Michael D. Glasser

Jeffrey S. Prusan

TSCM

TECHNICAL SECURITY COUNTER MEASURES

The real story behind sweeping for eavesdropping devices

Innovative Solutions....Effective Security

Corporate Defense Strategies
Mack-Cali Corporate Center
50 Tice Blvd.
WoodCliff Lake, New Jersey
07677
Phone 201-573-5900 or Fax

TSCM

Outline

- Tools used for sweeps
- Demo of how phones are tapped
- Signs that your offices are “Bugged”
- Who gets “Bugged”?
- How corporate spies infiltrate your infrastructure
- Spy shop “toys”
- What to do if you suspect you’ve been bugged
- Planning an execution of a successful sweep
- How to protect your company in the future against eavesdroppers

Copyright 2003 Corporate Defense Strategies

TSCM

Tools Used for Sweeps

Copyright 2003 Corporate Defense Strategies

TSCM

Tools used for sweeps

- Time Domain Reflectometer
- NearField Detector
- Non-Linear Junction Detector
- Spectrum Analyzer
- Oscilloscope
- Physical Inspection

Copyright 2003 Corporate Defense Strategies

TSCM

Time Domain Reflectometer

Copyright 2003 Corporate Defense Strategies

TSCM

Time Domain Reflectometer

Time Domain Reflectometry is the analysis of a conductor (wire, cable, or fiber optic) by sending a pulsed signal into the conductor, and then examining the reflection of that pulse.

By examining the polarity, amplitude, frequencies and other electrical signatures of all reflections; tampering or bugs may be precisely located.

Any device or wire attached will cause a detectable anomaly, the TSCM technician will then perform a physical inspection at the location of the anomaly.

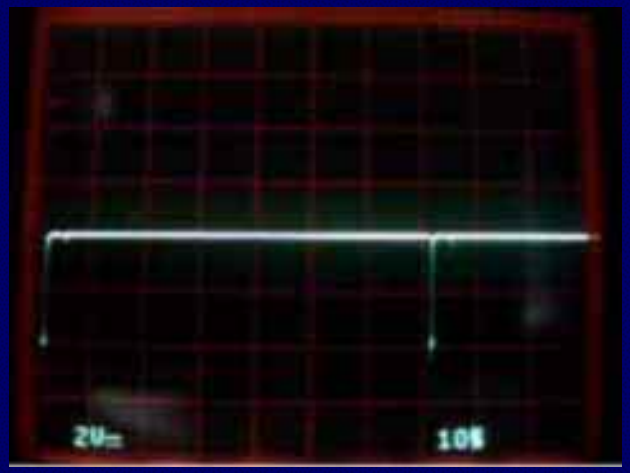
TDR analysis will usually NOT detect capacitively isolated devices or inductive taps. In the case of capacitively isolated device or inductive tap, the TDR sweep is always supplemented by a detailed high frequency cross talk evaluation and a detailed physical inspection.

Copyright 2003 Corporate Defense Strategies

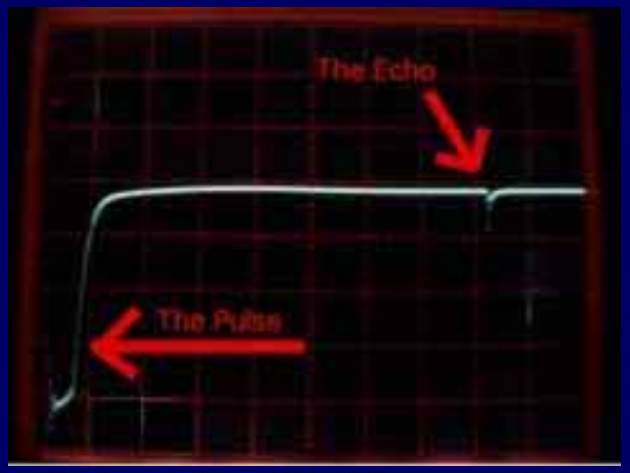
TSCM

Time Domain Reflectometer

The delay between the initial pulse and the reflected pulse indicate the length of the cable (or the location of an anomaly). The delay is divide by the speed of light, and multiplied by the proper velocity of propagation (based on the capacitance of one foot of cable), and then divide the result by two. On a ten mile section of cable a resolution of one tenth of an inch or better is typical (512,000 point TDR).



Signal Generator Pulse injected into cable



Echo Received from Pulse (Reflection)

Copyright 2003 Corporate Defense Strategies

TSCM

NearField Detector

Copyright 2003 Corporate Defense Strategies

TSCM

NearField Detector

A NearField Detector is designed to detect low level radio frequency (RF) radiation from transmitters, receivers, computers, etc. One of the two antennas detects towards positive while the other detects towards negative, therefore, if the source of RF energy is away from the two antennas (i.e. 20 feet or more) both antennas receive essentially the same amount of energy and the meter remains at zero. As the ratio of the distance between the RF source and the antennas decreases, one antenna receives more RF than the other and the meter swings on that direction. ***This effect is known as near field or differential detection.***

Copyright 2003 Corporate Defense Strategies

TSCM

NearField Detector

2055HA - NEAR FIELD RF DETECTOR/DIFFERENTIAL RF PROBE (MK IV)

This differential antenna detector covers from 10 to over 1,000 MHz and solves many of the problems encountered in very high level signal locations such as metropolitan areas. The level of radio frequency (RF) radiation from computers and other electronic equipment can also be observed with this unit. Supplied with amplifier/indicator assembly, RF head, two antennas, head extension rods and cables, special 2,000 ohm headset and carrying case. Uses two 9-volt batteries and incorporates internal battery test circuits.

The 2055HA covers frequencies ranging from lower than 10,000 Hz (10 Khz) to over 1,000 MHz or 1 GHz. The system consists of: amplifier/indicator assembly, RF head assembly, head extension rods, head extension cable, two multi-section antennas, two right angle BNC connectors, special 2,000 ohm headset, carrying case and instructions.

Copyright 2003 Corporate Defense Strategies

TSCM

NearField Detector

NEARFIELD DETECTORS

TO OPERATE: Insert the RF head assembly into the BNC connector on the top of the amplifier/indicator assembly and position so the two cover screws face the operator. Connect the two antennas with right angle adapters to the RF head and position so they are parallel. If the frequency of interest it above 500 MHz, collapse both antennas fully. For frequencies between 100 and 500 MHz, extend both antennas one section. For frequencies below 100 MHz extend both antennas two sections.

Insert the 2K ohm headset supplied into the HEADSET-2K jack. Do NOT use a low impedance headset (it simply won't work). The headset is worn with the gray stethoscope tube under the chin and the sound output holes facing slightly forward (roughly 30 degrees) or with the ear hook. Turn the unit ON and place the TONE/AUDIO switch in the TONE position. Zero the Meter with the ZERO SET control at the top of the unit. press the + BATTERY Test button. The meter will swing to the right and a reading in excess of + .8 indicates satisfactory battery conditions Pressing the - button causes the meter to swing to the left and again, a reading in excess of -.8 indicates a satisfactory battery condition.

Pass the antennas over the test areas If a source is located, the Meter will swing in the direction of the source and pass through zero when the source is perpendicular to the two antennas. Since the tone heard through the headset has a pitch proportional to the meter readings it is not necessary to observe the meter while searching for the source.

The lowest pitch tone indicator zero and the tone increases in pitch on either side of zero. The RF head can be extended with the extension handles and cable. Plug the cable BNC connector into the BNC jack at the bottom of the RF head. Plug the mini-plug into the jack located to the left of the BNC plug on the amplifier/indicator assembly.

Copyright 2003 Corporate
Defense Strategies

TSCM

NearField Detector

The 2055HA say also be used as a single antenna RF detector by removing the left antenna and zeroing the unit. The meter will swing only to the right when a source is located If the meter goes beyond full scale to the right, the zero may be suppressed to the left of center as required. The TONE/AUDIO switch causes either a tone proportional to the meter reading (TONE) or demodulated AM audio (AUDIO) to occur at the headset. the DC output of the op-amp is accessible through the RECORDER jack. This output is designed to drive a strip chart recorder.

Should either battery become weak (i.e. below .8), replace both batteries by removing the top and bottom screws from the amplifier/ indicator assembly and carefully lifting off the back cover. Alkaline batteries are always preferred. While the back cover is off, note the three screw-driver adjust potentiometers The one in the upper center above the upper integrated circuit is the rough zero. The control to the right (as viewed from the back) of the integrated circuit is the gain control, The control below and slightly to the right of the gain control is the base tone adjustments To re-enter the position of the ZERO SET control, set that control to mid-range and adjust the rough zero control for zero indication on the Deter. To adjust the base tone, zero the meter and set this control for a tone output of roughly 5 to 20 Hz. As with any piece of electronic equipment, remove the batteries during periods of prolonged storage.

Copyright 2003 Corporate Defense Strategies

TSCM

Non-Linear Junction Detector

Copyright 2003 Corporate Defense Strategies

TSCM

Non-Linear Junction Detector

Back in the early 70's a method was developed to detect eavesdropping devices though the analysis of harmonic emissions caused by an illuminating signal when it is reflected off of a target. A few years later this method was used by the Super scout NLJD system (which was the first commercially available and patented NLJD).

Semiconductors contain multiple layers of silicon, a P-Type and an N-Type, the point where they meet is called a Non Linear Junction. This junction also appears in nature when dissimilar metals come in contact with one another (such as that used in the old crystal radio set). Also, the rust on a screw, the springs in a car, or the support structure in any piece of furniture may also contain non linear junctions (resulting from corrosion).

A Non Linear Junction Detector finds potential eavesdropping devices by flooding a suspect area or target with a spectrally pure microwave RF signal (usually around 888 or 915 MHz). Various frequencies are then monitored for a reflected harmonic signal.

The instrument typically has an antenna and a control unit. The antenna is mounted on an extendable pole, and really nothing more than a microwave waveguide which both emit and collects the signals (with a duplexer). The control unit is usually a multiple channel, highly sensitive radio receiver tuned to specific second, and third harmonic frequencies. While it is possible to measure the 4th, 5th, 6th, and other harmonics those above the third are only of limited TSCM value.

Copyright 2003 Corporate Defense Strategies

TSCM

Non-Linear Junction Detector

Power Level Issues

Non Linear Junction Detectors are available in a variety of power outputs ranging from the "civilian" version with an output below 25 mW, to the restricted Government version with a power output over 2 watts ERP. The Soviet and Chinese government actually use NLJD instruments which generate hundreds of watts of power, but often cost the TSCM specialist their vision (and other soft tissue damage) due to high levels of non-ionizing radiation. On an added note a NLJD should not be directed to any human or other living creature due to the potential of serious bodily harm. You can actually knock out a cardiac patients pacemaker from a distance with one, or cause serious soft tissue damage such as cornea injury, loss of hearing, kidney failure, and so on. As the power output increases the greater the range of the unit, and the penetration into solid materials.

As the power level increases, the sensitivity of the unit will decrease.

Normally a 2 Watt NLJD will detect an eavesdropping device through several inches of concrete, inside a wall, or buried deep inside a couch. The lower power units (50-100 mW) on the other hand will only detect eavesdropping devices inside a book, or devices only an inch or so away from the antenna (such as behind a few layers of sheetrock). Non Linear Junction Detector transmit power is relatively meaningless. The sensitivity and bandwidth of the receiver is a far more important issue. Cheap units use high power to overcome poor receiver sensitivity and poor noise figures. In general the better units (more effective) are the lower powered ones.

Much like an X-ray the power level must be variable based on the density of the object being inspected. Of course the more power you generate the more "alerting" your activities become, and the higher the risk of personal injury (just like taking an X-Ray). Generally a 1.5 Watt ERP unit with a variable output (adjustable down to around 5 mW ERP) works well, but if you use Digital Signal Processing or DSP in the unit to increase sensitivity the power levels can be drop to well below a Watt.

Copyright 2003 Corporate Defense Strategies

TSCM

Spectrum Analyzer

Copyright 2003 Corporate Defense Strategies

TSCM

Spectrum Analyzer

A good Digital Spectrum Analyzer is the "workhorse" of the TSCM industry.

When coupled with a computer, printer, and vector signal analyzer will detect virtually any RF eavesdropping device made (including the ones used by the FBI, NSA, CIA, SVR, CSE, MI5, GCHQ, etc).

Copyright 2003 Corporate Defense Strategies

TSCM

Spectrum Analyzer

The Tektronix 494A/P and 497A/P Spectrum Analyzer are the more recent additions to the 490 family. They include better frequency stability, markers, and better programming functions. Typical frequency of the 494A/P is from 10 kHz to 22 GHz, external mixers will increase the range to 40 GHz (or 325 GHz). The 497A/P model has operations similar to the 494 but the frequency coverage is limited to 100 Hz to 7.1 GHz. The 490 series has since been replaced by the FSE series out of Germany. Used instruments are commonly available for around $25,000 for a 494A/P, and $15,000 for the 497A/P. The 494A/P is the only spectrum analyzer in the Tektronix 490 family that ever saw wide spread usage in the TSCM industry. The 494 A/P version was fairly popular with all U.S. government agencies performing TSCM. The units are fairly easy to operate, lightweight, but temperamental when "bumped around". When used with an external demodulator the 494A/P becomes an excellent instrument for TSCM teams who travel heavily and are unable to transport a lab grade instrument.

Copyright 2003 Corporate Defense Strategies

TSCM

Oscilloscopes

Copyright 2003 Corporate Defense Strategies

TSCM

Oscilloscopes

All TSCM teams should have at least two Digital Storage Oscilloscopes, one should be a rugged hand held unit, and the other should be a lab grade unit with a 1 GHz bandwidth. Al least one unit should be computer controllable, and should be capable of direct postscript printing or computer control. The units most commonly found in the TSCM industry are the Tektronix TDS784 and the THS720 Digital Oscilloscopes, along with the Fluke 190 series. Both units are fully computer controllable, rugged, and designed to take years of abuse. DocuWave software and a PC should be used to control the scopes and store traces and data. The TDS784 offers 4 channels with a digitizing rate of 1GS/s (1 Billion samples per second) and work well for high resolution TDR work. When used to monitor the wideband output of a search receiver signals identification is made considerably easier. The THS720 Digital Oscilloscope offers 2 channels with a digitizing rate of 500 MS /s (500 Million samples per second). It comes in a small handheld case, and works well in the field, an excellent piece of equipment.

Copyright 2003 Corporate Defense Strategies

TSCM

Physical Inspection

Copyright 2003 Corporate Defense Strategies

TSCM

Physical Inspection

Regardless of how much technology you have physical inspection is still a crucial part of any TSCM sweep.

It is still necessary to get on your knees and up on the ladder!

Copyright 2003 Corporate Defense Strategies

TSCM

Demo of how phones are tapped

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

Others know your confidential business or professional trade secrets.

This is the most obvious indicator of covert eavesdropping activities. Theft of confidential information is a multi-billion dollar underground industry in the United States. Often the loss of your secrets will show up in very subtle ways so you should always trust your instincts in this matter. When your competitors know things that are obviously private, or the media finds out about things they should not know, then it is reasonable to suspect technical eavesdropping or bugging.

Secret meetings and bids seem to be less than secret.

Confidential meetings and bids are very popular targets for corporate spies. How would you like the plans for the corporate takeovers you're planning to become public knowledge? Would copies of your product designs be of any use to your competitors? Would it be beneficial for your competitors to know how much you're quoting for the same project?

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

You have noticed strange sounds or volume changes on your phone lines.

This is commonly caused by an amateur eavesdropper when they attach a wiretap, or activate a similar listening device. Surveillance devices often cause slight anomalies on the telephone line such a volume shift or drop-out. Professional eavesdroppers and their equipment usually do not make such noises; so if this is going on it could indicate that an amateur eavesdropper is listening in.

You have noticed static, popping, or scratching on your phone lines.

This is caused by the capacitive discharge which occurs when two conductors are connected together (such as a bug or wiretap on a phone line). This is also a sign that an amateur eavesdropper or poorly trained spy is playing with your phone lines. It could be nothing more then a problem with your phone line or instrument, but a TSCM person should evaluate the situation to make sure.

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

Sounds are coming from your phones handset when it's hung up.

This is often caused by a hook switch bypass, which turns the telephone receiver into a eavesdropping microphone (and also a speaker). There is probably somebody listening to everything you say or do within twenty feet of the telephone (if this is happening).

Your phone often rings and nobody is there, or a very faint tone, or high pitched squeal/beep is heard for a fraction of a second.

This is an indicator of a slave device, or line extender being used on your phone line. This is also a key indicator of a harmonica bug, or infinity transmitter being used. Of course it may also be nothing more then a fax machine or modem calling the wrong number (but a TSCM person should evaluate the situation to make sure).

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

You can hear a tone on your line when your phone is on the hook (by using an external amplifier).

To check for something like this you would have to obtain a "recorder starter" interface (with a VOX option), or some kind of a high gain audio amplifier such as a uAmp or Kaiser 1059. Then with the phone hung-up listen to your telephone wiring. If you hear a faint solid dual tone it is a dead giveaway of someone using a "slave" eavesdropping device on your (or one of your neighbors) telephone lines. Such devices create a "command tone" when the subject hangs up the phone (so you must ensure that all of your phones are hung-up).

On an added note: the most common command tones for illicit eavesdropping devices are 2100 Hz and DTMF-C, but any tone combination may be used.

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

Your AM/FM radio has suddenly developed strange interference.

Many amateur and spy shop eavesdropping devices use frequencies within or just outside the FM radio band, these signals tend to drift and will "quiet" an FM radio in the vicinity of the bug. Look for the transmissions at far ends of the FM radio band, and at any quiet area within the FM band. If the radio begins to squeal then slowly move it around the room until the sound become very high pitched. This is referred to as feedback detection or loop detection and will often locate the bug. The "stereo" function should be turned off so the radio is operating in "mono" as this will provide a serious increase in sensitivity. If you find a "squealer" in this manner then immediately contact a TSCM and get them to your location FAST.

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

You car radio suddenly starts "getting weird"

Keep in mind that the antenna your car radio uses may be (and often is) exploited by an eavesdropper, and that such usage may interfere with radio reception (so be concerned if you automobile radio suddenly starts getting weird).

Your television has suddenly developed strange interference.

Television broadcast frequencies are often used to cloak a eavesdropping signal, but such a devices also tends to interfere with television reception (usually a UHF channel). Televisions also "suck in" a lot of RF energy and because of this are very sensitive to any nearby transmitters (this is technically called "Bandwidth, and TV signals use a lot of it). A small handheld television with a collapsible antenna may be used to sweep a room. Carefully watch for interference around channel numbers 2, 7, 13, 14, 50-60, and 66-68 as these frequencies are very popular with eavesdroppers.

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

You have been the victim of a burglary, but nothing was taken.

Professional eavesdroppers often break into a targets home or office, and very rarely leave direct evidence of the break-in; however, occupants of the premises will often "pickup on something not being right" such as the furniture being moved slightly.

Electrical wall plates appear to have been moved slightly or "jarred".

One of the most popular locations to hide eavesdropping devices is inside, or behind electrical outlets, switches, smoke alarms, and lighting fixtures. This requires that the wall plates be removed. Look for small amounts of debris located on the floor directly below the electrical outlet. Also, watch for slight variations in the color or appearance of the power outlets and/or light switches as these are often swapped out by an eavesdropper. Also note if any of the screws which hold the wall plate against the wall have been moved from their previous position.

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

A dime-sized discoloration has suddenly appeared on the wall or ceiling.
This is a tell tale sign that a pinhole microphone or small covert video camera has been recently installed.

One of your vendors just gave you any type of electronic device such as a desk radio, alarm clock, lamp, small TV, boom box, CD player, and so on.
Many of these "gifts" are actually Trojan horses which contain eavesdropping devices. Be very suspicious of any kind of pen, marker, briefcase, calculator, "post-it" dispenser, power adapter, pager, cell phone, cordless phone, clock, radio, lamp, and so on that is given as a gift. That little gift the salesman left for you may be a serious hazard.

A small bump or deformation has appeared on the vinyl baseboard near the floor.
Strong indicator that someone may have concealed covert wiring or a microphone imbedded into the adhesive which holds the molding to the wall. Such deformation will often appear as a color shift, or lightening of the color.

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

The smoke detector, clock, lamp, or exit sign in your office or home looks slightly crooked, has a small hole in the surface, or has a quasi reflective surface.

These items are very popular concealment for covert eavesdropping devices. Often when these devices are installed at a target location they are rarely installed straight. Also watch out for things like this that "just appear", or when there is a slight change in their appearance.

Certain types of items have "just appeared" in your office of home, but nobody seems to know how they got there.

Typical items to watch for and beware of are: clocks, exit signs, sprinkler heads, radios, picture frames, and lamps.

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

White dry-wall dust or debris is noticed on the floor next to the wall.

A sign that a pinhole microphone or video camera may have been installed nearby. It will appear as if someone has dropped a small amount of powdered sugar either on the floor, or on the wall.

You notice small pieces of ceiling tiles, or "grit" on the floor, or on the surface area of your desk.

Prime indicator that a ceiling tile has been moved around, and that someone may have installed a hidden video camera or other eavesdropping device in your office or near your desk. Also watch for cracks or chips in the ceiling tiles. Amateur and poorly trained spies tend to crack or damage acoustical tiles. The ceiling tiles in any executive areas should never contain any cracks, nicks, gouges, or stains. Any ceiling tile that becomes damaged (for what ever reason) should immediately replaced and the cause to the damage documented. In such cases it is also wise to have a TSCM specialist inspect the area around the chipped, broken, or damaged tile to determine if a hostile eavesdropping device may have been introduced.

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

You notice that "Phone Company" trucks and utilities workers are spending a lot of time near your home or office doing repair work.

If you see the same or similar vehicles more then three times then you may have a serious problem (at least according to the U.S. State Department training course on counter surveillance).

Telephone, cable, plumbing, or air conditioning repair people show up to do work when no one called them.

A very common ruse which eavesdroppers use to get into a facility is to fake a utility outage, and then show up to fix the problem. While they are fixing "the problem" they are also installing eavesdropping devices. Some of the more popular outage involve power, air conditioning, telephone, and even the occasional false fire alarm.

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

Service or delivery trucks are often parked nearby with nobody (you can see) in them.

These vehicles are commonly used as listening posts, be very cautious of any vehicle which has a ladder or pipe rack on the roof. Also, be wary of any vehicle which has tinted windows, or an area which you cannot see though (like a service van). The listening post vehicle could be any vehicle from a small Geo Tracker, Suburban, Blazer, Trooper, or Cargo Van. Look for any vehicle which could conceal a person in the back or has tinted windows. Also, keep in mind that the eavesdropper may relocate the vehicle several times, so look around. Typically, eavesdroppers like to get within 500-750 feet from the place or person they are eavesdropping on.

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

Your door locks suddenly don't "feel right", they suddenly start to get "sticky", or they completely fail.

Prime evidence that the lock has been picked, manipulated, or bypassed. Try to always use biaxial locks with sidebars (such as ASSA or Medeco). Also, only use double sided deadbolts in all doors, and good quality window bars on all windows, and a good quality door bar on all doors not used as a primary entry doors.

Furniture has been moved slightly, and no one knows why.

A very popular location for the installation of eavesdropping device is either behind, or inside furniture (couch, chair, lamp, etc.) People who live or work in a targeted area tend to notice when furnishings have been moved even a fraction of an inch. Pay close attention to the imprint which furniture makes on rugs, and the position of lamps shades. Also watch the distance between furniture and the wall as eavesdroppers are usually in a hurry and rarely put the furniture back in the right place.

Copyright 2003 Corporate Defense Strategies

TSCM

Signs that your offices are “Bugged”

Things "seem" to have been rummaged through, but nothing is missing (at least that you noticed).

A "less than professional spy" will often rummage through a targets home for hours, but very rarely will they do it in a neat and orderly fashion. The most common "rummaging" targets are the backs of desk drawers, the bottom of file cabinets, closets, and dresser drawers.

Copyright 2003 Corporate Defense Strategies

TSCM

Who Gets “Bugged”?

Copyright 2003 Corporate Defense Strategies

TSCM

Who Gets "Bugged"?

High Threat Occupations

Attorney
Doctor
Chiropractor
Dentist
Architect
Police Officer
Court Clerk
Judge
Elected to any public office
Any type Sales or Marketing
Labor or Union Official
Fashion
Advertising
Personnel Directors

Mayor
Selectman
School Principal
College Professor
Product Engineer
Software Developer
Executive at any large company
Scientist at any large company
Employed by any defense contractor
Employed by the Department of Energy
Any minister or religious leader
Corporate Buyer or Purchasing Agent
Employee of a Construction Contractor

Copyright 2003 Corporate Defense Strategies

TSCM

Who Gets "Bugged"?

High Threat Personal Situations

Involved in any type of litigation or lawsuit
Been questioned, arrested or arraigned by the police
In the process of getting married, divorced, or separated
A minister or religious leader (i.e.: priest, rabbi, deacon, bishop, elder...)
Running for any type of elected public office
Elected to any public office (i.e.: mayor, selectman, school principal)
Executive or scientist at any large company
Recently filed a insurance claim
Engaging in political demonstrations or activism
Employed by a defense contractor, Department of Energy, etc...
Private Investigators have been "poking" around
You are in the upper income bracket

Copyright 2003 Corporate Defense Strategies

TSCM

Who Gets "Bugged"?

High Threat Business Situations

Your company has stock which is publicly traded (or will be soon)
Your company is having labor problems, union activities, or negotiations
Your company is involved in any type of litigation or lawsuit
Your company has layoffs pending (or they have just happened)
Your company is involved in the fashion, automotive, advertising, or marketing industry
Anyone can be the target of covert eavesdropping, however; some people are under greater risk than others because of financial position, occupation, legal, or domestic situation.
Spouses bug each other on a regular basis
Parents bug children
Businessmen bug other businessmen
Scientists bug other scientists
Students bug professors
Attorneys bug other attorneys (and their clients)
Insurance companies bug accident victims, and other claimants
Construction companies bug other construction companies
Salesmen bug clients
Collection agencies bug debtors
Police officers bug suspects
Executive recruiters bug personnel directors
Rock fans bug rock musicians
Department stores bug customers and merchandise

Copyright 2003 Corporate Defense Strategies

TSCM

Spy Shop “Toys”

Copyright 2003 Corporate Defense Strategies

TSCM

Spy Shop "Toys"

The U.S. State Department estimates that at least 800 million dollars of illegal bugging and eavesdropping equipment is imported and installed into corporations in the United States each year. The majority of this equipment is illegally imported into the United States from France, Germany, Lebanon, Italy, Canada, Israeli, England, Japan, Taiwan, South Africa, and a host of other countries. Additionally, anyone with a soldering iron and a basic understanding of electronics can build and install an eavesdropping device. The raw materials to build such a device may be easily obtained at Radio Shack, or salvaged from consumer electronic devices such as cordless telephones, intercom systems, and televisions. In the United States over six millions dollars worth of surveillance devices are sold to the public each day. Most of these products are sold from storefront operations, spy shops, attorneys, and via private investigators located in major metro areas such as New York, Miami, Los Angles, San Francisco, Dallas, Chicago, and Minneapolis. This does not include the tens of billions spent each year for legitimate eavesdropping products purchased by law enforcement, military, and intelligence agencies. This equipment is commonly sold over the counter, via mail order, and through the Internet. Most of these bugging devices cost only a few dollars, but highly sophisticated, quality products may be purchased for less than one thousand dollars. In New York City alone there are over 85 companies which will not only sell you the eavesdropping device, but will break into the targets office to install the device, and for an additional fee will provide a monitoring and transcription service.

Copyright 2003 Corporate Defense Strategies

TSCM

Spy Shop "Toys"

The FBI and other federal law enforcement agencies have repeatedly indicated that they lack the resources and training to enforce or properly investigate the technical security threat within the United States.

Technical surveillance and industrial espionage is a serious problem which can have a VERY GRAVE IMPACT on your company and your own personal freedoms.

Copyright 2003 Corporate Defense Strategies

TSCM

What to do if you suspect you've been "bugged"

Copyright 2003 Corporate Defense Strategies

TSCM

What to do if you suspect you've been "bugged"

1. **Contact a qualified TSCM firm. (Corporate attorneys are a good resource for this type of information)**
2. Make contact from a place other then the suspect location.
3. Do NOT call the telephone company for help.
4. Do NOT call the police of the FBI for help.
5. Do NOT discuss your suspicions with anyone else, except on a need to know basis.

Copyright 2003 Corporate Defense Strategies

TSCM

Planning and execution of a proper sweep

Copyright 2003 Corporate Defense Strategies

TSCM

Planning and execution of a proper sweep

1. Client Initiates Secure Contact

Client reviews Granite Island Group's web site and related TSCM materials
Contact is made away from suspect facility (pay phone at airport, etc...)
Contact is not made via a suspect telephone, cordless, or cellular telephone
Initial arrangements for secure face-to-face meeting (if requested)
Materials sent to Granite Island Group regarding suspect facility

2. Initial Meeting and Commissioning

Initial and secure face-to-face meeting (if requested)
Initial meeting at sterile location away from any suspect facility
Discussion regarding clients concerns, and vulnerabilities
Commissioning of TSCM services, if appropriate
Formulate plan in case an eavesdropping device or security hazard is found

Copyright 2003 Corporate Defense Strategies

TSCM

Planning and execution of a proper sweep

3. Pre-Inspection Survey, Research, and Facility Reconnaissance

Review of facility blueprints
External RF survey (9 kHz to 26.5/40 GHz)
Facility exterior reconnaissance

4. Vulnerability Analysis

Threat assessment
Physical security assessment
Electronic security assessment
Internal RF survey
Audit of communications systems and facilities
Inventory of furnishings, fixtures, and artifacts
Evaluation of structural elements (walls, ceilings, floors)
Sketch of suspect area and facilities
Identification of sensitive areas
Development of threat model
Performed during normal office hours (with appropriate cover)

Copyright 2003 Corporate Defense Strategies

TSCM

Planning and execution of a proper sweep

5. Silent/Passive Walk-Thru

No noise, non alerting activities only, nothing to alert the eavesdropper
Automated bug and wireless microphone detection (9 kHz to 3 GHz)
Initial VLF inspection of all AC, telecom, LAN, and HVAC wiring
Initial detection of infrared devices and laser surveillance devices
Video camera, tape recorder, VLF, and ultrasonic detection
Overt threat detection
Initial evaluation of physical security, locks, alarms, etc...
Most PI, spy shop, and amateur bugs will be detected during this phase
Very popular as it only takes 4 hours for a brief "Walk Though Inspection"
TSCM services above this level starts radically increasing in cost

6. Passive Inspection - RF and Light Spectrum Monitoring

No noise and non alerting activities only, nothing to alert the eavesdropper
Music softly playing, "client on phone", drapes pulled
Full passive RF spectrum sweep (20 Hz to above 110 GHz)
Full passive light spectrum sweep (300nm to 1710nm / 83 THz to 450 THz)
Most PI, spy shop, and advanced amateur bugs will be detected during this phase

Copyright 2003 Corporate Defense Strategies

TSCM

Planning and execution of a proper sweep

7. Active Inspection - Non Alerting

Minor Noise is created, however; it should not alert the eavesdropper
VLF/RF check - AC mains (all electrical outlets)
VLF/RF check - AC mains (all light switches/fixtures)
VLF/RF check - HVAC controls
VLF/RF check - Alarm and access control sensors
VLF/RF check - Fire and safety sensors/alarms
VLF/RF check - Other
All phone lines evaluated and traced back to central office
All artifacts documented, recorded, and inspected
Oblique lighting inspection of all walls and artifacts
Initial inspection of baseboards, windows frames, and door jambs
Initial inspection of all wall plates (electrical, PBX, LAN)
UV lighting sweep (below 400nm / 100THz)
IR lighting sweep (above 700nm / 180THz)
Visible spectrum light sweep (350nm to 750nm / 90THz to 195THz)
Tuned forensic light source and filter sweep (250nm to 1750nm / 65THz to 455THz)
Check for telephone set modifications/problems
Check for PBX software and hardware anomalies
Check for voice mail modifications/problems
Inspection of all computer and LAN connections
Inspection of all laser printers and computer output devices
Law enforcement and professional bugs will be detected during this phase
Typical threat level for most corporate offices

Copyright 2003 Corporate Defense Strategies

TSCM

Planning and execution of a proper sweep

8. Active Scan - Alerting

Chirp detection of hidden microphones and other transducers
IR, audio, and ultrasonic jamming (as required)
Render the eavesdropping device temporarily inoperative
Inspection of all furnishings (desks, chairs, plants, etc)
Open ceilings and walls (move ceiling tiles and panels)
Thermal inspection
HVAC and duct work inspection
Acoustical leakage inspection
Bore scope inspection of all electrical wall plates and boxes
Detailed inspection of all lighting fixtures
Inventory of all conductors, conduits, wall studs, etc...
Detailed electromagnetic energy search (above 110 GHz)
Professional eavesdropping devices will be detected during this phase
Typical threat level for a Fortune 500 corporate offices and law firms

Copyright 2003 Corporate Defense Strategies

TSCM

Planning and execution of a proper sweep

9. Active Scan - Alerting/Evaluation

Verify and TDR/FEXT/NEXT trace all conductors
TDR trace - Telephone System Wiring
TDR trace - Computer Network Wiring
TDR trace - Cable Television and CCTV
TDR trace - AC mains (all electrical wiring)
TDR trace - AC mains (all light switches/fixtures)
TDR trace - HVAC controls
TDR trace - Alarm and access control sensors
TDR trace - Fire and safety sensors/alarms
TDR trace - Other
PBX, ESS, and SN translation evaluated (as available)
Voice mail system evaluation
Xerox machine inspection
Fax machine inspection
Verify security of PBX, alarm, HVAC, audio systems
Evaluate all artifacts (i.e.: furniture, books, computers, etc...)
Wall, floor, and ceiling cavity inspections
Intense physical inspection (every cubic centimeter)
Diplomatic, law enforcement, and intelligence devices detected at this phase
Typical threat level for attorneys, defense contractors, and aerospace firms

Copyright 2003 Corporate Defense Strategies

TSCM

Planning and execution of a proper sweep

10. Special Inspection Activities (used only as needed)

Non Linear Junction Detector (NLJD) inspection - active and passive
X-ray, radiographic, and fluoroscope inspection
Magnetic anomaly inspection

11. Preventive Actions (available only by special request)

Seal and dust all cavities, wall plates, artifacts, etc...
Install acoustic, ultrasonic, IR, and RF "cloak" as needed
Install IPM alarms and associated security system
Installation of encryption devices
Installation of high security locks, doors, and hinges
Installation of physical security devices
Client education and training

Copyright 2003 Corporate Defense Strategies

TSCM

Planning and execution of a proper sweep

12. Post Inspection Activities

Verbal presentation of findings before leaving
Presentation of hard copy report (if requested)
Corrective actions
Follow up actions
Recurring TSCM services (if appropriate)

13. If an Eavesdropping Device or Activity is Detected

Collection of documentation regarding device or activity
Notification of Law Enforcement Agencies (if appropriate)
Forensic Identification and Analysis of Device
Counter-surveillance activities
Counter-intelligence activities

Copyright 2003 Corporate Defense Strategies

TSCM

Conclusion

Thanks to

The Granite Island Group

Gloucester, MA

Copyright 2003 Corporate Defense Strategies