TSCM Quarterly

ISSUE Q3 2017

WWW.REIUSA.NET

WHAT'S INSIDE

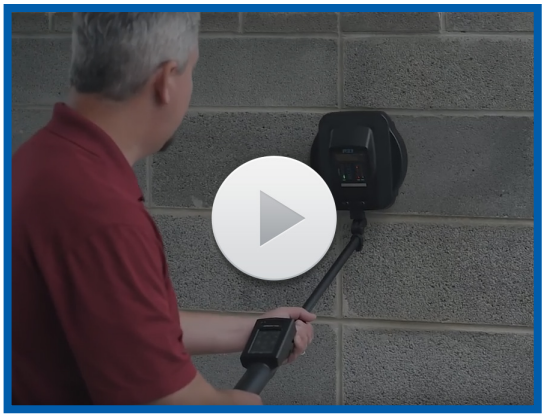
Research Electronics International
455 Security Drive Cookeville, TN 38506 USA
+1 931 537-6032 | 800-824-3190 (US only)
Fax +1 931 537-6089
www.reiusa.net

NEW NLJD LOCATES ELECTRONICS IN A VARIETY OF ENVIRONMENTS

The new ORION 900 HX Non-Linear Junction Detector from REI detects electronic semi-conductor components through dense materials such as bricks, concrete, and soil. The longer 900 MHz wavelength excels at detecting older, less refined circuitry and also penetrating building and construction materials compared to the shorter wavelength of the 2.4 GHz model, which excels at detecting modern, surface mounted circuitry in normal office environments.

For those with both applications, a new ORION HX Deluxe package is available which includes interchangeable 900 MHz and 2.4 GHz antenna heads. The antenna heads are easily exchanged in under twenty seconds by simply turning a pair of thumb screws. The touch screen controller on the ORION handle automatically recognizes the attached antenna and displays the corresponding data.

The ORION antenna head is a transceiver (transmitter and receiver) that radiates a 1.25 MHz-wide digital spread spectrum signal to determine the presence of electronic components. When the signal encounters semi-conductor junctions (diodes, transistors, circuit board connections, etc.), a harmonic signal returns to the receiver.



ORION HX Deluxe introduction video

The receiver measures the strength of the harmonic signal and distinguishes between 2nd or 3rd harmonics. When a stronger 2nd harmonic signal is present, visual, audio, and haptic feedbacks alert users that a junction has been detected.

The standard transmit power of the ORION 900 HX FCC model is 1.4 W EIRP with operating frequencies between 905 and 925 MHz. A higher power "G" model with 3.2 W EIRP and a wider frequency range is also available. Due to the variety and complexity of compliance organizations across the globe, several different ORION models exist. Consider the following when selecting your ORION:

- What is your application - office-like environments, or areas with dense materials like brick or concrete?
- Do you need a CE, FCC, or IC compliant model?
- Do you prefer a touch screen or keypad?

Visit the REI website for more information about the ORION 900 HX and the ORION HX Deluxe.

All new ORION orders will come with the quick-disconnecting handle, allowing customers to add-on the alternate antenna head at any time.

ANDRE ONE-DAY TRAINING COURSE

REI will be hosting a one-day ANDRE training at REI headquarters in Tennessee. This one-day course will provide a thorough overview of the ANDRE's functionality and several hands-on exercises in our dedicated project rooms.

November 16, 2017
8:30 AM - 4:30 PM CST
Cookeville, Tennessee USA

Countermeasures Core Concepts - Level One is a prerequisite for the ANDRE course. The cost for the complete day of training, with complimentary lunch, is $295 per person. Seating is limited to 20 students.

Course Topics

- Broadband Receiver Technology
- RF Detection Overview
- Basic ANDRE Operations
  - Histogram View
  - Zoom Function
  - Signal List
  - Audio Functions
- Probes and applications
- Hands-on Exercises

Register Now

WHEN TSCM AND CYBERSECURITY COLLIDE

Is your company evaluating how to protect its intellectual assets? An IBM-sponsored study reports that the average cost of a data breach is $3.62 million and the average size of data breaches is on the rise. Today's existing internet and mobile phone networks serve as digital listening posts anywhere in the world. There are more frequent occurrences where technical security vulnerabilities are opening the door to cybersecurity threats:

GSM-modified wireless keylogger

Disguised as a USB wall charger, this radio transponder/antenna/GSM combination can remotely transmit sensitive log-in information and passwords captured from a wireless keyboard. These devices also have the capability to continue transmitting on an internal battery even after being unplugged from the wall.

Wireless keyboards that are not utilizing Bluetooth or that are not encrypting their data streams are susceptible to this threat. Even with the onset of touch screens, people are still continuing to purchase keyboards and over 60% of workers prefer having a keyboard to accompany their tablet.

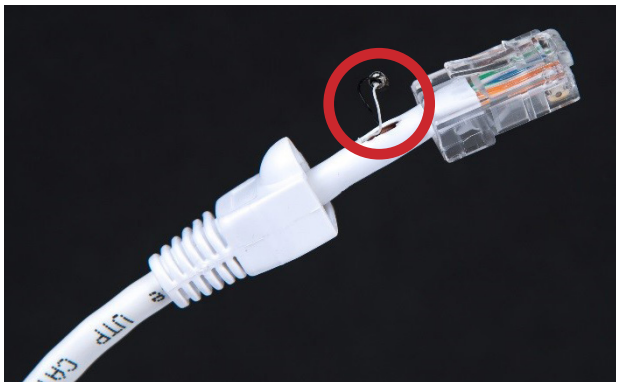
Wi-Fi IP camera

This IP camera can operate on your existing Wi-Fi network or on its own network. For under twenty dollars, this device transmits amongst regular network traffic could be used to spy on executives to garner blackmail material or to steal trade secrets. With 1080p HD video output, this device can transmit for days when attached to an external battery or other power supply.

Wiretaps transmitting information

A trusted conversation takes place between a corporate executive and IT professional as they troubleshoot an issue or as they discuss a recently-discovered security vulnerability that could leave the company exposed to a data breach. Without their knowledge, their conversation could be transmitted via a hard-wired microphone on a Cat5 cable. Desk lines can be a target for the loss of confidential information.

Standard network cable



Microphone embedded inside network cable

Despite a focus on cybersecurity, traditional surveillance devices are thriving and can be used to increase the threat of an attack. Cybersecurity Ventures predicts global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the next five years. As funding sources shift, do not overlook the importance of thorough physical security audits and TSCM practices.

OSCOR REMOTE MONITORING OVER POWERLINES

In the previous REI newsletter we discussed the importance of spectrum analyzer mobility in order to locate transmitters. Detecting and identifying types of signals is very important, but locating transmitters is equally, if not more important if you want to find malicious surveillance devices, and that requires a portable receiver. Moving the spectrum analyzer reveals changes in signal amplitude as it gets closer or further away from a signal's source.

We've also discussed in another issue how to connect to the OSCOR with Virtual Network Computing (VNC) software for remote monitoring. With 3rd party VNC software, an Ethernet cable and a laptop, and a wireless router for wifi connection, the OSCOR can be turned into an in-place RF monitor. This can be useful for monitoring meeting rooms or conference areas for temporary observation. One significant benefit to using the OSCOR in this situation is the OSCOR continuously sweeps a 10 kHz-24 GHz span and is not limited by antenna frequency range. That means you can remotely monitor 24 GHz or zoom to any frequency within the span.

OSCOR and EoP

In this article we'll discuss another option for remote in-place monitoring with the OSCOR using existing power lines. Ethernet over Power (EoP) is a way to network computers and home devices using power lines.

Sending signals over power lines has been around for many years. In fact, power companies have been sending control signals over power mains since the 1920s and have used this way to determine how they switch to off-peak rates. In recent years, the convenience of wireless networking had almost obscured this medium into obsolescence, but advancements in speed and utility have renewed applications for its use.

Setting Up a Network

We tested the OSCOR on a powerline network which proved to be a quick, simple, and discreet way to observe RF activity from another room. One very important benefit to this is that setting it up didn't require IT support.

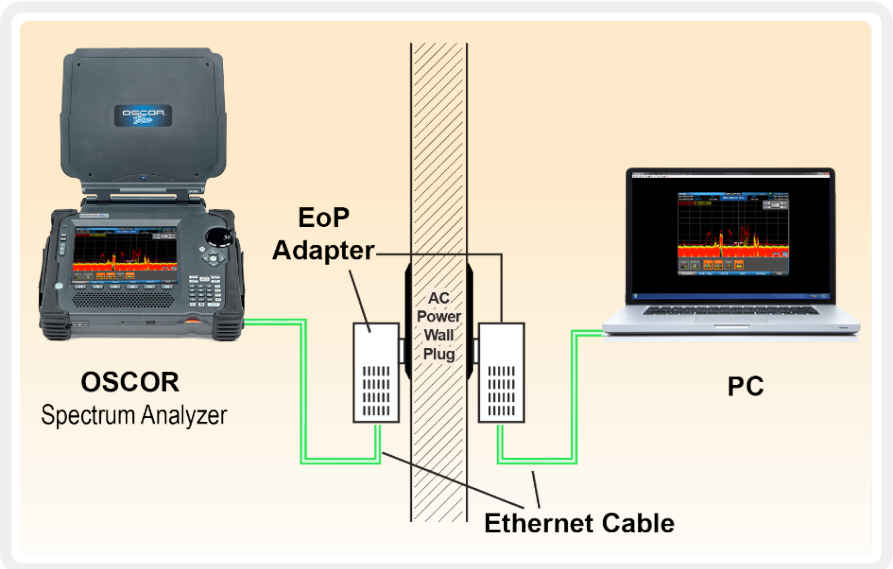
Nothing against IT, but it means:

1. It's simple enough you should be able to do yourself, in many cases passing lists of approvals
2. The number of people involved can be controlled
3. Technical complications are minimized
4. Setup does not interfere with existing networks

The powerline network we tested included 2 NETGEAR Powerline 1000 adapters with advertised speeds of 1000Mbps. Most adapters support Gigabit-class network capacity and can auto-detect and auto-connect. A pair of Ethernet cables were included. On the PC, we also installed TightVNC Viewer version 1.3.10. There may be other suitable VNC programs, but this is one we had used before and were familiar with.

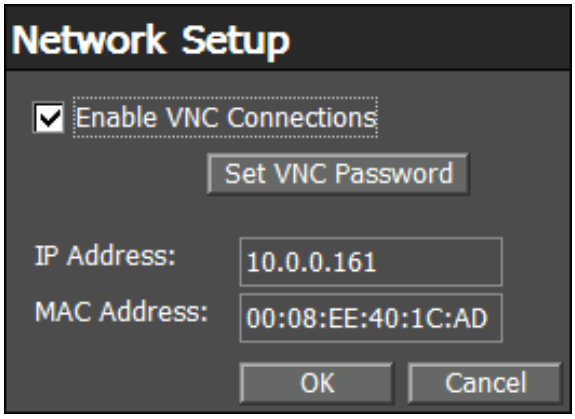
One Ethernet cable connects the OSCOR to one of the powerline adapters. The second Ethernet cable connects the PC to the 2nd powerline adapter. Both adapters plug directly into a wall outlet (the outlets must be on the same phase).

Continued on next page >



OSCOR REMOTE MONITORING OVER POWERLINES

An IP address must be acquired on the OSCOR from the System\Network dialog screen. A VNC password must also be set on the OSCOR (must be 8 characters with 1 number and 1 capital letter). Write down or take a picture of this IP address and password and hit "OK" (see below). Both the IP address and password must then be entered into the "VNC server" field of the "New Connection" dialog box. Then select "Connect".

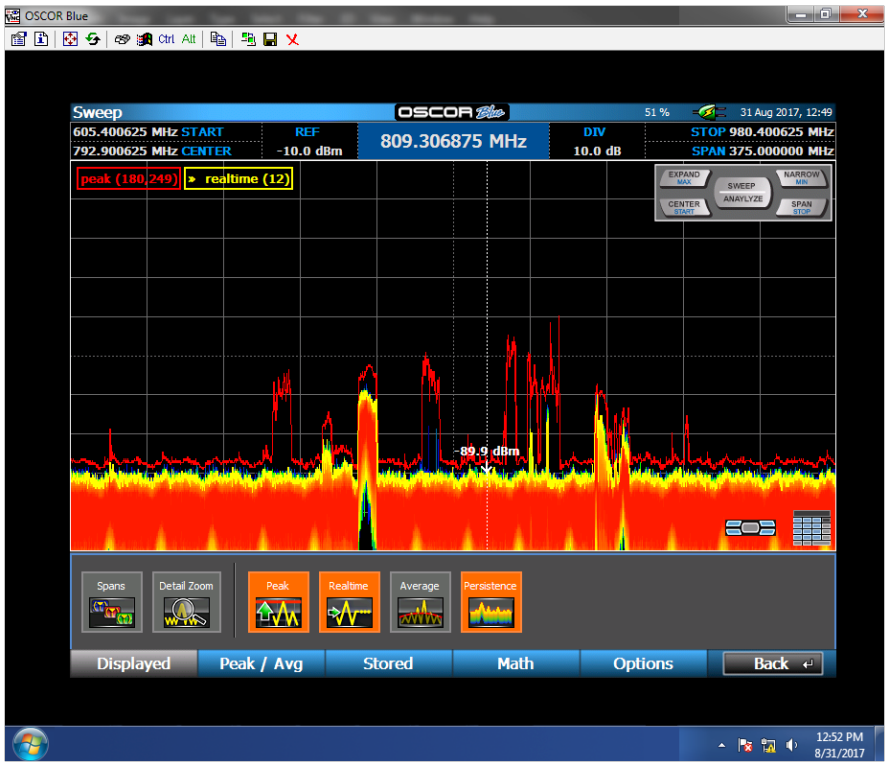


A live view of the OSCOR screen should appear in the VNC Viewer with the ability to change views, navigate the menu structure, change between Sweep/Analyzer modes, and control the OSCOR just as if you were sitting in front of it. Trace Record, Spectrogram and waterfalls can all be controlled from the PC. Screen shots can be captured and saved to files and even transferred to the PC through a menu function in the VNC Viewer. The PCs keyboard and mouse make navigation and typing easy. Once the adapters are synced, controlling the OSCOR is simple.

There are a few limitations we observed in our test:

- Power adapters will not work on filtered power lines.
- Power adapters must be on the same power phase.
- While the OSCOR refresh and sweep speeds don't change, the VNC connection only updates approximately once every 2 seconds.
- There is a potential for network interruptions, however, the network did reconnect automatically. We also found that adding a router to the network eliminated interruptions.
- A recording can be made of a suspect signal and saved as a .wav file, then transferred and listened to on the master PC to determine if it is room audio. However, live audio cannot be listened to.

The OSCOR is both portable and versatile, and in situations where stationary monitoring is needed, a remote powerline connection may be an excellent solution for concealment, deployment, and detection.



The OSCOR screen as seen remotely in the VNC Viewer software.

Announcement: REI will be releasing an OSCOR Blue and OSCOR Green software update this fall. Watch our website for more information!

2017 TRAINING CALENDAR

Advanced Equipment Use Level 3
September 25 - 29

Countermeasures Core Concepts Level 1
October 2 - 6

RF OSCOR Course Level 2
October 9 - 13

TALAN Telephone Countermeasures Course Level 2
October 9 - 13

TALAN Certification Level 3
October 16 - 20

Countermeasures Core Concepts Level 1
October 30 - November 3

RF OSCOR Course Level 2
November 6 - 10

TALAN Telephone Countermeasures Course Level 2
November 6 - 10

RF OSCOR Course Level 2
November 13 - 17

Countermeasures Core Concepts Level 1
November 27 - December 1

RF OSCOR Course Level 2
December 4 - 8

TALAN Telephone Countermeasures Course Level 2
December 4 - 8

VoIP Course Level 3
December 11 - 15

2018 TRAINING CALENDAR NOW AVAILABLE

TSCM IN THE NEWS

BRITISH AND IRISH LIONS SWEEP FOR LISTENING DEVICES
Source: Sky Sports
Article: http://bit.ly/2u623sz

AUSTRALIAN GOVERNMENT SPYING ON CHINESE EMBASSY, STATE-RUN NEWSPAPER SAYS
Source: The Guardian
Article: http://bit.ly/2t7KKoM

RUSSIAN AGENT JAILED FOR SPY PLOT ON LITHUANIA'S PRESIDENT
Source: Newsweek
Article: http://bit.ly/2sG1vXt

SPY CAMERAS FAST EVOLVING TO FEATURE IN UNEXPECTED OBJECTS
Source: Korea Herald
Article: http://bit.ly/2uzizOK

A HACKER TURNED AN AMAZON ECHO INTO A 'WIRETAP'
Source: Wired
Article: http://bit.ly/2uiNRy2

HIDDEN CAMERA FOUND INSIDE WALGREENS BATHROOM
Source: New York Post
Article: http://nyp.st/2w4xnXW

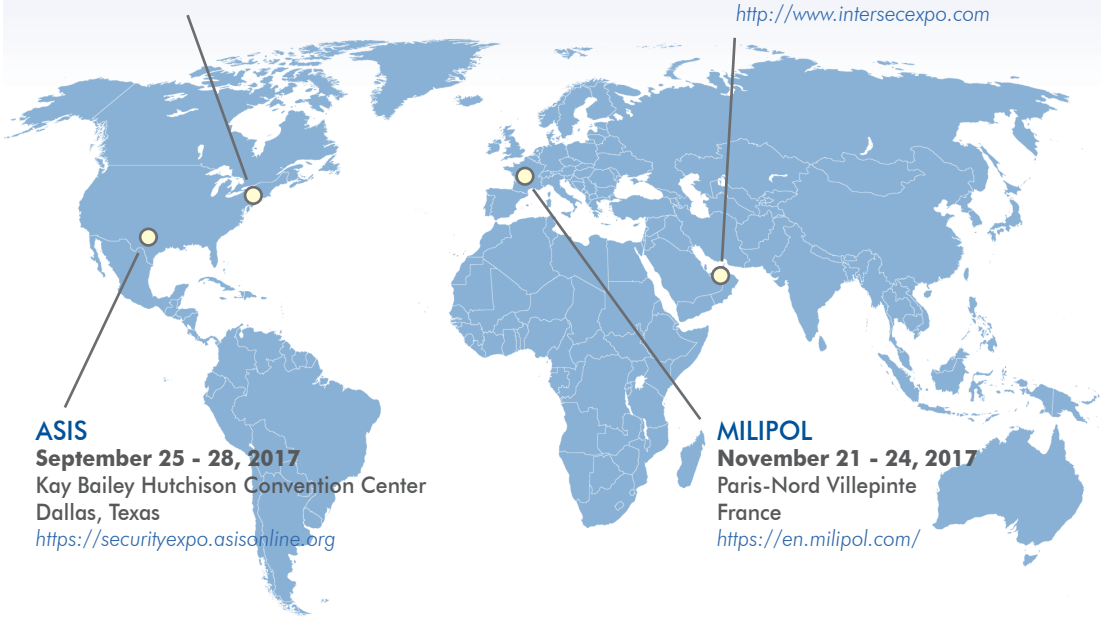
HOW RUSSIAN SPIES BUGGED THE US STATE DEPARTMENT
Source: CNN
Article: http://cnn.it/2wyGlzZ

POLICE: INTERNATIONAL CORPORATE ESPIONAGE TARGETED LOCAL COMPANY
Source: WCVB
Article: http://bit.ly/2wxEp8b

TRADESHOWS & SEMINARS

ISC EAST
November 15 - 16, 2017
Javits Center
New York, New York
http://www.isceast.com/

INTERSEC
January 21 - 23, 2018
Dubai International Convention and Exhibition Center
Dubai, UAE
http://www.intersecexpo.com



ASIS
September 25 - 28, 2017
Kay Bailey Hutchison Convention Center
Dallas, Texas
https://securityexpo.asisonline.org

MILIPOL
November 21 - 24, 2017
Paris-Nord Villepinte
France
https://en.milipol.com/

REI®

For questions or comments, or to subscribe, please email newsletter@reiusa.net.