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

Using MAC Addresses in the Lawful Interception of IP Traffic

P. Branch
Centre for Advanced Internet Architectures
Swinburne University of Technology
Hawthorn, Vic 3122

A. Pavlicic
Centre for Advanced Internet Architectures
Swinburne University of Technology
Hawthorn, Vic 3122

G. Armitage
Centre for Advanced Internet Architectures
Swinburne University of Technology
Hawthorn, Vic 3122

***Abstract*–In this paper we report on our investigations into the feasibility of using MAC addresses rather than IP addresses as an identifier in Lawful Interception. We found that MAC address interception in PPPoE and Broadband Ethernet environments can be very easily subverted. Consequently, we believe that MAC based interception is a poor option for lawful interception.**

Keywords – Network security, Network management

I. INTRODUCTION

Lawful Interception is the process of intercepting within a network, communications between parties of interest to Law Enforcement Agencies. The interception is legally authorised and is conducted without the intercepted parties being aware of it. Law Enforcement Agencies include state and federal police, intelligence agencies and independent commissions against corruption. Lawful Interception is often referred to as 'wiretapping' or 'phone-tapping' [1].

It is little appreciated how important Lawful Interception is to the Law Enforcement Agencies. Lawful Interception is a powerful tool in criminal and security investigations. It is not just used for gathering of evidence for court cases, but also to identify networks of relationships between suspected criminals. Governments throughout the world insist that before a telecommunications company can receive its operating license, it must have in place an adequate Lawful Interception system. Governments can and have delayed or cancelled the rollout of new services by telecommunications companies because they were unable to meet their Lawful Interception obligations [2].

Until a few years ago, Lawful Interception was the sole responsibility of the telecommunications companies. However, with the increasing popularity of the Internet and with the increasingly diverse ways that it can be accessed, interception within public access networks has become much less effective than it was. Internet cafes, public libraries, Internet kiosks and, to a lesser extent corporations and universities, all provide access to Internet services that is not easily intercepted within the access networks. Consequently, Law Enforcement Agencies have started to turn their attention towards interception of Internet services [3], [10], [12].

Unfortunately Internet Lawful Interception is quite difficult. How can the identity of the sender or receiver of a communication be traced from a stream of IP packets? How can the person sending or receiving an individual IP packet be identified? How can identity be traced in the Internet?

This is a very difficult problem to solve. When the person is using a publicly available web service that is already connected through an ISP (as is becoming increasingly common in public spaces such as airports, libraries and Internet cafes) then the problem is close to intractable. There is no login process at the ISP that might possibly be used to identify the person. The only way that the identity can be traced is by monitoring the service (such as an email server) that the person uses. Where the service is located outside the jurisdiction of the Law Enforcement Agency then intercepting such communications is close to impossible.

A more tractable situation is where the targeted party uses a public access network (such as a publicly available Wireless LAN) to connect to their ISP. In this case it is possible to identify the owner or recipient of IP traffic by monitoring RADIUS and DHCP exchanges during startup and login. However, the monitoring process is complicated and potentially error prone.

Consequently, other options have been proposed. One of the possible identifiers proposed in the recently released ETSI Technical Standard describing service specific interception is to attempt to intercept traffic based on the end user's MAC address [4]. In this case interception devices would be configured to capture traffic to or from user devices with a specific MAC address. This does not address the Internet kiosk scenario, but it does provide some mechanism of interception where the targeted user consistently uses the same device (such as a laptop computer or PDA) to access their communications. Of course linking MAC address to individual users is an issue in itself that is beyond the scope of this paper. In this paper we assume that a targeted individual's MAC address is known and we investigate how effective interception based on MAC address is.

Our work shows that MAC address interception is almost trivial to subvert. We believe interception based on MAC address will completely ineffective, even if the issue of linking identity to MAC address is solved. Consequently, we think that the ETSI standard should remove it from the list of possible target identifiers, or at lease not the ease with which interception based on it can be subverted.

The rest of the paper is structured as follows. Section II looks at Internet interception techniques and discusses the recently released ETSI standards for Internet interception. Section III reports on our investigations into the

ISBN 0-646-44190-6

effectiveness of MAC based interception, an option within the ETSI standard. Section IV is our conclusion.

II. Internet Interception

Internet interception relies on sniffers monitoring packets within the network. Sniffers are placed at strategic points and configured by a management system to capture traffic based on some criteria [8], [9], [10], [11].

The mechanism that is used for these systems is quite complex. A typical scenario is as follows:

- The warrant is served on the ISP. It specifies a party or organisation whose communication is to be intercepted.
- The ISP operator checks their register of users and identifies the warranted party's username. The username is entered on the Lawful Interception device.
- When the user to be intercepted connects to their ISP, a Dynamic Host Control Protocol (DHCP) server supplies the user's computer with an IP address.
- The user logs on with their username. Another exchange occurs between the user's machine and (typically) a RADIUS server. The Lawful Interception Device notes that the username is one that is to be intercepted. It records the user's IP address for interception of subsequent traffic.
- The user is authenticated and traffic to and from the user is allowed by the ISP's Network Access Server. The Lawful Interception Device intercepts all IP packets either to or from the user's IP address for delivery to the Law Enforcement Agency.
- When the DHCP lease nears expiry, a new DHCP IP address allocation sequence is carried out. Again, the Lawful Interception device notes the IP address.
- When the DHCP lease time ends and if no new DHCP address allocation has occurred, then the Lawful Interception device stops interception of traffic to or from that IP address.

Obviously this is a complex and error prone mechanism. Many things can go wrong. If part of the RADIUS or DHCP dialogue is missed, all or part of a message may be lost. There is the difficulty of keeping track of IP leases that time-out. There is the problem of distributed RADIUS servers where authentication is given over to a third party who may or may not have a warrant served on them. All in all, this is a cumbersome procedure. Also, it is worth noting that it will only trap some of the communications a user might make. If a user makes use of a wireless 'hotspot' provider who includes access through their ISP as part of the service, then the communication will not be detected.

Consequently attention has recently turned to alternative mechanisms for linking identity to communications. One possibility listed in the ETSI standard for Internet access interception is to base interception on MAC addresses [6]. This is very similar to current forms of access network interception where identity is linked to a handset or SIM card. However, there are two major differences. The first is that, unlike most handset identifiers, there is no record of MAC address owners. Any large scale interception based on MAC address would require MAC addresses to be tracked to owners in a way that is not done at present. The second is that MAC addresses can be faked (spoofed). It is MAC address spoofing and its consequences for Lawful Interception that we investigate in the next section.

III. Robustness of MAC Address Based Interception

In this section we describe some work where we tested the robustness of using MAC address as an identifier for Lawful Interception purposes. We were interested in how easy it would be to avoid detection by spoofing the MAC address.

There are many different configurations that can be used in ISP network design. The simplest is Dial-up where the user dials up their ISP via a modem and then establishes a PPP connection over which packets are transmitted.

A configuration commonly used with DSL access networks makes use of PPPoE where IP packets are encapsulated with PPP and then placed within an Ethernet frame. In this model when the client initiates a DSL connection a PPPoE virtual connection is established between the user's machine and the Network Access Server. In PPPoE the session id and the MAC address are combined to define the session.

Finally, there is Ethernet Broadband. This is commonly used with Cable Modem access networks. In this approach the client's cable modem and the carrier's CMTS provide a bridged Ethernet connection between the user's host and the ISP's network. Encapsulation of user data is via Ethernet. A Network Access Server prohibits access to the wider Ethernet until authentication has been successfully completed. Typically a PPP connection will be used to carry authentication information from the client to the ISP's authentication server, but once authentication is complete, user data is encapsulated in Ethernet frames.

In our work we investigated the PPPoE and the Broadband Ethernet scenarios.

The configuration shown in Fig. 1 was used to investigate the robustness of MAC address interception in a PPPoE environment. In this environment a PPPoE connection was established between the user machine and the Network Access Server. We ran a simple Lawful Interception detection system based on TCPDUMP within the Network Access Server system to detect and capture traffic containing the user's MAC address. We assumed the MAC address was known and statically entered into our Lawful Interception device.

ISBN 0-646-44190-6

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

For all our experiments our Network Access Server was a FreeBSD system running PPP, IPNAT, PAP and CHAP. The RADIUS server was another FreeBSD system running FreeRADIUS. The PPP software supported PPPoE.

Our initial tests of the Lawful Interception mechanism were very effective. MAC address interception is straightforward and effective in capturing traffic where the MAC address is known.

We then investigated the effects of spoofing the MAC address in the PPPoE system. The MAC address, although a hardware address burnt into the Ethernet card when it is manufactured, can be spoofed. We used readily available software that modified the MAC address placed in the Ethernet frames.

In a PPPoE environment the PPPoE session is identified by the MAC address and a unique session identifier. Consequently, our expectation was that spoofing the MAC address would cause communications between the host and the network to fail. This is exactly what we found.

However, in our next experiment using PPPoE we spoofed the MAC address before connecting it to the network. In this case we were able to avoid interception altogether. Consequently, MAC address spoofing can be used to avoid interception with PPPoE.

The second experiment involved using a similar configuration to that used before but without using PPPoE. Again our MAC address interception worked well. Traffic was readily captured by a simple Lawful Interception program based on TCPDUMP running on the Network Access Server.

This time, however, when we spoofed our MAC address after connecting, communication was maintained but the Lawful Interception program no longer captured traffic to or from the User machine.

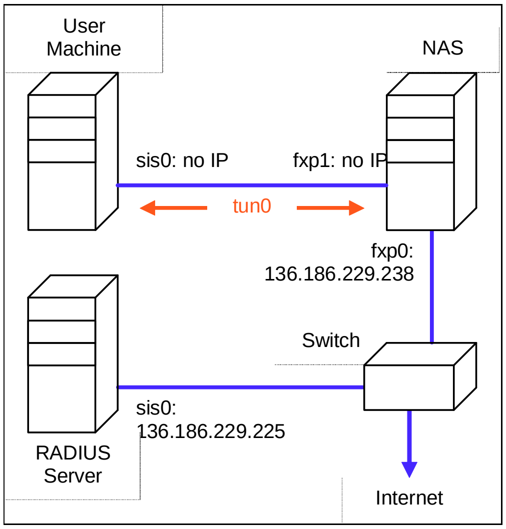

Fig. 1. Configuration for PPoE Interception Testing

Our experiments have shown that MAC address spoofing can very easily be used to avoid Lawful Interception.

IV. Conclusion

This paper has described some experiments used to test the robustness of MAC address based interception. We have shown that using MAC address spoofing, lawful interception can be subverted with little effort.

Consequently, we believe that MAC address interception is an unreliable basis for interception and should not be used. In the ETSI standard where it is suggested as a target identifier should, at the very least, be modified to note the ease with which it can be spoofed.

Lawful interception is a significant part of the larger issue of Internet crime detection and prevention. As new access networks and new applications are developed, detecting the identity of the receiver or sender of a communication will become increasingly important. This work has shown that a purely technical approach to this problem will probably fail. There is a need for some coherent approach that makes identification possible in emerging technologies but without compromising privacy any more than is necessary. Any effective solution is likely to involve regulatory, legal, political as well as technological elements.

The whole issue of traceability in the Internet is a key one for Internet crime prevention and detection. We will continue our work in this area by investigating other mechanisms that incorporate procedural as well as technical approaches. Finding a reasonable balance between traceability and privacy will be a difficult but essential and interesting challenge for the future.

References

[1] IETF “IETF Policy on Wiretapping,” IETF RFC 2804, 2000-05.

[2] Inspector-General of Intelligence and Security, Inspector-General of Intelligence and Security Annual Report 2001-2002. Canberra, Commonwealth of Australia, p. 31-44, http://www.igis.gov.au/fs_annual.html.

[3] Clarke, R., Dempsey, G., “Technological Aspects of Internet Crime Prevention,” Internet Crime, Australian Institute for Criminology, Melbourne University, 1998.

[4] ETSI ES 201 671, “Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic, v2.1.1,” 2001-09.

[5] ETSI TS 102 232 “Telecommunications security; Lawful Interception (LI); Handover Specifications for IP Delivery”, 2004-02.

[6] ETSI TS 103 234 “Telecommunications security; Lawful Interception (LI); Service-specific details for internet access services, v1.1.1“, 2004-02.

ISBN 0-646-44190-6

[7] CALEA, "AskCALEA - Frequently Asked Questions," Date Accessed 3 June 2003, Last Updated 21 March 2003, <http://www.askcalea.net/faqs.html>.

[8] ETSI TR 101 944: “Telecommunications Security; Lawful Interception (LI); Issues on IP Interception, v 1.1.1,” 2001-05.

[9] TIIT v1.0.0 (2002), “Transport of Intercepted IP Traffic,” Directorate General for Telecommunications and Post of the Ministry of Economic Affairs (Netherlands), 2002-09.

[10] Baker, F., Foster, B., Sharp, C., “Cisco Support for Lawful Intercept in IP Networks,” http://www.rfc-editor.org/internet-drafts/draft-baker-slem-architecture-00.txt, April 2003.

[11] Baker, F., “Cisco Lawful Intercept Control MIB,” http://www.rfc-editor.org/internet-drafts/draft-baker-slem-amib-00.txt, April 2003.

[12] Escudero-Pascual, A., Hosein, I., “Questioning Lawful Access to Traffic Data”, Communications of the ACM, Vol 47, Issue 3, 2004-03.

[13] Droms, R., “The DHCP Handbook”, Second Edition, SAMS, Indiana, 2003.

[14] Armitage, G., “Quality of Service in IP Networks: Foundations for a Multi-Service Internet”, MacMillan Technical Publishing, Indiana, 2000.

ISBN 0-646-44190-6