Lawful Interception of the Internet

Philip A. Branch

Centre for Advanced Internet Architectures. Technical Report 030606A
Swinburne University of Technology
Melbourne, Australia
pbranch@swin.edu.au

Abstract-This paper describes the state of Lawful Interception of the Internet and compares it with Lawful Interception of access networks. Lawful Interception is the process of secretly intercepting communications between parties of interest to Law Enforcement agencies. Internet interception is both more difficult and much more immature than access network interception. Refusal by the main standards body of the Internet (the IETF) to be involved in Lawful Interception has left a vacuum in the area which has been filled by complex hardware solutions with potential security and privacy risks. Interception of the Internet is likely to become more common in future than it is now. Without engagement of network researchers and Internet standards setting bodies, Lawful Interception will either be a potential threat to the security and privacy of Internet users, or governments may insist on draconian controls that will significantly affect the development of new Internet based services

Keywords- Lawful Interception, Law Enforcement, Security, Wiretapping

I. INTRODUCTION

Lawful Interception is the process of secretly intercepting within a network communications between parties of interest to Law Enforcement Agencies. 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 an important and 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. Being able to provide an adequate Lawful Interception capability is a necessary precondition for a telecommunications company being issued with a license to provide a publicly available telecommunications service. 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. In Australia, the body with responsibility for auditing Lawful Interception is the Inspector General of Intelligence Services [3].

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. It is part of the folklore amongst people working in Lawful Interception that criminals are amongst the first users of any new communications technology and that they will exploit any new techniques for communication [4]. There is some speculation that the September 11 attacks in New York were coordinated through a new technique of hiding messages within images (steganography) [5]. The Law Enforcement Agencies insist that any mechanism where one party can leave a message for another party needs to be interceptable.

Until a few years ago, Lawful Interception was the responsibility of the telecommunications companies. Telecommunications companies provide access to communications over a variety of access networks. The most familiar access networks are the Public Switched Telephony Network (PSTN), which provides the fixed line residential and business telephone services, Global System for Mobility (GSM), which provides mobile telephony, Cable modem broadband and ADSL which provide broadband access to Internet services.

Access networks enable subscribers to communicate with other subscribers and with service providers. The most familiar service providers are Internet Service Providers (ISPs) who provide access to the world-wide-web, email and other Internet based services. ISPs are themselves users of access networks, but they will typically use less familiar, higher

capacity access networks such as Frame Relay or ISDN. It is important to understand that the Internet is a network that makes use of many underlying access network technologies [6].

In recent years, interception within public access networks has become much less effective than it was. This is because of the increasing popularity of Internet based communications (particularly web-based email) and because of the increasingly diverse ways in which the Internet can now be accessed. If someone wishes to avoid their Internet communications being intercepted within the access network it is very easy to do so. Internet cafes, public libraries, Internet kiosks and, to a lesser extent corporations and universities, all provide anonymous means of access to Internet services. Consequently, Law Enforcement Agencies have started to turn their attention towards interception of Internet services [7].

Lawful Interception in Australia is governed by the Telecommunications (Interception) Act [8]. The Act specifies the procedures that must be carried out before a warrant to intercept communications from or to a person can be issued. For criminal investigations, a suitably authorised magistrate must approve the warrant. For intelligence gathering the Attorney General must approve the warrant. The Act specifies the obligations of carriers and carrier service providers (which includes most Internet Service Providers) and what the punishments are for failing to meet the requirements of the act. Unusually, the Australian legislation does not distinguish between the obligations of telecommunications companies and carriage service providers. It describes the requirements in quite vague terms and leaves the specifics up to the Law Enforcement Agencies. Elsewhere a distinction is usually made between access and service level interception.

Lawful Interception is an obligation that governments place on suppliers of communications services. If a telecommunications company or communications service provider wishes to offer a new service or technology to the public but it is not capable of being intercepted, it is unlikely that government will allow it to be offered. Unfortunately, some of the solutions deployed for Internet Lawful Interception are a potential threat to the privacy and security of Internet users.

The remainder of this paper explains how this situation has arisen and what can be done about it. The next section discusses the direction that Internet interception has taken since it began to receive more attention from the regulators. Section three contains a comparison between Lawful Interception in access networks and in the Internet. Section four critiques the main technique of Internet interception. Finally section five suggests some directions that network research might take to avoid the worst outcomes.

II. INTERCEPTION AND THE INTERNET COMMUNITY

Interception in general is a contentious area and interception within the Internet even more so. Whether or not it is legitimate for governments to intercept private communications and whether or not Internet researchers and engineers should help them has been the source of much heated discussion over the past few years [9].

Generally, the accepted reason to allow governments interception capabilities is to solve crimes or gather intelligence that will prevent crimes. Reasons for not allowing governments to intercept include threats to privacy and security. The potential abuse of individual's privacy is probably the main source of concern about Lawful Interception. Those on both the right and left of politics regard Lawful Interception with great suspicion. The right questions the legitimacy of the state spying on its citizens while the left suspects (with good reason) that it has been subject to more than its fair share of scrutiny. Certainly the history of Lawful Interception is not an edifying one. In the first half of last century, it was essentially unregulated. Anyone, if they knew who to ask, could arrange for a phone tap. During the Second World War, in the United States control of Lawful interception was taken over by the FBI. It is doubtful that this was an improvement, given our knowledge now of the staggering abuses of Lawful Interception in the decades that followed [10].

This appalling history has resulted in most of us mistrusting, to at least some extent, government use of Lawful Interception. The following quote by the Foundation for Information Policy Research (a UK based group concerned with online privacy) captures the feelings many of us have towards Lawful Interception [11].

'Those who question the arrangements for oversight of interception are often supposed to be critical of the rights of the state to conduct secret surveillance. FIPR supports carefully targeted government surveillance of telecommunications in the fight against serious crime and for the collection of foreign intelligence.

'However public support for these activities has been very seriously eroded by the poor management of previous governments…'

Privacy is not the only reason for concern about Lawful Interception. Security of communications is an equally significant, although probably less well understood one. Interception capabilities provide a hole in the security of a network for the purpose of eavesdropping. By definition Lawful Interception compromises network security. Network access points for Lawful Interception are privileged locations within the network. Whoever controls these points can view any traffic he or she chooses. Consequently, mechanisms for interception need to be very strongly protected against hack attacks.

In general, although often controversial, access network interception is an accepted part of access network operation. This is definitely not the case with Internet interception.

There is something of a three-way argument going on regarding Lawful Interception of the Internet. There is the point of view, largely held by the regulators, that the interception obligations of ISPs can and should be

very similar to access network providers. Diametrically opposed is the view that governments cannot be trusted with the power to intercept communications of its citizens and Internet engineers and researchers should not involve themselves with such activities. Finally there is a third point of view, holders of which note that government will insist that ISPs be able to intercept and that interception, if done badly, threatens privacy and security. Also, failure to provide effective interception solutions is a threat to the rollout of new services. However, holders of this point of view believe that interception techniques need to be as open and as well understood as possible so that security mechanisms and audit techniques can be subject to the intense scrutiny they deserve [12].

The author shares this third point of view. If Internet engineers and researchers are not engaged in designing interception systems and informing legislators of what is possible and reasonable, then the results will probably be disastrous. Poorly designed Lawful Interception systems are a threat to the security and privacy of Internet users. Those of us working on new network technologies need to be aware of Lawful Interception requirements. Developing approaches to Lawful Interception that are robust, do not compromise security and privacy and provide Law Enforcement Agencies with only the information that legislation entitles them to, is a legitimate, important and urgent area of network research.

It seems that amongst Internet engineers, this point of view is becoming more accepted. This is because legislators have recently, in some cases, placed unreasonable demands on ISPs, and some of the consequent systems that have been rolled out to attempt to meet these demands are very worrying [13]. Also the terrorist attacks in New York and Bali have put paid to any hopes that Law Enforcement Agencies would not attempt to intercept the Internet.

Regardless of the views of technologists, interception of communications at the ISP level is receiving greater attention from Law Enforcement Agencies than it has done in the past. The Australian government has shown that it is quite prepared to legislate to control new services, even where the legislation effectively destroys the service [14]. Where national security is concerned there is no doubt that if a service cannot be intercepted it will not be allowed to be offered to the public. Consequently, ISPs are now finding themselves obliged by Law Enforcement Agencies to provide an interception service comparable with that provided by access network owners [7]. Unfortunately, because of the nature of the Internet, this is a difficult obligation for ISPs to meet and the systems implemented to meet the obligations are a source of great concern.

The next section compares Lawful Interception in Access networks with Lawful Interception in the Internet and explains why the latter is so much more difficult than the former.

III. COMPARISON OF LAWFUL INTERCEPTION IN ACCESS NETWORKS AND THE INTERNET

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 [15] used throughout Europe and much of Asia (and soon to include Australia), and CALEA used throughout North America [16]. Both the ETSI and CALEA standards have well defined interfaces that can be used as building blocks for a secure and auditable 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 information the telecommunications company must report to the Law Enforcement Agency. HI 2 deals with Intercept Related Information. It provides 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. 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 [17]. 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 that circuit and transmitting it to the Law Enforcement Agency.

However, for reasons outlined earlier, interception in the access network has become less effective than it was. This has led to a much greater emphasis being placed on intercepting at the services level. In the case of ISPs, this means intercepting Internet traffic.

Unfortunately, Internet interception is 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 [18]. A service such as email is transmitted by segmenting the content of the message into smaller data units. These data units are then prefixed with a destination address and, using well-established rules, the data segments (now referred

to as 'packets') are forwarded onto the next node in the network. This process continues until the packets arrive at their destination and are reassembled.

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 number. 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.

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

Unfortunately the difficulty is compounded by an absence of international standards. Unlike interception in the access networks there are no international standards for interception of IP networks. The one body that might have been able to provide some direction in this area is the Internet Engineering Task Force (IETF). The IETF in a famous decision in 1999 (contained in RFC 2804) decided it would not support standards track work in this area [12]. This has had some undesirable, and perhaps unforseen outcomes. These are discussed later in the paper.

Interception of the Internet is in a much less mature state than within access networks. Interception of Internet traffic is inherently more difficult than in access networks, requires more computational power and is not supported by the main Internet standards formulating body. In the lead up to the decision by the IETF, there was some speculation that the problems were so difficult that Law Enforcement Agencies would accept that interception in the Internet was just too hard and would not insist on it [9]. However, this did not happen. Law Enforcement Agencies have insisted that ISPs provide Lawful Interception capabilities. It is how ISPs have attacked this problem that is a cause for concern and is the topic of the next section.

Hardware-based Systems for IP Interception

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 basic element of an IP network is the router. A router is responsible for deciding where to send a packet based upon its destination address. Most routers have a multicast capability where they can send copies of any packets to multiple destinations. This is sufficient hardware for implementing Lawful Interception in IP networks. However, because there has been no standards development, router software for Lawful Interception has not been developed. Consequently, Lawful Interception solutions have been developed that are separate from the router.

The Lawful Interception 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 [19]. 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 itself 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 [20]. 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 have been compromised by a foreign intelligence agency to illegally intercept communications [21]. This is a fundamental risk associated with a standalone system. Unlike a router, its internal functions are unknown to all except those who manufacture it. 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 protocols that have been in use for over a decade are still being found [22]. 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, because they place great computational demands on them, sniffers handle poorly. If mobile Internet based services cannot be intercepted then government will probably prohibit their deployment.

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.

This approach to Lawful Interception should be of concern to anyone who uses the Internet. It seems unlikely that sniffer-based systems are the best approach to Lawful Interception in IP networks, but even if they are, the consequences of poor design or installation should have warranted research by network engineers in this area. There are many questions about these systems that need answers. How can these systems 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? There has been very little such research. If sniffer systems are to be the basis of Lawful Interception in the Internet, then these questions need to be answered.

The proliferation of sniffer-based systems and the lack of research in Internet Lawful Interception are responses to a situation created by the refusal of the IETF to be involved in standards work in this area. This is a regrettable outcome. In the next section we suggest how Internet Lawful Interception could proceed if supported by standards or similar bodies.

IV. ALTERNATIVE APPROACHES TO INTERCEPTION IN IP NETWORKS

An approach to Lawful Interception that does not involve sniffers is to use existing protocols and hardware as much as possible. Much of the functionality of 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. Some research into how these can be constructed to provide the same functionality as a Lawful Interception sniffer is well overdue.

Just as important is identifying how to implement the checks and balances that Lawful Interception in the access network supports. How can a similar concept as Intercept Related Information be provided within IP Lawful Interception? How can strong audit mechanisms be implemented in IP Lawful Interception?

Cisco Systems recently released two informational Internet drafts describing how they will approach Lawful Interception [23, 24]. The approach is very similar to that of the ETSI standard for access network interception. It involves integrating Lawful Interception into the router. This overcomes many of the weaknesses associated with sniffer-based systems. In this model, the ISP takes responsibility for loading the warrant so that separation of responsibility is restored. Router security is well understood so

including Lawful Interception functionality within the router is less likely to introduce security holes within the network than sniffer systems. No new hardware is introduced so reliability is less likely to be compromised. Implementing Lawful Interception within the router for new technologies is likely to be less painful than implementing it within a sniffer. Finally, since little or no new hardware is introduced, cost is less likely to be impacted.

However, this approach does introduce some new problems. Routers are commodity items purchased not just by ISPs but by corporations. How can access to Lawful Interception functions be restricted to ISPs? How can audits be done to ensure that these facilities are not abused?

It is interesting that Cisco Systems have decided to take on work in this area. The author of the two Internet Drafts is Fred Baker. Baker is one of the most respected engineers of the IETF, responsible for representing Cisco Systems in IETF deliberations. In 1999 he was one of the authors of RFC 2804 where the decision was made not to pursue a standards track in Lawful Interception. However, in March 2003 he released a number of Internet drafts describing Cisco System's approach to Lawful Interception. This was perceived by the Internet community to be a change in position of some note. In an interview following the release of the drafts he was asked what he now felt about Lawful Interception [25]. His response :

'I have some moral and ethical issues (about Lawful Interception), but I think quite frankly that the place to argue this is in Congress and in the courtroom, not a service provider's machine room when he's staring down the barrel of a subpoena'.

Perhaps now that Cisco Systems have acknowledged that their customers need such a capability, their approach will generate de-facto standards for Lawful Interception in the Internet.

V. CONCLUSION

Lawful Interception of the Internet is immature and current solutions are much less than perfect with potential for endangering communications reliability, security and privacy. This should be a matter of concern to everyone who uses the Internet. There is a need for approaches to Lawful Interception that are standardised, do not rely heavily on additional hardware and are flexible enough to support future technologies.

There needs to be investigations into developing techniques for ensuring that Law Enforcement Agencies receive all the information they are entitled to, but no more. In particular, an Intercept Related Information facility for IP networks needs to be developed. 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.

There needs to be an awareness of Lawful Interception by technology developers. In the current security climate if a new technology cannot be intercepted, it is unlikely that governments will allow it to be offered commercially.

Lawful Interception is not a capability that Law Enforcement Agencies will give up. It is in the interests of everyone who uses the Internet for legitimate purposes that it is done as efficiently and reliably as possible, while at the same time minimizing the risk to privacy and security. 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, <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 1997, <http://www.aph.gov.au/library/pubs/bd/1997-98/98bd067.htm>.

[3] Inspector-General of Intelligence and Security, "Inspector-General of Intelligence and Security Annual Report 2001-2002," Commonwealth of Australia, Canberra, 22 October 2002.

[4] C. Bell, "Exploiting emerging technology corruptly in the NSW public sector," Independent Commission Against Corruption 24 April 2001.

[5] K. Maney, "Bin Laden's messages could be hiding in plain sight," in *USA Today*, 2001.

[6] G. Armitage, *Quality of Service in IP Networks: Foundations for a Multi-Service Internet*, 1 ed. Indianapolis: MacMillan Technical Publishing, USA, 2000.

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

[8] "An Act to prohibit the interception of telecommunications except where authorised in special circumstances or for the purpose of tracing the location of callers in emergencies, and for related purposes.," *Commonwealth Parliament of Australia*, 1979.

[9] IETF Network Working Group, "Raven Discussion Archive," Date Accessed 3 June 2003, Last Updated 17 August 2000, <http://www1.ietf.org/mail-archive/working-groups/raven/>.

[10] W. Keller, *The Liberals and J. Edgar Hoover: Rise and Fall of a Domestic Intelligence State*. Princeton, New Jersey: Princeton University Press, 1989.

[11] Foundation for Information Policy Research, "Interception of Communications in the United Kingdom: A response to the Home Office consultation paper (CM 4368 JUNE 1999)," Foundation for Information Policy Research, London, 16 August 1999.

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

[13] P. Wouters, "Dutch tapping law: Almost all providers break the law," Date Accessed 3 June 2003, Last Updated 17 May, <http://www.opentap.org/ct/ct.aftappen-eng.html>.

[14] J. Schulze, "Canberra a datacast strangler," in *The Australian*, 2003.

[15] European Telecommunications Standards Institute, "Telecommunications Security; Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic," 2001.

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

[17]   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, <http://www.epic.org/privacy/wiretap/stats/penreg.html>.

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

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

[20]   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, <http://www.fbi.gov/congress/congress00/kerr072400.htm>.

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

[22]   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>.

[23]   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>.

[24]   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>.

[25]   D. McCullagh, "Inside Cisco's Eavesdropping Apparatus," Date Accessed 29 May 2003, Last Updated, <http://news.com.com/2010-1071-997528.html?tag=fd_nc_1>.