

INSIDE THIS ISSUE:

The Basic Anatomy of a Phone Line Tap

NEW TSCM Telephone Security Course BTC-110

Training Calendar

OSCOR OPC Version 5.04 Now Available

REI Users Conference San Antonio Texas Nov. 7-9

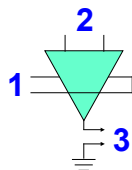
In the News: TSCM Related Headlines and News

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

The Basic Anatomy of a Telephone Line Tap

This article is a continuation of previous articles on telephone threat concerns and will provide a brief description of the basic anatomy of a phone line tap. While it is impossible in this newsletter to provide a lengthy technical description of different tap configurations, this article attempts to provide an introduction to the basics and a better understanding of tap detection methods. It is important to note that these phone tap descriptions could be utilized to attack both analog and digital telephone systems (using commercially available digital phone decoders, digital audio can be recovered from a digital system using these tapping methods).

Below is a basic general circuit diagram for a tap where the Green triangle represents an amplifier circuit. The leads labeled #1 represent the power supply to the tap circuit, the leads labeled #2 represent the actual tap onto the line, and the leads labeled #3 represent the means of transferring the signal to some other source.

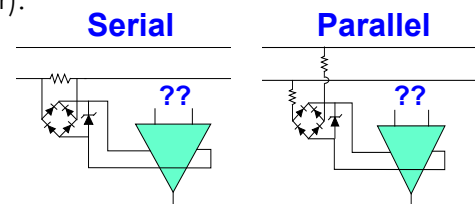


Each of these connections to the tap circuit

provides a potential opportunity to detect and locate the tap.

Power Supply Taps

If the tap draws power from the existing telephone line, then the tap is referred to as a "Parasitic" tap and is relatively easy to detect simply because when the tap is operating the circuit will draw power from the phone line. This drop in power may be measured using a simple Digital Multi-meter. There are 3 common types of test that will reveal this type of tap by measuring Voltage, Current, or Loop resistance. The figures below show two configurations of parasitic taps: a series parasitic (meaning that the power is drawn from a single line) and a parallel parasitic (meaning that the power is drawn across the pair).



If the Tap draws power from another source (Non-Parasitic) such as a battery or external supply, then relying on Multi-meter type methods for detecting the tap are much less reliable mainly because it is relatively easy to extract the signal from a phone line without

CONTINUED ON PAGE 2

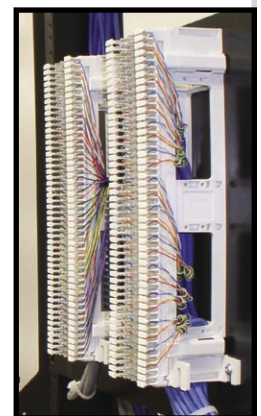
NEW TSCM Telephone Security Course: BTC-110

Are you up to speed on the latest telephone security issues?

Telephone eavesdropping threats are becoming more difficult to detect as newer telephone systems (both analog and digital) are becoming more technically advanced.

REI is pleased to announce a new three (3) day telephone security training course designed to provide the technical security specialist with a good basic understanding of digital and analog telephone systems and countermeasure tests. This course will introduce students to the basic operation of analog and digital telephone systems and the inherent weaknesses of these systems. Students will also be introduced to different

CONTINUED ON PAGE 4



Anatomy of a Telephone Tap

CONTINUED FROM PAGE 1

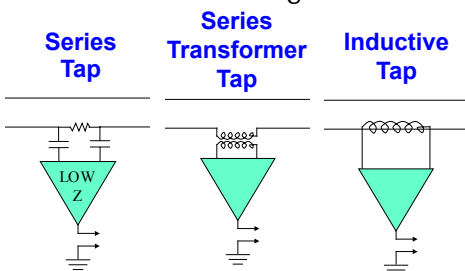
drawing enough power from the line or changing the impedance of the line to detect the tap with multi-meter methods. Therefore, better testing methods are required for non-parasitic taps.

Tapping Methods

There are many tapping methods. Some of the basic methods are broken into categories below for a brief discussion.

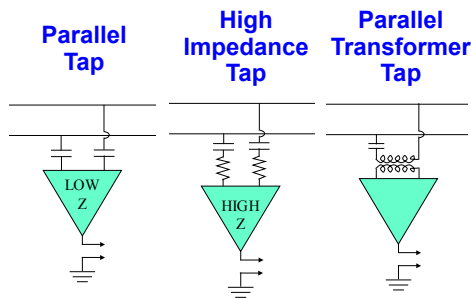
Series Taps

The following diagrams show different types of series taps. The first example requires that an in-line resistor is added to the line. This version (Series Tap) is typically easier to detect due to the voltage drop on the line. However, the Series Transformer Tap and Inductive Tap are more difficult to detect with multi-meter resistance measurements simply because multi-meter testing is based on a Direct Current test, and transformers and inductors basically look like a low ohm short circuit in this type of testing. In other words, the line resistance is changed very little. Therefore, to see the series transformer tap and the inductive tap requires more sophisticated testing methods that rely on a higher frequency measurement of the line impedance. A TDR provides increased reliability, but detection is not guaranteed.



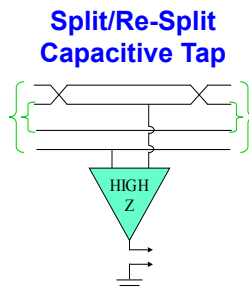
Parallel Taps

The following diagram provides some examples of parallel type taps. These tap examples will not be seen by conventional voltage or resistance testing because the in line capacitors block any DC testing of the line. Therefore, more sophisticated testing methods that rely on higher frequency testing to penetrate the blocking capacitors are required for detection. A TDR will work in many cases, however, the Capacitive coupled, high impedance tap will still provide little response to a TDR and still be difficult to detect at longer ranges.



Split/Re-split Tap

In the following diagram, the tap is not directly connected to the main pair that is carrying the information.



To understand this tap, it is important to understand the concept of a balanced pair. A balanced pair means that the 2

conductors that make up the pair are twisted together. This twisting ensures that the internal inductive and capacitive effects of the wires effectively cancel each other out so that the wire can carry higher frequency signals for much greater distance with minimal signal loss. In the diagram above, the green brackets indicate the balanced pairs that the phone system is designed to expect. However, if 2 conductors of the pair are not twisted with each other, but are twisted with other conductors, then these other conductors will absorb much of the signal information due to the capacitive coupling of the twisting. In most cases, the phone system will continue to function properly, but the result is that an unused pair in the cable bundle will now have a good signal level and can be tapped for information. This type of coupling is easily achieved by intentional miswiring the connectors on both ends of the cable. Furthermore, in older buildings that were wired using flat cable, an unused pair may pick up enough signal from the main pair that the unused pair can easily be tapped for information. This type of signal leakage is often referred to as "Cross Talk". In summary, this type of tap will not be detected with Multi-meter or TDR testing methods of a single main pair. The TDR may give some indication that the pair is not properly balanced, but detection is not clearly indicated in the one pair because the actual tap is present on other conductors. This type of tap can only be detected by testing all wiring combinations. For

CONTINUED ON PAGE 3

REI TRAINING CALENDAR

- October 9-13
Technical Surveillance Countermeasures (TSCM 201)
- October 16-20
Advanced TSCM Concepts (ATC 301)
- October 31 - November 2
Basic Telephony Course (BTC 110)
- October 31 - November 3
Technical Security Equip. (TSE 101)
- November 6 - 10
Technical Surveillance Countermeasures (TSCM 201)
- November 7 - 9
Users Conference in San Antonio Texas
- November 13 - 17
Equipment Certification Course (ECC 240)
- December 5 - 7
Basic Telephony Course (BTC 110)
- December 5 - 8
Technical Security Equip. (TSE 101)
- December 11 - 15
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

Anatomy of a Telephone Tap

CONTINUED FROM PAGE 2

example if there are 8 conductors in a cable bundle, there will be 36 total combinations of potential pairs: (1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 2/3, 2/4, 2/5, 2/6, 2/7, 2/8, 3/4, 3/5, 3/6, 3/7, 3/8, 4/5, 4/6, 4/7, 4/8, 5/6, 5/7, 5/8, 6/7, 6/8, 7/8) or it is calculated as $(7+6+5+4+3+2+1=28)$ and then it is important to test each individual conductor to ground. This adds another 8 pairs to the test.

In summary there are other variations of line taps that are described above and there are certainly additional types of phone threats that are not covered in this article. This article is only intended to pro-

vide some of the basics. The main point is that to reliably detect different types of taps, there are many types of tests that should be conducted on many combinations of conductors.

This fall, REI will introduce a new Digital Telephone Analyzer that will address all of the technical issues described above including new patented testing technology that will increase detection reliability and provide testing functions specifically for Digital Phone Systems.

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



OSCOR OPC Version 5.04 Now Available

REI is pleased to announce the release of OSCOR OPC Version 5.04 Program Key and OPC Software. If you have an older version, you are urged to obtain a new key and new OPC Software.

This release provides:

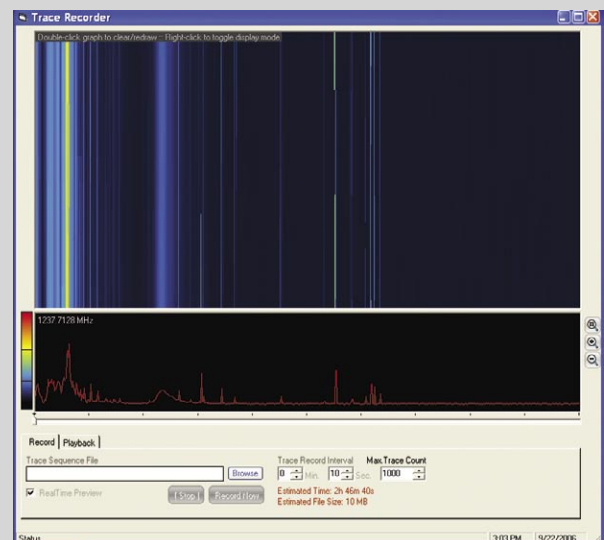
- Greater report configuration flexibility & print control,
- Updated printing WYSIWYG dialog,
- Improved date handling to be more internationally aware,
- Improved job structure,
- Manual editing of the signal in the list classification column,
- ITU/FCC signal classification can now be applied to ALL signals if desired,
- Improved trace window updates while running in Auto-Mode.

If you have an OSCOR version 5.0 and would like to receive a new program key and software, please use the link below: <http://www.reiusa.net/opc5>

If you are interested in upgrading your pre-5.0 OSCOR to current specs, contact REI at sales@reiusa.net



Additionally, 5.04 allows for a new Trace Recorder (waterfall) application that will be released in the coming weeks as a software download (no new key needed), see screenshot to the right.



REI Users Conference in Texas

November 7-9
San Antonio Texas
 Hosted by AT&T

This 3-day Conference 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.

This conference will cost US\$495 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.



Photo courtesy San Antonio Convention Center.

Telephony Security Course

CONTINUED FROM PAGE 2

types of analog and digital telephone system attacks, and how to detect these types of attacks.

BTC-110 course topics include:

- Telephone History
- Basic Telephony
- Basic Analog Tests & Equipment
- Digital Telephone Systems
- Digital System Capabilities
- Basic Digital Tests
- Digital Telephone System Weaknesses
- Digital Telephone System Log Files

REI has expanded its training facilities specifically for this course by adding a Telephone Testing Classroom including a complete, isolated

digital phone system with six (6) individual phone block test stations. Additionally, this phone system is wired with phone sets in seven (7) project rooms creating a real-world environment. This digital phone system gives students the ability to practice the concepts and tests taught in the BTC-110 course on an actual "live" digital telephone system.

The new BTC-110 course and additional training facilities demonstrates REI's continued commitment to providing World Class TSCM training and equipment.

For available dates, check REI's website or e-mail sales@reiusa.net.



NEWS HEADLINES: Corporate Espionage & Information Theft...

"One in three UK directors steals company secrets..."

The Business Online (UK)
 September 10, 2006
 Source: www.thebusinessonline.co.uk
 Article: <http://tinyurl.com/hg58p>

"Bugging the Boardroom"

BBC News, September 5, 2006
 Source: <http://news.bbc.co.uk/>
 Article: <http://tinyurl.com/hjqkl>

"Corporate Snoops...gumshoes will do what most execs can't or won't..."

BusinessWeek Online
 October, 2006
 Source: <http://www.businessweek.com>
 Article: <http://tinyurl.com/zy4uq>

"Out of the Shadows, a Pretexter's Tale"

CNET News, September 26, 2006
 Source: <http://news.com.com/>
 Article: <http://tinyurl.com/ongks>

"Coke Re-Evaluates Trade Secret Protections"

WJLA TV Atlanta, July 7, 2006
 Source: <http://www.wjla.com>
 Article: <http://tinyurl.com/fu92f>

"Industrial espionage made easy"

myadsl.co.za (Financial Times), June 2, 2006
 Source: <http://www.mybroadband.co.za>
 Article: <http://tinyurl.com/hjtzk>

"Briefly: WestJet apologizes to Air Canada over spying"

International Herald Tribune, May 29, 2006
 Source: <http://www.iht.com>
 Article: <http://tinyurl.com/j9ojx>

"Man tried to tap woman's phone"

Asbury Park Press, September 9, 2006
 Source: <http://www.app.com>
 Article: <http://tinyurl.com/f6b7x>

