

Harness IP metadata for lawful intercept

Thibaut Bechetoille, CEO of Qosmos, examines how IP metadata can considerably help law enforcement agencies fight cyber crime.

"In IP communications, metadata is detailed information that describes and maps communication patterns with utmost granularity."

Cyber criminals continuously find new ways to evade detection by conventional lawful intercept techniques. Chat rooms, blogs, interactive gaming applications and social websites are among the new hiding places for predators to conduct activities that threaten public safety and national security. With more than 1.5 billion Internet users, thousands of protocols and web applications, and numbers growing, current lawful intercept solutions based on traditional deep packet inspection (DPI) will be less and less effective – unable to keep up with the exponential increases in IP communications, methods of access, and volume of content generated.

Just as criminals grow their levels of sophistication for illegal Internet activities, so must law enforcement agencies (LEAs) improve their capabilities to detect, mitigate and prevent threats. The logical approach – perhaps the only viable approach considering the formidable challenges – is by leveraging metadata that can be extracted from IP traffic.

The maturity of the Internet has brought with it a radical change in communications and how information can be exchanged. People are no longer linked exclusively to physical subscriber lines and can easily hide and subvert their identity. The same person can communicate in multiple ways – for example, via VoIP, instant messaging, Webmail, FTP and social networks such as mySpace, Facebook and Twitter – and from different access points via a desktop, laptop or mobile phone. Complicating matters further is the fact that most people maintain multiple accounts and logins across their communications preferences.

Many Internet applications can now be used for more than their originally intended purpose. A webmail account can have sub-accounts with "dead mailboxes" where different people can use the same login and password to share storage space and information. A Skype chat can be used to transfer computer files and web links. Increasingly,



computer game sites now provide instant messaging and an advanced level of social networking and interaction through motion avatars. All introduce more options for devious minds to perpetrate and hide unlawful activity.

Finally, internet traffic is transmitted using IP protocols, the most common being HTTP. But there are also many regional protocols and a constant stream of new protocols for Web 2.0 applications – many of which do not follow the OSI reference model.

All of the above overwhelms the capabilities of conventional Lawful Intercept solutions. Every new innovation – from peer-to-peer applications to Web 2.0 and 3.5G mobile networks – diminishes their effectiveness while cyber criminals gain more opportunities for unlawful activity and less chance of being detected.

What is IP metadata?

Metadata is data about data. In IP communications, metadata is detailed information that describes and maps communication patterns with utmost granularity. For lawful intercept, metadata greatly expands LEAs' visibility into detected VoIP, email and webmail, instant messaging, and any applications with chat or file sharing.

IP metadata can be used to quickly identify all of a suspect's multiple web identities, to reconstruct links between a suspect and contacts for every instance and type of IP communication, and to uncover intentionally hidden information on the web.

Conventional lawful intercept solutions with traditional DPI (deep packet inspection) provide a form of IP network investigation by enabling operators and LEAs to sort through traffic using pattern-matching techniques. The traditional technology can pick out specific messages by email address, IP address, VoIP phone number, etc. but are not designed with pervasive IP metadata in mind. Traffic payload analysis is a complex, time-consuming and expensive process with limited results. They typically focus

on the IP packets that transit a network, not the metadata that provides a detailed understanding of traffic/capabilities to identify targets in real-time across multiple applications, physical locations, terminals and web identities.

For example, an LEA's street investigation uncovers the email address of a suspected drug trafficker. The email address is traced to a mobile IP address which is monitored with Network Intelligence to detect and map IP activity, contacts and content of all communications from and to the address; as well the suspect's now known web identities from different IP addresses. The LEA, with Network Intelligence, is able to identify other participants in the local drug ring, overseas suppliers, arrangements for drug deals and size of deals in near real-time. The information can be used to capture not only the suspect and cache of drugs before street distribution, but accomplices as well, putting an end to the entire operation.

IP metadata therefore improves LEAs' situational awareness of Internet criminals and response times to new threats. It provides cyber security specialists with a more complete view of network status and activity, as well as the scalability to keep pace with expanding IP technologies, protocols and usage. It enables LEAs and lawful intercept systems providers to implement much stronger cyber security – with automatic detection and mapping of suspicious IP communication patterns to create real-time views and a much deeper understanding of threat situations. IP metadata also offers new opportunities to minimize the massive data storage and lengthy post-processing times associated with conventional lawful intercept by extracting significant information and structuring it as metadata as soon as it becomes available.

Gaining the metadata advantage

IP metadata is not readily available on a network operator's servers. Peer-to-peer and social networks, for example, reside on third-party servers outside of an operator's control. Metadata therefore must be extracted directly from the traffic that transits the operator's network, using a new breed of technology to deliver the IP metadata advantage without the development time, cost and risks.

Network Intelligence, which is a sophisticated evolution of DPI, does exactly that. It quickly identifies events and thoroughly extracts and analyses detailed information – content and metadata – from any IP network. Network intelligence is not a productised, single-application, security solution, but rather an intelligent technology platform upon which to build a complete range of cyber security applications. The reusable technology building blocks support rapid development of powerful, custom, lawful intercept solutions that can be tailored to specific LEA needs and easily upgraded on an ongoing basis to meet the challenges of new IP applications and protocols. In fact, the technology allows LEAs to create their own protocol plug-ins to expedite response to new threats without having to wait for a new software release from a third party, systems provider.

Staying ahead of cyber threats

IP technology and opportunities for its malicious use continue to evolve, making traditional DPI techniques increasingly ineffective and obsolete. The tracking and

information-processing solutions now predominately used for lawful intercept already struggle to keep pace with the exponential increase in IP communications traffic, applications, protocols and volume of content generated. The only technological response to these challenges is to design solutions with true network intelligence capabilities using information extraction and IP metadata.

Network intelligence enables LEAs to better protect the public by staying ahead of the criminals that operate in the virtual world. Traffic for a specific target can be lawfully intercepted in real-time across multiple applications, physical locations, terminals and web identities. Traffic can be indexed by numerous categories such as target identifiers, time stamps, content, application, call characteristics and more.

Lawful intercept solutions that use network intelligence as their foundational building block improve LEAs capabilities to anticipate potential threats before they materialize. With automated metadata computation and information correlation, they can automatically detect suspicious communication behavioral patterns. They can also improve response times to new threats and the cost of lawful intercept by dramatically reducing the time and resource requirements to process greater and greater amounts of IP traffic data.

"Network Intelligence enables LEAs to better protect the public by staying ahead of the criminals that operate in the virtual world."

The flight of the Condor

Phonak Communications has launched the world's first full duplex encrypted wireless system to provide small covert and special operations teams with on-the-go communication flexibility.

The Condor system is a license-free all-in-one communication solution that is usable straight out of the box. It comprises a palm-sized and easy-to-wear radio unit, discrete under-the-shirt wiring, and a choice of Phonak headsets.

The system allows up to six colleagues to communicate in full duplex mode (simultaneously talking and listening), and additional colleagues can also listen in via the same closed network; all of this over a secure encrypted channel.

Essentially for mobile teams, Condor does not require connection to a base station and is therefore 100% mobile. It uses only free-to-use frequencies so no licenses are required, making Condor instantly usable whatever the place of operation.

Users can communicate at distances of up to 1km; and the system is quick to configure with simple pairing and no PC required. Team leaders can quickly and easily create the user-defined networks they require for operational success.

"The Condor system takes covert and special team communications to the next level", commented Evert Dijkstra, Managing Director of Phonak Communications. "One hundred percent mobile, completely secure, and usable without a base station, Condor ensures that mobile teams no longer need rely on a mish-mash of technologies. Instead they can employ this flexible system and concentrate on what really matters – achieving operational success."

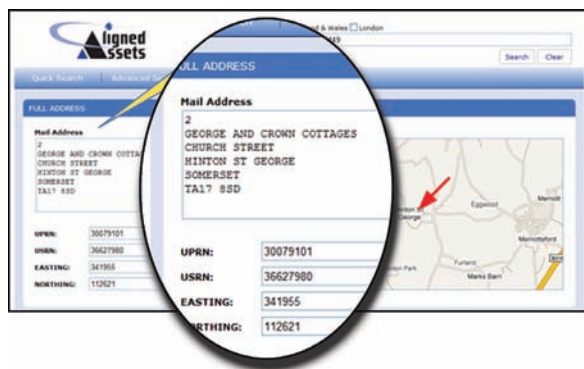


License-free and usable straight out of the box, the Condor by Phonak Communications.

A single contact point

With accurate address data essential to the workings of police forces across the UK, Carl Hancock of Aligned Assets considers the numerous datasets available and how it can often be difficult to know which one to chose. Is there a way round this common situation?

SinglePoint's search facility works with a wide variety of databases. Address searches can be combined with searching a names database, intelligence database, and force-specific gazetteers.



The NLPG

With the introduction of the FiReControl project the Fire and Rescue Services across England are moving toward a full scale adoption of the NLPG at brigade level and increasingly Police forces are looking at the NLPG and its uses.

There remains, however, some unease as to the completeness of the available address datasets, and though the NLPG has standardisation and methods for constant updating, in a profession where good data can mean the difference between life and death, it is understandable why there may be some hesitation. In the case of PAF and AddressPoint, some might say that years of assured usage offer a level of reassurance that the NLPG is not yet able to.

There is also a lot of discussion about a National Emergency Services Gazetteer which would not only contain the address data that would be found in the NLPG, but additional information that is essential to the emergency services. It has been observed that many crimes occur in locations such as a street corner, ATM or bus stop, most of which will not be held by existing datasets. The creation of this gazetteer would undoubtedly give the police even more essential data, which would be as easily accessible through SinglePoint as is any of the existing datasets.

Flexibility

Designed with flexibility in mind, SinglePoint will work regardless of which gazetteer management system is used, and is compatible with any 3rd party GIS. This latter point allows for the visualisation of the address in MapInfo, ESRI or even Google Maps, offering not only a far greater tangibility to the data but assistance in incident recording and crime mapping.

SinglePoint is a key tool for adding value to existing data, value that is expandable through the use of adaptor technology. This takes SinglePoint far beyond any address look up tool that is currently on the market since the adaptors allow its search facility to work with a wide variety of databases. Address searches can for example be combined with searching a names database, intelligence databases and force specific gazetteers.

Spencer Chainey observed; "The problems with address-based data are consistent across all data products and not one in particular. This is often why many police forces have to turn to several address based data sources rather than being confident in relying on one that meets all their needs."

SinglePoint might not solve the problems within the data, but accessing and searching through a single portal will remove many of the problems and inefficiencies currently associated with multiple data sources.

Traditionally the address data of choice has been that provided by the Ordnance Survey – AddressPoint, which is now slowly being replaced with OS Address Layer 2. In addition to this there is PAF from the Royal Mail and new to the mix is the National Land and Property Gazetteer (NLPG) – address data direct from the local authorities of England and Wales.

Each has merits, but when dealing with such vast quantities of information it is impossible to draw direct comparisons when it comes to questions of accuracy or usefulness. To date this has left a dilemma of which to choose and in many cases the emergency services have opted to hold multiple gazetteers in order to make sure that every address was covered.

In his report of Feb 2008 entitled *Examining the use of address-based data products in policing in GB*, Spencer Chainey found that police forces were using on average almost five different sources of address data, his reasoning – "because not one single product meets all their needs."

This naturally creates inefficiencies, as accessing each dataset can be time consuming, yet is the only method by which assurance can be gained that the information used is accurate and up to date. If all the data was alternatively combined to produce a "super gazetteer" all that would be created are large scale duplications and the ability to update individual sets would be greatly reduced.

The SinglePoint Solution

Whilst the argument rages on about which is the best dataset to use, gazetteer specialists Aligned Assets have circumnavigated the issue by developing a multi-gazetteer search engine called SinglePoint.

Designed to combine multi-gazetteer functionality with sub-second response times, SinglePoint offers the emergency services a single portal through which all their address gazetteers can be searched simultaneously with the same ease as if searching just the one. By doing it this way, time is saved though only the one search, whilst updating is easy as each gazetteer is maintained in isolation to the next.

"Designed with flexibility in mind, SinglePoint works regardless of which gazetteer management system is used, and is compatible with any 3rd party GIS."

➤ Carl Hancock,
Aligned Assets.

