

INSIDE THIS ISSUE:

TSCM Concerns With Digital Phone Systems

REI Expands TSCM Training Facilities

In the News: TSCM related headlines and news

Using the LAA for Increased Detection Range in the 1.5-3GHz Band

Training Calendar

NEW VPX-64 Extended Pole Camera

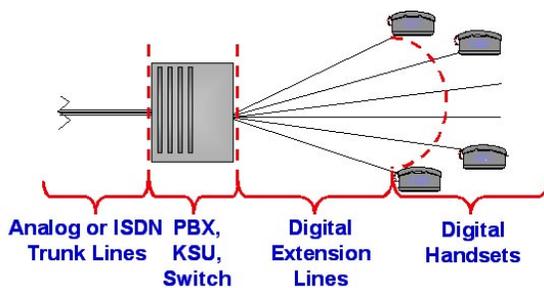
TSCM Tips

Questions, comments, suggestions, or to add someone to the REI Quarterly Newsletter mailing list, please e-mail: newsletter@reiusa.net

TSCM Concerns With Digital Telephone Systems

While entire books could be written about the subject of telephone system surveillance attacks, REI plans to present a series of articles in the next few newsletters to address some concerns over potential digital phone system threats. This article is the first in the series and presents some readily available threats to Digital Extension Telephone Lines.

For reference, a very general description of a Digital system is described below for the purpose of clarifying basic terminology.



Most digital phone systems utilize basic ISDN technology to encode audio and digital control signals in a binary format. This binary format is then modified to unique system communication protocols to ensure that other vendors cannot simply develop inexpensive replacement handsets for the system. To learn more about ISDN basic

technology, the site below provides a good introduction.

<http://www.ralphb.net/ISDN/index.html>

There has often been an opinion that Digital Phone systems are fairly secure because of unique system protocols. However, there are many inexpensive products that are readily available and could easily be used to "tap" an internal digital extension phone line. This includes products that have been designed to provide a means of legally recording important phone conversations, but could also present an audio surveillance threat. Below is a link to an example of a commercially available call recording product which could be used surreptitiously:

<http://www.usbcallrecord.com/>

It is important to understand that these recording products when placed in line on a digital extension are capable of recording and/or storing all conversations without interfering with normal communications. They have basically solved the decoding problem and provide an easy solution to recovering digital audio from a line. Also, it should be noted that these recording devices are phone system specific, but if the phone system type is known, it would be rather easy to purchase the correct decoding and

More on page 3

REI Expands TSCM Training Facilities

REI has expanded its Center for Technical Security with three new additions:

NLJD Training Wall that includes compartments for test targets at varying depths (2 inches to 16 inches) of concrete, block, and brick (with and without reinforcing steel), allowing trainees to hone their skills using the ORION and the High Gain ORION by detecting targets at different depths of varying materials. This training wall provides trainees with hands-on practical

More on page 4



NEWS HEADLINES: Corporate Espionage & Information Theft...**"WestJet faces new spying allegations"**

The Globe Advisor
December 9, 2005
WestJet ran '007 Project,' of corporate espionage Air Canada says...
Source: www.theglobeandmail.com
Article: <http://tinyurl.com/nbjhu>

"Pirates snatch rose's secrets"

The Observer Guardian, UK
February 19, 2006
Stolen information about new hybrid rose in highly competitive flower industry...
Source: <http://www.guardian.co.uk/>
Article: <http://tinyurl.com/h2rly>

"Toyota staffers charged in Ferrari espionage"

TSN Canada, January 16, 2006
Formula One technology stolen...
Source: <http://www.tsn.ca>
Article: <http://tinyurl.com/et3vn>

"Biotech company sues former UConn professor over trade secrets"

Boston Globe
January 16, 2006
Source: <http://www.boston.com>
Article: <http://tinyurl.com/lyfxv>

"Attempt to Steal Vital Korean LCD Technology Foiled"

The Chosun Ilbo, South Korea
January 16, 2006
Source: <http://english.chosun.com/>
Article: <http://tinyurl.com/fmbyj>

"Circus Company Goes to Trial in Spy Suit"

USA Today
February 27, 2006
Claims Ringling Bros. President supervised spying efforts...
Source: <http://www.usatoday.com>
Article: <http://tinyurl.com/lxado>

"Ogdensburg man arrested for eavesdropping at LSC Court Complex"

Newswatch 50 WWTI (ABC)
March 1, 2006
Source: <http://www.newswatch50.com>
Article: <http://tinyurl.com/fkyr5>



Using The LAA-1530 for Increased Detection Range in the 1.5 GHz to 3 GHz Band

The LAA-1530 (Log-periodic Active Antenna) is a high gain log-periodic directional antenna with a built-in pre-amp (powered by an external 9V battery) with a frequency range from 1.5 GHz to 3 GHz. This antenna was designed for use with the OSCOR to provide increased detection range and directional resolution. While current built-in antennas for the OSCOR have adequate sensitivity, the LAA provides greatly increased sensitivity in this frequency range for identifying and locating signals such as 1.8 GHz Cell band, 2.4 GHz 802.11 WAN signals, 2.4 GHz video transmitters, etc.... The increased gain is achieved with an antenna gain exceeding 6 dB and a pre-amp of 20 dB combined with a high-pass filter to greatly reduce the system noise from lower frequency signals.

The built-in Discone antenna on the OSCOR covers 1.5 to 3 GHz, providing omni-directional coverage. The LAA not only provides increased detection range, but also directional resolution for pinpointing the source of the transmitter. To use the LAA with the OSCOR, connect the LAA directly to the Whip Hi/Discone input (labeled "HF/UHF") in the OSCOR connector tray and set the OSCOR input mode to Discone. With the Sweep display set to the full 1.5 to 3 GHz span, the user can simply manually point the

LAA in various directions of interest to see if additional signals are detected.

In summary, the LAA provides an inexpensive way to greatly increase the detection range and direction resolution of signals in the frequency range from 1.5 to 3 GHz, enhancing the capabilities of the OSCOR. For more information on the LAA-1530, contact REI at sales@reiusa.net.



REI TRAINING CALENDAR

April 24-28
Technical Surveillance Countermeasures (TSCM 201)

May 9-11
Technical Security Equip. (TSE 101)

May 15-19
Technical Surveillance Countermeasures (TSCM 201)

May 22-26
Advanced TSCM Concepts (ATC 301)

June 6-8
Technical Security Equip. (TSE 101)

June 12-16
Technical Surveillance Countermeasures (TSCM 201)

June 19-23
Equipment Certification Course (ECC 240)

August 1-3
Digital Telephony Course (DTC 110)

August 15-19
Technical Security Equip. (TSE 101)

August 21-25
Technical Surveillance Countermeasures (TSCM 201)

Questions, comments, suggestions, or to add someone to the REI Quarterly Newsletter mailing list, please e-mail: newsletter@reiusa.net

Cont. Page 1: Digital Phone System Concerns

recording system. Furthermore, many digital phone systems inherently send audio down the phone line to the switch even when the handset is hung up (on hook). In this type of system, the switch basically ignores the audio unless a call is in progress. Hence, it is important for the TSCM professional to be able to identify if digital audio is being sent down the line even when the handset is on hook. Also, for a good inspection, it is recommended that the digital phone extension lines should be disconnected from the switch and from the handset to be thoroughly analyzed for electronic threats on the line. This analysis may consist of various electronic tests including TDR analysis, capacitance testing, audio listen with line bias, impedance

testing, and line balance testing.

This short article does not contain sufficient space to address these various testing methods, and there are many other issues to consider when investigating telephone lines. Hence, future articles will follow to address additional telephone issues and testing methods including topics such as analog audio leakage on digital systems, different types of taps, switch/re-switch, software attacks, and traditional phone system compromise. Look in future REI Newsletters for these articles.



NEW VPX-64 Extended Video Pole Camera

REI is pleased to announce a new Extended Video Pole Inspection Camera (VPX-64) for security inspections and tactical applications. The VPX-64 is a self-contained, lightweight pole camera for inspecting hard to reach or dangerous areas for potential security hazards, breaches, and/or for tactical applications.

The VPX-64 provides additional reach over the Standard VPC-64 Video Pole Camera: the expandable pole extends from 38 inches to 12.5 feet with no external cables or reconfiguration, giving the typical user a reach of over 16 feet. The entire system fits inside a self-contained portable case.

The camera head has built in variable illuminators providing crisp color images even in dark or low light situations. All controls are configured on the large (6.4 inch diagonal) color TFT monitor,

providing a quick and easy-to-use inspection system right out of the case. The display monitor also provides a video output for other uses. Rechargeable battery packs (typical run time is between 1.5 – 2 hours) as well as a charger are included.

The new VPX-64 improves physical search capabilities providing enhanced inspection of high ceilings and tall or immovable objects in hard to reach areas.

For more information, contact REI at sales@reiusa.net.



TSCM TIPS

UV Marking Pens

Using a UV Marking Pen can be a simple, but very useful sweep tool. A UV Marking Pen uses ink that cannot normally be seen by the human eye, unless illuminated by a UV light. A UV pen can be used to make notes on walls or other areas, noting certain items of interest, without leaving any visible marks (for instance where a false corrosive junction has been identified with a Non-Linear Junction Detector). Also, it can be used to identify outlet boxes that have been thoroughly inspected by making a line across the outlet cover screw, indicating if the cover has been removed or tampered with. If you aren't currently using a UV pen, considering adding one to your tool kit.



For more information on TSCM and REI equipment, consider REI's Center for Technical Security training courses. Course descriptions and training dates can be found on REI's web site (www.reiusa.net/training) or e-mail sales@reiusa.net.

If you have TSCM Sweep Tips that you would like to share, please send them to support@reiusa.net.

Cont. from Page 1: Additional TSCM Training Facilities

knowledge of how an NLJD will react to depths, material type and density of potential environments.

Telephone Testing Classroom containing a complete, isolated digital phone system, including six phone block test stations for telephone system inspection training. Additionally, this phone system is



wired with phone sets in five of the other project rooms, creating a real-world environment. This digital phone system will give students the ability to practice using TSCM equipment on actual "live" phone systems, to detect and identify

potential threats. This classroom and equipment will be specifically used for future training classes.

Multimedia Project Room simulating multimedia presentation rooms found in many corporate environments. This room presents some unique TSCM situations due to the electronics and layouts commonly found in multi-media rooms. Trainees test their TSCM skills against live targets in this type of unique environment.



REI's Center for Technical Security continues to be the largest commercially available, unclassified TSCM training facility in the world, with over 6,000 square feet of dedicated classrooms and sweep exercise rooms for hands-on application. Regularly scheduled classes are taught monthly by REI's three full-time instructors.

For more information on TSCM training, contact REI at sales@reiusa.net.

