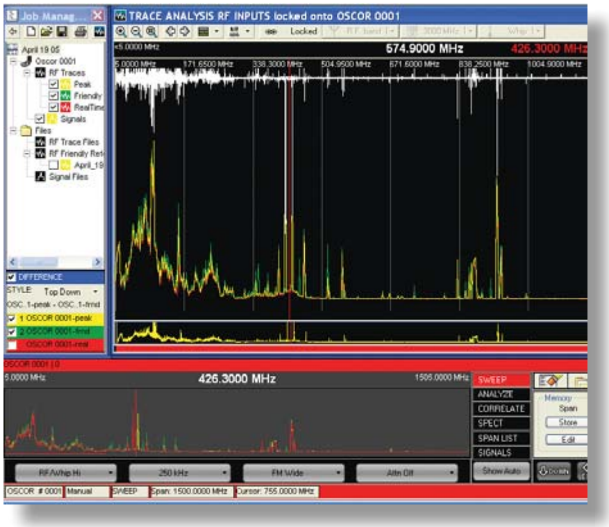
REI®
RESEARCH ELECTRONICS INTERNATIONAL
NEWSLETTER
Q1 2009
A Quarterly Information Publication

INSIDE THIS ISSUE:

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

Modern RF Search Techniques



RF searching techniques for TSCM applications have evolved over the past years to keep up with the dynamic nature of evolving RF threats. Early TSCM RF sweeps were based on simply "dialing" through the spectrum, listening for anything peculiar. Then, with the introduction of phase correlation technology several years ago (REI US Patent 5,241,699 and 6,397,154) it became easier to automatically detect and confirm analog modulated bugging devices; however this did little for digitally modulated devices which may not follow any standard or normal protocol and could easily be encoded and encrypted so that the challenge of demodulating a digitally encrypted bug can be almost impossible.

Today's TSCM RF analysis techniques focus on isolating signals transmitted within the vicinity of the target sweep area from those in the normal ambient RF environment. This method is recommended over trying to demodulate a signal to determine its threat potential. This was the reason REI implemented Comparative Trace Analysis (US Patent 7,058,530) with OSCOR version 5.0 for detecting transmitters regardless of modulation scheme. The main point is that while the OSCOR 5.0 retains the ability to do correlation for analog signals, relying solely on correlation may create a false sense of security by ignoring digital signals. It is more reliable (and faster) to use a Trace Analysis approach which is modulation indifferent, in order to determine if a signal is being transmitted locally or from a distance in the ambient environment. Additional information on the application of Trace Analysis can be found in the "RF Trace Analysis Primer" at the following link: http://www.reiusa.net/quick/Trace_Analysis.

Moreover, it is important to consider the possibility of other sophisticated transmitter schemes such as burst or frequency hopping transmitters. With today's

Continued on page 4.

The Risks of Corporate Espionage

Industrial espionage can generate an out-of-sight out-of-mind attitude for companies that don't understand the value of intellectual properties or until confronted directly with the reality and cost of having information stolen. But Corporate Security Officers and Chief Information Officers (CIOs) around the world are seeing the need for greater diligence to prevent attacks, especially in economically challenging times.

According to Merriam-Webster Dictionary, industrial espionage is "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company." Unfortunately this definition seems to ignore espionage spawned from overzealous business competition, where one business may resort to espionage tactics (not necessarily illegal) to gain information providing an advantage over a competitor or to harm a competitor in some way. Regardless, information loss doesn't have to be espionage (illegal/unethical) to be costly to the victim.

Theft of corporate information occurs every day but is difficult to identify and track and often goes unreported. Disclosure of a breech acknowledges exposure to future loss and can be viewed as an embarrassment to the company and its stockholders, furthering financial loss (i.e. stock price affects from information loss acknowledgement).

Continued on page 5.

Shipping Equipment to REI

Shipping TSCM equipment around the world creates the potential for shipping and customs issues which can lead to delays or unfounded fees, particularly when the products being shipped are so technical in nature and often misunderstood or incorrectly categorized.

Occasionally we experience import/export issues with equipment returned to REI for upgrade and/or repair; usually causing unnecessary tariffs, customs duties, or simple delays because of missing paperwork or mislabeled product information. Should you need to return equipment to REI (Domestic or International), please follow these steps to minimize potential unnecessary delays or fees:

- Contact REI to obtain a Return Merchandise Authorization Number (RMA) **BEFORE** shipping any equipment to REI. This gives us the opportunity to coordinate any special needs or considerations for the return and possibly prevent problems before they occur. Getting an RMA is easy and can be done by calling or emailing REI *sales@reiusa.net*.

- Clearly write the RMA number on the outside of the returned package. Doing this helps receiving personnel to quickly identify the package as a customer return, thereby triggering expedited handling and processing.

- Include with the returned equipment a letter with the following:
  1. The name and contact information of the person returning the equipment
  2. The RMA
  3. How you would like to be contacted for approval of any non-warranty repairs or upgrades
  4. Shipping instructions and where the upgraded/repaired equipment should be returned
  5. Payment details for any upgrades, repairs, and shipping payment
  6. A commercial invoice stating the following:
     "This enclosed equipment is U.S. Goods being returned for repair,"
  7. Send a copy of the commercial invoice and shipment details to your sales person (or *sales@reiusa.net*).

This is crucial for international shipments to minimize unnecessary tariffs, fees, or customs delays which are out of REI's control. Please note that any excess charges will be invoiced to the customer. NOTE: REI suggests using UPS or Federal Express for shipping equipment to REI. DHL no longer services Algood TN, and therefore is no longer a recommended shipper. Please contact REI if you have any questions, or if you need to obtain an RMA: *sales@reiusa.net*

Training Center Grows With Building Expansion

The recent expansion has doubled the size of the REI's building providing much needed space for manufacturing, engineering, research and development, and sales and administration. This expansion also provided much needed space to expand REI's TSCM Training facilities.

As the largest commercially available TSCM Training Center in the World, REI now has more than 10,000 square feet (929 square meters) of dedicated classrooms and sweep project rooms to simulate live target rich office suites, hotel rooms, conference rooms, break rooms and office cubicles.

These additional class and project rooms provide a student capacity of up to 52 students per week. The additional space also provides the opportunity to run a combination of telephony/ RF component detection, as well as foreign language courses simultaneously. Last year, REI provided more than 50 week long courses at REI's Training facility. REI's courses cover basic and advanced procedural concepts of conducting a counter surveillance investigation. More information on REI's complete TSCM training curriculum can be found on the next page of this newsletter. Course descriptions, schedules and registration details are also available at the REI website by selecting the "Training" link at *www.reiusa.net*. If you haven't been to an REI training class recently, we hope you will visit our new training facilities soon.

2009 TSCM Training Curriculum

REI's TSCM training program has continued to grow in offerings for 2009. REI now has 6 full time TSCM Instructors providing training in English, German, and Spanish at REI's training facility in Tennessee, USA as well as custom training courses at customer's location (contact sales@reiusa.net for more information on a custom training course at your site). There are two main "tracks" within REI's current curriculum: General RF/TSCM and Telephone Countermeasures. Available courses in each "track" are listed below:

General RF/TSCM

TSE-101 Technical Security Equipment

Pre-requisites: none
Description: Four (4) day training course designed to introduce and familiarize the technical security specialist with the various Countersurveillance products and their basic sweep procedures.
Topics: Threat Overview of commercially available devices; overview and operation of CPM-700, ORION, NJE-4000, OSCOR OSC-5000, and Microwave Down Converter.

TSCM-201 Technical Security Countermeasure Course

Pre-requisites: TSE-101
Description: Five (5) day training course on procedural concepts of conducting a TSCM investigation. Attendees will be presented with a variety of search exercises to simulate various environments and technical attacks.
Topics: History of Technical Security, Technical Security's Role in Overall Facility Security, Acoustical and Microphone Threats, Radio Frequency and Microwave Threats, Carrier Current Threats, Infrared Threats, Physical Search Procedures, Non-Linear Junction Detector, Broadband Field Strength Meters and Spectrum Analyzers.

ECC-240 REI Equipment Certification Course

Pre-requisites: TSE-101 and TSCM-201
Description: Five (5) day course will provide two (2) days of equipment review and advanced training and three (3) days skills testing to determine student skill levels for use of the OSCOR and MDC-2100, ORION NLJD, and the CPM-700 Countersurveillance Probe/monitor. Upon successful completion of the testing, students will be granted R.E.C. (REI Equipment Certified) credentials including a certificate. The R.E.C. credentials will be valid for one-full-year.

ATC-301 Advanced TSCM Concepts

Pre-requisites: TSE-101 and TSCM-201
Description: Five (5) day course provides TSCM technicians with an advanced understanding of RF signal analysis and theory including the relevance of Inverse Squares Law, Frequency Domain, Time Domain, Wavelength versus Frequency, Modulation Schemes.
Topics: RF Receivers, Oscilloscopes, Spectrum Analyzers and harmonic receivers, as well as carrier current analysis, sub carrier analysis, microwave analysis, and base band analysis.

Telephone Countermeasures

TCC-110 Telephone Countermeasures Course

Pre-requisites: none
Description: Four (4) day Telephone Countermeasures Course provides an overview of analog and digital telephone systems and the inherent vulnerabilities of each, as well as methods for the detection of attacks on both analog and digital telephone systems.
Topics: Basic Telephony, Testing Equipment, Basic Analog Tests, Digital Telephone System overview, Digital System Capabilities, Basic Digital Tests, and Digital Telephone System Weaknesses.

DTC-210 Digital Telephone Security and TALAN Operation Course

Pre-requisites: TCC-110
Description: Five (5) day Digital Telephone Course provides an in depth instruction on digital telephone system testing including the operation of the REI TALAN Telephone and Line Analyzer.
Topics: Telephone system characteristics and vulnerabilities, countermeasure tests including FDR (Frequency Domain Reflectometry), Voltage/ohms tests, Digital demodulation and audio detection, Non-Linear Junction Detection (NLJD) on a wire, digital telephone countermeasure analysis procedures, and other line testing and analysis.

TEC-250 TALAN Certification Course

Pre-requisites: TCC-110 and DTC-210
Description: Five (5) day course providing one and a half days of refresher training on the TALAN Telephone and Line Analyzer, and two and a half days of pass/fail certification testing; the last day is reserved for retraining and retesting advanced concepts of the TALAN. Individuals successfully completing the course will receive certification that the individual has demonstrated satisfactory proficiency with the TALAN.
Topics: The TEC-250 Course includes a written test, as well as the following hands-on operational tests on the following TALAN test functions: DMM (Digital Multimeter), Audio Tests (including digital demodulation), RF Line Driver, Telephone Unit Test, Line NLJD Test, FDR Frequency Domain Reflectometry Test, and Line Tracer Test.

All REI courses include both classroom instruction as well as hands on exercises where students apply learned TSCM concepts in real world project rooms with live devices. REI's training center has over 12 dedicated project rooms of varying environments and construction examples providing attendees with numerous opportunities to apply course concepts in live environments. Classes are taught regularly (over 50 offerings throughout the year). Additionally, REI can create custom courses delivered at almost any location around the World.

If you want to brush up on your skills or just test yourself against REI's project rooms, contact REI at sales@reiusa.net to get registered for an upcoming course or discuss other training options.

REI

Modern RF Search Techniques

continued from page 1

modern technology, it is very easy to design and build very small listening devices that will store large blocks of audio and then send the information out periodically in an RF burst. It is important to understand that this type of device may have a widely varying burst period and duty cycle. The burst period is how often the transmitter will send a signal and the duty cycle is the percentage of time that a transmitter is actually transmitting. For example, a Burst device with a 1 minute period and 1% duty cycle will only transmit every 60 seconds and will be "on" (transmitting) for 600 msec (6/10 of a second). It should also be noted for this example that since this theoretical device is only transmitting 1% of the time, the bandwidth of the transmit signal will increase by a factor of 100 in order to transmit the full information. In other words, the signal may only transmit for a short time, but it should be easy to see for a fast receiver because it will occupy a wide bandwidth. It is not practical to have an extremely low duty cycle and low bandwidth; the fear of this type of threat is unfounded because it violates basic laws of physics for transmitting useful information.

There are, of course, an infinite number of variations of bursting periods, duty cycles, and digital encoding schemes. One example of a difficult type of technology to "see" with a TSCM receiver is the DECT (Digital Enhanced Cordless Telecommunications) protocol technology (http://en.wikipedia.org/wiki/DECT). This technology is now cheap and readily available in cordless phones (DECT phones can be purchased online for less than US$100), and it is actually very difficult for many receivers to see this type of transmitter because of the very short bursting and frequency hopping characteristic of this protocol. It is an interesting exercise to compare detection times of this type of device for different receivers.

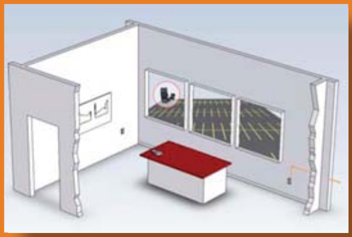
Furthermore, one of the most useful features of the OSCOR OPC version 5.0 software is the ability to analyze certain portions of the spectrum while allowing the OSCOR receiver to continue to run as fast as possible to maximize the probability of catching a transmission event. In order to do this, the user should operate the OPC in an "Unlocked" mode. In this manner, the OSCOR receiver will continue to sweep it's maximum frequency spectrum and create waterfall style data while the user is manually investigating much smaller portions of the spectrum using the OPC stored spectrum peak trace data.

This methodology works very well for comparing different portions of the frequency spectrum from different parts of a building in order to determine the relative location of the source of transmitters. Using this technique, it is quick and reliable to determine the presence of sophisticated digital transmitters (including bursting devices) to determine if a signal is a potential threat or not. REI highly recommends receiving training and practice using this type of technique to increase reliability for the detection of sophisticated devices. We clearly cannot rely simply on audio correlation and location for detecting modern bugs.

In summary, the most important point is to have a TSCM receiver that covers the spectrum completely and rapidly in order to see modern digital transmitters. It is also very important to have a receiver with very high storage and peak trace capture capability so that if a detection event occurs anywhere in the spectrum, you have documented evidence of the time and frequency of the transmit event. When REI developed the OPC software for OSCOR version 5.0, this was the main focus of our development. It continues to be the main focus of our engineering efforts and further improvements will be forthcoming. While the OSCOR has been around for many years, the technology and methodology of it's usage has dynamically changed to adapt to the evolving threat. REI is forever dedicated to continuing this evolution in all of our product development. Consider attending a training course at REI's Center for Technical Security to learn more, www.reiusa.net/training.

PEAK VS FRIENDLY

The most basic method of trace analysis is a 2-step process:



1. Capture a Friendly Reference Trace at a safe distance from the target sweep environment. Typically this can be done in the parking lot of the building at a reasonable distance from the Target Room. This Peak Trace is called the Friendly Trace. This data should be captured for at least 5 minutes, but better performance will be achieved by increasing the Friendly Capture time.

2. Capture Peak Trace Data from the target sweep environment, and then compare the differences between this trace data and the Friendly Trace. Again, this trace data should be captured for at least 5 minutes, but allowing the Peak capture to run for longer times will increase reliability against intermittent signals such as burst or frequency hopping threats.

To find out more about OSCOR's Trace Analysis capabilities, consider REI's TSCM training classes -- contact sales@reiusa.net for more information.

The Cost of Espionage

continued from page 1

So how big is the problem and who's at risk? Tim Barker of the Orlando Sentinel in his article "Are you safe from corporate spies" summed it up this way, "There is an easy way to figure out if you might be a target: If you sell anything worth buying, you've got something worth stealing."

According to the PricewaterhouseCoopers study 2007 Global Economic Crime Survey, "Of the 5,248 companies in 40 countries that took part in the research project, over 43% reported suffering one or more significant economic crimes during the previous two years."

A recent article by Kevin Greenberg at Forbes.com tells of a study by Purdue's Krannert School of Management where CIOs were surveyed about the loss of intellectual properties in 2008. The value of lost information is staggering. Of the 119 respondent CIOs, the value of stolen information last year was $559 million or $4.6 million per company.

Most companies assume malicious information theft won't happen to them; however, establishing a value for a company's intangible and intellectual assets often brings light to the risk. The problem is that determining the value of an organizations intangible assets appears confusing if not impossible. The reality is that it is not as difficult as it sounds. Statistics show on average 70% of a companies assets are "intangible." The example above demonstrates this using Coca-Cola. This "Intangible Value" comes from many things including not only trade secrets, product designs, computer code and formulas, trademarks and patents, but also information such as customer lists, sales information, company and product strategies, goodwill, image, brand and competitive advantage, etc.

Any of these targets can result in loss of profitability, reputation, image, competitive advantage, core technology, and goodwill. Espionage attacks these specific information items, and these assets have real monetary value that is affected and is at risk from espionage etc. Forms of espionage used to obtain competitor intelligence typically fall into one of three categories: White, Gray and Black Zones. The White Zone contains legal and reasonably ethical methods of intelligence gathering such as open source and competitor profiling. Open sources of information gathering can include internet, newspapers, trade shows, annual reports and even the hiring of former employees. The Gray Zone includes activity that may be legal but not particularly scrupulous or ethical, like dumpster diving or misrepresenting oneself to gain information - not necessarily illegal, but likely unethical. The Black Zone is activity that uses clearly illegal and unethical methods such as eavesdropping (technical surveillance), theft of information, computer hacking, recruitment of moles, direct theft, terrorism and coercion. etc.

The bottom line is that it really doesn't matter if the information was obtained legally or ethically, all that really matters is what is the financial risk or exposure due to the lost information (espionage). Once organizations realize this, they can then properly adjust the security spending appropriately, dispersing security resources according to the financial value at risk, tangible or intangible. The key is applying the appropriate resources to the appropriate risks.

More to protect than secrets and product designs

Example: Coca-Cola *2007 Coca-Cola Earnings Release

$142.3 Billion	Company VALUE* or Worth Total Market Value defined by stock price
- $43.3 Billion	Total ASSETS* (Cash, property, building, inventory, equip., etc.) Usually protected by security
$99 Billion	Intangible Value (intellectual & intangible property, brand equity, etc.) Not tracked by accounting, usually not protected by security

70% of the companie's value is intangible assets, of course, this is before the economic crisis.

PRODUCT FOCUS

CMA-100

Countermeasures Amplifier

The CMA-100 is a high gain audio amplifier that is used to detect and identify certain types of surveillance devices connected to building wiring including telephone wiring, LAN, Server systems, de-energized AC power, etc....

A well shielded microphone attached to wiring can be difficult to detect. The CMA-100 is an ideal tool to analyze miscellaneous wiring for audio content. Some problem scenarios of that can be discovered with a High Gain Amplifier are:

1. Microphones can easily be installed in miscellaneous wiring such as thermostats, motion detectors, intercom speakers, AC junction boxes, etc…
2. Utilizing an unused pair of wires or LAN wiring to connect directly to a shielded microphone in the suspect environment.
3. A phone set with a hot microphone or hot earpiece used as a microphone.
4. Many digital phone systems have audio leakage that occurs on the digital lines due to cross talk within the phone set. A CMA can be used to expose this type of vulnerability.

The CMA-100 is designed to provide flexible features and will prove to be very useful in many sweep environments.

2009 REI TRAINING CALENDAR

TCC-110
Telephone Security
Countermeasures Course
April 14 - 17

TSE-101
Technical Security
Countermeasures Course
April 14 - 17

DTC-210
Digital Telephony Course
April 20 - 24

TSCM-201
Technical Securities
Countermeasures Course
April 20 -24

TSE-101
Technical Security
Equipment Course
May 5 - 8

TSCM-201
Technical Securities
Countermeasures Course
May 11 - 15

TCC-110
Telephone Security
Countermeasures Course
June 2 - 5

TSE-101
Technical Security
Countermeasures Course
June 2 - 5

DTC-210
Digital Telephony Course
June 8 - 12

TSCM-201
Technical Securities
Countermeasures Course
June 8 - 12

TEC-250
Telephone Equipment
Certification
June 15 - 19

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

Visit our online calendar

IN THE NEWS

PROTECTING FEDERAL BUDGET FROM PRYING EYES
globeandmail.com
Source: www.globeandmail.com
Article: http://www.theglobeandmail.com/servlet/story/RTGAM.20090124.wbudget_lockdown23/BNStory/National

PUTTING A PRICE ON CYBERSPYING
Forbes Magazine
Source: www.forbes.com
Article: http://www.forbes.com/2009/01/28/cyber-espionage-ip-technology-security

DECT WIRELESS EAVESDROPPING MADE EASY
The Register
Source: www.theregister.co.uk
Aritcle: http://www.theregister.co.uk/2008/12/31/dect_hack/

WORLD'S SMALLEST FUEL CELL
The New Scientist
Source: www.newscientist.com
Article: http://www.newscientist.com/article/dn16370-worlds-smallest-fuel-cell-promises-greener-gadgets.html

NEB. MAN SUES EX-WIFE FOR PUTTING RECORDER IN TOY
WBIR News
Source: www.wbir.com
Article: http://www.wbir.com/news/local/story.aspx?storyid=73798

IPHONE OR SPYPHONE
The 33TV
Source: www.the33tv.com
Article: http://www.the33tv.com/pages/content_landing_page/?Use-of-Cell-Phone-Spy-Software-Could-Be-=1&blockID=171723&feedID=460

ONE IN FOUR WOMEN SPY ON PARTNER
The Telegraph
Source: www.telegraph.co
Article: http://www.telegraph.co.uk/scienceandtechnology/4371411/One-in-four-women-spy-on-partners.html

SPYING ON EMPLOYEES
Financial Post
Source: www.financialpost.com
Article: http://www.financialpost.com/working/story.html?id=1200495

COURT SHUTS SITE SELLING KEY LOGGING SPYWARE
Security Management Magazine
Source: www.securitymanagement.com
Article: http://www.securitymanagement.com/news/court-shuts-site-selling-key-logging-spyware-004868

Research Electronics International
455 Security Drive • Algood, TN 38506 USA
TEL +1 931.537.6032 • FAX +1 931.537.6089
www.reiusa.net