TOYO Corporation
Quest for Precision

SYNESIS and the Lawful Intercept Use Case

WHITE PAPER

By Steve Wong
steve.wong@toyotechus.com
https://www.linkedin.com/in/stephencwong/

INTRODUCTION

Lawful Intercept (LI) is a term used to describe a scenario when a government Law Enforcement Agency (LEA) is granted the legal means to conduct electronic surveillance on a targeted entity; the entity could be a corporation, or it could be an individual. For example, some of the law agencies which could make use of lawful intercept include the FBI, CIA and SEC.

The concept was first conceived many decades ago and was applied to public switched telephone networks (e.g. wiretapping). LI today encompasses modern packet switched networks (also known as IP or Internet Protocol networks) which may carry electronic network correspondence (e.g. e-mails) or audio communication (e.g. VoIP).

This will be the focus of this white paper express as we discuss the processes involved in LI and the electronic network tools used.

THE BASICS

For the rest of this paper, please refer to the graphic (*see figure 1*) which illustrates how a LI could be deployed at a Service Provider (SP).

When an individual is suspected by a LEA of engaging in illegal activities, they will seek authorization from a court (e.g. a judge) to survey the target. Forms of illegal activities can be of both the criminal type (e.g. blackmail) or civil type (e.g. misappropriation of trade secrets, inside

Figure 1: Lawful Intercept Networking Basics

trading). If the court concludes there is a reasonable belief that criminal activities are taking place, it grants the request for the survey.

The Communictions Assistance for Law Enforcement Act, also known as CALEA, describes how Service Providers (SP) in the United States must support LI. Two standards define LI and they are:

- Telephone Industry Association (TIA) specification J-STD-025
- Packet Cable Electronic Surveillance Specification (PKT-SP-ESP-101-991229)

J-STD-025 defines the interfaces between a Telecommunications Service Provider and a Law Enforcement Agency to assist the Law Enforcement Agency in conducting lawfully authorized electronic surveillance.[1]

The PacketCable™ Electronic Surveillance Specification or PKT-SP-ESP-I01-991229 is a specification that defines the interface between a Telecommunications Carrier and a LEA to assist the LEA in conducting lawfully authorized electronic surveillance.[2]

Armed with this order, the law enforcement agency makes the request to the SP of the target to intercept his network communication. For example, if the target is a subscriber of a hypothetical service provider called CB&T for his Internet service, the LEA makes the request to CB&T for the survey. For the purposes of this white paper, we will assume target's SP is known by the LEA.

CB&T is legally bound to comply with the LI request. User Internet activities through any service provider is never anonymous. The SP knows your name, contact information and most importantly, your public IP address. Open a browser and type "What is my IP address?" and the search engine will report your public IP address.

Figure 2: Single-mode Passive Fiber Network TAP supporting 1G | 10G | 25G | 40G | 100G

Figure 3: SYNESIS - 100G Network Capture Appliance (Portable)

Thus, with your known IP address, a SP can track and capture every single activity that you partake on the Internet. This includes e-mails that you send, websites that you visit, VoIP calls you make, instant messages that you send and purchases that you make. It is akin to having a video camera record every action on your monitor, however in a far more precise and exact manner.

TOOLS

The essential equipment that makes this all possible and that SPs need to acquire to support LI requests are Network Test Access Points (TAPs) and "network packet recorder." A "network packet recorder" can also be referred to as a "network capture" appliance.

What is a TAP? According to Garland Technology, a leading manufacturer of TAPs, it is a hardware device that allows network traffic to flow from ports A to B, and B to A without interruption, and also creates an exact copy of both sides of the traffic flow, continuously and without compromising network integrity. The duplicate copy can be used for any number of purposes, including monitoring, security or analysis.[3]

Network TAPs provide 100% packet data and are CALEA (The Commission on Accreditation for Law Enforcement Agencies, Inc.) approved for LI cases. An alternative, SPAN (Switched Port Analyzer) or port mirroring is not approved, as it is prone to dropped packets, changing time frames and packet duplication.

Network TAPs are classified into two categories based on the type of media that they are designed for -- whether

it is electrical or optical. In high speed 100G networks, the media interface is optical (*see figure 2*).

The other piece is the network recorder appliance, a specialized hardware tool that also resides at the SP. The tool has filtering capabilities so that it can be programmed to look only for data packets associated with a target's IP address and record them in digital form, ignoring other data packets from other users. That usually means the data is initially stored onto some sort of data storage device.

What is captured includes outbound data packets; that is data that is initiated on the target side such as launching a website or sending an e-mail. It includes inbound data packets as well. This is data that is sent back to the target. For example, the results from a query at a search engine such as Google.

These tools must have the ability to capture and store extremely large amounts of data; typically starting in the hundreds of terabytes and scaling to the petabyte range. A petabyte is a 1,000 terabytes or 1,000,000 gigabytes.

And they can continuously record all the data packets associated with that particular IP address for a given period of time - for example, from July 1, 2019 12:00am to July 15, 2019 12:00am. The time period for the surveillance will be stated in the LI request.

The underlying base surveillance equipment and technology that a SP uses to comply with a LI request, TAPs and network capture appliances, have been available for at least a decade or two. However, network speeds have dramatically increased over the last twenty years. Today within most if not all SPs, network speeds of 100G and greater is not uncommon.

Thus, these two critical components, TAPs and network recorder appliances, must have the ability to operate at data rates of 100G and up today and at higher data rates in the near future.

But surprisingly there is only one capture appliance tool in the marketplace today that can completely capture data at 100G (and even 200G). This capture tool is called SYNESIS and it is designed and engineered by TOYO Corporation.

SYNESIS is the brand name of an entire product line of high speed network capture appliances. The portable versions (*see figure 3*) are used for troubleshooting and field support applications and the distributed or rack mount versions are used for more permanent deployments in data centers.

Figure 4: SYNESIS - 100G Network Capture Appliance (Rackmount)

The distributed or rack mount versions versions have expandable storage to allow for more capacity to be added over time and as budget permits (*see figure 4*).

The inability to record completely at these high data rates compromises the completeness and integrity of the surveyed data. More importantly, incomplete data captures may not hold up in a court of law.

But the ability to capture at these data rates turns out to be far more challenging. In the "*The Forgotten Requirement of Network Analysis*"[4] white paper, we have made the case that to perform filtering and capture at data rates of 100G or more, tools that are designed around Field Programmable Gate Array (FPGA) technology are mandatory.

First invented in 1985, FPGAs were initially used in telecommunications and networking applications. Today they are also found in consumer, automotive and industrial applications.[5]

CPU-based appliances built around general purpose processors (e.g. Intel®, AMD®) no matter what generation they are, how many cores/threads they have or how many PCI Express lanes they can support simply cannot match the FPGA's ability to run an extremely high number of processes in parallel and at high speeds.

Furthermore unlike Application Specific Integrated Circuits (ASICs), FPGAs can be easily reprogrammed to implement new capabilities and features without having to redesign the hardware.

"*The Forgotten Requirement of Network Analysis*" white paper refers to Xilinx, a leader in the FPGA space. A couple of years ago the company demonstrated the ability to manage 400G data links using FPGA technology that is already a few years old.[6]

Hence if you are a SP, and you are considering acquiring tools to support LI requests, you must make sure that they are designed around FPGA technology.

In this author's opinion this perhaps is the single most important requirement. Everything else is secondary.

LI REQUEST FULFILLED

Once provisioned by the SP, the intercept very quickly begins to pass captured network information to the initiating LEA. This continues until the specified end time of the warrant.

SYNESIS is configured to satisfy the "Mediator" portion of the LI specifications[1,2] and can be configured to support various input or capture scenarios and output interface options.

There are a variety of ways in which the data is passed over to the LEA but this is beyond the scope of this white paper. What is important to note is that the SP is not responsible for performing any analysis of the data. And once the data has been turned over to the LEA, it is purged from the SP's systems.

Meanwhile back at the LEA, with the data from the SP, analysts will reconstruct the communication threads from the captured data. This information will then be analyzed, collected, documented and saved to determine if the activities rise to the level of an indictment and as evidence for any criminal proceedings.

OTHER IMPORTANT POINTS

There are some other noteworthy points to mention.

SPs have strict rules and procedures that govern which personnel are authorized to use these tools to support the LI. Obviously in the wrong hands, access to these tools and the data they collect can be abused. It is strictly prohibited for anyone other than the initiating agency to view the resultant captured data.

Although the white paper implies there are manual steps involved in the fulfilling of a LI request, in actuality, a great deal of the process occurs electronically and typically is automated.

It is believed that at any given time, a large SP is handling a very large number of LI requests simultaneously. And that number is expected continues to grow over time.

CONCLUSION

Higher speed subscriber links require higher speed Lawful Intercept technology to keep pace. SYNESIS[7] is the only solution that is able to record and collect 100G and up to 200G network traffic without losing a single bit. This is an absolute requirement in order for Service Providers to be able to carry out Lawful Intercept requests.

ACKNOWLEDGEMENTS

The author would like to acknowledge Angelo Bustos[8] and Chris Johnson[9] for their insights and contributions to this white paper.

REFERENCES

[1] Telecommunication Industry Association Standard
[2] PacketCable Electronic Surveillance Specification
[3] https://www.garlandtechnology.com/network-tap
[4] https://toyotechus.com/wp-content/uploads/2018/06/The-Forgotten-Requirement-of-Network-Analysis.pdf
[5] https://en.wikipedia.org/wiki/Field-programmable_gate_array
[6] Attig, Michael and Brebner, Gordon. *"400 Gb/s Programmable Packet Parsing on a Single FPGA". Xilinx.* https://www.xilinx.com/publications/about/ANCS_final.pdf
[7] www.synesis.tech
[8] *Angelo Bustos' contact information:* angelo.bustos@toyotechus.com
[9] *Chris Johnson's contact information:* chrisj@oasyscorp.com

TOYOTech
42840 Christy Street, Ste. 110, Fremont, CA 94538
Phone 510-438-9548 | E-mail: info@toyotechus.com
http://www.toyotechus.com