TSCM Journal
2019 ISSUE 2
REI®
WWW.REIUSA.NET

ANDRE WHIP ANTENNA: SIMPLE ENHANCED DESIGN

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

The most commonly used antenna included with the ANDRE Near-field Detection Receiver is the Whip antenna. It is significantly larger than the other antennas and is an effective general-use antenna for locating RF signals. In this article, we dig into how the whip antenna is designed and why it is considered the more commonly used antenna in the kit.

A whip antenna is a basic antenna design, typically consisting of a straight, flexible wire or rod connected to a receiver. Shown in the picture is the Standard RF Probe from the CPM-700 Deluxe, which is a traditional whip antenna. When the CPM-700 and ANDRE antennas are viewed side by side, it's obvious the ANDRE antenna is a very different design.

So is it really a whip antenna?

Well yes, and no: it's referred to as a Whip antenna because its use is similar to the standard CPM-700 RF probe. However, it is much more than a simple whip antenna. To be specific, it is a hybrid between a fat monopole and a circular dipole antenna. But that complicated description is a bit wordy for a product label.

By merging multiple antennas in this particular design, broadband sensitivity is maximized across a wide frequency band. This benefits the user by not having to change antennas as often while searching an extensive radio frequency range for possible illicit devices. The length of the ANDRE Whip antenna allows users to see devices transmitting as low as 30 MHz and as high as 6 GHz. Possible devices in that range include baby monitors, GSM bugs and Wi-Fi transmitters.

The effectiveness of any antenna is a balance between sensitivity, direction, and distance. Antennas, such as the Locator Probe, are designed to operate in a wide frequency band similar to the Whip, but at a shorter distance from the target. The downconverter antenna is very effective as well, but only operates in a directional

Continued >

WHIP ANTENNA Cont'd

fashion. The ANDRE needed an effective, general-purpose antenna that offered users a reliable, broad frequency range. While the directional antenna included with the ANDRE provides greater detection distance, the Whip outperforms the directional at lower frequencies.

With a design much more robust than a traditional whip antenna, its versatility makes it the likely first choice to begin a counter-surveillance sweep. Learning how to use the multiple ANDRE antennas together based on their strengths saves users time and increases the effectiveness of their sweeps. If you are interested in training specifically geared towards TSCM and the operation of the ANDRE, please visit the REI Training Center.

REI

THE 7 BENEFITS OF REI TRAINING COURSES

REI trains hundreds of students every year with varying levels of experience. We have found that our students benefit most from a training program that combines classroom instruction with hands-on experience, and have designed the REI Training program around this concept.

Here are seven additional benefits of a 5-day course at REI's training center:

EXCLUSIVE TRAINING FACILITY

REI's Training Center has over 10,000 square feet of newly renovated classrooms and simulation rooms. Our instructors have applied decades of experience into designing project rooms where students practice detecting and locating hidden electronics. As one of our trainers said, "We can offer a better quality training on site because the environment is controlled."

HANDS-ON LEARNING OPPORTUNITIES

While students can expect to log time in the classroom throughout each course, they will also use investigative equipment in practical applications. The project rooms simulate real-world situations where students practice using equipment and training to locate hidden threats.

EXPERIENCED INSTRUCTORS

REI's six full-time instructors have over 60 years of combined technical security experience. They work hard staying up to date on modern threats and current practices for conducting TSCM investigations.

MULTI-TIERED CURRICULUM

The Countermeasures Core Level One course introduces students to the components of a counter-surveillance investigation and the necessary equipment used in an investigation. By the end of the week, students will be ready to branch into a Level 2 RF or Telephone TALAN course for more specialized understanding of each subject, and beyond that to a Level 3 Certification course.

PRODUCT EVALUATION

Purchasing TSCM equipment can be an expensive undertaking and technically intimidating. Having the opportunity to evaluate the equipment throughout a Countermeasures Course may help with the decision. It may also provide a more thorough understanding of the quality, capability and even the limitations of REI products. Plus, if you decide to purchase equipment, you'll be prepared to put it to work right away.

BENEFITS OF REI TRAINING COURSES - CONTINUED

CHECK UNDER THE HOOD

"No one knows our equipment better than we do," Anthony Reep, Technical Instructor. Students attending the Core Level 1 course receive a factory tour, where they will see REI's in-house manufacturing operation. We pull the curtain back for students, so they can see the quality and care that goes into the products and how that benefits the customer.

NETWORKING OPPORTUNITIES

REI trains students from all over the globe with different nationalities and cultures. We value the shared knowledge and experiences of our students, and we encourage others to collaborate and learn from this opportunity. A recent student summed up his training experience well when he said, "TSCM is such a niche line of work - getting to connect with people from around the world is invaluable."

For more information regarding training courses you can visit ***https://reiusa.net/rei-training-center/***

UPDATED TRAINING CLASSROOMS

Over the past 12 months, all of our training classrooms have been renovated to provide a more comfortable and advanced training environment.

UPCOMING BIPS

The Business Intelligence Protection Seminars will explain the threats posed by electronic eavesdropping devices and illicit surveillance. Wrongful exposure of sensitive information can put a company's security at risk. The mere perception of compromised information can lead to negative publicity, damaged alliances, and loss of employee or shareholder confidence.

BIPS presentation topics include:

- Modern threat overview
- Introduction of new REI products including the ANDRE Deluxe, ORION HX Deluxe, and TALAN 3.0
- Product-specific Q&A

Seminars begin at 9:00 AM. Registration is free and refreshments will be provided.

Trenton, New Jersey
Homewood Suites by Hilton Hamilton
960 US Highway 130
Hamilton, NJ 08690
MAY 16 2019

Austin, Texas
Embassy Suites Austin Central
5901 North I-35
Austin, TX 78723
JUNE 4 2019

Dallas, Texas
Embassy Suites Dallas Market Center
2727 N. Stemmons Freeway
Dallas, TX 75207
JUNE 6 2019

USB CABLES CAN HIDE A NEW PAYLOAD THREAT

Modern Threats

In previous articles, we discussed how lines sometimes blur between cyber security and TSCM, where skills from both disciplines may be needed to identify threats. Here's a recent example that illustrates this, where transmitters and receivers can be used to initiate a cyber attack.

There are USB cables that can be controlled remotely via wireless/bluetooth to inject a payload with command line/keystrokes onto a computer. The computer can be remote controlled, accessing networks, files, control settings, permissions, or a critical information. It could also be used to inject a virus.

One particular product that has been covered in recent security forums is the USBNinja by RFID Research Group. When dormant, USBNinja is a regular USB cable, able to transfer data and charge devices. From the outside, there is no reason to suspect it is anything but a standard USB cable. But a Bluetooth PCB is masterfully concealed inside the housing.

When it receives a command from a smartphone with the manufacturer's app, or from the custom Bluetooth remote controller, it changes from a passive to an active controller, emulating a USB mouse and/or keyboard to deliver the payload to the host.

Open source programming standard, Arduino IDE, provides completely customizable payload development capability. USBNinja will supply payload examples that inject keystrokes and move and click the mouse.

USBNinja offers several kits from beginner to professional and includes Micro-USB, USB Type C, and Lightning cable (Apple). Current and voltage are the same as standard cables (4-25V@10mA). The wireless Bluetooth controller includes a 3.6V 40mAh rechargeable battery, with a 98-328 ft/30-100m range with the 2,3, or 18 dBi antenna. The smartphone app also allows Bluetooth access.

In this YouTube video, Vincent Yiu of USBNinja demonstrates how it works:
https://www.youtube.com/watch?v=UhBK-M2iXwA

The 2 primary defense strategies being discussed online regarding these USB payload attacks are:

1. Impose impractical restrictions on all USB devices

2. Establish awareness and prevention policies

There are actually many measures that can be employed to help reduce the threat - whitelisting/blacklisting peripherals; IT controls (locking unused ports); locking down approved devices, HR policies restricting personal devices, etc. They mainly relate to passive preventative measures and all have holes that can be exploited. For now, until there's a silver bullet for this attack, it's best to remain vigilant using any unfamiliar USB cables.

SPY STORIES FROM HISTORY

Queen Elizabeth's Spy Master

The Stage

England's Queen Elizabeth I, daughter to Henry VIII, became England's ruler in 1558. One of her first acts as queen was the establishment of an English Protestant church, of which she was made Supreme Governor. During her reign, tension was high between Protestants and Catholics and Queen Elizabeth was constantly concerned for her throne.

In 1567, Elizabeth's Catholic cousin, Mary Stuart, Queen of Scots was forced to give up her Scottish throne and fled to England, where she was placed under house arrest. There were rumors and plots among Catholics to overthrow the queen and replace her with Mary. England's military was weak, the treasury lean, and relations with neighboring countries tenuous. Security depended on intelligence.

Sir Francis Walsingham, Elizabeth's Principal Secretary, was a spy master with a zeal against Catholicism. He built an intelligence network over several decades at home and abroad of well connected, educated spies. Walsingham was one of the authors of a law called Bond of Association that passed in Parliament in 1586 authorizing the execution of anyone attempting to usurp the throne or assassinate the Queen.

The Babington Plot

That same year, while still under house arrest, Mary, Queen of Scots began getting letters from Anthony Babington, a Catholic rebel who was part of a group who wanted to kill the Queen, and return England to the Catholic Church. Gilbert Gifford was an exiled Catholic and one of Walsingham's operatives who built a relationship with Babington, stoking his rebellious appetite. Gifford worked out a way with conspirators to smuggle coded correspondence to and from Mary concealed in beer kegs. What Mary and Babington's collaborators didn't know, was every letter passed through Walsingham, who deciphered the code and forged copies. He even altered a reply from Mary with a request for the names of all the conspirators working with him. Babington, being young and impressionable, eagerly provided them.

The Reveal

In one of the letters Babington wrote to Mary, he detailed plans of her rescue and asked her permission to kill the Queen. Mary's reply agreed with the plans, but she did not authorize the assassination. When the letter passed to Walsingham, a postscript was added authorizing the assassination. Walsingham had all he needed to bring the conspiracy to light. Within days, Babington, Mary and the other conspirators were arrested. Babington, begging for the Queen's mercy, was tried and executed in 1586. Mary was tried and beheaded in February, 1587. Walsingham continued serving the Queen a few years longer but battled illness to his end. Admired by Protestant intelligentsia, despised by Catholics, Sir Francis Walsingham died in 1590, broke and out of favor. But England's original Spy Master influenced the course of history.

SPANISH VOIP PLUS+ LEVEL 3 TALAN TRAINING

REI ofrece un curso de español de 5 días sobre VoIP del 30 de septiembre al 4 de octubre en el Centro de Capacitación REI en Cookeville, TN, USA.

DESCRIPCIÓN

Este curso introducirá a los estudiantes a la tecnología emergente de VoIP desde una perspectiva de contravigilancia. Los estudiantes obtendrán una comprensión de los conceptos básicos de hardware y software de la red VoIP. Si bien el enfoque se centrará en probar las características de una red para determinar posibles amenazas y vulnerabilidades, los estudiantes usarán soluciones de hardware y software adicionales para capturar y analizar múltiples tipos de tráfico de red.

Cursos de requisitos previos: Contramedidas Conceptos básicos y Contramedidas telefónicas de TALAN.

Haga clic aquí para registrarse o para más información.

REI is offering a 5-day Spanish VoIP course from September 30 to October 4 at the REI Training Center in Cookeville, TN, USA.

DESCRIPTION

This course will introduce students to the emerging technology of VoIP from a counter surveillance perspective. Students will gain an understanding of VoIP network hardware and software basics. While the focus will be on testing the characteristics of a network to determine potential threats and vulnerabilities, students will use additional hardware and software solutions to capture and analyze multiple types of network traffic.

Prerequisite Courses: Countermeasures Core Concepts and TALAN Telephone Countermeasures

Click here to register or for more information

RECENT TRADESHOW REVIEW

The 2019 Tradeshow seasons is in full swing and officially kicked off with a team from REI attending IDEX in Abu Dhabi, UAE. The REI booth had a consistent flow of people and generated great discussions about TSCM. We look forward to exhibiting at this show in the future.

After returning from IDEX, our crew was off again the following week for Security and Policing in Farnborough, UK. REI co-hosted a booth with International Procurement Services, LTD (IPS). Security and Policing is an annual show with opportunities to meet government, military, law enforcement and public safety/security entities.

2019 TRAINING CALENDAR

RF OSCOR Course Level 2
April 29 - May 3

VoIP
May 6 - May 10

RF OSCOR Course Level 2
May 6 - May 10

Advanced Equipment Use
May 13 - 17

Countermeasures Core Concepts Level 1
June 3 - 7

RF OSCOR Course Level 2
June 10 - 14

TALAN Telephone Countermeasures
June 10 - 14

VoIP
June 17 - 21

Countermeasures Core Concepts Level 1
July 15 - 19

Countermeasures Core Concepts Level 1
August 12 - 16

RF OSCOR Course Level 2
August 19 - 23

TALAN Telephone Countermeasures
August 19 - 23

VoIP
August 26 - 30

Countermeasures Core Concepts Level 1
September 9 - 13

Spanish Levels 1 & 2
September 16 - 27

CLICK HERE TO REGISTER

TSCM IN THE NEWS

FIRINGS AND LAWSUITS FOLLOW DISCOVERY OF SECRET BUGGING DEVICES AT LAW FIRM; 'IT'S VERY JOHN GRISHAM
Source: ABA Journal
Article: https://bit.ly/2CoQPmI

IN BREXIT'S CITY OF SPIES, EAVESDROPPERS ARE EVERYWHERE
Source: Bloomberg
Article: https://bloom.bg/2HokTTN

TRIBUNAL HEARS HOW DENTAL TECHNICIAN FOUND HIDDEN CAMERA IN OFFICE
Source: Irish Examiner
Article: https://bit.ly/2XWMIHH

THE SPY INSIDE YOUR CAR
Source: FORTUNE
Article: https://bit.ly/2Tbzoff

CARROLLTON MAN PLAYS 'SECRET' RECORDING IN CIVIL COURT, GETS TAGGED WITH FELONY EAVESDROPPING CHARGE
Source: The Telegraph
Article: https://bit.ly/2UGfJW8

APPLE AIRPODS LIVE LISTEN CAN EAVESDROP ON CONVERSATIONS FROM ANOTHER ROOM
Source: The Independent
Article: https://ind.pn/2D1URlU

Stay up to date with REI on Twitter and LinkedIn

Follow us @REI_TSCM for TSCM in the news and information about upcoming shows and events.

TRADESHOWS & SEMINARS

BIPS NORTH EAST
Business Intelligence Protection Seminar
May 16, 2019
Trenton, NJ
https://reiusa.net/news/bips/

MILIPOL PARIS
November 19-22, 2019
Paris-Nord Villepinte Exhibition Centre
Paris, France
https://en.milipol.com/

BIPS TEXAS
June 4 & 6, 2019
https://reiusa.net/news/bips/

LEA-DER
May 15-16, 2019
Hotel LIONS
Prague, Czech Republic
http://www.lea-der.org/

For questions or comments, or to subscribe, please e-mail newsletter@reiusa.net.