NetOptics®

The Growing Impact of Social Networking Trends on Lawful Interception

White Paper

How Bin Laden Evaded Lawful Interception

Osama Bin Laden was able to circumvent the Internet and yet send an almost uncountable number of emails—pointing out frustrations that Lawful Interception personnel can encounter when monitoring suspicious activities and people. Although his compound had no phone or Internet capabilities, Bin Laden was able to stay in touch with his far-flung network of operatives without leaving digital fingerprints. He merely typed a message on his unconnected computer, saved it to a thumb drive and passed that to a courier who later plugged it into a memory drive at an Internet café, copied Bin Laden's message into an email and sent it. Any responses would be copied to the flash drive and transported back to Bin Laden. Though arduous, the effectiveness of his strategy left officials amazed that he could sustain such a breadth of communication for so long.

Link to article

This paper discusses the intensifying challenges faced by Law Enforcement Agencies and Service Providers as innovation and speed of adoption open new vulnerabilities to crime and terrorism. The paper explores new solutions and resources for these Service Providers in fulfilling government-mandated Lawful Interception requirements.

Lawful Interception (LI) is the legal process by which a communications network operator or Service Provider (SP) gives authorized officials access to the communications of individuals or organizations. With security threats mushrooming in new directions, LI is more than ever a priority and major focus of Law Enforcement Agencies (LEAs). Regulations such as the Communications Assistance for Law Enforcement Act (CALEA), mandate that SPs place their resources at the service of these agencies to support surveillance and interdiction of individuals or groups.

CALEA makes Lawful Interception a priority mission for Service Providers as well as LEA; its requirements make unique demands and mandate specific equipment to carry out its high-stakes activities.

A Fast-Changing Environment Opens New Doors to Terrorism and Crime

In the past, Lawful Interception was simpler and more straightforward because it was confined to traditional voice traffic. Even in the earlier days of the Internet, it was still possible to intercept a target's communication data fairly easily.

Now, as electronic communications take on new forms and broaden to a potential audience of billions, data volumes are soaring, and the array of service offerings is growing apace. Lawful Interception Agencies and Service Providers are racing to thwart terrorists and other criminals who have the technological expertise and determination to carry out their agendas and evade capture. This challenge will only intensify with the rising momentum of change in communication patterns.

Traffic patterns have changed: In the past it was easier to identify peer-to-peer applications or chat using well-known port numbers. In order to evade LI systems, the bad guys had to work harder. Nowadays, most applications use standard HTTP and in most cases SSL to communicate. This puts an extra burden on LI systems that must identify overall more targets on larger volumes of data with fewer filtering options.

Social Networking in particular is pushing usage to exponential levels, and today's lawbreakers have a growing range of sophisticated, encrypted communication channels to exploit. With the stakes so much higher, Service Providers need robust, innovative resources that can contend with a widening field of threats. This interception technology must be able to collect volume traffic and handle data at unprecedented high speeds and with pinpoint security and reliability.

LI Strategies and Goals Vary, but Requirements Remain Constant

Today, some countries are using nationwide interception systems while others only dictate policies that providers need to follow. While regulations and requirements vary from country to country, organizations such as the European Telecommunications Standards Institute (ETSI) and the American National Standards Institute (ANSI) have developed technical parameters for LI to facilitate the work of LEAs. The main functions of any LI solution are to access Interception-Related Information (IRI) and Content of Communication (CC) from the telecommunications network and to deliver that information in a standardized format via the handover interface to one or more monitoring centers of law enforcement agencies.

High-performance switching capabilities, such as those offered by the Net Optics Director™ family of solutions, should map to following LI standards in order to be effective: They must be able to isolate suspicious voice, video, or data streams for an interception, based on IP address, MAC address or other parameters. The device must also be able to carry out filtering at wire speed. Requirements for supporting Lawful Interception activities include:

- The ability to intercept all applicable communications of a certain target without gaps in coverage, including dropped packets, where missing encrypted characters may render a message unreadable or incomplete
- Total visibility into network traffic at any point in the communication stream
- Adequate processing speed to match network bandwidth
- Undetectability, unobtrusiveness, and lack of performance degradation (a red flag to criminals and terrorists on alert for signs that they have been intercepted)
- Real-time monitoring capabilities, because time is of the essence in preventing a crime or attack and in gathering evidence
- The ability to provide intercepted information to the authorities in the agreed-upon handoff format
- Load sharing and balancing of traffic that is handed to the LI system

From the perspective of the network operator or Service Provider, the primary obligations and requirements for developing and deploying a lawful interception solution include:

- Cost-effectiveness
- Minimal impact on network infrastructure
- Compatibility and compliance
- Support for future technologies
- Reliability and security

Net Optics' Comprehensive Range of Solutions for Lawful Interception

Net Optics serves the LI architecture by providing the access part of an LI solution in the form of Taps and switches. These contribute functional flexibility

Internet Traffic Rising Feverishly, with No End In Sight

According to an article in *Search Engine Watch*, the amount of time spent online is increasing exponentially, especially among cell phone users, who are both driving and driven by software applications such as Facebook, Twitter, Orkut, and gaming applications. Video content remains the fastest-growing aspect of Social Media; Facebook and Twitter are only expected to continue their expansion into world markets. In addition, a recent study by Strategy Analytics reveals that the number of people accessing the Internet via cell phone has quadrupled over the last four years. Dealing with these burgeoning numbers places unprecedented challenges on SPs, along with huge investments of time and time and capital in LI solutions equipment. Nevertheless, the need for LI solutions will soar—making it even more imperative that SPs realize the greatest value for their investments in these solutions: efficiency, high performance, low latency, reliability, and scalability.

and can be configured as needed in many settings. Both the Net Optics Director solution family and the iLink Agg™ solution can aggregate a group of links in traffic and pick out conversations with the same IP address pair from any of the links.

Following are further examples of Net Optics products that can form a vital element of a successful LI initiative:

Test access ports, or Taps, are devices used by carriers and others to meet the capability requirements of CALEA legislation. Net Optics is a global leader in the range and capabilities of its Taps, which provide permanent, passive access points to the physical stream.

Net Optics Taps reside in both carrier and enterprise infrastructures to perform network monitoring and to improve both network security and efficiency. These in-line devices provide permanent, passive access points to the physical stream. The passive characteristic of Taps means that network data is not affected whether the Tap is powered or not. As part of an LI solution, Taps have proven more useful than Span ports. If Law Enforcement Agencies must reconfigure a switch to send the right conversations to the Span port every time intercept is required, a risk arises of misconfiguring the switch and connections. Also, Span ports drop packets—another significant monitoring risk, particularly in encryption.

Director xStream™ and iLink Agg xStream™ enable deployment of an intelligent, flexible and efficient monitoring access platform for 10G networks. Director xStream's unique TapFlow™ filtering technology enables LI to focus on select traffic of interest for each tool based on protocols, IP addresses, ports, and VLANs. The robust engineering of Director xStream and iLink Agg xStream enables a pool of 10G and 1G tools to be deployed across a large number of 10G network links, with remote, centralized control of exactly which traffic streams are directed to each tool. Net Optics xStream solutions enable law enforcement entities to view more traffic with fewer monitoring tools as well as relieving oversubscribed 10G monitoring tools. In addition, law enforcement entities can share tools and data access among groups without contention and centralize data monitoring in a network operations center.

Director Pro™ and Director xStream Pro data monitoring switches offer law enforcement the ability to perform better pre-filtering via Deep Packet Inspection (DPI) and to hone in on a specific phone number or credit card number. Those products differ from other platforms that might have the ability to seek data within portions of the packet thanks to a unique ability to filter content or perform pattern matching with hardware and in wire speed potentially to Layer 7. Such DPI provides the ability to apply filters to a packet or multiple packets at any location, regardless of packet length or how "deep" the packet is; or to the location of the data to be matched within this packet. A DPI system is totally independent of the packet.

For further information on Tap technology:

www.netoptics.com
Net Optics, Inc.
5303 Betsy Ross Drive
Santa Clara, CA 95054
(408) 737-7777
info@netoptics.com

Customer First!

Disclaimer: Information contained herein is the sole and exclusive property of Net Optics Inc. The information within this document or item is confidential; it shall not be disclosed to a third party or used except for the purpose of the recipient providing a service to Net Optics Inc. or for the benefit of Net Optics Inc. Your retention, possession or use of this information constitutes your acceptance of these terms. Please note that the sender accepts no responsibility for viruses and it is your responsibility to scan attachments (if any).