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

Spread Spectrum and TSCM Implications

The purpose of this article is to briefly explain the concept of Spread Spectrum Signals and to address some of the issues associated with detection for counter surveillance purposes.

The basic concept of Spread Spectrum is that the energy that would normally be used to transmit a signal is spread across a wider frequency spectrum. Spread Spectrum technology has been around for many years, and it has been implemented in many different forms. A common type of implementation is called Direct Sequence Spread Spectrum (DSSS). In this process, a digital signal is mixed (using an OR function) with a higher data rate pseudo-random code. The data rate of the code determines the amount of spreading and the spreading factor. This has the effect of increasing the signal bandwidth and reducing the peak energy of the signal making it more difficult to detect.

For example, if a 200 KHz wide digital signal is transmitted within a 50 mwatt transmitter, then the signal may have a peak power of 1 mwatts/KHz at a spectrum analyzer at some undefined range. If a DSSS process is implemented with a spreading factor of 100, this would result in a signal that now has a signal bandwidth of 20 MHz (versus 200KHz) and a peak power of .01 mwatts/KHz making the signal somewhat more difficult to see with a TSCM spectrum analyzer at the same range. Hence, a large spreading factor makes the signal more difficult to detect. And, there is the technical possibility of spreading below the receiver noise floor so that the signal becomes invisible at a sufficient range from the transmitter. However, there are some technical issues that prevent a spread spectrum signal from being "below the noise floor" and invisible to a countersurveillance sweep.

First, extremely wide spreading requires long pseudo-random codes, and the Transmitter and Receiver must be synchronized using a special cross correlation broadband receiver. This becomes more difficult with large spreading factors and very low signal levels.

The second, and most important consideration is the Inverse Square Law of propagation (ISL), and the very good assumption that the countersurveillance receiver should be much closer to the transmitter than

the listening post. In simple terms, the ISL says that as the range from the transmitter is increased, the power decreases with the square of the range. So, if the range is doubled, the power decrease is quadrupled. Getting close to a transmitter will cause the received signal energy to increase dramatically. For example, at 1 meter from a transmitter, the signal strength will measure 100 times stronger than at 10 meters, and 10,000 times stronger than at 100 meters. Furthermore, the listening post may be on the other side of building walls, outside in a parking lot, or even across the street. Propagation through walls creates additional loss and requires that the transmitter
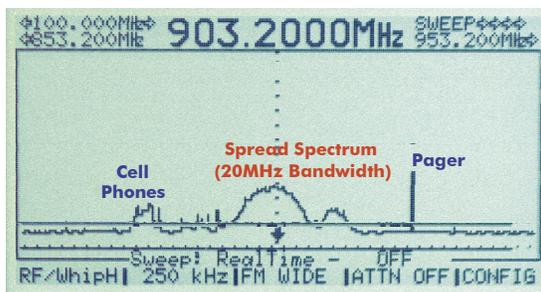
Common Business Security Vulnerabilities

In today's business environment, information is King; managing, sharing, and distributing that information is equally, if not more important. Technological advances such as e-mail, computer networking, fax machines, phone lines, video-conferencing, etc. allow us to overcome physical barriers to conducting business, no longer limiting the flow of information to the walls of the office building. While the exchange of information and business data has become more efficient, it has also become more vulnerable than ever. Making problems worse, most security personnel are not focused on potential information leaks until a problem has already occurred, damaging an organizations net worth.

The biggest vulnerability to today's corporate security professional may very well be related to information security. From the birth of a simple company directive or business plan, to its crumpled death in a trash can, the data and information will have passed effortlessly beyond locked doors and security checkpoints through fax machines, printers, copiers, filing cabinets, numerous employees, conferencing systems, and possibly hundreds of computer systems, not to mention discussed by employees in the company break room, at home, or other public locations. By identifying paths and potential vulnerabilities, the corporate security professional can quickly recognize

Security Vulnerabilities (cont. from page 1)

TSCM TIPS

Locating Infrared Transmitters
To locate an infrared transmitter after the OSCOR has indicated a signal, run your finger around the antenna to "break the line of sight" from the transmitter. When the signal disappears, your finger is in between the OSCOR IR antenna and the transmitter, giving you the direction of where the transmitter is located.

Equipment Tip:
Test the CPM-700 RF probe (50kHz - 3GHz) before each sweep to ensure that it has not been damaged by ESD discharge. To test the probe, collapse the probe and then hold the probe near the LCD screen of the CPM-700. You should hear a buzzing response from the LCD screen indicating that the probe is working properly.

For more information on performing TSCM sweeps, consider REI's Center for Technical Security training courses. Course descriptions and training dates can be found on REI's website (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.

---

a variety of information vulnerabilities:

Computer systems: Today's corporate security personnel must work closely with MIS/IT departments to ensure adequate security measures are in place (i.e. hard/strong password policies, network login procedures, remote e-mail/network access policies, physical controls, and proper network security applications, etc.).

Copiers, fax machines, and photocopiers: Modern copiers, fax machines, and printers contain computer processors and storage devices, enabling them to store and/or recall data, making them an easy target that could be exploited to gain proprietary information. Not to mention the paper copies that usually set on these machines before the recipient actually retrieves the hard copy paper.

Removable storage devices: USB storage devices encourage the mentality of, "What I can't do at work I can finish at home." A full page of text requires about 20 kilobytes of disc storage and with a 1 Giga byte USB device I could go home with 50,000 pages of text at one time. Today's laptops and even some desktop systems come with memory card readers built right in that will read several types of common flash memory cards.

Wireless presentation microphones: These are probably the most common source of "self-bugging". These are extremely inexpensive, and common in conference rooms or other environments where presentations are given. Many modern multimedia conference rooms are already equipped with this type of equipment and can broadcast outside the building.

Computerized Telephone/Conferencing systems: Modern PBX and ACD systems pose a huge threat to our information security. Some systems even allow voice mail messages to be e-mailed to a users selected address as attached .wav files, potentially sending confidential voice mails throughout the world-wide-web. Additionally, every office in a typical business building has at least one telephone, or likely a speakerphone, containing at least one microphone (speakerphones usually contain multiple microphones), that can easily be used to harvest intelligence or eavesdrop. Video Conference systems can also provide an open channel for an uninvited guest to "sit-in" on a private meeting from miles away. These systems need to be properly "secured" when not in use.

Trash: The simple act of throwing away a document may very well be handing the information to the competition. We have all read of cleaning personnel being paid to harvest the trash, or others helping themselves to dumpsters full of proprietary and confidential information. Once garbage is placed in a trash can or dumpster outside of a building, it is typically considered not illegal for someone to take it, in effect stealing corporate secrets. Proper disposal of company documents and document shredding is a must.

Business Travel/Trade Shows: Traveling employees and their laptop computers represent a treasure trove of competitive intelligence. Employees who travel or represent the company at trade shows or other events need to be aware of what information is appropriate to discuss, and what information should not be disclosed.

Sales Enquiries & Company Visitors: One of the most common competitive intelligence techniques is to pose as a potential customer, asking whatever information is desired. Prospective customers and/or company visitors should be qualified before any information is shared.

Employee Awareness: A regular security awareness briefing for all employees helps to not only raise awareness, but also the total level of security for the entire organization. The weakest link often lies with an organizations own people. Making sure that all employees recognize potential security threats increases the chance of preventing a breach of security.

In today's business world, it is imperative to know what your competition is up to, and more importantly secure yourself from potential information theft/loss. Information security represents the biggest potential loss for a company, and can usually be easily avoided with some simple attention from the proactive corporate security professional.

REI TRAINING CALENDAR

June 13 - 17
Technical Surveillance Countermeasures
(TSCM 201)

August 23 - 25
Technical Security Equipment
(TSE 101)

August 29 - September 2
Technical Surveillance Countermeasures
(TSCM 201)

September 13-15
Technical Security Equipment
(TSE 101)

September 19 - 23
Technical Surveillance Countermeasures
(TSCM 201)

September 26 - 30
Advanced TSCM Concepts
(ATC 301)

October 24-28
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

Shipping Equipment to REI: Return Authorization Procedure

With the summer months here and many people taking vacations, we are anticipating a great number OSCOR's being sent in for upgrades in the next few months. With this demand we also want to minimize the time that our customers may be without their equipment when returning it to REI for upgrades.

In an effort to better serve our customers and minimize the time our customers may be without their equipment, REI wants to let everyone know about our Return Authorization Procedure. Our intent is to streamline the process of returning equipment to REI for Upgrade and/or Repair Return. Please note the following procedure:

- Contact REI to obtain a Return Authorization Number BEFORE shipping any equipment to REI.
- Clearly write the Return Authorization Number on the outside of the returned package.
- Include with the returned equipment a letter with the following:
  1. The name and contact information of the person returning the equipment,
  2. The Return Authorization Number,
  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,"

    This is crucial for international shipments to avoid unnecessary tariffs, fees, or customs delays.

Please contact REI if you have any questions, or if you need to obtain an Return Authorization Number.

Spread Spectrum (cont. from page 1)

be of sufficient strength to overcome the range and propagation losses. Therefore, even if a sophisticated transmitter may be "below the noise floor" at the listening post, it is most certainly well above the noise floor, and easily detectable, in the target environment with any reasonable sweep receiver.

Broadband Detectors and Spread Spectrum
It is important to consider how a Broadband detector responds in the presence of a Spread Spectrum signal. Broadband detectors do not rely on tuned narrowband filters for detection; instead they rely on receiving the total energy from the transmitter. Therefore, whether a signal is spread or not spread has no impact on the performance of a broadband detector. A broadband detector is impacted more by the ambient RF environment and the range to the transmitter because the broadband detector depends on receiving the total energy from the transmitter and being close to the transmitter so that the Law of Inverse Squares gives a very large response. For example, received signal strength at 10 centimeters from a transmitter is 10,000 times stronger than at 10 meters from the transmitter. This is a 40dB gain without even considering going through walls. Therefore, the transmitter will not be "below the noise floor", and should easily be detected with a broadband detector.

To summarize, it is important to understand the issues associated with Spread Spectrum Signals; however, Spread Spectrum signals are not difficult to detect with sophisticated spectrum analyzers such as the OSCOR and/or good quality broadband detectors such as the CPM-700. For more information visit our website or e-mail sales at sales@reiusa.net.