(54) Title: A SYSTEM FOR THE UNOBTRUSIVE INTERCEPTION OF DATA TRANSMISSIONS

(57) Abstract: An interceptor system (10) for lawful interception in a communications network overcomes the problem of requiring servers of considerable processing capacity by using a traffic interceptor (9) which is a hardware component such as a traffic analyser port (9) which intercepts the data and duplicates it sending one set of data to network filters (21). There is provided a management system which handles legal warrants for interception and through service filters (22) and a database (17) ensures that data which has a target identifier is transmitted onwards and the remainder is destroyed in a secure manner.
"A system for the unobtrusive interception of data transmissions".

Introduction

This invention relates to an interceptor system for the lawful interception of data communications in a communications network, the communications network comprising a plurality of user terminals, a point of presence (POP) server, a network access server (NAS) and a radius server, the communications network transmitting data having identifier data identifying at least the source and intended recipient of the transmitted data.

Due to recent changes in European law, managers of communication networks are now required, under certain circumstances, to provide law enforcement agencies with access to data transmissions occurring on their networks. Law enforcement agencies possessing a suitable warrant may compel the network manager to retrieve all communications made by or to a specified individual or entity connected to that network. There have also been relatively stringent guidelines and standards implemented which must be adhered to by the network manager when intercepting targeted communications. One such requirement is the necessity for the interception to be undetectable by the targeted individual or entity. This has proved to be particularly difficult when dealing with computer based networks.

Another disadvantage of the known systems is that several different architectures such as WAP, email and internet may be controlled by a single provider. This provider will have to supply a system to intercept data travelling on each network. This further increases the costs to the network manager.

Therefore, it is an object of the present invention to provide a system for the lawful interception of data communications in a data communications network that overcomes at least some of these problems and will allow interception of communications in an unobtrusive, more efficient manner.
Statements of Invention

According to the invention, there is provided an interceptor system for the lawful interception of data communications in a communications network, the communications network comprising a plurality of user terminals, a Point of Presence (POP) server, a Network Access Server (NAS) and a radius server, the communications network transmitting data having identifier data identifying at least the source and intended recipient of the transmitted data, characterised in that the system further comprises:-

a management system for the reception of a legal warrant containing target identifier data for interception of data transmitted, including the identifier data;

means to update a target identifier database according to the target identifier data received;

a Traffic Interceptor (TI) for intercepting data to and from one of the servers in an unobtrusive manner;

means to duplicate the data and allow one set of the duplicated data proceed to its desired destination in a seamless manner and pass the other set of the duplicated data as processing data to a network filter stage;

a network filter stage having access to the most recent target identifier lists, the network filter stage having a receiver for the processing data and a comparator for comparing the identifier of the processing data with the target identifier data in the target identifier database;

means in the network filter stage for separating the processing data into matching data in which the data corresponds to a target identifier data in the target identifier database and unmatched data;

means to transmit the matching data to a service filter for reconstruction of the data into a usable format;
means to delete the unmatched data in a secure manner; and

means to transmit the reconstructed data in a secure manner to the
management system for onward transmission in accordance with the legal
warrant.

The TI can be a Traffic Analyser Port (TAP) or layer 2 switch port which is spanned.
The advantage of having such a system is that the TI, when for example a TAP, can
intercept data in an unobtrusive manner. The data travelling through the TAP is
duplicated. Due to the fact that data is not redirected to another point in the network,
a delay is not introduced into the signal which could signal that the data was under
surveillance. Furthermore, because the TAP has no transmission lines, it cannot be
called by another entity and therefore is undetectable by a calling method. In addition
to these, because the TAP is a passive entity, the TAP is not susceptible to Denial of
Service (DOS) attack. Furthermore, the entire system cannot be accessed via the
network as data can only flow into the system from the network side and cannot flow
out. In addition to all of these, the target data may be retrieved in an efficient manner
and may be transmitted over a secure connection to the management system for
storage and eventual onward transmission to a law enforcement agency.

In another embodiment of the invention, the network filtering stage implements Policy
Based Routing (PBR) to filter unwanted data transmissions from the duplicated data
set as unmatched data. By using policy based routing, a significant amount of traffic
may be filtered out automatically. This will reduce the software processing
requirements of the system significantly and help reduce the costs. Data to and data
from a particular address or server may be filtered out from the processing data in a
simple and efficient manner.

In another particularly preferred embodiment of the invention, the network filtering
stage is provided by a layer 3 switch. By using a layer 3 switch, the switch may
implement policy based routing in hardware. This further speeds up the filtration of
the data as the filtering is now achieved in hardware rather than software. The cost
in both time and monetary terms of software processing of the data is much reduced
and the entire system becomes highly scaleable and much cheaper to assemble. Should the filtering demands of the system increase substantially, an additional switch may be added which would be far cheaper, for example, than installing further servers such as SUN servers.

In a further embodiment of the invention, the means to transmit the data in a secure manner to the management system is provided by way of a fast ethernet Local Area Network (LAN). This provides a secure and stable way to transmit data across the system. The TAP may be additionally provided with a dedicated line for connection to the network filter stage. By having a fast ethernet line and dedicated lines, a highly secure system will be operated. Attack from outside is prevented.

In a still further embodiment of the invention, there is provided means to dynamically update the target identifier database in response to retrieved data. If the target data in the target identifier database is a user name, the system may retrieve a temporary IP address for the target should he contact a radius server. The IP address may then be added to the target identifier database and communications to and from that IP address may be traced. This will allow for a much more comprehensive system. Items may also be removed from the list thereby preventing clogging the list up with data that is no longer relevant.

In another embodiment of the invention, there is provided a WAP server and the TAP intercepts data from the WAP server in an unobtrusive manner. Alternatively, there may be provided an SMTP server in which the TAP intercepts data from the SMTP server. In addition to this, there may be a DHCP server and the TAP intercepts data to and from the DHCP server in an unobtrusive manner. As an alternative to the above, the system may have target identified data comprising an IP address and the TAP intercepts data to and from that IP address in an unobtrusive manner. The system can be adapted to intercept a variety of different technologies and data formats and retrieve data from them. The important thing is that there is provided the software to reconstruct the data from the LEA or if it is encrypted, to decrypt the data using the network managers decryption keys. Several different data transfer methods can be accessed by the one system, thereby negating the need from the network manager to increase his expenditure and purchase a different interception
system for each network he controls. By having the flexibility of the allowing
interception of multiple technologies, the network manager will also reduce his
training costs as personnel will only have to familiarise themselves with a single
system.

In a further embodiment of the invention, there is provided a system in which the
service filter is provided with a protocol service filter for each protocol to be
intercepted in the communications network. This will allow for one system to handle
a multitude of different technologies and report them to a single point.

In a further embodiment of the invention, the management system further comprises
an Intercept Region Manager and Delivery Manager. This will reduce the workload of
the Delivery Manager by providing Intercept Region Managers (IRMs) that can control
the local network filter and service filters at a local level. Certain networks may
comprise several IRMs and the Delivery Manager can be used to control and
synchronise the IRMs by keeping all the IRMs with the most up-to-date data.

In a still further embodiment of the invention, the Intercept Region Manager further
comprises a Network Filter Manager and Service Filter Manager. The IRM may have
these to control the several network filters and service filters under its control. The
managers can keep their filters synchronised with the most up-to-date information.

In a further embodiment of the invention, the Delivery Manager further comprises
means to receive and process a warrant from an Law Enforcement Agency (LEA) as
an active warrant, means to store the active warrants and assign a unique target ID
to each warrant, storage means to store data pertaining to the Intercept Region
Manager and means to establish a secure connection to a LEA and transmit
matching data to the LEA. By having such a system, the Delivery Manager may
authenticate a warrant and associated target data before updating any databases.
The Delivery Manager can also be concerned with obtaining secure transmissions of
data which will not delay other functions of the system by keeping this feature
separate. At the Delivery Manager, there may be provided a billing means to
calculated and bill out information that was retrieved for an LEA.
In another embodiment of the invention, there is provided a method of unobtrusive interception of data communications in a communications network comprising a plurality of user terminals, a POP server, a NAS server and a radius server, the method comprising the steps of receiving a warrant from a Law Enforcement Agency containing target identifier data; entering the target identifier data in a target identifier database and comparing the processing data with target identifier data in the target identifier database, characterised in that the method comprises the steps of:

intercepting the data communications to and from one of the servers in a non-obtrusive manner by passing the data through a traffic interceptor;

duplicating the intercepted data and allowing one set of the duplicated data proceed to its desired destination and passing the other set of the duplicated data as processing data to a filter;

extracting any data which matches with target identifier data and passing that data to reconstruction filters for reconstruction of that data into usable format;

deleting the remaining unmatched processing data in a secure manner; and

passing the reconstructed data to a management system for the onward transmission to a Law Enforcement Agency.

This method will allow the data communications to be retrieved without the target being aware of any surveillance taking place. There is no trace of the data being duplicated and there is no way for the target entity to find out whether his transmissions are being monitored. Furthermore, it is a relatively simple and inexpensive method to implement.

In another embodiment of the invention, the method includes the step of filtering according to policy based routing. This will enable the filtering to be done predominantly in hardware and avoid excessive processing requirements.

In another embodiment of the invention, the method includes the steps of passing
data through a layer 3 switch. All the benefits of the layer 3 switch, including policy based routing, may be used by the method, thereby decreasing the processing requirements and decreasing the time taken for filtering the data.

In another embodiment of the invention, there is provided a method which includes the step of dynamically updating the target identifier database with data retrieved from the network. By keeping the database updated at all times dynamically, the system may add and delete information from its database as it becomes no longer relevant. Also, the most up-to-date information is sent to all IRMs so that they may monitor all forms of communication used by the target entity.

In another embodiment of the invention, the communications network further comprises a WAP server and the method includes the step of intercepting the data communications to and from a WAP server.

Alternatively, the communications network further comprises a SMTP server and the method includes the step of intercepting the data communications to and from the SMTP server.

The method may also include the steps of monitoring an IP address and intercepting data communications to and from that IP address. In addition to these, the communications network may further comprise a DHCP server and the method includes the step of intercepting the data communications to and from the DHCP server.

In essence, several different technologies may be catered for by the one data communications interception method.

In another embodiment of the invention, the method includes the step of generating billing information according to the data downloaded to the management system. This will enable the ISP to recoup some of the costs in implementing one of these systems by billing the LEA for data obtained over its network.

Preferably, suitable GURs may be provided in a known manner.
Detailed Description of the Invention

The invention will be more clearly understood from the following description of some embodiments thereof, given by way of example only, with reference to the accompanying drawings, in which:

Fig. 1 is a diagrammatic view of the system for the lawful interception of data according to the invention;

Figs. 2 and 3 are flow diagrams of one way of carrying out the invention, and

Fig. 4 is an overview of service filters used in the invention.

Referring to the drawings and initially to Fig. 1, there is illustrated the internet 1 and an access network 2, having dial up input devices 3 and permanent IP connection devices 4, all of which are fed through routers 5 and load balancers 6 to an internet service provider network (ISP) 7, either by wires or wireless connectors 8. Traffic interceptors 9 are provided in this embodiment by traffic analyser ports (TAP) node which in turn feed through an interceptor system, indicated generally by the reference numeral 10, through dedicated lines 11. The interceptor system 10 is illustrated as a lawful interception mediation device for IP (LMD-IP) connected to a lawful interception middleware (LAN) 12 and a lawful interception management system (LMS) 13. Essentially, the LMS 13 enables the set-up of maintenance of lawful interception ancillary services, while the LMW is the middleware product which includes message routing, queuing, formatting and protocol conversion which enables this LMW 12 to communicate with third party systems, for example, mediation devices. However, these are not described in any more detail below.

The interceptor system 10 includes a management system 16, referred to sometimes as a management and delivery system, connected to a target identifier database 17 and is fed through an Intercept Region Manager (TRM) 18, a network filter stage, indicated generally by the reference numeral 20, which network filter stage 20 comprises a receiver filter 21 and service filters 22.
Referring now to Figs. 2 and 3, if a legal law enforcement agency (LEA) issues a warrant in step 100 the warrant is then sent to the management system where in step 102, it is either accepted in step 103 and the target identifier database 17 is updated or alternatively, in step 104, it is rejected. Similarly, if a customer has a warrant and provides it in step 101, the same procedure takes place. However, with customer warrants, they may not necessarily always allow full interception. For example, the type of interception the customer could require would have to be closely monitored and agreed under general legal data protection law in the particular jurisdiction. However, it is envisaged that, for example, a customer might be able to have monitored and downloaded, all traffic to certain sites e.g. for suspected industrial espionage which could give rise to a court order following interception and delivery to a third party and not a LEA.

In step 104, traffic is received and then in step 105, it is duplicated. In step 106, one set of the traffic is transmitted onwards seamlessly and the other set of the traffic in step 107 is transmitted to the system where the database is again consulted and in step 109, a match is queried and either there is no match, in which case, in step 110, the data is destroyed, or, if there is a match, then in step 111, the data is processed and delivered to the law enforcement agency or customer, as required by the legal warrant.

It will be appreciated that the lawful interception mediation device for IP (LMD-IP) enables ISPs to intercept IP traffic concerning targets for whom a valid warrant has been received from a Law Enforcement Agency (LEA). As will be seen from the above, the target's traffic is intercepted on the ISP's network based on its assigned IP address or on specific application level attribute values. The intercepted traffic content together with associated intercept related events are delivered to the Law Enforcement Monitoring Facility (LEMF). Obviously, these will vary from organisation to organisation.

Essentially, the LMD-IP comprises the following modules.

The management system 16 or what is effectively delivery and management D&M
18 which is responsible for receiving the intercept warrant and forwarding the
information to the Intercept Region Managers IRMS 18. Subsequently on reception
of the resulting intercepted traffic it formats the data for delivery to the LEMF. The
D&M is responsible for the delivery of the intercepted data to the monitoring
facilities. The architecture allows for the deployment of distributed Delivery Agents
throughout the network.

Intercept Region Manager, IRM 18, is located at each of the interception points on
the network and ensures that the active Service and Network Filters at the local
interception point are updated as targets are added and deleted. In addition as
dynamic information pertaining to an active intercept is learnt the IRM ensures the
appropriate Filters remain synchronised. The interaction between the IRM and the
Service and Network Filters 21 and 22 is shown in Fig. 1 An RPC based
middleware component is provided to allow for the deployment of geographically
dispersed interception nodes.

Service Filter (SF) 22, reassembles the IP application data streams and applies
filters based on the application layer protocols. The intercepted traffic is encrypted
and forwarded to the management system 16 for onward delivery. The service filter
implements filtering of IP data.

Network Filter (NF) 22, filters traffic based on layer 3 and 4 protocol information.
The packet's source and destination IP addresses and port numbers are compared
against the defined filters and candidate traffic forwarded to dedicated service
filters. The NF implements stateless filtering of datagrams. Traffic flows requiring IP
reassembly, for example SMTP data, are forwarded to specific Service Filter
nodes. All other traffic is load balanced by the network filter 21 to a logical grouping
of service filter nodes. The network filter 21's functionality is implemented in
dedicated Commercial Off the Shelf (COTS) hardware using the policy based
routing feature of COTS L3 switch/routers. Due to the high volumes of data only L3
switch/routers supporting hardware based implementation of access lists are
deployed. The network filter 21 is not further discussed in this specification.

The Traffic Interceptor (TI) 9, as explained, duplicates the traffic on the ISP's
networks and forwards it to the network filters 21. The TI's 9 are dedicated hardware devices which may be realised using Traffic Analyser Ports (TAP) nodes or alternatively by spanning a Layer 2 switch's port. The TI 9 ensures that traffic can only flow from the backbone to the network filter 21 and that no traffic flows from the network filter 21 to the backbone. The TI 9 is not further discussed in this specification as such hardware construction and functionality is well known.

All communication between the IRM 18 and the Filters 20 is achieved using a physically isolated Fast Ethernet LAN thus ensuring only the IRM 18 can communicate with the Filters 20. In addition, as the network filters 21 are physically isolated from the ISP's backbone, via the Traffic Interceptors 9, they are not detectable from the ISP's network. The traffic intercepted by the network filter 21 is forwarded on dedicated point-to-point links to the relevant service filter 22. The communication between the D&M 18 and IRM 18 may optionally be configured to use either a secure or non-secure transport connection based on the deployment topology.

The management system or DRM 16 provides the external interface to the LMD-IP. It allows for the activation of warrants and delivery of the intercepted data to the specified LEMF. On reception of a warrant, the management system 16 stores the warrant information within the database 17. If required, connections are established to the specified LEMF delivery points. Any information useful in identifying the target is forwardable to the IRMs 18 for onward propagation to the Service and Network Filters 21, 22. The identification information specified may include one of more of the following: the target's email address(es), user name, hardware address, MSISDN and permanent IP address, if available. Other suitable identifiers may be added.

The management system or D&M 16 provides time synchronisation between the components modules and is comprised of various components detailed below.

An Interception Management Controller handles all interaction with external users concerning the adding and deleting of validated warrants. Activation requests received from either the User Interface or LWM are recorded in the database 17.
prior to onward propagation to the interception points. The received warrant will necessarily contain data relating to the target's identification together with delivery instructions. Only data pertaining to the identification of the target is forwarded to the Intercept Region Managers 18.

The database 17 is a repository of all active warrants and acts as a central data store for other components of the system. New warrants received are stored and a unique target ID assigned to them prior to being forwarded to the Intercept Region Managers 18.

A region manager store is provided and maintains data concerning all Intercept Region Managers 18 under the control of this management system 16. Information regarding the connectivity to each of the IRMs 18 is stored together with details of the current status of the particular interception nodes.

A Delivery Point Directory is provided and is responsible for the establishment and maintenance of secure connections to the Law Enforcement Monitoring Facility. The establishment of secure communications requires both server and client side authentication. On reception of a warrant specifying a delivery LEMF to which no communications are established this module initiates connectivity. Failure to establish connectivity results in the warrant being rejected.

A delivery agent module receives the data from the interception nodes. The data consists of intercepted related events, IRI, together with the intercepted content (CC). The Delivery Agent is responsible for formatting the data for delivery to the LEMF.

In the scenario where data intercepted for a target has been encrypted by the local ISP it is the responsibility of the Delivery Agent to invoke the decryption of this data prior to delivery.

The module receives management information form the interception nodes, i.e. traffic interceptors 9, which it forwards to the Region Manager Store. In addition management information is generated to enable subsequent billing for the
interception service.

As explained above, the Intercept Region Manager 18 is responsible for the local management of the interception points on the network. As detailed above, each interception node is comprised of a number of service filters 22 and network filters 21 together with components required for the management of these entities. The IRM 18 consists of a Service Filter Manager and a Network Filter Manager.

The Service Filter Manager function of the IRM 18 is responsible for managing the communications with the Service Filters 22. It ensures that all target identification data specified in the received warrant is propagated to all Service Filters 22. As the set of identification information changes during the lifetime of a warrant, such as a dynamically assigned IP address, the Service Filter Manager ensures all SFs under its control remain synchronised.

The Service Filter Manager is the point of delivery for all data originating at the service filters 22. The data received from the service filter 22 includes:

- Intercepted data for delivery to the management system D8M 16. This data is forwarded to the Delivery Agent for onward delivery to the LEMF.

- Generated alarms which are forwarded to the management system 16.

- Keep-alive messages. On failure to receive a keep-alive message from a particular service filter 22 within the allotted time the Service Filter Manager forwards an alarm to the management system D8M 16.

- Network events to be delivered to the LEMF. These events are forwarded to the Delivery Agent located at the management system D8M 16. In addition, these events may result in updates being forwarded to a Network Filter Manager, forming part of the IRM 18 and described below, and may require the re-synchronisation of the Service Filters 22.

The Service Filter Manager handles the synchronisation of time between all the
filters 20.

The Network Filter Manager module manages the dedicated network filter 21 hardware. Network filtering is based on the use of the Policy Based Routing, PBR, features of L3 switch routers. PBR allows the forwarding of datagrams based on a combination of source and destination IP addresses and port numbers. This feature allows the filtering of traffic streams of interest thus greatly reducing the volume of traffic to be processed by the service filters. The following is an example of the streams typically of interest:

- traffic to and from the SMTP server
- traffic to and from the POP3 server
- traffic to and from the Radius server, described below
- traffic to and from IP Addresses assigned to targets

The Network Filter Manager allows the dynamic configuration of filters as targets are added and removed and IP addresses assigned and unassigned to these targets.

The Network Filter Manager is comprised of two components. The device independent component presents a view of the configured system while at the same time abstracting the device specific details. This component permits the initialisation and status monitoring of the device together with allowing the adding, deleting and viewing of the configured filters. The device dependent component maps the device neutral view of the system configuration to the particular L3 device. This clean separation between the two components provides a flexible approach in allowing for the deployment of different vendor devices as dictated by the customer's network topology.

When supported by the device the Network Filter Manager supports the configuration of load balancing across multiple ports to the relevant service filter 22.
The service filtering sub-system of service filters is responsible for filtering on application level data streams and determining if the traffic is to be intercepted. The service filter 22 is a software component that comprises one or more service filter functions together with supporting functionality. A service filter function is provided for each protocol to be filtered. On detecting data to be intercepted the service filter 22 formats the data as required for delivery to the LEA. The physical delivery of the data to the LEMF is the responsibility of the management system D8M 16. An overview of the service filter functionality is shown in Fig 4.

At an interception point multiple instances of Service Filter platforms can be deployed as dictated by the volume of data to be intercepted. The co-ordination between the deployed service filters 22 is the responsibility of the Service Filter Manager.

The Service Filter 22 module is comprised of a number of components, including, an IP re-assembly module, filter module, a Local Delivery Manager and Local Manager protocol service filters.

The IP Re-assembly module receives the incoming IP datagrams and builds up the TCP/UDP data streams. Users of the service register with the module by specifying what application protocol streams are of interest. An application data stream is specified via the following parameters:

- the protocol type, UDP / TCP,
- an associated well known port number,
- optional server IP address,
- an indication as to whether all data streams or a specified subset, i.e. only those originating externally or matching specific targets' IP Addresses, are of interest.

On reception of a datagram the protocol type together with the source and
destination port are compared against the list of registered users and if a match occurs the IP datagram is reassembled in an IP reassembly module. The reconstructed application protocol data of the specified type is then forwarded to that registered user. All other datagrams are forwarded unassembled to a default service level filter. The default service filter handles raw IP datagrams and is not concerned with the application data stream. The information passed to the service user includes the source and destination IP Addresses and port numbers together with the received application data stream. All non-IP traffic received is discarded by the module. The module is implement over a libpcap interface (see Fig. 4). The libpcap provides a system independent interface to enable portability between different operating systems.

This filter module maintains the list of active targets. The target identifier information is maintained in such a manner as to allow fast matching of targets based on the specified selection criteria. The module includes the matching of targets based on email address, IP address, user name, MSISDN and hardware address. On the matching of an entry in the active target list the corresponding target-ID is returned. The module also provides an indication as to whether a specified address is internal or external to the domain.

Intercepted data passed to the Local Delivery Manager is formatted for delivery to the Service Filter Manager. The module packages the call content (CC) data based on associated target-ID and ensures its delivery to the SFM in a timely manner. The intercepted data is interpreted by the module and where required an associated intercept related information (IRI) event is generated and forwarded to the SFM.

The Local Manager handles all communication with the Service Filter Managers. The data exchanged includes updates to the active target list received from the SFM together with the data intercepted by the active Service Filters being forwarded to the SFM.

Management information is also exchanged between the SFM and Local Manager. The module maintains information on the local platform including counters and thresholds and is responsible for the generation of alarms and keep-alive
messages.

The protocol service filters interpret specific application level data flows and intercept data pertaining to active targets.

A Radius Service Filter module registers with the IP Re-assembly module for the interception of traffic to and from the Radius server and thus detects when a temporary IP address is assigned to a target (Network Login) and additionally, when the temporary IP address is unassigned.

The User-Name attribute contained in either in a Radius Access Request or Start Accounting-Request is passed to the Filter Module which returns an indication as to whether it identifies a target for which a warrant is open. For an active target the target-id is returned. The Service Filter extracts the Framed-IP-Address either from the Accounting request or from the subsequent Access Accept and forwards the event to the Local Delivery Manager. If the user specified in the Radius packet is not the subject of an outstanding warrant the data is discarded.

On detection of a Radius Stop Accounting-Request indicating the termination of a session for an active target the module informs the Local Delivery Manager.

A POP3 Service filter receives all data transferred to or from the POP3 server from the IP Re-assembly module. The User attribute of the POP3 data stream is passed to the Filter Module and if it matches a target the associated target-ID is returned and assigned to the data stream. The Local Delivery Manager is informed that an email read event has occurred. All subsequent traffic received for the specific target is forwarded to the Local Delivery Manager. On termination of the TCP connection all local data is discarded and the Local Delivery Manager informed.

All data between to and from the SMTP server is forwarded to the SMTP Service Filter by the IP Re-assembly module. The RCPT and FROM attributes are extracted from the application data stream and passed to the Filter Module. If one of the attributes matches an active filter the associated target-ids, if any, are returned. If no target-id is returned the data stream is discarded. Otherwise the
message content and associated target-ID is forwarded to the Local Delivery Manager.

A WAP Server Filter receives all data to and from a WAP Gateway.

The associated MSISDN attribute is retrieved from the data stream and passed to the Filter Module. If a target-id is returned the data stream is passed to the Local Delivery Manager. Otherwise, if no target-id is returned, the data is discarded.

A DHCP Service Filter processing the intercepted DHCF traffic flows between the client and the DHCP Server(s). The client hardware address, chaddr, specified in the DHCP Acknowledgement is passed to the Filter Module and compared against the list of active targets' hardware addresses. If a match occurs the IP Address specified in the Acknowledgement is extracted.

The Local Delivery Manager is informed of the new IP Address together with the associated target ID.

On detection of the Release of the DHCP assigned IP Address the Service Filter informs the Local Delivery Manager of the event.

A SSL Decryption module intercepts https traffic between the ISP’s Web Server and the known target identified by the target's assigned IP Address. The encrypted data together with the associated target-ID is forwarded to the Local Delivery Manager for deciphering and forwarding to the LEMF.

This approach avoids the necessity of propagating the ISP’s private key to the interception nodes. However it requires that the ISP provides an interface to retrieve the secret key associated with the target’s SSL session or alternatively that the ISP’s makes available its private key to the D&M.

In the specification the terms “comprise, comprises, comprised and comprising” or any variation thereof and the terms “include, includes, included and including” or any variation thereof are considered to be totally interchangeable and they should all be
afforded the widest possible interpretation.

The invention is not limited to the embodiments hereinbefore described but may be varied in both construction and detail.
CLAIMS

1. An interceptor system (10) for the lawful interception of data communications in a communications network, the communications network comprising a plurality of user terminals (3, 4), a Point of Presence (POP) server, a Network Access Server (NAS) and a radius server, the communications network transmitting data having identifier data identifying at least the source and intended recipient of the transmitted data, characterised in that the system further comprises:

   a management system (16) for the reception of a legal warrant containing target identifier data for interception of data transmitted, including the identifier data;

   means to update a target identifier database (17) according to the target identifier data received;

   a Traffic Interceptor (TI) (5) for intercepting data to and from one of the servers in an unobtrusive manner;

   means to duplicate the data and allow one set of the duplicated data proceed to its desired destination in a seamless manner and pass the other set of the duplicated data as processing data to a network filter stage;

   a network filter stage (21) having access to the most recent target identifier lists, the network filter stage (21) having a receiver for the processing data and a comparator for comparing the identifier of the processing data with the target identifier data in the target identifier database;

   means in the network filter stage (21) for separating the processing data into matching data in which the data corresponds to a target
identifier data in the target identifier database and unmatched data;

means to transmit the matching data to a service filter for reconstruction of the data into a usable format;

means to delete the unmatched data in a secure manner; and

means to transmit the reconstructed data in a secure manner to the management system for onward transmission in accordance with the legal warrant.

2. A system as claimed in claim 1, in which the Traffic Interceptor is a Traffic Analyser Port (TAP).

3. A system as claimed in claim 1, in which the traffic interceptor is a layer 2 switch port.

4. A system as claimed in any preceding claim, in which the network filtering stage implements policy based routing (PBR) to filter unwanted data transmissions from the duplicated data set as unmatched data.

5. A system as claimed in any preceding claim, in which the network filtering stage is provided by a layer 3 switch.

6. A system as claimed in any preceding claim, in which the means to transmit the data in a secure manner to the management system is provided by way of a fast ethernet local area network (LAN).

7. A system as claimed in any preceding claim, in which the traffic interceptor is connected to the network filter stage on a dedicated line.

8. A system as claimed in any preceding claim, in which there is provided means to dynamically update the target identifier database in response to retrieved data.
9. A system as claimed in any preceding claim, in which there is provided a WAP server and the TAP intercepts data from the WAP server in an unobtrusive manner.

10. A system as claimed in any preceding claim, in which there is provided an SMTP server and the TAP intercepts data from the SMTP server in an unobtrusive manner.

11. A system as claimed in any preceding claim, in which there is provided a DHCP server and the TAP intercepts data from the DHCP server in an unobtrusive manner.

12. A system as claimed in any preceding claim in which the target identifier data comprises an IP address and the TAP intercepts data to and from that IP address in an unobtrusive manner.

13. A system as claimed in any preceding claim, in which the management system further comprises an Intercept Region Manager and Delivery Manager.

14. A system as claimed in claim 11, in which the Delivery Manager further comprises means to receive and process a warrant from an Law Enforcement Agency (LEA) as an active warrant, means to store the active warrants and assign a unique target ID to each warrant, storage means to store data pertaining to the Intercept Region Manager and means to establish a secure connection to a LEA and transmit matching data to the LEA.

15. A system as claimed in claim 13 or 14, in which the Intercept Region Manager further comprises a Network Filter Manager and Service Filter Manager.

16. A system as claimed in claim 13, in which the Service Filter Manager is provided with a protocol service filter for each protocol to be intercepted in the communications network.
17. A method of unobtrusive interception of data communications in a communications network comprising a plurality of user terminals, a POP server, a NAS server and a radius server, the method comprising the steps of receiving a warrant from a Law Enforcement Agency containing target identifier data; entering the target identifier data in a target identifier database and comparing the processing data with target identifier data in the target identifier database, characterised in that the method comprises the steps of:

intercepting the data communications to and from one of the servers in a non-obtrusive manner by passing the data through a traffic interceptor;

duplicating the intercepted data and allowing one set of the duplicated data proceed to its desired destination and passing the other set of the duplicated data as processing data to a filter;

extracting any data which matches with target identifier data and passing that data to reconstruction filters for reconstruction of that data into usable format;

deleting the remaining unmatched processing data in a secure manner; and

passing the reconstructed data to a management system for the onward transmission to a Law Enforcement Agency.

18. A method of unobtrusive interception of data communications in a communications network as claimed in claim 17, in which the method includes the steps of filtering the processing data according to policy based routing techniques.

19. A method as claimed in claims 17 or 18 in which the method includes the step of passing data through a layer 3 switch.
20. A method as claimed in claim 17, in which the method includes the step of dynamically updating the target identifier database with data retrieved from the network.

21. A method as claimed in any of claims 17 to 20, in which the communications network further comprises a WAP server and the method includes the step of intercepting the data communications to and from a WAP server.

22. A method as claimed in any of claims 17 to 21, in which the communications network further comprises a SMTP server and the method includes the step of intercepting the data communications to and from the SMTP server.

23. A method as claimed in any of claims 17 to 22, in which the communications network further comprises a plurality of IP addresses and the method includes the step of intercepting the data communications to and from a particular IP address.

24. A method as claimed in any of claims 17 to 23, in which the communications network further comprises a DHCP server and the method includes the step of intercepting the data communications to and from the DHCP server.

25. A method as claimed in any of claims 17 to 24, which includes the step of generating billing information according to the data downloaded to the management system.
FIG. 2
From Fig. 2

On Set To System

Compare with Database

Match ?

No Destroy

Yes Transmit

One Set Onwards

FIG. 3
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L29/06 H04M7/00 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L H04Q G06F H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database consulted during the international search (name of database and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>WO 00 42742 A (NOKIA NETWORKS OY ;HIPPELAEINEN LASSI (FI))&lt;br&gt;20 July 2000 (2000-07-20)&lt;br&gt;abstract&lt;br&gt;page 1, line 16 –page 5, line 2&lt;br&gt;page 10, line 8 –page 14, line 14&lt;br&gt;page 14, line 16 –page 16, line 2</td>
<td>1-8, 12-20, 23,25</td>
</tr>
<tr>
<td>X</td>
<td>WO 99 17499 A (NOKIA TELECOMMUNICATIONS OY ;HAUMONT SERGE (FI))&lt;br&gt;8 April 1999 (1999-04-08)&lt;br&gt;page 3, line 21 –page 5, line 25&lt;br&gt;page 12, line 14 –page 13, line 34</td>
<td>1-5,7,8, 12-20,23</td>
</tr>
<tr>
<td>A</td>
<td>WO 01 47222 A (ERICSSON INC)&lt;br&gt;28 June 2001 (2001-06-28)&lt;br&gt;page 4, line 1 –page 10, line 23</td>
<td>1-25</td>
</tr>
</tbody>
</table>

Date of the actual completion of the international search: 20 June 2002

Date of mailing of the international search report: 28/06/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016

Authorized officer

Karavassilis, N
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>AU 2617399 A</td>
<td>01-08-2000</td>
</tr>
<tr>
<td>WO 9917499</td>
<td>08-04-1999</td>
<td>FI 973806 A</td>
<td>27-03-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 9351598 A</td>
<td>23-04-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2304172 A1</td>
<td>08-04-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 1277771 T</td>
<td>20-12-2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9917499 A2</td>
<td>08-04-1999</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2001518744 T</td>
<td>16-10-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TW 429710 B</td>
<td>11-04-2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0147222 A2</td>
<td>28-06-2001</td>
</tr>
</tbody>
</table>