Newsletter 2/07

July 2007

ELAMAN works closely with its clients to develop a total system solution to their needs and to ensure that they are equipped, trained and manned to meet the formidable challenges in the field of communication.

Adding new products solutions to our portfolio is an ongoing process. Therefore from now on ELAMAN provides a Newsletter whenever important innovations are coming up.

Kind regards
Your Elaman Team

News

Pinpoint localization of mobile phones

The GSM mobile finder (GSM-MF) enables pinpoint localization of mobile phones.

The device provides 50 reception channels for selection of an unassigned frequency. The wide range of its reception dynamics (-100 dBm to +7 dBm) ensures localization of both adjacent and distant mobile phones, in combination with active GSM-off-air systems (MTL3, GSM XPZ, GA900 etc.).
An especially designed aerial enables systematic direction detection and, thus, a rapid approach to the sought mobile phone.

Mobile Finder

The compact design of the device ensures concealed operation. Absolute reception field strength of the respective channel is shown on a display (1 dB steps). Relative field strength is signaled through changing tone pitch or intermitted sound.

Blocking & Shaping of IP Traffic

The CS 2000 has created a new network applications' platform - a general purpose deep packet processing platform combined with an open Linux server blade. It is designed for applications focused on real-time network traffic processing.
CS-2000 provides the application developer high-speed processing, high-speed RAM, a high-speed database, and a structured programming language for data plane-resident packet operations.
This results in:

- No more CPU interrupt latency
- No more PCI bus bandwidth constraints
- The power to operate on every packet – every bit of every packet – on the wire in real-time

The CS-2000 also provides conventional Linux server resources for off-line analysis and non real-time application functions.

CS 2000

The CS-2000 enables users to implement their ideas, build differentiating service features:
e.g. *Shaping of IP-Traffic:*
Reducing bandwith for voice over IP (VoIP) in order to avoid the usage of VoIP in IP networks
or *Blocking of URLs:*
Blocking of Skype, etc.

The Programming platform for CS 2000 is PacketWorks IDE (see overview)

PacketWorks IDE Summary of Benefits:

Improved Deep Packet Processing Application Development
- Program, compile, and debug CS-2000 application on a PC
- Comprehensive RAVE program debugger supports:
  - Application break step through
  - LIBPCAP traffic simulation (before and after)
  - Variable tracing
  - Memory use and allocation
- More traditional text-based RAVE language speeds development and supports multi-programmer projects
- Visual RAVE offers fast GUI-based programming
- Functional reference utilities available for modification/ incorporation into applications

Fast Path to High-Speed Network Applications
- Easy access to CloudShield's high-performance, high-capacity applications-ready platforms
- Flexible porting options easily extend performance range of existing application to suppoert multi-gigabit deployments
- Developers ramp up in hours-to-days, not weeks-to-months

A Complete Developer's Environment
- Based on widely-deployed Eclipse open framework
- Available C++, Java, and other language IDE plug-ins
- Supports team-based CS-2000 applications development
- Projects / Developers can work with CVS-protected files

elaman GmbH • German Security Solutions
Seitzstraße 23 • 80538 Munich • Germany
Tel: +49-89-24 20 91 80 • Fax: +49-89-24 20 91 81 • info@elaman.de • www.elaman.de
HRB München 153662 • Ust-IdNr.: DE814086265 • Geschäftsführer: Holger Rumscheidt

IP Sniffling & Hacking

Monitoring of IP Data becomes more and more important. IP-Monitoring Systems currently on the market will never be able to monitor and demodulate all IP-Traffic within IP networks due to e.g. encryption, different access levels, rerouting, new protocolls, VPNs etc.

Therefore the direct access to a PC is the only way to access data. Sniffling and Hacking is one way to realize this. Elaman provides in this ready made products training like

1) FinFisher (USB-Sticks)

- Finfisher1-Memory stick for stripping important data from a PC
- Finfisher2-Memory stick for stripping specific files from a PC
- Finfisher3-Manipulation/intrusion software for unauthorized access to a PC
- Finfisher4-Memory stick/CD used to strip usernames/passwords from a PC
- Finfisher5- CD used to access a PC and change all passwords
- Finfisher6-Software used to remotely extract information from a target's PC, using highly encrypted links and being virtually undetectable

2) Training in Hacking

The **Fintraining-Basic** for one week hacking overview-product training (advanced course is available upon request).

The **Hacking course** for two weeks includes the issues of profiling of foot-printing, scanning and enumeration as well as attacking of passwords, web security, bluetooth, networks, wireless LAN, root kits and exploits.

The **VoIP Course** for one week includes:

- Type of attacks
- Practical exercise
- IP Telephony Operating
- System Level Security VoIP Network Security
- Design Considerations

For further information please contact us as we have an accurate schedule for the whole course.

Finfisher USB Sticks

...and keep in mind

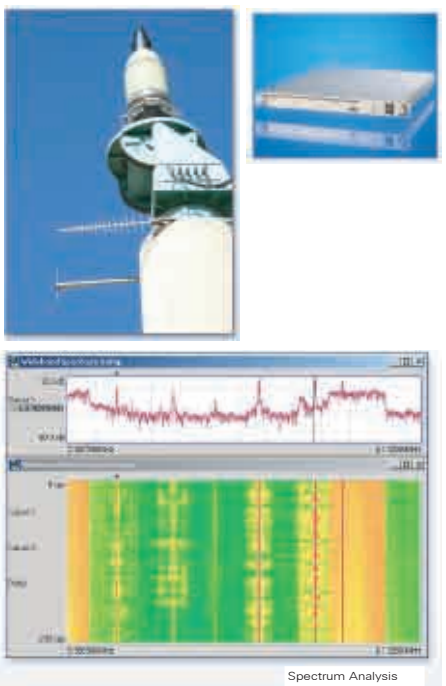
Milipol PARIS 2007 9-12 october

...one of the most important worldwide exhibition and show for special security equipment with focus on law inforcement agencies.

Radio Monitoring and Surveillance Solutions (RMS)

Specialized in the application of the digital signal processing and pattern recognition to communication intelligence: we have the capability to design, produce and deliver complete RMS solutions especially for the operation of RMS for Law Enforcemnt Agencies. We offer comprehensive products for signal analysis, automatic detection & classification, demodulation & decoding, as well as for wideband signal acquisition & processing. We can supply the whole range, from a single stand-alone product to a complete RMS solution, from a single source.

- Antennas
- Tuners
- Broadband Technology
- Broadband Search and Direction Finding Systems
- Signal Analysis
- Signal Detection and Classification
- Speech Technology
- Virtual Devices and PC-Based Architecture



Antennas, Broadband Tuners, Signal Analysing

Counter Surveillance Equipment (TSCM): Telephone Line Analyzer Detector

- Digital Demodulation to confirm that the telephone line is not passing audio (demodulation code is upgradeable for new phone systems, expected to cover 80% of world's PBX/ACD phone systems)
- Frequency Domain Reflectometer (FDR) similar to TDR to check for taps on the line
- NLJD Line Trace Probe for verifying electronic taps and tracing wires to locate electronics
- Audio Oscilloscope with active input (20Hz to 20KHz)
- High Gain Audio Amplifier (20Hz to 20KHz)
- Digital Multimeter tests voltage, current, resistance & capacitance
- Bias Generator +-80 VDC, direct digital control to use with Audio Amplifier, NLJD, and FDR.
- Automatic Internal Pair Switching automatically performs tests on all pair combinations
- RF Broadband Detector tests lines for RF up to 8GHz
- Multi-Test Database System performs multiple tests at once on all pair combinations, storing data in a database for comparison against other lines and historical comparison

Telephone Line Analyser Detector

Passive Telephone Line Monitoring

The Zebra system is a powerful telecommunications monitoring solution. The Zebra system is suitable for law enforcement as well as intelligence gathering and is scalable from 16 E1 carriers (or equivalent channels) to more than 5,000 E1 carriers (or equivalent) in one integrated system. Passive SS7, R2MFC and SS5 protocol stacks support passive monitoring between switches in a carrier network, as well as between the gateway switches. The same passive protocol stacks support interception of satellite streams. A passive ISDN stack supports trunk-side interception of PBX traffic.
The support for these interfaces and protocols allow the Zebra system to be applied to any type of monitoring in the carrier network, including PSTN and PLMN networks.
Passively – the system connects passively to carriers or bearers between switches. Hi-Z buffers hide the Zebra system from the monitored network. No additional load is placed on the monitored network. Sessions on the monitored carriers/bearers are detected by protocol analysis or VOX activity. The system can be configured to record all traffic on the monitored carriers/bearers.

Such a passive monitoring system is capable of monitoring any configuration of protocols on its input carriers, including: SS7 ISUP and TUP, SS5, R2MFC. When no signaling is available recordings can be triggered on VOX. Future versions of the system will support H.323, SIP and other packet protocols.

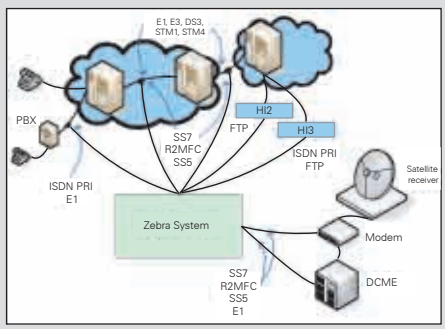
The philosophy of the Zebra passive monitoring system can be summarized as: store everything, filter for known targets, and search the past for new targets.
The management of large amounts of carrier cable can be a challenge, especially in large passive monitoring systems. We offer a modular coupling system that supports the connectivity management of large numbers of monitored carriers in conjunction with optional high impedance buffering (Hi-Z) and LED indication of the status of passively monitored carriers.

User workstation - for filtering and browsing stored intercepts, playing audio and viewing fax/modem intercepts.
The Zebra enhanced user station that will offer sophisticated filtering and searching, playback and visualization of content, as well as the viewing of fax/Internet sessions.

The Zebra enhanced user station is also designed with integrated link/network analysis to assist investigators in the visualization of associations between targets.

Administration workstation

- User management
- Interception management – the configuration of intercepted carriers, including machine assisted SS7 CIC mapping and the automatic classification of SS5, SS7 signaling and SS7 audio channels
- Signal and signaling analysis – allows the administrator to view signaling messages, listen in real-time to channels, manually record channels and visualize the content of recordings
- Health monitoring



Zebra Architecture

For further Information please don't hesitate to contact us at:

elaman GmbH
German Security Solutions

Seitzstrasse 23
80538 Munich
Germany

Tel: +49-89-24 20 91 80
Fax: +49-89-24 20 91 81

info@elaman.de
www.elaman.de

HRB München 153662
Ust-IdNr.: DE814086265

Managing Director:
Holger Rumscheidt