Ultra Sentient Integra

Voice & Data Interception for Enterprise Compliance

Features

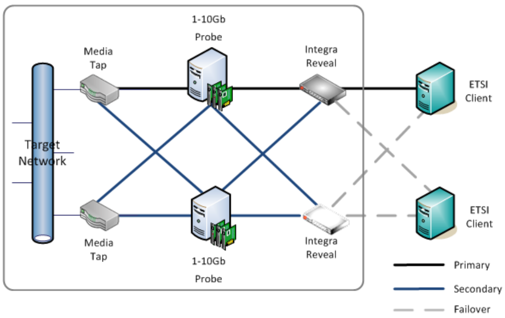
- Capture, storage and analysis of voice and data in real-time or retrospectively
- Redundant hardware configuration to ensure interception integrity
- Integration with Cisco Call Manager to obtain signalling data directly to correlate with intercepted media data

Enterprises that rely on electronic communications to do business have to ensure that their employees are compliant with company regulations when communicating internal and external. It is necessary for them to monitor voice and data conversations internally within the network and externally with third parties. The monitoring of conversations should not only be limited to voice and email traffic but needs to include other technologies such as video-over-IP, web browsing, web mail, instant messaging and social media which can all be used to exchange confidential information.

Ultra Sentient Integra provides enterprises with the capability to intercept, collect, store and analyze voice and data conversations in real-time or retrospectively of voice and data.

Integra Probe

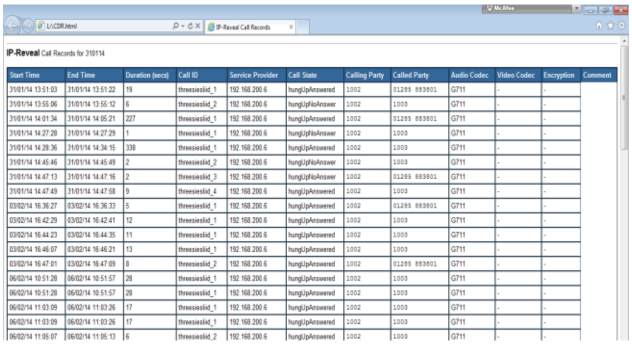
Integra Probes capture traffic using fibre/copper network taps or via SPAN ports. They then perform de-duplication and filtering before forwarding the packets to one or more Integra Reveal servers in NHIS-1 format. It is also possible for the probe software to read in and forward previously captured data from pcap files.



Integra Reveal

Integra Reveal servers perform deep packet inspection (DPI) on packets forwarded from Integra Probes or third party ETSI 102 232-x data sources. They identify data such as voice or video over IP, web browsing, instant messaging and web mail regardless of whether they are using standard or non-standard TCP/UDP ports.

Integra Reveal correlates packets by traffic type so that it can be processed correctly. There are currently 40 flow handler modules which process traffic including TCP, UDP, DNS, SSH, SSL, L2TP, HTTP, SIP, RTP, RTCP, MSN, Xbox and Skype.



IP-Reveal Call Records for 310114

Start Time	End Time	Duration (secs)	Call ID	Service Provider	Call State	Calling Party	Called Party	Audio Codec	Video Codec	Encryption	Comment
31/01/14 13:51:03	31/01/14 13:51:22	19	threesieslid_1	192.168.200.6	hungUpAnswered	1002	01285 883801	G711	-	-	
31/01/14 13:55:06	31/01/14 13:55:12	6	threesieslid_2	192.168.200.6	hungUpNoAnswer	1002	1003	G711	-	-	
31/01/14 14:01:34	31/01/14 14:05:21	227	threesieslid_1	192.168.200.6	hungUpAnswered	1002	01285 883801	G711	-	-	
31/01/14 14:27:28	31/01/14 14:27:29	1	threesieslid_1	192.168.200.6	hungUpNoAnswer	1002	1003	G711	-	-	
31/01/14 14:28:36	31/01/14 14:34:15	338	threesieslid_1	192.168.200.6	hungUpAnswered	1002	1003	G711	-	-	
31/01/14 14:45:46	31/01/14 14:45:49	2	threesieslid_2	192.168.200.6	hungUpNoAnswer	1002	1003	G711	-	-	
31/01/14 14:47:13	31/01/14 14:47:16	2	threesieslid_3	192.168.200.6	hungUpNoAnswer	1002	01285 883801	G711	-	-	
31/01/14 14:47:49	31/01/14 14:47:58	9	threesieslid_4	192.168.200.6	hungUpAnswered	1002	1003	G711	-	-	
03/02/14 16:36:27	03/02/14 16:36:33	5	threesieslid_1	192.168.200.6	hungUpAnswered	1002	01285 883801	G711	-	-	
03/02/14 16:42:29	03/02/14 16:42:41	12	threesieslid_1	192.168.200.6	hungUpAnswered	1002	1003	G711	-	-	
03/02/14 16:44:23	03/02/14 16:44:35	11	threesieslid_1	192.168.200.6	hungUpAnswered	1002	1003	G711	-	-	
03/02/14 16:46:07	03/02/14 16:46:21	13	threesieslid_1	192.168.200.6	hungUpAnswered	1002	1003	G711	-	-	
03/02/14 16:47:01	03/02/14 16:47:09	8	threesieslid_2	192.168.200.6	hungUpAnswered	1002	01285 883801	G711	-	-	
06/02/14 10:51:28	06/02/14 10:51:57	28	threesieslid_1	192.168.200.6	hungUpAnswered	1002	1003	G711	-	-	
06/02/14 10:51:28	06/02/14 10:51:57	28	threesieslid_1	192.168.200.6	hungUpAnswered	1002	1003	G711	-	-	
06/02/14 11:03:09	06/02/14 11:03:26	17	threesieslid_1	192.168.200.6	hungUpAnswered	1002	1003	G711	-	-	
06/02/14 11:03:09	06/02/14 11:03:26	17	threesieslid_1	192.168.200.6	hungUpAnswered	1002	1003	G711	-	-	
06/02/14 11:05:07	06/02/14 11:05:13	6	threesieslid_2	192.168.200.6	hungUpAnswered	1002	1003	G711	-	-	

Intercepted HTTP traffic can be viewed by the Integra operator using the Ultra Reveal web-cache utility which recreates the web pages as they were viewed by the target. For audio and VoIP data, an SSL/TLS encrypted, full HI1 management interface for the warranting of targets and the reporting of management events and alerts/alarms is available. This interface comes with a fully documented API and example Java and C++ code.

Integra Reveal has an integrated packet analyzer that converts data from the Integra Probe's IPOD format into the ETSI 102 232-5 industry standard for transmission to the LEA system. Alarms and management information can be converted into ETSI 101 671 HI1 compliant messages before being forwarded to the LEA. If required, non-standard codecs such as G.722, G723.1, G729, GSM, ILBC, SPEEX NB/WB can be converted to G711a for use by reception software that does not natively support them.

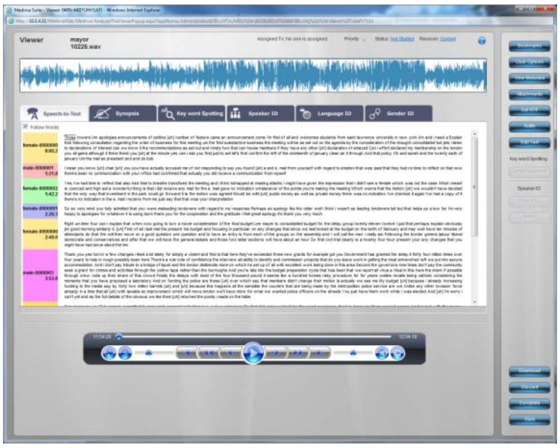
Redundancy

To ensure maximum availability, Integra systems are deployed as a redundant pair of Integra Probes and a redundant pair of Integra Reveal servers. Both systems simultaneously process the intercepted data but only the primary system outputs to the law enforcement monitoring facility (LEMF).

In the event of an Integra system failure or failure of the monitoring infrastructure (e.g. tap or SPAN port), the standby system takes over, instructs the failed system to reboot and continues to process data until the primary system becomes operational.

Audio Analytics

A number of different audio analytics can be run on files as they are imported in to the system. These include speech detection, speaker, gender and language identification, key word spotting and speech-to-text conversion. These services can be distributed across multiple servers to increase the scalability and availability of the solution.



Web Interface

The Integra web interface allows the operator to perform management, data handling, replay and transcription functions.

Management

The operator can configure the Integra Probes, set user and group security permissions, create data retention policies, manage alarming and alerting, view audit trails, and view usage reports.

Security

There are approximately 250 separate permissions on management tasks as well as the ability to observe/access/modify permissions on individual files and cases. In addition restrictions can be placed on management, configuration and reporting options. Users and groups can be linked to AD or other LDAP servers. A complete audit trail is available to ensure appropriate use of available resources.

Data Handling

Integra Web is based on 'cases' (often referred to as hearings, missions or tribunals depending on how they are being used) and 'importers'. Cases are a group of various file types brought into the system and grouped together by business logic to fit a particular workflow.

Files belonging to a case are given a unique serial number and are stored into a selected repository so they can easily be replayed or transcribed at a later date.

Storage availability and usage over time can be viewed from the reports menu which allows administrators to monitor the importers and their progress. Cases can be archived to other storage or exported to other Integra systems from the web interface which makes administration of the system easy.

In the event of errors or problems such as storage approaching capacity a comprehensive set of warnings and alarms are available which can be configured individually as to how they are raised e.g. GUI, email, SNMP, relay card or SMS.

Replay, Transcription and Visualization

The first step in the process of replay and analysis of audio and video data is to find the relevant records. The GUI has optimised screens available for different types of record or task.

Text searching of metadata is enhanced by the search engine which allows for searches that match the meaning and not necessarily the full text specified. This enables to operator to find important pieces of data that may be missed if they were relying on exact string text matching. The search results allow users with sufficient administrative permissions to open a file to allow replay, transcription and further audio and video analysis is available. In addition, search results can be assigned, reprioritized and have their access restricted.

.

Ultra Electronics
SURVEILLANCE AND SECURITY SYSTEMS
316 Botley Road
Burridge
SO31 1BQ
United Kingdom
Tel: +44 (0)1489 557 373
Email: information@ultra-sss.com
www.ultra-sss.com
www.ultra-electronics.com