Pipeline
Knowledge Is Power

www.pipelinepub.com Volume 4, Issue 11

Every Move You Make: Collecting Data for LAES in Next-Generation Networks

by Joe Hogan

Lawfully Authorized Electronic Surveillance (LAES) is challenging service providers to retain data through various criteria and across multiple next-generation networks such as WiMAX, cable and IMS—not an easy task when considering the expansive subscriber bases and massive amounts of data traveling across any given service provider network. This standard addresses the interfaces between a service provider and a law enforcement agency to assist the agency in conducting electronic surveillance; however, in the continuous mad scramble that is telecom today, this is easier said than done.

What does LAES Mean for Service Providers?

Lawful network surveillance and data retention mandates have gone from low-visibility, back-office functions to a critical need, for which operators may be required to compile millions of customer records in a matter of hours to turn over to authorities. The sheer volume becomes a stumbling block for operators, and the consequences of non-compliance are severe—it can lead to fines and even lawsuits, if surveillance is done improperly.

Further complicating this mandate is the emergence of converged services. With so many different types of data services, the laws are expanding to include information about all communication sessions, including phone calls, text messages, emails, and video and picture messages. This mandate brings cellular service to mind, but in actuality, extends across all providers of wireless, wireline, broadband, and cable services.

While all services are subject to LAES mandates, 85 percent of all intercepts executed worldwide are for communications over a mobile or portable device. To track these transactions, roving surveillance is of utmost importance. As networks grow in complexity with the deployment of next-generation infrastructures such as IMS, the demands made on systems that collect and correlate this data are steadily increasing.

New Regulations

LAES has been in play for several years; however, in the past couple of years, new global regulations have been put in place. For example, the European Union adopted Directive 2006/24/EC in March 2006, requiring the retention of data generated or processed in connection with publicly-available electronic communications services and public communications networks. Essentially, this means that operators of public telephone services and Internet service providers must retain personal data such as the calling number, the user ID, and the identity of a user of an IP address anywhere from six months to two years. The aim is to ensure that the data retained is available for the purpose of the investigation, detection, and prosecution of serious crimes.

While these types of regulations put specific parameters in place for service providers and ultimately provide valuable information to local, state and federal law enforcement agencies, they also add to the ever-growing challenge of efficiently retaining data. As IP-based traffic increases and networks bear the load of next-generation services, it becomes more difficult for operators to retain the necessary data for quick access by law enforcement. This is particularly true when operators do not mediate, charge, or bill for IP data on a usage basis, resulting in a lack of usage information and storage mechanisms.

Smooth Criminals

As service provider networks get smarter and surveillance laws more robust, criminals are also evolving to more effectively fly under the radar. The Internet provides a gateway to anonymity for sophisticated surveillance targets, enabling them to avoid controlled networks and ultimately, detection. These targets can also access many different types of networks with different identities, such as IP address, MAC address, SIP URL, email address, IMSI, and TN. This creates correlation challenges and makes the jobs of both service providers and law enforcement more difficult.

To nail these smarter targets, new tools are needed to ensure that authorities have

the same investigative abilities available in the PSTN domain, such as telephone number identity, and associated call records. This puts even greater pressure on operators with the dramatically increasing volumes of traffic for IP-based services and the lack of usage information and storage mechanisms for IP data.

LAES and other surveillance systems must be sophisticated enough to track this longer-term type and intent of fraud and malice. For example, a terrorist may not actually send a malicious email but instead use a Web-based email system, such as Hotmail, Yahoo, or Google, to write an email and save it as a draft. An individual from another IP address can then open the email draft and read it before deleting it. Such a pattern allows fraudulent organizations to transmit information without an email trail, and thus, service provider networks and surveillance laws are forced to further broaden their parameters and regulations to monitor long-term criminal activity.

Fraudulent and malicious activity will continue to challenge both operators and law enforcement officials. By supporting the evolving complexity and volume of data across next-generation networks, service providers should be prepared to confront new dangers posed by sophisticated, modern targets.

Business as Usual

So now we know why LAES is a positive thing for the public as well as law enforcement; the question is, how can service providers today overcome the obstacles set forth by these regulations while still maintaining business as usual?

Transforming diverse network traffic into a useful record sounds good in theory; in reality, it requires a series of steps, not to mention supporting technology. Operators must support multiple networks for multiple services, and collect from multiple sources to accurately capture and retain data. To do this, they must quickly track and identify target traffic—easier said than done when executing millions of transactions per day, rolling out new services and providing superior service to each and every subscriber. After all, the main focus is on the bottom line.

Scenario:

There are a number of solutions out there—but what is most important when balancing LAES compliance with a booming business?

Performance, for one thing. Operators should look for high performance volumes and low latency, as well as a technology that scales both horizontally and vertically with high availability. This may sound like a tall order, but it's crucial to ensuring effective data retention. Additionally, the solution must support network probes with application layer information likely to be required in future regulations, such as email not provided by CSPs, Internet telephony and other P2P services. The final and must crucial point may seem obvious, but it's the key to compliance: the solution must efficiently store relevant retained data.

Once a data retention strategy is set, service providers must then manage this initiative cost effectively, minimize its impact on day-to-day network operations, manage and authorize warrants in a timely manner, and incorporate secure handoff of the information to law enforcement agencies.

Piece of cake, right?

Not when you consider the multitude of transactions going over a network each day. It's almost unfathomable to think of tracking and storing each one in such a way that enables almost immediate access when a third party demands it. For starters, it's very difficult to compile user transaction data for all activities and services. Secondly, IP traffic generates at least ten times more records than voice traffic.

So why does IP generate so many more records? While one phone call typically produces one call detail record, a single IP-based session can produce tens or hundreds of records based on the user's plan, the time of day, and the type of data transferred. These records don't come packaged in a convenient bundle; rather, they can arrive out of sequence and are regularly incomplete. Additionally, the number of potential identifiers for each device may be different, adding a new layer of complexity to the process.

The next challenge doesn't come with capturing data, but with the data itself. Service providers struggle to correlate data from individuals with intercept warrants. To do this, pure sources of data are required to ensure the integrity of the information. On top of that, operators must coordinate the identifiers associated with an individual's traffic across multiple wireline and wireless phone numbers, as well as email, SIP and MAC addresses.

No Silver Bullet

Unfortunately, there's no silver bullet out there that enables service providers to snap their fingers and be LAES compliant. However, there are solid strategic elements that when brought into use, can ease the burden of data retention. There is also sophisticated technology available that, when coupled with data retention initiatives, can enable accurate, efficient data tracking and storage for LAES. Stopping crime might be the goal of law enforcement agencies—but for service

providers, preventing fraud and malice from impacting the bottom line is priority number one.

If you have news you'd like to share with Pipeline, contact us at editor@pipelinepub.com.