RESEARCH ELECTRONICS INTERNATIONAL

NEWSLETTER
Q4 2006

INSIDE THIS ISSUE:

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

Traditional Telephone Test Methods and Equipment

Throughout history, there have been many testing methods to detect and locate telephone taps or other devious methods of comprising the security of a telephone line. One of the best resources is *Telephone Eavesdropping and Detection* by Charles L. Taylor. The purpose of this article is to provide a brief overview of some types of equipment that has been historically used for testing telephone systems for technical threats. It should also be noted that there have been many telephone analyzers that were designed for this purpose, however most telephone analyzers contain some limited form of the basic testing functions described in this article.

Multi-Meter

A Multi-Meter (or more commonly called a DMM for Digital Multi-Meter) is a portable device that measures common static electronic parameters such as voltage (AC or DC), current, resistance, and capacitance. Measuring these types of parameters may provide some indication of a telephone tap. For example, if there is a parasitic type tap that draws power from the telephone line, then it is expected that the DMM will measure a slight voltage drop on the line. Furthermore, if there is a series type tap, then it is expected that the line resistance will increase due to the added in-line device. There are other types of taps that may also be detected using a DMM, however a DMM test is NOT a completely reliable test method mainly because it is relatively easy to design taps using transformers, high impedance resistance values, and blocking capacitors to make the tap practically invisible to most DMM testing methods. Therefore, it is important to understand that a telephone analyzer that relies heavily on DMM type testing methods is NOT reliable against even a moderate technology telephone tap.

Time Domain Reflectometer, TDR

A Time Domain Reflectometer, or TDR, is a very useful device for analyzing the integrity of a line. It works on the same basic principal as RADAR. A high frequency pulse is launched down a wire and if there is an impedance anomaly on the wire, a portion of the pulse will be reflected and can be measured.

CONTINUED ON PAGE 2

ORION Featured in News Story: Cell Phones in Prisons

A recent Fox News Undercover Investigation report explores the problem and technological solutions of contraband cellular phones being smuggled inside prisons and into the hands of dangerous criminals where they can be used to jeopardize criminal cases, endanger witnesses, even costing lives… This epidemic in the correctional system represents the fastest growing form of prison contraband.

The ORION Non-Linear Junction Detector is featured in this news story as one of the leading technologies being used to combat the cellular phone problem inside correctional facilities.

For more information on this news story, see Fox29 online:
http://www.reiusa.net/quick/Fox_Cell_Phones_Prison
Or, see the News section on REI's web site.

455 SECURITY PLACE • ALGOOD TN 38506 USA • TEL +1 931.537.6032 • 800.824.3190 (US ONLY) • FAX +1 931.537.6089 • WWW.REIUSA.NET

Traditional Telephone Test Equipment

CONTINUED FROM PAGE 1

It is important to understand that wiring is designed as a transmission line to deliver signals from one location to another. Any change in the physical characteristics of the wiring will result in an electromagnetic change which is basically an impedance anomaly. TDR's are mostly used to evaluate the integrity of a wire to search for faults, breaks or other major flaws or problems in a wire (not necessarily to look for telephone taps or technical compromises). Impedance anomalies result from wiring splices, an open, a short, phone blocks, phone jacks; or for TSCM purposes a connection from a telephone tap. Hence, a TDR can provide some ability to analyze the integrity of a line and potentially find the location of a Telephone Tap.

However, one basic difficulty when using a TDR is that while the TDR is transmitting or "launching" the pulse, it is basically blinded during the transmission period. For example, it cannot receive a reflection from an impedance anomaly if it is still transmitting the pulse. Different pulse widths are available when launching a pulse (also referred to as shooting a line). Therefore a narrow pulse (for example, 2 nanoseconds) is used to look for short-range anomalies, while a much wider pulse (1 microsecond) must be used for long range searching. Also, from looking at the TDR results, it is practically impossible to tell if an impedance anomaly is the result of the normal wiring plan passing through a connection block, or if it is the result of a tap. One recommendation is to compare the TDR graph of each pair combination in a wire. It is expected that each pair will pass through the connect block at the same range whereas a tap is only expected to exist on the main pair of interest.

In conclusion, a TDR is a useful piece of test equipment, but it must be well understood. Additionally, the pulse width selection must be manually adjusted and the graphs must be properly interpreted and compared to other pair combinations to gain any useful information.

Audio Amplifier

An audio amplifier is an important piece of equipment, especially when dealing with basic analog telephone systems. An audio amplifier gives you an indication if a phone line is being used to pass audio when it shouldn't be passing audio (for example: if the phone has been compromised with an open microphone, the speaker phone is unknowingly turned on, or an eavesdropping microphone is using unused phone wire pairs to carry the information out of the target area).

The most common type of phone amplifier is the traditional Butt-Set. Modern Butt-Sets often have features that include voltage readings and sometimes a simple TDR function that might tell you line length, but nothing more.

The biggest problem with using a Butt-Set (or other analog audio amplifier) is that the audio amplifier is very limited. It will not provide indication of a low level audio signal. And, it does not provide any capability to demodulate a digital audio signal; therefore, it is impossible to know if a digital system has been compromised by sending audio down a line that is supposedly not in use.

Line Tracer

Line tracers are used to physically trace a line or to identify the end of a specific line. They typically work on the principal of putting a low frequency signal on a line and using a separate handheld receiver to trace the wiring. Earlier line tracers operated on audio frequencies, however more modern and more reliable models use a low frequency of a few hundred Kilohertz. A line tracer is a very useful tool when it is required to physically search a long length of wiring.

CONTINUED ON PAGE 4

REI Users Conference California

Two Dates and Locations

February 21-23
Los Angeles

February 26-28
San Diego

These 3-day Conferences will:

- Introduce the new Trace Recorder for the 5.0 OSCOR,
- Demonstrate the OSCOR 5.0 methodology for trace analysis and RF mapping,
- Provide hands-on exercises for these new operational approaches, and
- Introduce REI's new Digital Telephone Analyzer.

These conferences will cost US$ 695 per attendee & will include lunches each day. REI can provide you with a recommended hotel where conference attendees will receive a discounted rate.

If you are interested in attending this Conference, please contact Michelle Gaw at +1 931-537-6032 or michelle@reiusa.net to reserve your seat.

NEWS HEADLINES: Corporate Espionage & Information Theft...

"Bosses get into 007 gadgets"
CNET News
November 20, 2006
Source: http://www.cnet.com
Article: http://tinyurl.com/y9lks9

"Business data breaches found to be more costly than thought..."
Government Executive
October 23, 2006
Source: http://www.govexec.com
Article: http://tinyurl.com/yb7y5v

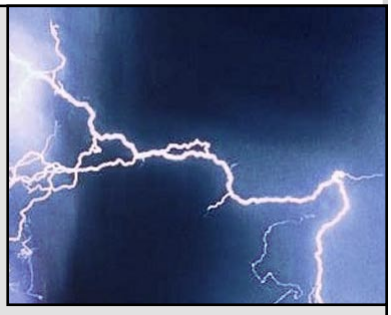
"Office Technology: Is it safe to make a copy..."
North Bay Business Journal
December 4, 2006
Source: http://www.busjrnl.com
Article: http://tinyurl.com/yjrh8g

"HP settles with California in spy scandal"
CNET News
December 7, 2006
Source: http://www.cnet.com
Article: http://tinyurl.com/yb3cr2

"Espionage alert to Bahrain firms"
Gulf Daily News, December 5, 2006
Source: http://www.gulf-daily-news.com
Article: http://tinyurl.com/ykausv

"Curse of the keystroke loggers who cost businesses £1bn a year"
The Scotsman.com
December 3, 2006
Source: http://www.scotsman.com
Article: http://tinyurl.com/ycqxa7

TSCM TIPS



ESD Precaution

For OSCOR & CPM-700 users, remember that electro-static discharge (ESD) is much more prevalent during the winter months and can damage your equipment.

To prevent ESD on the CPM, use caution when using the chrome, telescoping standard RF antenna (50kHz-3GHz); alternatively use the "hardened" all black European probe which is ESD protected.

When using the OSCOR, make sure the OSCOR is plugged into a grounded outlet and touch the chassis of the OSCOR to discharge any potential static energy.

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.

2007 REI TRAINING CALENDAR

January 16 - 18
Telephone Security Countermeasures Course (TCC 110, formerly BTC)

January 16 - 19
Technical Security Equip. (TSE 101)

January 22 - 26
Technical Surveillance Countermeasures (TSCM 201)

Jan 29 - Feb 2
Advanced TSCM Concepts (ATC 301)

February 6 - 8
Telephone Security Countermeasures Course (TCC 110, formerly BTC)

February 6 - 9
Technical Security Equip. (TSE 101)

February 12 - 16
Technical Surveillance Countermeasures (TSCM 201)

March 6 - 9
Telephone Security Countermeasures Course (TCC 110, formerly BTC)

March 6 - 9
Technical Security Equip. (TSE 101)

March 12 - 16
Technical Surveillance Countermeasures (TSCM 201)

March 19 - 23
REI Equipment Certification Course (ECC 240)

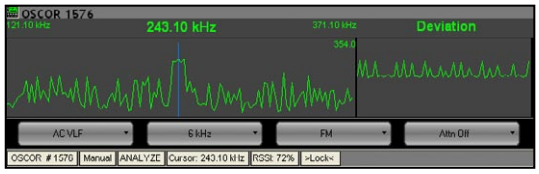
Questions, comments, suggestions, or to add someone to the REI Quarterly Newsletter mailing list, please e-mail: newsletter@reiusa.net

Traditional Telephone Test Equipment

CONTINUED FROM PAGE 2

Carrier Current Spectrum Analyzer

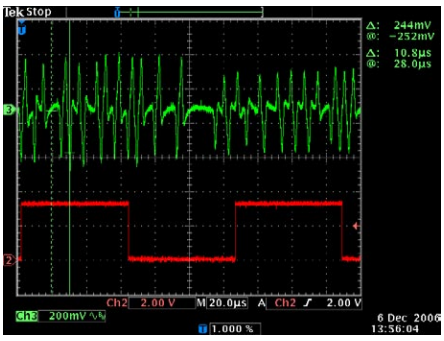
A spectrum analyzer is a useful piece of equipment to determine if a signal has been modulated (transferred) to a higher frequency and transmitted over the wiring.



A spectrum analyzer provides a unique capability to visually see signals that exist at different frequencies. The OSCOR has a built-in Carrier Current capability up to 5 MHz and with the optional Carrier Current Probe (CCP-700), the OSCOR can display signals modulated on a wiring system up to 150 MHz. The important point is that wiring should be evaluated for Carrier Current threats, and these types of threats will not be detected by basic DMM and audio type testing methods.

Oscilloscope

An oscilloscope is a useful piece of test equipment that provides the ability to visually see the waveforms in a wiring system.



For most audio signals, it is clear to see when audio is present because the waveforms correlate to the formation and presence of spoken words. However, in some cases, just listening to an audio amplifier of a line does not verify that there are digital signals present because the digital frequency of transmission may not be in an audible frequency range. A spectrum analyzer, as previously described, provides some added indication that signals may be present, but it would be useful to visually see the digital signals to verify that there is digital transmission on the line. The figure shown is a digital signal taken from a good digital oscilloscope and it shows clear digital signals.

Summary

Throughout history there have been many testing methods that have been used to look for telephone taps and compromises. This article only provides a very brief overview of some of these methods. While all of these tools and methods are useful in analyzing telephone systems, used individually they cannot reliably evaluate the integrity of a line. Reliable and accurate telephone line analysis requires a combination of the tools and tests listed above, as well as some tests and tools outside the scope of this article.

REI has developed a new soon-to-be-released Telephone And Line Analyzer that integrates and automates standard telephone testing tools (as described in this article), as well as new Patented testing technology (digital demodulation, line NLJD, FDR, etc); this new product will establish a new state of the art in telephone testing for both Digital and Analog telephone systems. This new Telephone And Line Analyzer, called the TALAN, will be released in 2007. Additional information on this product will be coming soon.

Look in future REI Newsletters for information on this new product.