



Hammond Street Developments Pty. Ltd.

A.B.N. 32 074 649 595

P.O. Box 5062, RINGWOOD, Victoria, 3134

Ph: +61 3 9875 5900 Fax: +61 3 9877 5699

www.hsd.com.au

DISCUSSION PAPER

CONVERGENCE OF LAWFUL INTERCEPTION AND NETWORK TELEMETRY

Author: Michael Nancarrow and Mark Wolfe

Date Created: Thursday, February 17, 2005

Version: Draft 1.0

CONTENTS

DISCUSSION PAPER	1
CONVERGENCE OF LAWFUL INTERCEPTION AND NETWORK TELEMTRY	1
1 ABSTRACT	3
2 AUTHORS	3
3 COPYRIGHT	3
4 FORWARD	4
5 APPROACH TO NETWORK TELEMTRY AND LAWFUL INTERCEPTION	5
6 NETWORK TELEMTRY FOR LAWFUL INTERCEPTION	6
7 AGILITY AND PASSIVE INTEGRATION	7
8 NETWORK TELEMTRY PATTERN	8
8.1 PACKET ACQUISITION	9
8.2 DATA SUBSCRIBERS	9
8.3 BUSINESS LAYER	9
9 L2TP EXAMPLE	10
9.1 PACKET ACQUISITION	11
9.2 DATA SUBSCRIBERS	12
9.2.1 LCP DATA SUBSCRIBER	12
9.2.2 LI PACKAGER DATA SUBSCRIBER	12
9.3 BUSINESS SYSTEMS LAYER	12
9.3.1 OPERATIONS SUPPORT COMPONENT	12
9.3.2 LI TRIGGERING COMPONENT	13
9.3.3 LI FORWARDING COMPONENT	13
9.4 TARGET IDENTIFIERS	13
10 SUMMARY	14
11 REFERENCES	14

1 ABSTRACT

Telecommunications companies are coming under increasing pressure to meet their Lawful Interception obligations. While significant information exists on the requirement, there is very little support and in some cases, resistance to developing interception capabilities.

In recent years, the telecommunication industry has become very competitive leaving providers to closely align expenditure with revenue raising activities. Many organisations view the implementations of interception capabilities as expenditure that doesn't provide any tangible outcomes for the business. To exasperate the problem, when interception is required, System Administrators are expected to almost instantly deliver on what can be a very complex requirement with little support from the carrier.

The solution to the problem is changing the approach to interception solutions. If carriers can view their networks as an untapped well of information that can lead to improved efficiencies and service quality, then carriers can realise a return on an investment that supports interception capabilities.

This paper investigates how a change of approach can provide tangible outcomes by converging Lawful Interception with Network Telemetry. To support this approach, this paper provides a model and practical examples on how to deliver such solutions.

2 AUTHORS

Michael Nancarrow is the CEO and Senior Consultant based in Melbourne. His firm, Hammond Street Developments, has been providing system integration and software development services to the ISP and Telecommunications industry since 1996. michael.nancarrow@hsd.com.au

Mark Wolfe is a Systems Architect at Hammond Street Developments. Working with many Telecommunications companies, Mark has amassed significant knowledge and experienced delivering LI solutions into a wide variety of commercial digital networks. mark.wolfe@hsd.com.au

3 COPYRIGHT

Copyright © 2005 Hammond Street Developments Pty Ltd, All Rights Reserved.

The contents of this copied, reproduced or published in part or in whole, without the written authorisation of Hammond Street Developments Pty Ltd.

We believe that the ideas presented in this paper are universal and we encourage distribution within your organisation. Please provide feedback so it may be considered for future research and development efforts.

4 FORWARD

Over the past decade, the Internet has grown around the world into a new and efficient means for people to communicate and collaborate. Unfortunately, criminals and terrorists also use the Internet to coordinate and perpetrate crimes.

Governments are now moving quickly to introduce and/or amend legislation that provides for the Lawful Interception (LI) of Internet and Internet related services. These laws empower Law Enforcement Agencies (LEAs) to perform LI from the Internet under similar lawful constructs as performing LI from switched voice networks.

In 1997, the Federal government of Australia, introduced the *Telecommunications Act, 1997* (the Act). The Act provides a framework that compels carriers and carriage service providers (CCSPs), including Internet Service Providers, to provide special assistance and lawful interception capabilities to Law Enforcement Agencies (LEAs). Many other countries around the world are implementing similar legislation.

It is a well-established fact that Lawmakers in Australia and around the world have been unable to keep up with the development and implementation of new digital communications technology. Large corporations and government agencies used telecommunications companies like Telstra for digital communication infrastructure. The domestic Internet access market was pioneered by small SMEs that grew from what effectively was a self-funding hobby, converting interested people into network engineers.

As demand grew and profitability increased, expansive, distributed networks were created from inexpensive equipment providing a new communications media to the home. Unlike RF communication (CB Radio) and switched phone systems, the Law Enforcement Agencies had no method intercepting (tapping) these communications, therefore, leading to the revisions of the Telecommunication Act. This of course, occurred well after extensive network infrastructure has been deployed with little or no consideration to interception requirements.

In a paper published by Philip Branch, Senior Lecturer in Telecommunications at Swinburne University of Technology, Philip said; *"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 the 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."*

Caught between multiple international standards, privacy concerns and politics, equipment manufactures of IP and Internet products are just only now considering to how include interception into their products. The void between a CCSPs infrastructure and their obligation to provide interception capabilities to LEAs is becoming ever greater with the development of new IP technologies such as VoIP.

In recent days, competition in the Internet industry has become intense creating a paradigm that is not conducive to LI solutions or to the base requirements of needing them. Competitive pricing has increased the uptake of Internet services shifting communications away from mediums where LI capabilities exist. Competitive pricing has also reduced revenue on a per subscriber basis placing significant pressure on profit margins.

Available capital funds are spent on expanding services offerings and improving the performance in a never-ending effort to reduce churn and create new revenue streams. For many CCSPs the costs of LI solutions are seen as prohibitive, creating a very unwelcome paradox between spending funds on activities related to generating revenue and spending on LI technology that doesn't provide any fiscal benefit other than being able to legally provide the service in the first place. Nevertheless, CCSPs do benefit from safe, secure and prosperous communities and while delivering upon LI obligations does not provide any immediate returns, it does provide invaluable long term, tangible benefits.

5 APPROACH TO NETWORK TELEMETRY AND LAWFUL INTERCEPTION

There is no doubt that System Administrators endure constant demands and time pressures. In a paper written by Andrew Cowie from Operation Dynamics, he identifies how the time demands for a system administrator can escalate rapidly. Andrew states: -

'Ever increasing complexity means that people charged with maintaining production systems face an impossible task: they need to spend time developing new ways to manage their platform but are constantly fighting fires which prevent them from concentrating on the real challenges at hand.'

Without a positive approach, LI will become an extortionary burden on System Administrators and ultimately, to the CCSP. This begs the question: 'How can resources spent on LI be used by the CCSP to more efficiently deliver services?'

To answer the question, it can be broken down onto two smaller questions: -

1. How can we reduce the burden of LI on System Administrators and other CCSP staff? and
2. Where can additional value be found in LI systems?

Before we can start to answer the question, we first must identify who the stakeholders are. A traditional view would suggest that the LEAs are the business drivers and the CCSP is the technical solution provider.

This approach creates an environment where there is very little chance for a CCSP to realise any return on their investment into LI solutions, therefore, LI will just become another burden (like tax compliance) on the CCSP. The CCSP will then be inclined to minimise the resources spent on LI and most probably abdicate the problem to the System Administrator. Setting in place all the environmental variables that Andrew Cowie identifies in his paper, the cost of LI capabilities will spiral out of control with the System Administrator being held responsible.

Understanding interception obligations is not only the responsibility of the Legal Council of a CCSP, from an System Administrators point of view, the legal council should be seen as the business with the requirements and the [Telecommunications Act](#) is their business requirements document.

If a different approach is taken where LI capabilities are a subsidiary service of operating a commercial network, other more productive outcomes can be produced. Changing the purpose of each stakeholder is the first ingredient.

Stakeholder	Purpose	Reason
The CCSP executive/business	Primary Business Driver	Without LI capabilities, the business may contravene the Telco Act. Like Taxation, the business must operate within the law. The business is also a user of network related data that is commonly used for Service Level Agreements and Charging and Billing.
Law Enforcement Agencies	User/Subscriber	The users of a LI service.
CCSP System Administrator	Network Management	Development and support of the services provided by the CCSP. Users of network related data.

The common thread between all stakeholders is the dependency on network related data in the execution of their activities. If instead of implementing an LI capability, the CCSP chooses to implement a 'Network Telemetry' solution, the rationale behind allocating resources is changed from one of begrudging LI requirements, to a project that will deliver efficiencies in network management, service delivery and LI obligations.

Tangible outcomes can be achieved from what was traditionally a black hole for time and money.

6 NETWORK TELEMETRY FOR LAWFUL INTERCEPTION

Changing the paradigm of LI being 'a cost of doing business' to 'a cost of improving business' will deliver tangible outcomes that may have not been identified when LI requirements were considered by a CCSP.

As a Systems Administrator, how many times do you wish you could log onto a box, send the network interface into promiscuous mode and run TCP Dump or any other packet capture device so you can see what is going on?

It is a well-established fact that Network Protocol Analyser tools such as Ethereal are an invaluable for Systems Administrators in diagnosing complex networking issues. When Systems Administrators have access to the packets on a network they can readily and efficiently diagnose problems and discover new methods of improving network efficiency and reliability. This in turn provides the Systems Administrator with more time to be proactive towards network management, thus reducing the number of spot fires that have to be resolved on a day-to-day basis.

The problem faced by the Systems Administrator is getting the packets in the first place. Distributed networks can place the point of data acquisition on the other side of the country from their physical location. Limiting System Administrators use of such powerful tools often forces them to resort to making configuration changes in a hit and miss effort to resolve a problem.

Billing systems are another example of how packet capture devices can provide a value to a business while delivering on the needs of LI. Net flow software can be easily implemented on packet capture devices removing the burden from busy routers and abstracting business application software from core infrastructure that is often under load delivering services to subscribers.

Furthermore, application developers and database administrators can build software such as usage meters using packet capture devices that present very little risk to the operation of core infrastructure responsible for delivering subscriber services.

When considering the technical requirements of LI, packet capture devices must be able to see all ingress and egress data for all subscribers. If the device used for packet capture can discreetly facilitate the needs of LI, the same devices can be used for Network Telemetry purposes providing a tangible return on investment (ROI) in the device.

If the load on infrastructure being used to deliver subscriber services can be reduced, the infrastructure can continue to be used as the subscriber levels expand and there will be less inclination to use it for other CCSP business requirements. In a nut shell, the funds used for Network Telemetry can also improve the longevity of core infrastructure.

Network Telemetry isn't only for System Administrators and Application Developers, the CCSP leadership team can greatly benefit from data describing subscriber's activity and wholesale providers' performance to SLAs.

The use of Network Telemetry has extraordinary value to all stakeholders of a CCSP, there are numerous tools available that can interpret packet capture into meaningful data designed to improve the efficiency of operating a commercial digital network and provide market intelligence.

The challenge for CCSPs is how to generate value from the mandatory requirements of LI. The first step in achieving this goal is to view the packets on a network as an un-tapped well of data and information that can inspire new innovations for all stakeholders.

7 AGILITY AND PASSIVE INTEGRATION

As for any business, agility is vital for the long-term prosperity of a business. For CCSPs, the business support systems must be flexible enough to integrate with a changing network environment.

For any business, especially technology based organisations, to operate a flexible and scalable environment, activities for the various skill bases need to be compartmentalised with succinct contracts of interface facilitated for the communications of data information between the compartments.

A classic example of where compartmentalisation fails in a CCSP is 'utilisation based billing models'. The Systems and Network Administrators are responsible for managing the servers a billing system is dependant upon. Application Developers and Database Administrators are responsible for facilitating the business rules of charging and billing. Nearly! With equipment vendors including net flow functionality into routing equipment, they shifted some of the charging and billing requirements from the Application Developers to the System and Network Administrators. Now, every time changes to a network are required, Systems and Network Administrators must facilitate the business rules and complexity of the billing formula for the CCSP.

To make matters worse, LI requirements are also abdicated onto the System and Network Administrators dumping more and more business complexity onto resources that are attempting to manage an ever-changing network environment.

Combining business support and service delivery requirements onto the same infrastructure places too many dependencies into one compartment, reducing flexibility and increasing risk to service delivery.

Using passive integration, compartmentalisation can begin to occur, and by design, packet-sniffing devices are passive and have the capability to deliver data to Network Telemetry and business support systems.

Examining a scenario where a CCSP adds another POP to a network, the use of passive packet sniffing devices will allow the expansion of services to occur far more efficiently.

When additional infrastructure is acquired or implemented by a CCSP, the Network and System Administrators can perform their duties of delivering subscriber services. By configuring a span port or installing a network tap, a passive sniffing device can be installed. All data requirements by the business support systems is provided by the sniffing device and the burden of complex business rules are removed from the systems that are delivering subscriber services.

Using passive sniffing devices, subscribers' data becomes available for billing systems, LI capabilities are facilitated, network tools for support become available all without the Network and System Administrators having intimate knowledge of the support systems.

There is no need to reconfigure or update routers or operate multiple billing systems that dramatically increase the risk to the entire operation. The network infrastructure and business support systems will become for more flexible and scaleable by abstracting dependencies to each other via simple and succinct contract of interface (a port span).

Minimising the number of resources required for configuration changes to a CCSP network or business formula is a vital ingredient in improving the efficiency and agility of the business. If a well designed strategic view is taken to the implementation of LI capabilities, the business will receive returns in efficiency, agility and service quality by simply taking an innovative approach to the mandatory requirements of LI.

8 NETWORK TELEMETRY PATTERN

The first section of this paper explored how a proactive approach to LI could bring about a ROI with the focus being on using LI components for telemetry purposes, when in reality, it is the other way around.

When providing for LI capabilities, a CCSP should implement a telemetry system that supports LI capabilities.

Basic Layers of a telemetry system

- Packet Acquisition
- Data Subscribers
- Business Systems

Attributes are passed from the business systems to the data subscribers. The attributes define the scope of data that the data subscribers are to provide the business system. Filters, like those used with TCP Dump, identify target packets within a data stream. Packets contain many attributes. One or more can be used to identify a stream of data.

Example: - UDP port 1701 and byte 1 are used to acquire the Link Control Protocol (LCP) packets of L2TP.

Packet filtering on promiscuous interfaces can be resource intensive. Filters should be kept as simple as possible and designed to filter only those packets require for the business systems purpose.

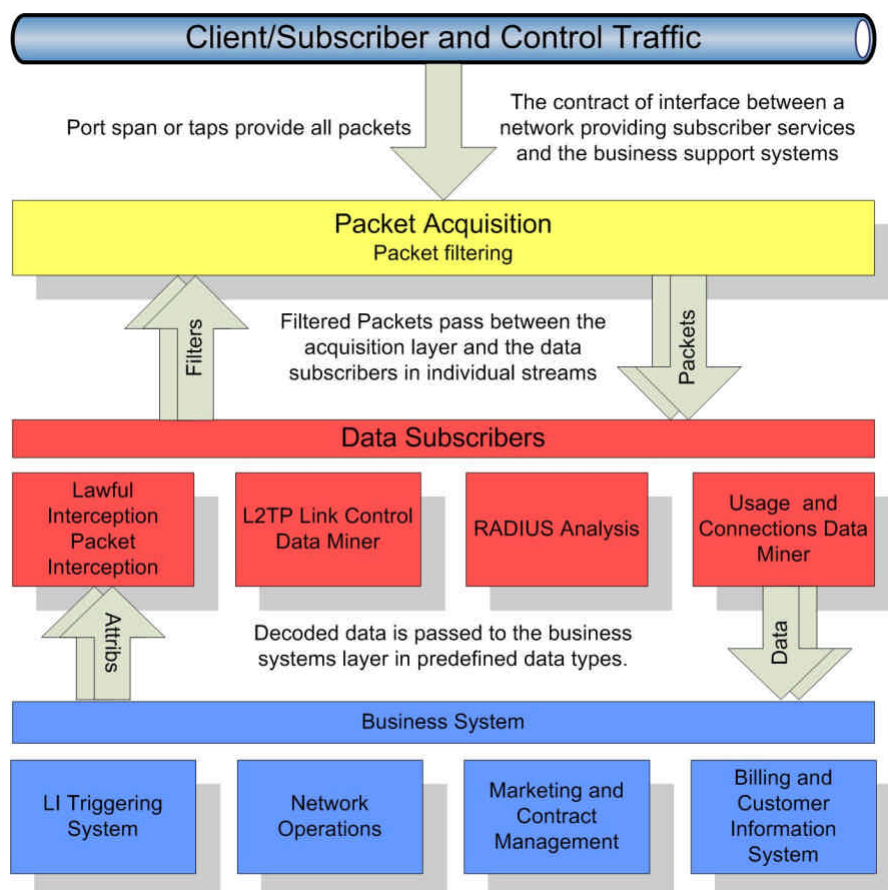


Figure 1 – Layers

Following this pattern allows for the compartmentalisation of the CCSPs' operations. Network Engineers build networks that deliver subscriber services and provide System Administrators interfaces that expose all packets on the network. System Administrators implement packet acquisition devices that facilitate an exchange of information between the network and business systems. Application Developers then develop data subscribers to mine information for business support systems.

8.1 PACKET ACQUISITION

The packet acquisition layer acquires target packets based on filters passed to it then forwards those packets to the next layer.

The packet acquisition layer is made up of packet sniffers. A packet Sniffer is a device that has access to the target traffic. Typically taps or spanning ports on a switch facilitate access to the traffic.

Filters are used to identify specific packets within a data stream. Packets contain many attributes. One or more of these attributes can be used to identify a stream of data.

Example: -

- UDP Port 1701 and byte 1 of the L2TP packet header are used to identify the Link Control Protocol (LCP) packets used by L2TP. LCP packets can be used for diagnoses of L2TP issues. Furthermore, the data can be used for triggering and building filters for interception of L2TP sessions.

A primary design consideration when using the acquisition layer is to acquire only those packets required by the next layer using the least complex filter possible.

Packets can be forwarded using any number of Inter-process Communication (IPC) methods. These can include sockets, memory mapped files and pipes. It is important to note the packet to is passed to the next layer unmodified. No data interpretation is performed in this layer.

8.2 DATA SUBSCRIBERS

The Data subscription layer receives packets from the packet acquisition layer and interprets them into data structures that are passed to the business layer.

The data subscription layer is comprised of one or more services that connect to packet sniffers through an IPC method. The services can be on the same physical device as the packet sniffer or on separate servers.

The primary operation of a data subscriber is to decode packets into their base data structure. Protocol analysis and/or aggregation routines can then be applied to the decoded packets to produce data in structures that meet the requirements of the business layer.

Example, decoding DHCP: -

- Decoding, decode the payload of the DHCP packet into a data structure
- Protocol Analysis, interpret one or more decoded packets and associate them with a transaction between a client and server
- Aggregation, count the number of transactions grouped by their type for a given time period.
 - Types – Discover, Offer, Request, Decline, Ack, Nack, Release and Inform.

8.3 BUSINESS LAYER

The business layer receives predefine data structures from one or more data structures. The data structure contains the output of a decoded, analysed, and if required, aggregated IP stream. This approach allows application developers to use data subscribers as an information source while having the complexities of network protocols abstracted into succinct data structures.

9 L2TP EXAMPLE

The convergence between LI requirements and telemetry can be clearly identified by providing by understanding of the components required to deliver LI solutions.

Our example network is based on a Network Service Provider (NSP) that retails ADSL from a Network Access Provider (NAP), wholesaler. L2TP is used to terminate subscriber sessions at the NSP.

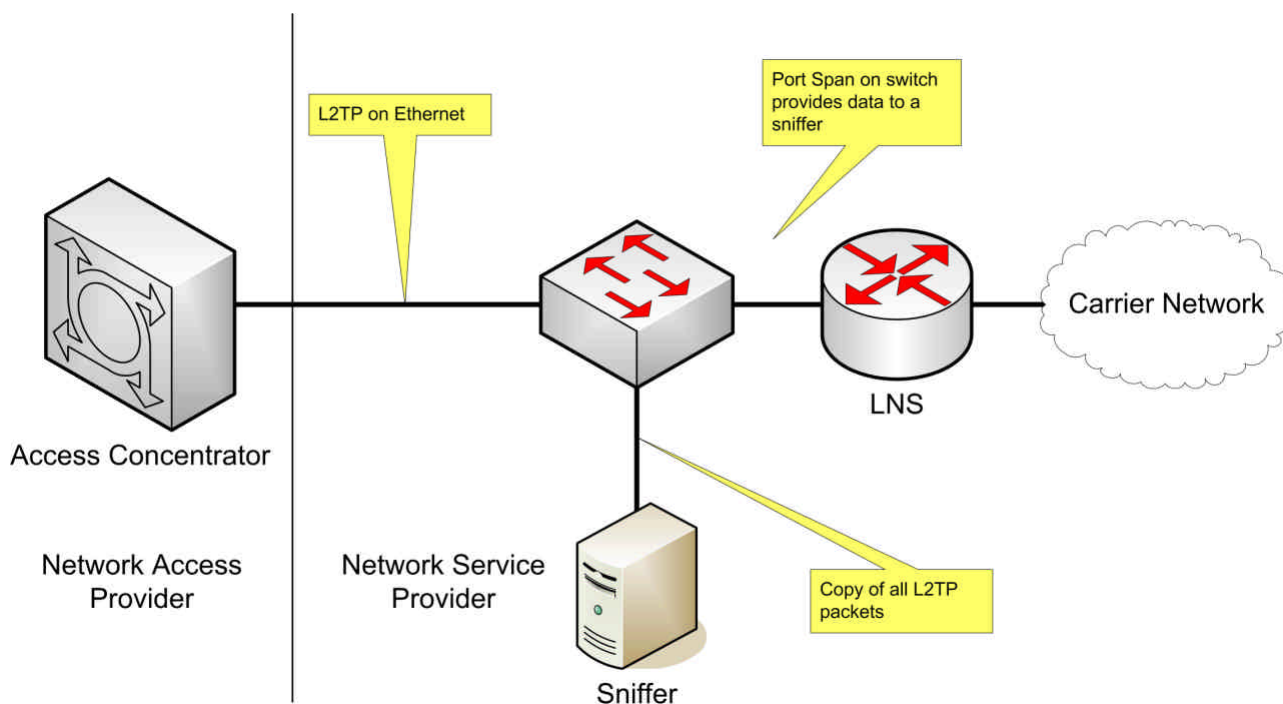


Figure 2 - Example Network

In this example we will look at how the three layers are applied to provide user connection information to a CCSPs support services along with providing LI capabilities.

The main difficulty of intercepting L2TP sessions is determining a filter that identifies only those packets for a target service. After reviewing RFC 2661 it can be determined that 6 attributes identify a packet in a data stream that belongs to an individual tunnel and session.

These attributes are: -

- LAC IP address
- LNS IP address
- Tunnel Identifier, egress data
- Session Identifier, egress data
- Tunnel Identifier, ingress data
- Session Identifier, ingress data

When an LAC and LNS are connected, two tunnels/sessions are created between client and server. The tunnels/sessions use a reserved session, ID0, for initial negotiation of subscriber sessions.

The Link Control Protocol (LCP) packets used for signalling are flagged in the first octet. Three packets form a start transaction and a single packet is used to end a session. These packets contain the attributes required for targeting, triggering and filtering a session.

The following figure illustrates how the three layers are applied to meet the needs of our example.

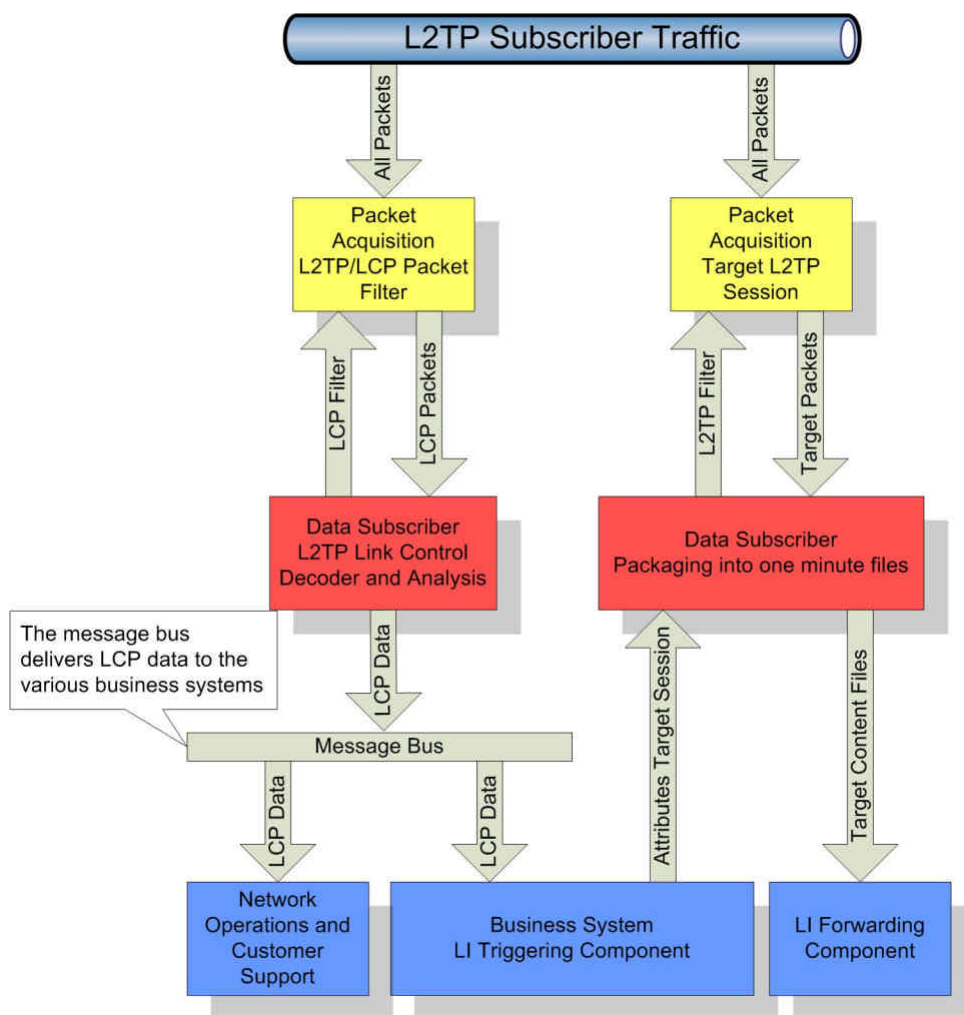


Figure 3 - Telemetry and LI solution for L2TP

9.1 PACKET ACQUISITION

Using a packet filter of an operating system with a network interface card operating in promiscuous mode can easily provide the packet acquisition layer.

When selecting an operating system, it is important to select one that has a packet filter that operates in kernel space. One of the biggest issues that effects performance is context swapping between user and kernel space. If packet filtering and acquisition is performed in user space, the kernel must swap context for each packet delivered by the network interface card in order to determine whether to keep it or not.

When considering that the filter must process tens of thousands of packets per second, context swapping to user space for the purpose of filtering will quickly lead to the kernel dropping packets due to the fact that they are not being processed fast enough.

Operating systems like MAC-OSX runs the Berkley Packet Filter (BPF) in kernel space. Abstracted through the Pcap library, filter strings are passed to the BPF and only the required packets are passed from the kernel to user space dramatically improving the performance of packet acquisition.

The filtered packets can be streamed between the packet acquisition layer and a data subscriber by using standard IPCs. When a data subscriber resides on the same machine as the packet filter, UDP sockets can be used as a light IPC, and because it is local, will not incur any reliability issues.

Where the data subscriber is on a remote machine, streaming using the FTP protocol works well. FTP is reliable, simple and can be secured using Transport Layer Security (TLS).

9.2 DATA SUBSCRIBERS

Our example requires two data subscribers: -

- An LCP protocol analyser
- A target session packager for LI

9.2.1 LCP DATA SUBSCRIBER

The LCP data subscriber requests only LCP packets by using a filter for UDP 1701 packets with the LCP flag set in the first octet of the L2TP header. LCP uses three packets to form a session creation transaction.

These packets are: -

- Incoming Call Request
- Incoming Call Reply
- Incoming Call Connected

A simple protocol analyser (contained with the data subscriber) looks for three packet combinations that form a start session transaction. Combining attributes from the three packets of a transaction, the protocol analyser forms a data structure that is encapsulated into a session creation message.

A similar process is used to end an L2TP session, however, only one packet is used. The Call Disconnect Notify (CDN) packet is sent from the LAC to the LNS when a session is ended. When the protocol analyser identifies a CDN packet, it forms a data structure that is then is encapsulated into a session end message.

These messages are then broadcast on a message bus to the business systems layer. In our example the business system layers are the support and LI system.

9.2.2 LI PACKAGER DATA SUBSCRIBER

This data subscriber passes a filter to the packet acquisition layer which is designed to acquire all and only packets for a target L2TP session. The arguments used to form the filter are passed to the data subscriber by the layer that has acquired the arguments from the LCP data subscriber.

In this example, packets received by the data subscriber are packaged into approximately one minute files and transported back to the business systems layer via FTP.

9.3 BUSINESS SYSTEMS LAYER

In this example there are three components in the business layer.

9.3.1 OPERATIONS SUPPORT COMPONENT

Using a message que subscriber, messages generated by the LCP data subscriber are received and stored in a database. When a session create message passed to the message bus, a record is inserted into a database. When an end session message is received, the associated session record is deleted from the database leaving only active session records.

A website provided by the business systems layer can provide simple access to the session information contained within the database. Connection information buried deep in a network that is only available to an elite few who can access core devices, can now be easily obtained by other support staff without risk.

9.3.2 LI TRIGGERING COMPONENT

Similar to the Operations Support Component, the LI Triggering Component also receives messages from the LCP Data Subscriber via the message bus and persists the messages in a database.

Contained within these LCP packets are the attributes that form a filter to acquire an individual session. Also contained in the LCP packets are Attribute Value Pairs. The LCP Data Subscriber decodes the AVPs and includes them in the create message.

Depending on the specific implementation of L2TP at a CCSP, the AVPs can be used for target identifiers. Two commonly used AVPs are: -

- Proxy Authentication Identifier -DSL
- Calling Line Number – Dialup

LI Triggering Component parses each create session message passed from the LCP Data Subscriber comparing the attributes to the target identifier provided in the warrant.

When a target service connects, the LI Triggering component acquires the tunnel/session identifiers from the create session message. An instance of the LI Packaging Data Subscriber is instantiated and the tunnel/sessions attributes passed to it.

When a session end message is received by this component, the Data Subscriber is notified to end the interception of the session.

If a warrant is served while the target service is connected, the session attributes are obtained from a list caching the L2TP session information.

9.3.3 LI FORWARDING COMPONENT

This component receives product files containing the target session packets from the LI Packaging Data Subscriber.

Along with the target identifier, the warrant will also have FTP server information for the Monitoring Centre (MC) to where the product files are to be delivered. The component formats the files are per the LEA requirements and then forwards them via FTP to the MC.

9.4 TARGET IDENTIFIERS

When looking at the L2TP example, the amount and type of target identifiers are limited to the AVP attributes. The number and types of target identifiers be extended by adding a RADIUS data subscriber.

When considering that RADIUS is commonly used to authenticate users as they enter a network via L2TP, there are attributes that can be used to join the RADIUS authentication transaction with the LCP session creation transaction.

By creating a RADIUS data subscriber that provides authentication messages, the data can be merged with the LCP session creation messages to extend the types of target identifiers.

10 SUMMARY

By changing the approach to lawful interception, a return on investment can be achieved from what was once a cost burden.

Using a passive approach to facilitating a telemetry system that supports a CCSPs business system as well as Lawful Interception can deliver agility to business systems that support core business activities.

Using a layered approach, compartmentalisation can occur between the various IT divisions of a CCSP delivering what was once inaccessible network and subscriber related data to the various business units.

11 REFERENCES

TELECOMMUNICATIONS ACT 1997,

<http://scaleplus.law.gov.au/html/pasteact/2/3021/top.htm>

Lawful Interception of the Internet, Vol.1 No.1

Author: Phillip Branch

http://www.swin.edu.au/sbs/ajets/journal/issue1/a_branch1.htm

Surviving Change

Building redundancy into the one system that never has backups: the human system

Author: Andrew Frederick Cowie

<http://www.operationaldynamics.com/reference/talks/SurvivingChange/>

Design and Implementation of DSL-Based Access Solutions

Author: Sanjeev Mervana and Chris Le

Publisher: Cisco Press

ISBN: 1-58705-021-8