAMETER client which supports the DIAMETER application communicates with a DIAMETER server, which also must support the specific DIAMETER application.

To carry the data needed for a DIAMETER server to authenticate, authorize and account for usage, the DIAMETER protocol uses Attribute-Value Pairs (AVP) within messages. An AVP consists of an AVP code and vendor ID to identify the attribute uniquely, as well as the value of that attribute. The format of a DIAMETER message permits many AVPs per message. The extendable nature of DIAMETER means that, although data types to be used and mandatory AVPs are defined in the base protocol, the meaning of what a specific AVP contains is defined in the applications.

As an example of DIAMETER's use, consider the Network Access DIAMETER application which would be employed at an ISP that offer's a dial-in service for it's network. [17]defines the *AA-Request* and *AA-Answer* commands which are sent to and from a DIAMETER server respectively and provide the basic messages needed to authenticate a user who is dialing in. Although both these messages are defined in [17], the data types, header format, and security considerations that are used by this specific application are all defined in the base DIAMETER protocol [12]. Similarly, a number of network access specific AVPs to use in the above messages are also defined in the application specific document.

3.2 IPsec and Encapsulating Security Payload (ESP)

The IETF has defined an architecture for providing security of traffic at the IP layer [9]. This architecture, commonly referred to as IPsec, defines the components of an IPsec compliant system in terms of providing services such as access control, integrity, authentication, and encryption. An implementation of IPsec on a host or router typically protects the IP traffic being sent and received.

A key component of the architecture, which specifies how encryption is supported, is the Encapsulating Security Payload (ESP) extension header [18]. ESP for both IPv4 and IPv6 traffic has been defined. ESP can be ap-

Australian Telecommunications Networks & Applications Conference 2004 (ATNAC2004), Sydney, Australia, December 8-10 2004

ISBN 0-646-44190-6

plied in two ways: transport mode or tunnel mode. Transport mode protects layers above the IP layer, but it does not protect the IP header. Tunnel mode protects an entire IP packet by tunneling (encapsulating) an entire encrypted IP packet within another - all of the inner packet's contents are protected.

Also of importance is the algorithm under which encryption takes place. In IPsec, the choice of algorithm for encryption (and authentication) is algorithm-independent. [9] defines the set of default algorithms that must be supported by an IPsec implementation, including the "null" algorithm.

In the IPv6 case, in transport mode, an ESP extension header has been defined to protect all fields that follow it in an IP packet. In figure 2 for example, which is reproduced from[18], the upper layer header and data (TCP in this case) can be both encrypted and authenticated using ESP. The ESP extension header is placed both before the fields to protect, and after them.

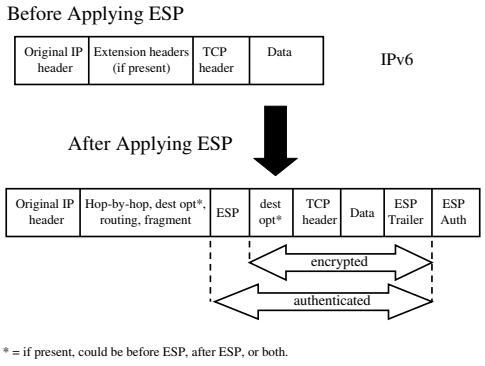

Figure 2: ESP extension header position for IPv6 (transport mode)

4 Sniffer based LI systems in future networks

4.1 IPv6 with RADIUS

The original RADIUS specification [6] is concerned with authentication for the provision of IPv4 based services. A number of new RADIUS attributes have been added to RADIUS to cater for the provision of IPv6 services by an ISP [19]. These include the *Framed-Interface-Id* and *Framed-IPv6-Prefix* attributes to specify to a NAS the IPv6 interface-ID and prefix that have been allocated by the RADIUS server to a user that is requesting an IPv6 service.

The same specification that defines the above attributes also states that, for full compliance to IPv6, a RADIUS implementation which supports IPv6 is required to also support IPsec.

Even though how an ISP's intra-network adheres to the compliancy requirements demanded by the RFC is an ISP internal issue, non-compliance should be an exceptional case. Non-compliance would also severely compromise the security of communications in the case where a roaming IPv6 service is offered.

Therefore, it follows that the RADIUS messages *Access-Request*, from a NAS to a RADIUS server, and *Access-Accept*, from the RADIUS server to the NAS, will have the attributes that identify the user-name and IP address in an encrypted format. A sniffer based LI system will, thus, not be able to know the IP address which has been allocated for a particular target.

4.2 IPv6 with DIAMETER

The network deployment scenario discussed in this section is one where an ISP offers an IPv6 service where AAA services are implemented using the DIAMETER protocol. A specific DIAMETER application is specified, by extending the base DIAMETER protocol for this scenario, in [12, 17].

So, for example, after a user dials in to a NAS, the NAS would send an *AA-Request (Authentication and/or Authorization Request)* command to a DIAMETER server with AVPs such as *User-Name* and *User-Password* for the user's name and password amongst others. The DIAME-

Australian Telecommunications Networks & Applications Conference 2004 (ATNAC2004), Sydney, Australia, December 8-10 2004

ISBN 0-646-44190-6

TER server would then respond to the NAS with an *AA-Answer* command with appropriate AVPs.

For the provision of IPv6 services, the *Framed-Interface-Id* and *Framed-IPv6-Prefix* AVPs have been defined to report to a NAS the IPv6 interface-ID and prefix(es) that have been configured for the user by the DIAMETER server. These AVPs would be present in the *AA-Answer* command from DIAMETER server to NAS. These AVPs would then be used by the NAS to tell the user's host the IPv6 address that is configured.

The security considerations specified in the base DIAMETER protocol are applicable in this case [12]. Therefore, the communication between a NAS and a DIAMETER server would be encrypted using IPsec ESP with a non-null encryption algorithm.

Just like in the case for an IPv6 service based on RADIUS authentication, a sniffer based LI system would not be able to detect that a target is attempting to use the ISP's services or that an IPv6 interface-ID and prefix has been assigned. A target's traffic based on the subsequent configured address would not be interceptable.

4.3 MIPv6 with AAA.

Mobile IPv6, as defined in it's latest Internet draft [11] has no inherent integration with any AAA infrastructure. This is, after all, not the concern of the Mobile IPv6 specification, and outside of it's scope.

The case exists, therefore, for a Mobile IPv6 service to either exist without support for AAA, or with support for AAA. In this section we cover the scenario where a Mobile IPv6 service is integrated with AAA. The scenario where a Mobile IPv6 service exists with no AAA infrastructure is not covered. This is because the goal of this paper is to compare future network deployments with how sniffer based LI systems are used in networks today, that is, in a network with inbuilt AAA infrastructure.

The process of defining how Mobile IPv6 will integrate with the AAA framework is in it's infancy. Today, a number of Internet drafts have begun to describe the specific requirements that are required of an AAA infrastructure by Mobile IPv6 [20, 21]. Whether or not the currently proposed AAA implementation protocol, DIAMETER, complies well with those requirements is a discussion that has not yet begun within the IETF's AAA working group. It should be noted that none of the proposed drafts consider LI to be an immediate requirement.

However, considering the flexible design inherent in DIAMETER, and that a suitable solution has been defined for Mobile IPv4 using an application of the base DIAMETER protocol [16], it is expected that an application of the base DIAMETER protocol will also be defined for use with Mobile IPv6.

As IPsec is a mandatory requirement in the deployment of DIAMETER, it is expected that the trigger that a sniffer based LI system would need, that is, the interception of a message which communicates to the DIAMETER server that a target is attempting to authenticate, would not be able to be interpreted as the message's contents would be encrypted.

5 Possible Solutions

5.1 Sharing Encryption Keys

A possible solution is to permit the LI system to be aware of the encryption keys used by the AAA infrastructure. This is a variant of a key escrow system [22, 23, 24]. It is a variant because the keys that are stored, the storing "trusted" system, and even the actual communication belong to the same entity - the ISP.

One of the major concerns with key escrow systems is the fact that governments or independent parties are entrusted with the public's privacy by their storing of the encryption keys used. Applied to the variant escrow system being considered this argument is still relevant though to a lesser extent because it's the ISP's communications that are being encrypted not the public's.

In this case, the relevant issue is that of the protection of a customer's privacy. There is the responsibility on the ISP to make the LI system resilient to external attack and for it to be subjected to strict access control. An internal or external attacker that infiltrates the LI system may be able to obtain the keys used to encrypt the AAA messages and use AAA info, such as the IP address allocated to a user, to perform illegal interceptions.

Australian Telecommunications Networks & Applications Conference 2004 (ATNAC2004), Sydney, Australia, December 8-10 2004

ISBN 0-646-44190-6

5.2 An LI protocol

Another possible solution is to introduce a communications protocol, at the application level, that enables an LI system to know when a target user starts and stops using the network, and what IP address to carry out its interception on.

Using the protocol, the LI system could tell the AAA server that it is interested in a particular target (username@domain). The AAA server would then, using the same protocol, inform the LI system of the target's login onto the network and the IP address to intercept on. The LI system, which could be sniffer based, would then be able to intercept the target's traffic. When the target user terminates his/her session, the AAA server, or access device, would then inform the LI system of this event, in order for it to stop interception. The LI system would also have to let the AAA server know when it is no longer interested in interception of the target's traffic.

Figure 3 presents the sequence of signals for the simple case described above. It represents a possible solution to the problem described in section 4.2. The DIAMETER messages shown in the figure (those between the NAS and the AAA server) are specified in [12, 17].

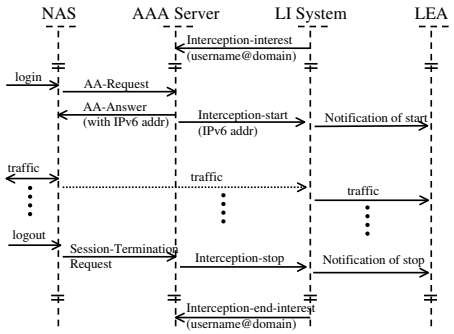

Figure 3: Sequence of signals involved in a LI protocol

5.3 Proprietary Solution

An alternative to introducing a protocol for the above function is to build interception capability into the AAA infrastructure itself. By this, we mean only to design interception functions into products which act as AAA servers, for example, and not to build it into the AAA protocols themselves. These systems would be proprietary in nature and if not also open to public scrutiny would not be recommended.

6 Conclusions

Sniffer based LI systems are being used today to provide LI capabilities at ISP premises. Typically, a sniffer is used to firstly capture messages of the RADIUS protocol to identify the IP address allocated to a target when logging in, and subsequently to capture all IP traffic to/from that IP address.

Sniffer based LI systems will not be suitable for future networks such as IPv6 and Mobile IPv6 networks. This is due to the requirement for the AAA infrastructure employed in these networks being required to support encrypted communications. In the relevant RFCs, the required compliance is towards using IPsec for encryption, that is, using IPsec with ESP and a non-null encryption algorithm.

The critical parts of the technical process, that of identifying when a target attempts to login and of identifying the IP address allocated to the target, will be uncapturable with a sniffer based LI system due to the aforementioned encryption.

The implication of this is that alternatives to LI systems based on sniffers are needed. Alternatives, such as those described in section 5 need to be researched more thoroughly and be discussed openly. A particular concern, considering the authoritative nature of governments and regulators is that a network service of the future may not be allowed to be provided if a suitable alternative is not available.

Another option, and arguably of more devastating consequence in terms of privacy, is for Lawful Enforcement Agencies to implement LI solutions that are agency-internal and not open to scrutiny by the public or network engineers.

Even though the IETF has decided to not inherently support interception in it's protocols, it does believe that open discussion and review of proposed LI systems and the publication of such research and weaknesses therein

ISBN 0-646-44190-6

should be encouraged [7].

Solving the LI problem for future networks in a way that maintains secure communications is a serious challenge for the Internet community and should be seen as needing research by the network research community.

References

[1] "Bills Digest no.67 1997-98, Telecommunications Legislation Amendment Bill 1997," Parliament of Australia, Oct. 1997.

[2] "Independent Review of the Carnivore System," IIT Research Institute, Independent Review IITRI CR-030-216, Dec. 2000. [Online]. Available: http://www.epic.org/privacy/carnivore/carniv_final.pdf

[3] "White Paper on Xaminer IP," Citadel Interception Techonologies, Tech. Rep., 2003. [Online]. Available: http://www.citadel.com.au/pdf/xaminer/Xaminer_whitepaper.pdf

[4] "Lawful Interception for IP Networks, White Paper," Aqsacom Inc., Tech. Rep., 2004. [Online]. Available: http://www.aqsacom.com

[5] *DCFD 3500*, http://www.toplayer.com/pdf/DCFD3500jul03pdf.pdf, Top Layer Networks, Inc.

[6] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," RFC 2865, June 2000.

[7] IAB and IESG, "IETF Policy on Wiretapping," RFC 2804, May 2000.

[8] S. Hagen, *IPv6 Essentials*. O'Reilly and Associates, Inc., 2002.

[9] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, Nov. 1998.

[10] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, Dec. 1998.

[11] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," draft-ietf-mobileip-ipv6-24.txt, June 2003.

[12] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," RFC 3588, Sept. 2003.

[13] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, 1988.

[14] O. Berthold, H. Federrath, and S. Köpsell, "Web MIXes: A system for anonymous and unobservable Internet access," *Lecture Notes in Computer Science*, vol. 2009, pp. 115–??, 2001. [Online]. Available: citeseer.ist.psu.edu/berthold01web.html

[15] P F Syverson and D M Goldschlag and M G Reed, "Anonymous Connections and Onion Routing," in *IEEE Symposium on Security and Privacy*, Oakland, California, 4–7 1997, pp. 44–54. [Online]. Available: citeseer.ist.psu.edu/syverson97anonymous.html

[16] P. Calhoun, T. Johansson, and C. Perkins, "Diameter Mobile IPv4 Application," draft-ietf-aaa-diameter-mobileip-13.txt, Oct. 2002.

[17] P. Calhoun, G. Zorn, D. Spence, and D. Mitton, "Diameter Network Access Server Application," draft-ietf-aaa-diameter-nasreq-14.txt, Feb. 2004.

[18] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406, Nov. 1998.

[19] B. Aboba, G. Zorn, and D. Mitton, "RADIUS and IPv6," RFC 3162, Aug. 2001.

[20] S. Faccin, F. Le, B. Patil, C. Perkins, F. Dupont, M. Laurent-Maknavivius, and J. Bournelle, "Mobile IPv6 Authentication, Authorization, and Accounting Requirements," draft-le-aaa-mipv6-requirements-03.txt, Feb. 2004.

[21] H. Ohnishi, M. Yanagiya, and Y. Ohba, "Mobile IPv6 AAA Problem Statement," draft-ohnishi-mip6-aaa-problem-statement-00.txt, Feb. 2004.

[22] D. Denning, "To Tap or not To Tap," *Communications of the ACM*, vol. 36, no. 3, pp. 24–33, Mar. 1993.

Australian Telecommunications Networks & Applications Conference 2004 (ATNAC2004), Sydney, Australia, December 8-10 2004

ISBN 0-646-44190-6

[23] S. Micali, "Fair cryptosystems, Tech. Rep. MIT/LCS/TR-579b, 1993. [Online]. Available: citeseer.ist.psu.edu/micali93fair.html

[24] M. Bellare and S. Goldwasser, "Verifiable partial key escrow," in *ACM Conference on Computer and Communications Security*, 1997, pp. 78–91. [Online]. Available: citeseer.ist.psu.edu/bellare97verifiable.html

ISBN 0-646-44190-6