Lawful Interception of IP Traffic

P. Branch

Centre for Advanced Internet Architectures
Swinburne University of Technology
Hawthorn, Vic 3122
pbranch@swin.edu.au

Australian Telecommunications Networks & Applications Conference 2003 (ATNAC2003), Melbourne, Australia, December 2003

Abstract – When compared with access network interception, Lawful Interception of the Internet is both more difficult and much less mature. However, Internet interception is becoming increasingly more important as Law Enforcement Agencies find that access network interception is becoming less effective. Unfortunately, the most common approach to Internet interception has some fundamental weaknesses, which may compromise security, privacy and network reliability. In this paper we explain how Internet interception differs from access network interception, highlight the weaknesses in existing solutions and suggest alternative approaches to Internet interception and how they might be developed.

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].

Although Lawful Interception is a useful tool in criminal investigations, there is great scope for it to be abused. Some effort has been made to minimize the risk of this by including audit mechanisms in the design of Lawful Interception systems and through third party oversight of Lawful Interception activities. In most Western style democracies, Lawful Interception is very tightly regulated with numerous checks and balances. In Australia for a Law Enforcement Agency to initiate an interception, a warrant must be obtained from a suitably authorised law officer, which is then served on the telecommunications company. The Law Enforcement Agency does not have direct access to the telecommunications company's network. The process of obtaining the warrant is separate from activating it. This separation of responsibility provides an important check on the activity of the Law Enforcement Agency that can be regularly audited.

Any communications can be subject to interception. Although most interception is of voice communications, faxes, emails, SMS messages, chat rooms and even multiplayer games, can all be subject to interception orders.

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].

Unfortunately Internet Lawful Interception presents many technical challenges to Internet Service Providers (ISPs). This paper describes those challenges, evaluates the main solution that has been developed, and suggests alternatives. The rest of the paper is structured as follows. Section II is a comparison between Lawful Interception in the Internet and in access networks. Section III critiques the commonly used hardware solutions used in IP Interception. Having identified flaws in existing solutions, Section IV suggests directions that IP Lawful Interception research might take.

II. Internet and Access Network Interception

Lawful Interception in access networks is highly standardised. There are a number of international standards that specify how each of the access networks is to be intercepted and how intercepted information is to be delivered to the Law Enforcement Agency.

The most important of these are the standards developed by the European Telecommunications Standards Institute [4] used throughout Europe and much of Asia (and soon to include Australia), and CALEA used throughout North America [5]. Both the ETSI and CALEA standards have

well defined interfaces that can be used as building blocks for a secure and auditable Lawful Interception system.

The ETSI standard defines three interfaces:- HI 1 concerned with warrant information, HI 2 concerned with Intercept Related Information and HI 3 for the content of communication. CALEA has similar interfaces. By separating functions into separate interfaces, responsibilities and procedures can be separated and regularly audited.

HI 1 is the administrative interface. It specifies how warrants are transmitted from the Law Enforcement Agency to the telecommunications company and what warrant related information the telecommunications company must report to the Law Enforcement Agency. HI 2 deals with Intercept Related Information. It specifies how such information as services the intercepted party accesses, who is calling the intercepted party, who the intercepted party is calling, any call-forwarding and other similar information, can be delivered to the Law Enforcement Agency. Often Intercept Related Information is the most important part of the intercept. In the United States 80 to 90% of intercepts are for Intercept Related Information only [6]. Finally, HI 3 specifies how the content of the call is to be delivered.

Intercepting access network traffic is, conceptually at least, quite straightforward. During call set up time a virtual circuit between the source and destination is set up. Information from this call set up can be extracted to form the Intercept Related Information. Interception of call content merely involves copying the content of the traffic that travels through the virtual circuit and transmitting it to the Law Enforcement Agency.

When compared with access network interception, Internet interception is much more difficult. Internet traffic is transmitted using the Internet Protocol (IP). The key characteristic that makes IP difficult to intercept is that it is a connectionless protocol. The protocol is 'connectionless' because packets are transmitted without any call set up process. Each packet contains sufficient information within itself to be routed to its destination [7].

Intercepting connectionless traffic presents many problems. The path through the network may not be the same for all the packets that make up the message. The Internet Protocol is designed to route around failed or congested nodes. This gives it great resilience but means that it cannot be assumed that traffic will flow in a predetermined path.

Within the Internet the same physical connection will carry traffic from many sources. To see if a particular packet travelling through a physical node is part of an intercepted communication, every packet travelling through it must be examined.

It is not at all clear what the best basis is to examine the packet. Access network interception is based on a subscriber or handset identifier. There is no analogous information within an IP packet. The nearest is the IP address. Unfortunately, IP addresses are often allocated dynamically at login time, so initiating a warrant on IP address is not possible.

Internet protocols are complex. Often IP packets contain other IP packets (IP tunnelling). Examining these to see if they contain information that might be subject to an interception warrant means that Lawful Interception equipment must be able to recognise when an IP packet is contained within other IP packets, and extract them accordingly.

Separating information about the communication from the intercepted content is much harder in IP networks. In IP, signalling information is tightly bound with the content of the communication. Separating one from the other to provide Intercept Related Information for IP communication is much more difficult than in access networks.

Finally, there is encryption. Use of encryption by the party being intercepted is entirely the concern of the Law Enforcement Agency. How they deal with it is and always will be their concern alone. However, ISPs often encrypt data passing through their network. Where this occurs, the ISP must either give the encryption keys to the Law Enforcement Agency or intercept it where it is not encrypted. The effect of this is to limit the locations within the network that interception can occur.

None of these problems are insurmountable, but any solution requires much greater computing power and complexity when compared with similar interception requirements in access networks.

When Internet interception began to become an issue for developers of Internet applications and ISPs, the IETF was asked to take a position on including standards-track documents to facilitate it. This resulted in much heated discussion culminating in RFC2804 where it was decided that the IETF would not support standards track work in Lawful Interception [8].

Unfortunately, a perhaps unforeseen consequence of this decision is that hardware solutions for Internet interception have proliferated, with little research into the best way to deploy them. These solutions, while filling the gap left as a consequence of RFC2804, are a cause for concern. They have potential to compromise security and privacy of Internet users as well as network reliability.

Interception of the Internet is in a much less mature state than within access networks and is inherently more difficult. In the absence of standard approaches to Interception supported by the IETF and a lack of research into the area, ISPs have had to resort to hardware based systems. These are the topic of the next section.

III. Internet Interception using Sniffers

The decision by the IETF not to sponsor a standards track for Lawful Interception is, in retrospect, to be regretted. The decision has had two consequences. Since work in this area was not going to contribute to IETF standards development it has meant that network researchers and

engineers have not involved themselves in it. Consequently, research into Lawful Interception in IP networks has been almost entirely neglected. Secondly it has meant that alternative hardware based interception systems that are separate from the IP network have evolved.

The solutions that have evolved have been based on hardware 'sniffers'. 'Sniffers' are systems that are plugged into the network at points of interest and then examine all traffic passing that point. They can be programmed to capture traffic of interest (say to or from a particular destination) for later reporting. These systems were originally developed to diagnose network faults. However, their development as Lawful Interception tools followed swiftly after RFC 2804.

In a sniffer-based Lawful Interception system, sniffers are installed at key points within the network to monitor passing traffic. The sniffer is attached to the network through an optical or wire tap, or attached to a broadcast hub. When used for Lawful Interception, it needs to be programmed to listen for specific IP addresses and capture any packets containing those IP addresses. These packets are then transmitted directly to the Law Enforcement Agency via the Internet or are stored on the sniffer for later downloading.

The IP addresses it needs to monitor are kept track of through a complex process of monitoring logins (RADIUS messages). RADIUS messages contain user login information and dynamically allocated IP addresses [9]. A warrant is loaded on the sniffer by entering a login user name. When the sniffer sees the user name in a login message, it captures the dynamically assigned IP address that the login message response contains, and configures its table of addresses to intercept so that it will capture traffic either to or from that IP address.

This is a complex and cumbersome process with many causes for concern.

Most serious is the way these systems are often deployed. Law Enforcement Agencies recognise that sniffer-based systems are expensive and complex, so have often installed such systems themselves within the ISP's network. They configure the sniffer to trap traffic of interest, install it on the ISP's network and, when the surveillance period is over, take the sniffer and examine the captured traffic at their leisure [10]. Although the intentions of the Law Enforcement Agencies are undoubtedly good, this procedure should worry us all. It severely compromises the mechanism for oversight of what actually gets configured on the sniffer. It might be capturing everyone's traffic that passes through the network. There is no separation of responsibility between the Law Enforcement Agency and the ISP that can be readily audited. If illegal interception has occurred as a result of malice, overzealousness or simple incompetence, it can be difficult to trace.

Standalone systems such as sniffer-based systems are more easily compromised than systems integrated into networking equipment. Most systems for access network interception are well integrated with the network. However, a significant minority are standalone systems that work on a similar basis to network sniffers. There is some evidence that some of these systems in Europe have been compromised by a foreign intelligence agency to illegally intercept communications [11]. This is a fundamental risk associated with such systems. Its internal functions are poorly understood except by the manufacturer. If sniffer-based systems continue to proliferate we can expect more of such cases.

Sniffer-based Lawful Interception systems are likely to be attractive and relatively soft targets for hackers. The attraction is easy to understand. Controlling such a system gives the controller information as to who is being monitored, power to monitor other's traffic and the ability to add, modify or delete warrants. It is not hard to imagine how such a target could be used for illegal purposes. However, Lawful Interception Sniffers are very new and for most ISPs, unfamiliar pieces of hardware, that are not well integrated into the network. Consequently, there are likely to be many security holes associated with them. Weaknesses in implementations of protocols that have been in use for over a decade are still being found [12]. It is highly likely that these new sniffer-based systems will have many security weaknesses.

Sniffer-based systems may compromise the reliability of Internet services. They require much new hardware to be introduced into a network. In general, the more complex a system is the more likely it is to fail. Additional hardware involves additional network administration, additional security administration along with Lawful Interception administration for each site.

Sniffer-based systems are unlikely to be a satisfactory solution to Lawful Interception for emerging services such as mobile Internet and pervasive computing. These services make heavy use of IP tunnels and router handovers, which place great computational demands on sniffer hardware.

Sniffer-based systems are expensive to install and operate. Lawful Interception sniffer systems start from $AUS 100,000 for simple systems and significantly more for more sophisticated systems. They require the introduction of significant amounts of additional hardware into a network. Typically, a sniffer system will be required at each point of presence within an ISP's network. As well as installation costs, there are operational costs for new systems to manage the new hardware and for extracting captured information and transmitting it to the Law Enforcement Agency.

It is likely that there are better approaches to IP interception than sniffer-based systems. However, until research into alternative approaches can be carried out, they are likely to be the only available solution for some time. If so, there are many questions about these systems that need answers. How can they be secured against hackers? How can the deployment of these systems be optimised to minimize costs? What features do such

systems need to enable meaningful audits? A key requirement in answering these questions is the development of a validated architecture for IP Lawful Interception.

In the next section we discuss this requirement and suggest directions that Lawful Interception research might take.

IV. Lawful interception Research

A. *An Architecture for IP based Interception*

One of the most urgent requirements for IP Lawful Interception to advance is a widely accepted architecture specifying what functions need to be carried out and where in the network they should be done. Such an architecture would provide a structure in which more specific problems of interception could be dealt with. It would provide the basis for the development of auditable systems as well as some separation of functions similar to the ETSI standards.

Cisco Systems recently released two informational Internet drafts describing how they will approach Lawful Interception [13, 14]. The approach is very similar to that of the ETSI standard for access network interception. It leaves open the question of how intercept information is to be collected, but provides the interfaces and identifies the functional components of a Lawful Interception system. Perhaps this approach will evolve to become the de-facto standard architecture for IP Lawful Interception.

B. *Application level interception*

The simplest approach to Internet interception is to intercept only at the Application level. That is, rather than intercepting and forwarding IP packets, deliver the content of the communication before or after it has traversed the IP network. So, using email as an example, rather than issuing a warrant against a suspect's ISP, the Law Enforcement Agency would issue the warrant against the suspect's mail operator. To meet their interception obligations all a Service provider need do is deliver email to or from a particular email address.

This approach to Lawful Interception is particularly attractive in applications such as Voice over IP, multiplayer games and video mail where service gateways are used.

Unfortunately, this approach can be subverted by using a service provider who is outside the jurisdiction of the Law Enforcement Agency. So, rather than using an Australian service provider, one in Europe or America might be used. Nevertheless, the approach might be a useful adjunct to other forms of interception. If so, then research is needed into how ETSI-like interfaces for Lawful Interceptions of this kind can be developed.

C. *Router based interception*

This is perhaps the most promising alternative to sniffer based interception. Much of the functionality needed for Lawful Interception is already provided through existing protocols. In particular, multicast, remote monitoring and network management protocols provide most of the building blocks for Lawful Interception. Research into how these can be constructed to provide the same functionality as a Lawful Interception sniffer is worthwhile.

V. Conclusion

This paper has compared Lawful Interception in IP networks with Lawful Interception in access networks. It has shown that Lawful Interception of IP networks is inherently more difficult than in access networks. It has demonstrated that Lawful Interception of the Internet is immature and that current solutions are much less than perfect with potential for endangering communications reliability, security and privacy. The paper has identified the need for approaches to Lawful Interception that are standardised, do not rely heavily on additional hardware and are flexible enough to support future technologies.

The goal of research into Lawful Interception is to ensure that Law Enforcement Agencies receive all the information they are entitled to, but no more. Policy and procedures supported by technology need to be developed to make illegal interception more difficult, or if it occurs, more easily traced than it is now. The paper highlights the importance of the development of a widely accepted architecture for IP Lawful Interception. Such an architecture would provide the structure for the development of secure, reliable and auditable Lawful Interception systems. The paper also highlights the need for alternatives to sniffer-based systems to be investigated.

It is in the interests of everyone who uses the Internet for legitimate purposes that Lawful Interception is done as efficiently and reliably as possible, with strong privacy and security safeguards. Finding solutions that meet these criteria is a challenge that network researchers and engineers will have to accept in the next few years.

References

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

[2] Australian Commonwealth Parliamentary Library, "Bills Digest No. 67 1997-1998, Telecommunications Legislation Amendment Bill 1997," Date Accessed 29 May 2003, Last Updated 28 October 1998, <http://www.aph.gov.au/library/pubs/bd/1997-98/98bd067.htm>.

[3] M. Acey, "Europe Votes For ISP Spying Infrastructure," in *Techweb News*, 1999.

[4] European Telecommunications Standards Institute, "Telecommunications Security; Lawful

Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic," 2001.

[5] "Interception of Digital and Other Communications," vol. 103-414, *Congress of the United States of America*, 2 ed, 1994.

[6] Electronic Privacy Information Center, "Approvals for Federal Pen Registers and Trap and Trace Devices 1987-1998," Date Accessed 28 May 2003, Last Updated 15 Feb 2002 1998, <http://www.epic.org/privacy/wiretap/stats/penreg.html>.

[7] D. Comer, *Internetworking with TCP/IP*, vol. 1, 4 ed. Upper Saddle River: Prentice-Hall, 2000.

[8] IETF Network Working Group, "IETF Policy on Wiretapping," Date Accessed May 2003, Last Updated May 2000, <http://www.ietf.org/rfc=2804>.

[9] C. Rigney, "RADIUS Accounting," Date Accessed 28 May 2003, Last Updated June 2000, <http://www.ietf.org/rfc/rfc2866.txt?number=2866>.

[10] D. Kerr, "Statement for the Record of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation on Internet and Data Interception Capabilities Developed by FBI," Date Accessed 3 June 2003, Last Updated 24 July 2000, <http://www.fbi.gov/congress/congress00/kerr072400.htm>.

[11] J. Figueiredo, "Israel reported to have Access to Confidential Dutch Tapping Data," in *Europemedia.net*, 2002.

[12] CERT/CC, "CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol," Date Accessed 27 May 2003, Last Updated 14 May 2003, <http://www.cert.org/advisories/CA-2002-03.html>.

[13] F. Baker, "Cisco Lawful Intercept Control MIB," Date Accessed 28 May 2003, Last Updated April 2003, <http://www.rfc-editor.org/internet-drafts/draft-baker-slem-mib-00.txt>.

[14] F. Baker, B. Foster, and C. Sharp, "Cisco Support for Lawful Intercept In IP Networks," Date Accessed 28 May 2003, Last Updated April 2003, <http://www.ietf.org/internet-drafts/draft-baker-slem-architecture-00.txt>.