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

Hammond Street Developments Pty Ltd

Lawful Interception

Generic Traffic Interception System

Owner	Hammond Street Developments Pty Ltd
Author	Michael Nancarrow
Classification	Confidential

COMMERCIAL-IN-CONFIDENCE

Classification – Confidential

Contents

Introduction

Over the 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 in a similar manner to performing LI from switched, voice networks.

Hammond Street Developments Pty. Ltd. (HSD) has been working with LEAs, Carriers and Carriage Service Providers (CCSPs), including Internet Service Providers and Telecommunication Companies to develop an LI solution for Internet Protocol (IP) services.

HSD has undertaken extensive research and development work to provide solutions that will assist CCSPs and LEAs in providing LI services. A system called the Generic Traffic Interception System (GTIS) has been developed in line with the LEAs and CCSP requirements. GTIS is currently installed at major CCSPs around Australia and is providing valuable product for evidence and intelligence purposes.

HSD has taken an approach to LI where the acquisition of Internet content is strictly lawful and driven by the parameters of a Warrant. GTIS is far more than just another network probe or wire tap. GTIS fully encompasses the application of a Warrant for the lawful acquisition of Internet content for target subjects.

GTIS is designed to reduce the risk of LI for all stakeholders. When LI Warrants are served on a CCSP, there needs to be a solution that is designed to securely and discreetly acquire only target service content and quickly move the content to a LEA Monitoring Centre (MC) for analysis.

The following list identifies the key design considerations behind GTIS.

1. Ensure that an LI Warrant is executed only within its parameters;
2. Acquire all IP traffic for a target service and minimise the risk of intercepted data being accidentally or deliberately obtained by unauthorised entities;
3. Ensure that only traffic for target service is acquired;
4. Acquire connection (session) related data for a target service;
5. Protect the identity of target services, package and encrypt all target content as quickly as possible;
6. Provide a readily available and consistent solution that simplifies the implementation of interception systems and reduces the number of people involved in implementing a Warrant;
7. Reduce the time taken to deliver intercepted data to an LEA;
8. Reduce the risk of losing data due to system failures;

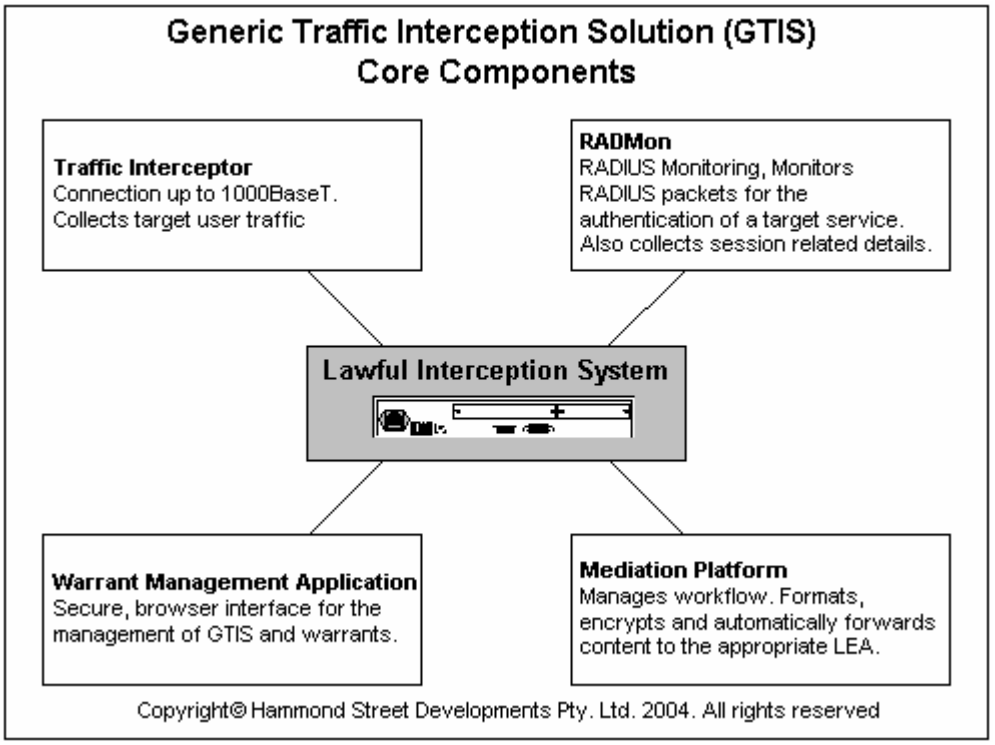
Network probes are easy to implement, however, GTIS provides a mediation platform, user interface, forwarding service and authentication integration to exactly orchestrate an LI Warrant. GTIS simplifies the capture of Internet services and ensures that the content is delivered in a secure and timely manner to the appropriate LEA.

About GTIS

HSD provides a complete collection of products, solutions and services designed to securely acquire IP packets and session related data for a target services and deliver the content to a LEA monitoring centre.

Together, these products are known as the 'Generic Traffic Interception System' (GTIS). The word Generic implies that the interception solution can be adapted into a broad range of network implementations including DSL, dial-up and ATM networks.

The following diagram depicts the core components of GTIS.



Traffic Interceptor

The GTIS Traffic Interceptors are able to acquire selected traffic from within a 10/100 or Gigabit Ethernet connection. Designed to be installed in geographically disperse locations (remote and local pops), target IP content is able to be captured, cached, and forwarded to a central GTIS Mediation Platform. The Traffic Interceptors can also acquire complete L2TP sessions.

RADMon

Remote Authentication Dial-In User Service (RADIUS) is the most commonly used authentication protocol used by CCSPs. RADMon (RADIUS Monitoring) monitors the RADIUS protocol scanning all packets for the authentication of a target service.

RADMon allows GTIS to transparently integrate with RADIUS servers. Used for triggering of interception and the collection of session related data, RADMon extends the range of attributes that can be used to identify target services and seamlessly initiate interception. LI Warrants can use username, calling line identifier (CLID), IP address or many other of the RADIUS attributes to identify a target service.

GTIS Mediation Platform

The Mediation Platform is the Hub of the solution. Regulating the workflow of the entire system, the Mediation Platform executes a Warrant exactly within its parameters. Controlling the activities of RADMon and the Traffic Interceptors, captured target content is stored, formatted, encrypted and automatically forwarded to the appropriate LEA within minutes of acquisition.

Warrant Management Services

Providing a fully functional secure web site, users and administrators can easily manage and monitor Warrants, logs and the other components of the GTIS solution.

The Warrant Management Application (WMA) has two user groups. Administrator and User. The Administration account is used by authorised staff that are responsible for the creation and management of Warrants. The user account can be provided to technical staff when assisting with support. The user account does not reveal any target or Warrant specific information. The administrator account provides the complete functionality of the WMA.

Security and Logging

Access to the website is over HTTPS and is usually restricted to a single IP and/or users that have a security certificate.

GTIS implements multiple layers of security to protect sensitive management and intercepted information. All servers and components used in GTIS are strengthened against attack and can only be accessed by authorised staff using secure communication protocols.

All maintenance user activities are fully logged and controlled. Service and maintenance of GTIS can occur remotely without sensitive information being available to support staff. Audit trails are generated by the Warrant Management Services web site and are designed to meet the harshest of investigations. The audit trails provide a level of detail on user and administrators activities.

GTIS is designed to protect the right to privacy while delivering information to LEAs within the parameters of an authorised interception Warrant.

The operating system has also been hardened against attack. The use of firewalls, IPsec tunnels and certificates all contribute to system security.

All sensitive data stored in the GTIS database is encrypted and target service content is only stored for the time needed to transfer it to an LEA monitoring centre.

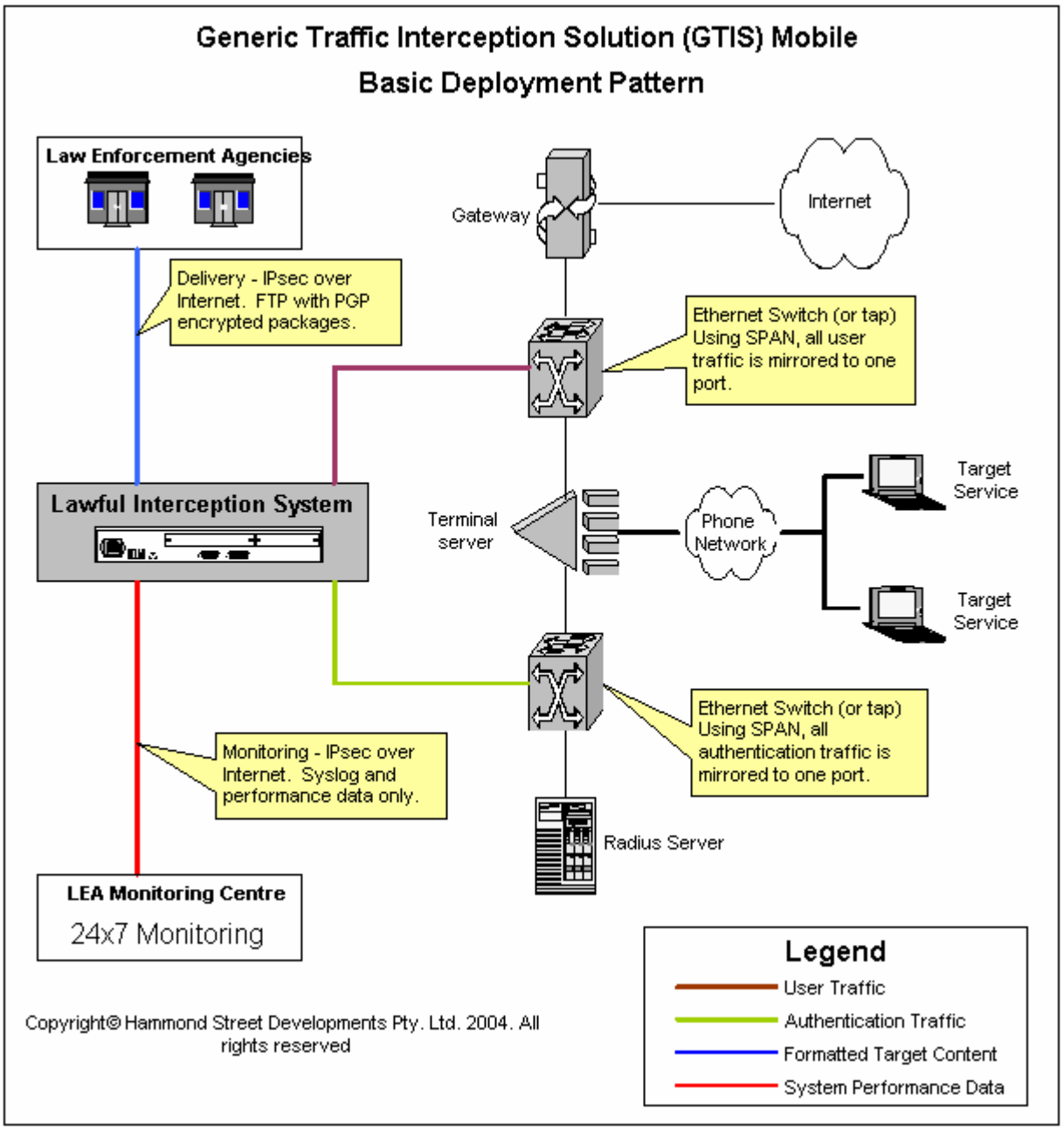
Deployment Options

Modular by design and built using Java and C++, GTIS scales easily. The software is designed to operate on the BSD, Solaris and OSX/Darwin operating systems.

GTIS Mobile Solutions

While HSD has delivered many multi-server solutions to CCSPs, the need for a mobile solution that LEAs could readily deploy became evident.

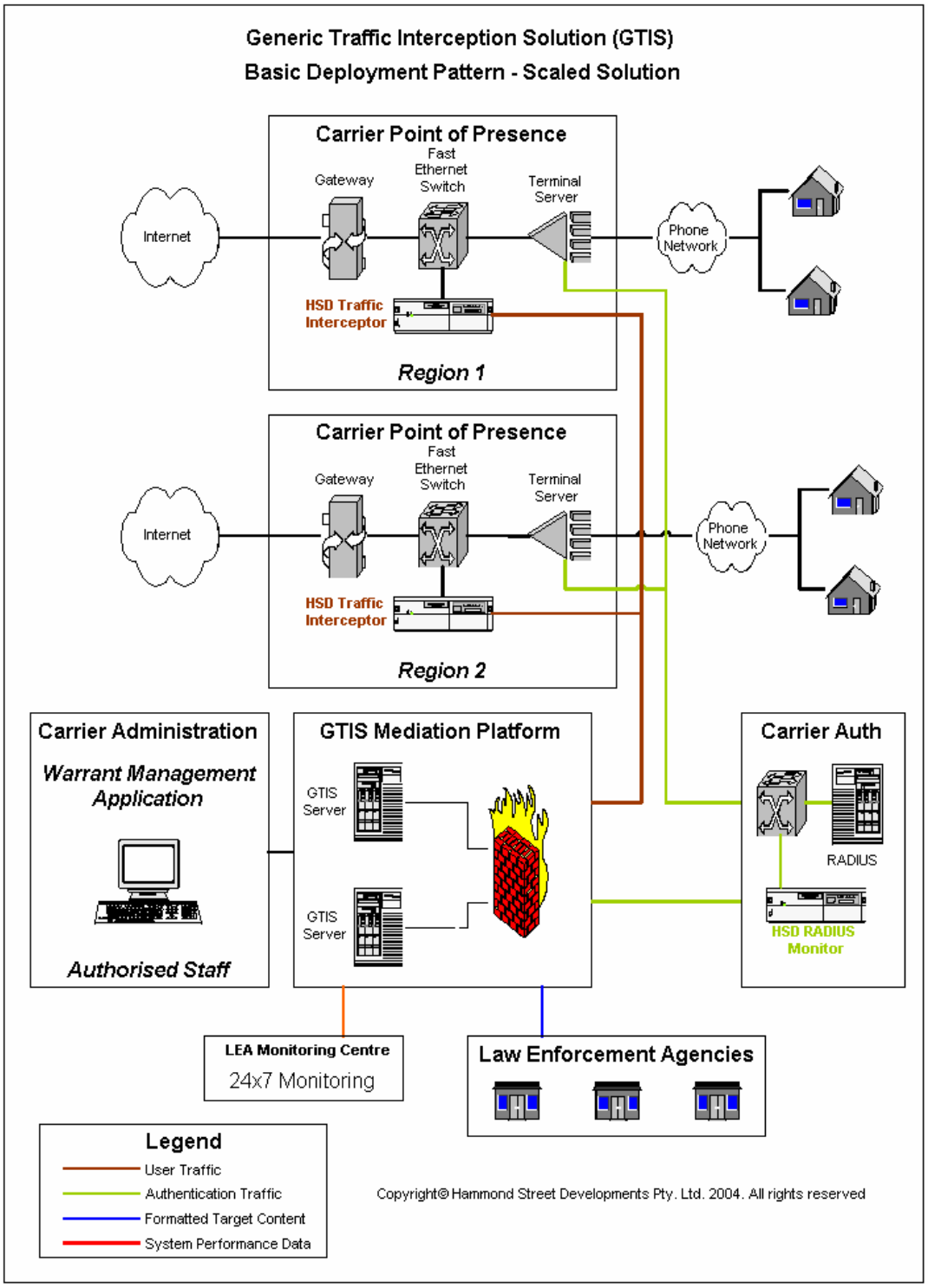
The HSD research department has set about combining all GTIS components into a compact solution that can be easily transported and implemented into a CCSP network with a minium of fuss. From the research, GTIS Mobile was born and has proven to be very useful and popular with Australian LEAs.



GTIS Permanent Solution

Removing all dependencies on ASIC (application-specific integrated circuit) based devices for packet filtering, GTIS can scale from an Apple G4 Powerbook to a large multi-server environment.

Any of the components can be installed on individual or multiple servers. Even the GTIS mobile systems can have additional Traffic Interceptors and RADMon servers attached to it. The Mediation Platform seamlessly manages multiple Traffic sniffers that can be located any where an Internet connection is available.



Specification

Providing all interception components on a 1RU Apple Xserve, LEAs in Australia have available to them a system that can quickly be deployed and offers all of the functionality and security provided by a large multi-server, fixed implementation.

Output Files

For each Warrant, GTIS produces a series of files for the management of Warrants and related content. Each Warrant is assigned to a LEA Monitoring Centre providing for multiple Warrants to be hosted by GTIS.

Unless an LEA obtains access to the Warrant Management Application there is no way of one LEA knowing about Warrants of another Agency.

The output files are designed to assist an LEA in creating automated workflows, monitoring and decoding systems. Nevertheless, the files can be easily manually processed in the situation where there are no automated systems.

The following table identifies the files: -

File Type	Description	Format	Purpose
Warrant Start	Sent when a Warrant is started	ASN.1	Workflow
Warrant End	Sent when a Warrant expires	ASN.1	Workflow
Warrant Suspend	Sent of a Warrant is suspended	ASN.1	Workflow
Warrant Resume	Sent when a Warrant passes the suspension end period	ASN.1	Workflow
Target Service Suspend	Sent if a target service is suspended		Workflow
Target Service Resume	Sent if a target service is resumed		Workflow
Session Start	Sent at the beginning of a target session	ASN.1	Payload
Session End	Sent at the end of a target session	ASN.1	Payload
Target Content	Contains all ingress and egress packets for a target session. Sent in one minute packages	ASN.1 header, TCP Dump format.	Payload
Checksum	MD5 checksum for each file	Text	Workflow

Session start and end files contain session related data and are sent when a target service is either authenticated or disconnects from the network.

Target content files contain all ingress and egress packets for a target service while it is connected to a network. During a session, the packets are accumulated into files and sent every minute. Taking a simple dialup account for example, a packet will arrive at a LEA monitoring centre anywhere between 10 and 70 seconds after it has been collected.

The content of all files are encrypted using a PGP key provided by the LEA at the time that the Warrant is issued.

Mobile Configuration

The following specification is for a single server GTIS Mobile system.

Item	Description
Server Type	Apple Xserve 1RU, Dual G4 processors, 1Gig RAM, 2 x 60Gig HDD Mirrored
Operating System	OSX Panther
Connectivity	10/100/1000BaseT
GTIS Software	All Components
Delivery VPN	IPsec
File Encryption	PGP
File Delivery	FTP
Database Encryption	AES
Number of LEA Monitoring Centres	5
Number of Con-current Target Services	6
Maximum Throughput	8 M/Bit per second
Maximum Single Session Throughput	4 M/Bit per second
Maintenance Cycle	Every 400,000 content files
System Messages	Syslog

External, additional Traffic Interceptors capable of 10 con-current sessions with a maximum throughput of 60M/bits per second can be easily added and remotely controlled by GTIS.

Summary

CCSPs are a constantly evolving environment where little consideration is given to LI of Internet services. Historically, it has been a very slow, haphazard, and an arduous process to have a target service intercepted and delivered in a clean, secure and timely manner.

Without the availability of an automated solution, handling of sensitive data by too many people required to implement a Warrant has caused undue risk for the CCSP, LEA and target service.

Using GTIS Mobile, an LI Warrant can be implemented in a large environment with minimal disruption while maintaining an 'Arms-Length' approach between the LEA and CCSP. Quick to deploy, GTIS can be implemented in even the largest of networks on a case-by–case basis within hours of a Warrant being issued. If a GTIS system is already in place, then the timeline is reduced to minutes.

A CCSP is only required to provide an Internet Connection, and two network connections, one with all user data and another with authentication traffic. After this, an authorised member of a CCSP enters in the warrant details through an intuitive web based interface and GTIS manages the process from that point on.

Interception can be based on a fixed range of IP addresses or authentication based, ie, username. Target service data can also be collected from L2TP tunnels.