How is a TSCM Bug Sweep Conducted?

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

"How is a TSCM Bug Sweep Conducted?"

Technical Surveillance Countermeasures (TSCM) is a search by specialists[1] to locate electronic eavesdropping, video voyeurism, GPS tracking, and/or data theft devices. *Bug sweeps* or *debugging* are generic terms for TSCM inspections.

Assuring personal privacy, protecting sensitive information and keeping intellectual property where it belongs is the goal of a TSCM bug sweep. This goal is expanded to include proactively identifying *all* types of espionage and information security vulnerabilities when applied to business environments.

The TSCM Bug Sweep Basic Steps

1. Discussion, evaluation and planning.
2. Detailed visual exam of sensitive areas.
3. Technical inspection of the areas.[2]
4. Information security survey.[3]
5. A post-inspection debriefing.
6. A final written report documenting findings, recommendations and due diligence.

The most commonly used procedures and instrumentation are listed by number. There are more, but like a doctor, the treatment is based on the symptoms. The exact procedures and instrumentation used will be based upon your concerns, location, security goals and what is in the environment.

The Technical Surveillance Countermeasures (TSCM)[4] portion of the inspection process is constructed so that procedures overlap each other in effectiveness, thus automatically creating a double-check analysis strategy.

1. Before the TSCM Sweep Begins

These items are discussed, in confidence:

- Suspicious incidents the client may have observed.
- The client's security concerns.
- Their goals for a successful resolution.

During follow-up inspections additional topics are added to the list:

- A discussion about problems or changes experienced since the last inspection.
- Implementation of previously made security recommendations.

Upon arrival, an initial orientation tour of the areas to be inspected provides the TSCM Technical Investigators with

[1] https://counterespionage.com/about-murray-associates/electronic-eavesdropping-detection/

[2] https://counterespionage.com/tscm-technology/

[3] https://counterespionage.com/advanced-tscm-explained/

[4] https://en.wikipedia.org/wiki/Countersurveillance

How is a TSCM Bug Sweep Conducted?

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

information about: access control, building construction, room contents, distances between areas, locations of IT/telecom rooms, etc.

All of this diagnostic information is used to plan the inspection strategy, and select the most effective test procedures to successfully resolve the concerns at hand.

2. Visual Examinations

A thorough physical examination of the bug sweep areas is conducted to discover electronic surveillance devices currently in place, and to locate any residual evidence from prior eavesdropping attempts. This phase of the inspection includes a detailed examination of: furniture; fixtures; wiring; ductwork; computers, and small items within the area.

TSCM physical inspections are augmented using the latest technology: hi-resolution endoscopes, thermal imaging,[5] Non Linear Junction Detection[6] (NLJD), and additional inspection tools. This is how eavesdropping devices which *do not* broadcast radio-frequency transmissions are discovered.

Examples of non-radio devices include:

- miniature voice recorders,
- transmitters which may be dormant, or have dead batteries,
- sound extraction using wires,
- carrier current over power lines,
- transmissions using infrared light,
- ultrasonic and laser microphones,
- covert spycams with internal SD cards,
- keystroke loggers.

These types of eavesdropping devices may be secreted in hollow walls, behind false ceilings, in or on furniture, fixtures and other common items.

Items having a legitimate place in the room and an ongoing source of power are inspected very carefully. These include computers, power strips, radios and clocks; all are common hiding places for bugs and spy cameras.

The newest testing procedure is an inspection of USB charging cables. These malicious USB spy cables[7] look exactly like legitimate cables. After passing the test cables deemed authentic. A tamperproof security seal is affixed, identifying it as being tested and legitimate. This also helps the user detect if the tested cable replaced with a spy cable in the future.

[5] https://counterespionage.com/tscm-technology/thermal-emissions-spectrum-analysis/

[6] https://counterespionage.com/tscm-technology/non-linear-junction-detection-nljd/

[7] https://counterespionage.com/malicious-usb-cables/

How is a TSCM Bug Sweep Conducted?

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

3. Technical Examinations

Detection of Non-Radiating Devices

Surveillance devices do not have to be transmitting, or even turned on, for TSCM technicians to discover them. Non-Linear Junction Detection[8] instrumentation can detect bugs operating in their standby mode, turned on by timers, broken, or even if their batteries are dead.

Tip: This detection technology is similar to the shoplifting detectors used at retail store exits. Just the fact that the bug contains electronic components is enough to sound the alarm.

Radio-Frequency Spectrum Analysis

Detection and demodulation of wireless surveillance (audio, video & data) is accomplished with the aid of spectrum analyzers.[9] These are basically sensitive, computer-aided radio receivers which can receive signals anywhere along the radio-frequency spectrum. Even though only certain areas of a building may be designated for a TSCM bug sweep inspection, surrounding areas also benefit from this particular test.

Optical Spectrum Analysis

Some electronic eavesdropping devices transmit intelligence by converting sound into infrared or laser light. This invisible light can be picked up optically from a distance and converted back into sound, video or data. Television remote control units operate on the same principle. Specialized TSCM instrumentation can detect this.

Concealed Space Examination

Spaces which cannot be directly viewed are optically examined using a flexible videoscope.[10]

Thermal / Infrared Spectrum Analysis

Minute amounts of heat are generated as electricity moves through a surveillance device's circuitry. Thermal imaging instrumentation[11] is used to detect active items by sensing their heat signatures. This technique can also see bugs hidden in antique furniture and other delicate items – without damaging them.

Tip: In addition to the above procedures, TSCM specialists may employ other specialized tests, based on the unique needs of a case.

---

[8] https://counterespionage.com/tscm-technology/non-linear-junction-detection-nljd/

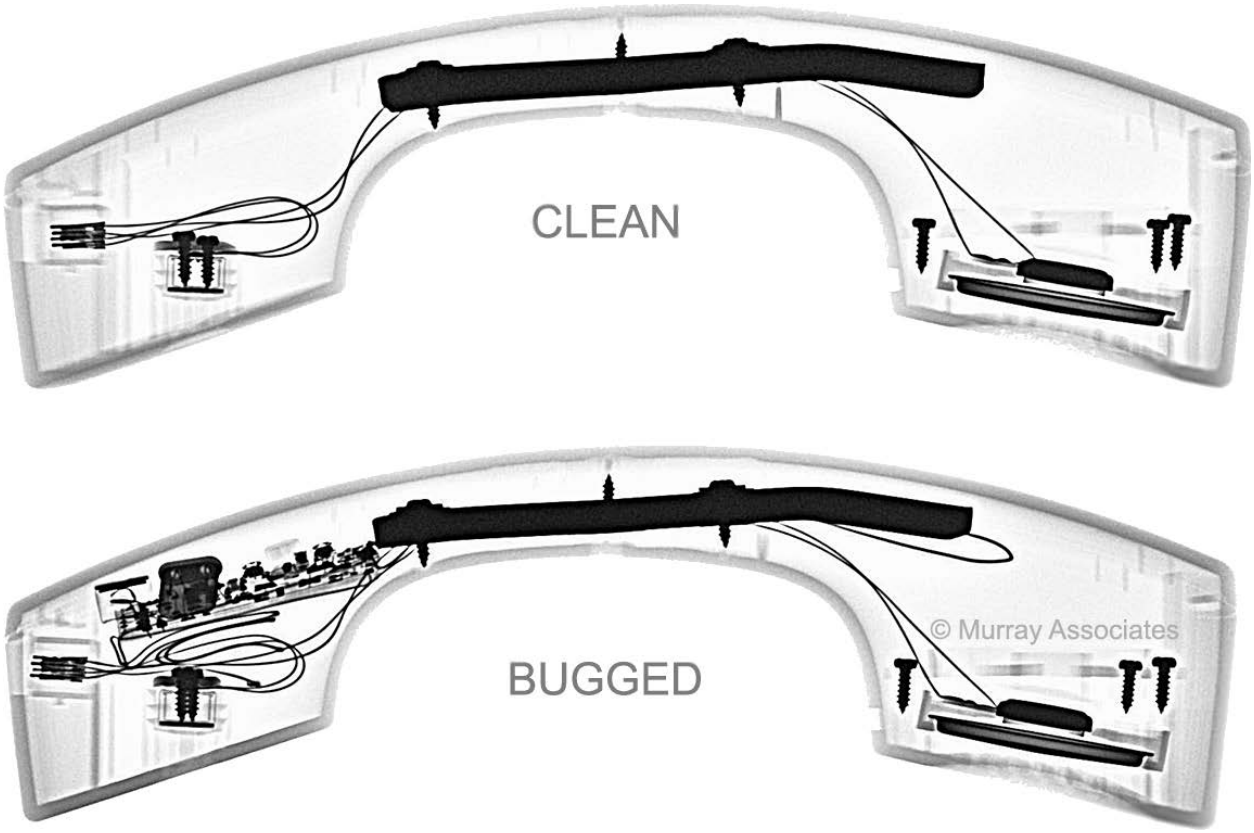
[9] https://counterespionage.com/tscm-technology/radio-frequency-spectrum-analysis/

[10] https://amzn.to/3l9VK2g

[11] https://counterespionage.com/tscm-technology/thermal-emissions-spectrum-analysis/

How is a TSCM Bug Sweep Conducted?

by Kevin D. Murray, CPP, CISM, CFE, CDPSE



Some modern telephone handsets cannot be opened easily, or at all. X-ray is the inspection solution.

TSCM X-ray Imaging & Analysis

X-ray analysis[12] during TSCM inspections offers the most assurance a room object isn't bugged.

We don't recommend this inspection service for everyone. Primary TSCM inspection techniques[13] are excellent for most situations. But, when the stakes are high enough—and the opposition is sophisticated enough—a TSCM X-ray deep clean is the logical option. There are also times when a TSCM X-ray deep clean is just smart due diligence.

In most cases, objects only need to be images and analyzed once. After the procedure these objects can be sealed with a tamper-proof security seal to deter opening, or exchanging them for an identical, but bugged, item.

[12] https://counterespionage.com/tscm-technology/x-ray-analysis/

[13] https://counterespionage.com/tscm-technology/

How is a TSCM Bug Sweep Conducted?

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

Internet of Things Exam

The Internet of Things (IoT) has introduced many not-so-obvious attack points into businesses. From printers to VoIP phones to AV presentation equipment, all are taken into consideration during the TSCM inspection process.

Hard-wired Communications Examination

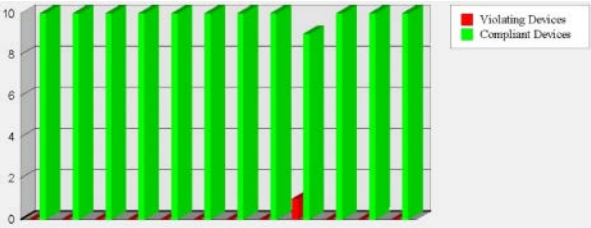
- Visual inspection of system components and connecting pathways.
- Frequency Domain Reflectometery (FDR) Analysis of the wiring paths.
- Carrier Current[14] analysis of wiring.
- Audio leakage analysis.
- Electrical characteristics analysis.

Wireless Communications Examinations

- Wi-Fi security and compliance analysis.
- Cordless telephone vulnerabilities.
- Cordless headsets, keyboard and mice.
- Wireless presenter's microphones.
- Other wireless communications (Bluetooth, FM, analog, etc.)

Wi-Fi Security and Compliance Audit

A Wi-Fi security[15] and compliance audit is an essential element of most TSCM inspections. It detects WiFi-reliant audio and video covert surveillance, and rogue network intrusion devices. Additionally, this test can detect compliance issues.



Tip: Just one loophole… Hackers are in. Data is out, and "You are out of compliance."

This test helps detect eavesdropping, data siphoning *and* government penalties due to compliance lapses.

Although a Wi-Fi inspection is part of a TSCM bug sweep inspection, it may also be ordered separately when Wi-Fi security and compliance are the sole concerns.

Some privacy laws and directives which may impact your Wi-Fi usage include:

- Sarbanes-Oxley Act – U.S. Public Companies
- HIPAA – Health Insurance Portability and Accountability Act
- GLBA – Gramm-Leach-Bliley Financial Services Modernization Act
- PCI-DSS – Payment Card Industry Data Security Standard
- FISMA – Federal Information Security Management Act

[14] https://en.wikipedia.org/wiki/Carrier_current

[15] https://counterespionage.com/wifi-security-checklist/

How is a TSCM Bug Sweep Conducted?

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

- DoD 8100.2 – Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense Global Information Grid
- ISO 27001 – Information Security Management

Tamper Detection

TSCM Technical Investigators use customized security seals to seal phones and other objects upon completion of an inspection. Items previously inspected and sealed will re-examined during future inspections to verify seal integrity. The seal numbers are recorded in the written report.

Between inspections clients are encouraged to visually examine these seals themselves. A damaged or missing seal may indicate tampering. A missing seal may also indicate the object being sealed was replaced, possibly with a pre-bugged identical-looking item. Either condition is a suspicious incident which should be investigated further.

Acoustical Ducting Evaluation

This phase of the inspection evaluates the possibility of sound migration—sometimes a surprising cause of information loss. Ductwork, open ceiling plenums, common walls / ceilings / floors can conduct sound in unexpected ways. Remediation recommendations help clients prevent this type of unnecessary information loss.

4. Information Security Survey

As part of the inspection process general security efforts already in place are observed to assess appropriateness and current effectiveness. This is important because security policies and hardware can quietly decay over time. Examples include:

- CCTV, locks, alarms.
- Employee compliance with good information security practices.
- Access control.
- Security officer efficiency.
- Potential for abusing in-place technologies.
- Security policies (in place, or needed).
- General security and safety observations are also made.

This element of the inspection provides clients with cost-effective recommendations for improvements, repairs, upgrades, and additions, as necessary.

Tip: Make sure you TSCM specialist does not sell, or profit in any way, from products and services they recommend. You need to be sure the recommendations are in your best interest, not their's.

5. On-Site Debriefing

An immediate debriefing may be held to discuss the results of the inspection. Urgent

security issues, and future protection strategies are discussed at this time.

6. The Written Report

A written counterespionage report should be rendered to document your TSCM security inspection, and due diligence. The report may also contain recommendations requiring your immediate attention.

Tip: Maintain a cautious attitude, and safeguard the report. It discusses security strategies which are not for general dissemination. It documents your proactive stance and due diligence on information security—a legal prerequisite for protection in court.

###

You may also want to read…

How Can You Tell if You Are Being Bugged, or if a Room is Bugged?[16]

What are the Benefits of Conducting a TSCM Bug Sweep?[17]

How Much Do TSCM Bug Sweeps Cost?[18]

Kevin D. Murray CPP, CISM, CFE, CDPSE is a business counterespionage consultant and TSCM specialist with over four decades of experience.

Murray Associates[19] is an independent security consulting firm, providing eavesdropping detection and counterespionage services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.

[16] https://counterespionage.com/how-to-tell-if-you-are-bugged/

[17] https://counterespionage.com/what-are-the-benefits-of-a-tscm-bug-sweep/

[18] https://counterespionage.com/how-much-does-tscm-bug-sweep-cost/

[19] https://counterespionage.com/about-murray-associates/electronic-eavesdropping-detection/