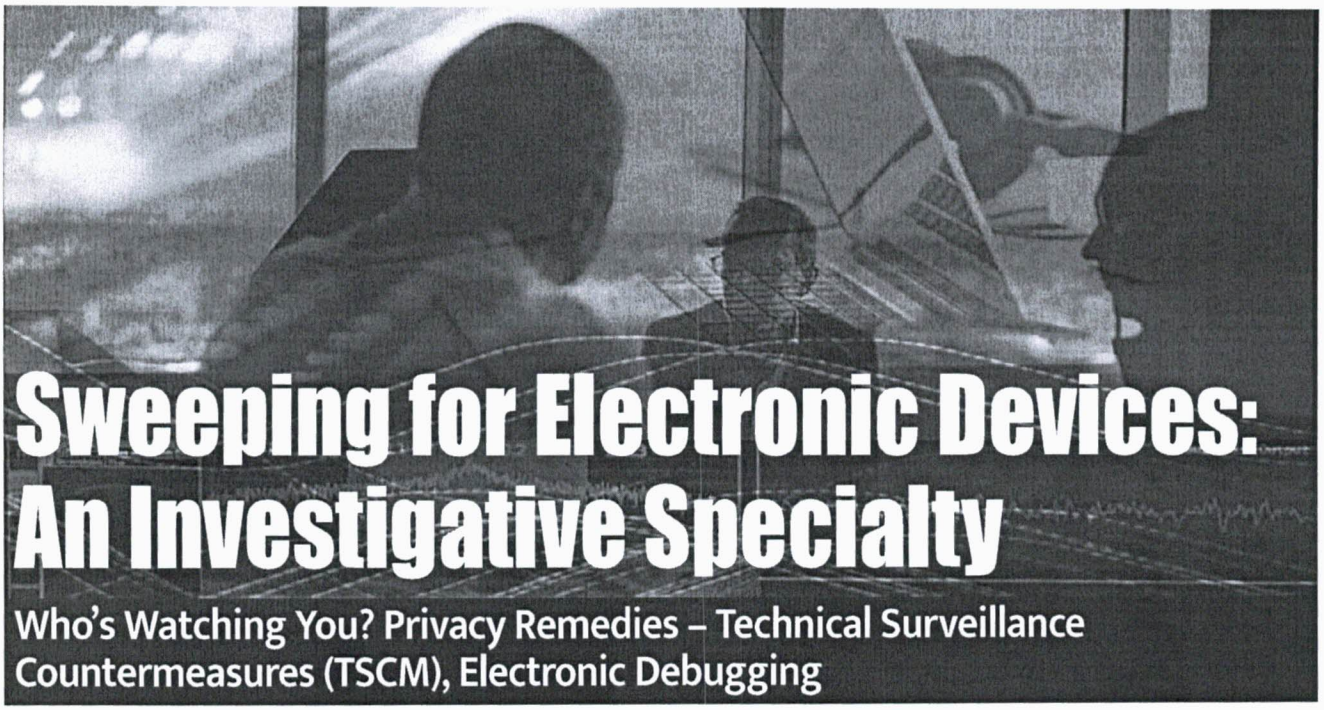


Sweeping for Electronic Devices: An Investigative Specialty

Who's Watching You? Privacy Remedies – Technical Surveillance Countermeasures (TSCM), Electronic Debugging

BY **JOHN M. GASPAR** AND **ANTHONY LUIZZO**

According to a U.S. Department of Justice Office of Justice Programs virtual library article (NCJ Number 44794), audio countermeasures, technical security countermeasures, and debugging are all terms used to describe the science of audio surveillance device detection and penetration prevention.[1]

The first evidence of tampering and/or restricting electronic communication can be traced back to April 1861 when a pro-secession mob in Baltimore cut the telegraph lines linking Washington D.C. with the North, motivated by exigencies over the secession of the southern states and an attack on Fort Sumter before the breakout of the Civil War.[2]

According to Encyclopedia.com *"Electronic Surveillance is defined as observing or listening to persons, places, or activities usually in a secretive or unobtrusive manner – with the aid of electronic devices such as cameras, microphones, tape recorders, or wiretaps."* Corporations use electronic surveillance countermeasures to maintain the security of buildings and grounds or to gather information about competitors.[3]

We live in a world where our privacy is being compromised in a wide number of ways, including but not limited to:

- Electronic eavesdropping (bugging)
- Bank account fraud
- Internet phishing
- Identity theft
- Internet harvesting
- IP address harvesting
- Web browser harvesting
- Automotive GPS info harvesting
- Smartphone app harvesting (maps, telephone, etc.)
- Auto airbag info harvesting (speed & crash data)

If the above is not intrusive enough, one of the worst offenders *is when your home or business is "bugged."* This type of intrusion violates one's personal and financial security.

Framing the Pre-Interview Client Questionnaire

The main job of an investigative advocate is to follow every lead and investigate every rabbit hole. As such, it's imperative that the debugging expert formulate a comprehensive set of pre-interview questions that help capture as much information as possible about the crime at hand. Sample questions might include:

- Have they gotten feedback on personal conversations in their home or business from people they did not share that information with?
- Did they get a gift from someone that requires a power source or an electronic device?
- Did someone new come into their house or business, a repairperson or a guest?
- Did the person have unsupervised access to their home?
- What access control do you have in your home or business? Does everyone have their code for the alarm or access control?
- Did you hide your key on your property?
- Are your key holders trusted?
- Do you have Nest, Ring, Honeywell, or any video camera in your home/business that can capture video activity for ingress and egress?
- Have you observed anything unusual? (Including buzzing. ringing sounds.)
- Have you noticed electrical devices and sockets tampered with?

Difference between residential and business debugging

As a matter of statistical reality, residential eavesdropping is less likely than business or organizational eavesdropping. Oftentimes, businesses are bug targets because of business-related issues such as formulas, product lines, boardroom decisions, contract negotiations, intellectual property, client lists, etc. Occasionally, these corporate lawbreakers decide to target business executives' residences, especially if they believe the information they are seeking might be therein.

A personal story: looking back to yesterday

What motivated me (John) to learn technical surveillance countermeasures (TSCM), aka electronic debugging, began in the mid to late 1980s, post my retirement from the NYPD. After my brief retirement, I opened APB Investigations – a licensed private investigations agency in New York City. I immediately began getting calls from customers to perform TSCM evaluations. This was a good fit for me in as much as I previously graduated from a Brooklyn Technical H.S., ma-

joring in academic college prep and electrical engineering. As part of my academic training in this discipline, I learned the ABCs of using an oscilloscope. This electronic test instrument captures information on electrical voltage signals used in debugging evaluations. This is when I realized that all roads lead somewhere, and my road would be to become a crackerjack debugger.

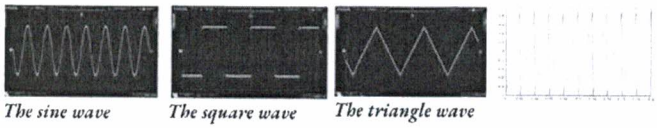
My mentor in TSCM, more commonly known as debugging, was a retired NYPD Transit Detective, Rainor Melucci. Rainor was known by his investigative colleagues as one of the nation's best debugging experts. My co-author Anthony Luizzo and I met him when he was the president of the Society of Professional Investigators (SPI). Over the years, he and Anthony and I became close friends and colleagues. In fact, the three of us are past presidents of SPI. Oftentimes, among other investigative jobs, we three would go out on debugging jobs.

As previously mentioned, our primary tool for detecting possible "bugs" was the oscilloscope. Oscilloscopes display an infinite number of waveforms which are analyzed for properties such as amplitude, frequency, rise time, time interval, distortion, and others. Further information on waveforms and buddy waves is outlined below. Additional information on using an oscilloscope can be found in an excellent article by Spark Fun Electronic Tutorials.[4]

A closer look at debugging technology

Finding a bug and installing a bug is a binary discipline – it is both an "ART" and a "SCIENCE." The art lies in the technologist's creativity in selecting the right tool to locate and/or install a hidden device, and the science lies in the technologist's ability to complete his or her work without ever leaving fingerprints at the scene! Some examples of devices used in the electronic surveillance cosmos include but are not limited to:[5]

Examples of Waveforms



The sine wave *The square wave* *The triangle wave*

The Present

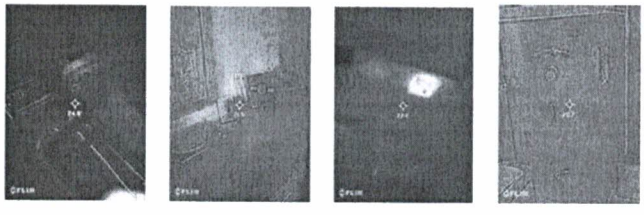
Modern day methods for supporting countermeasures for electronic eavesdropping include sophisticated equipment, knowledge of key areas to search, visual inspections, thermal imaging, and more.

The debugging process in many ways is like solving an investigation case. The investigator, or in this case, the tech, would review all the circumstances surrounding the intrusion of privacy; including who may have had access to enter the location(s). At this point, the technical surveillance counter measures (TSCM) search can begin.

Equipment includes but is not limited to:

Broadband receivers are designed to detect and locate all major electronic surveillance devices, including room, phone and body bugs, video transmitters, and tape recorders.

FLIR InfraRed (IR) Analysis



Hidden Camera Analysis

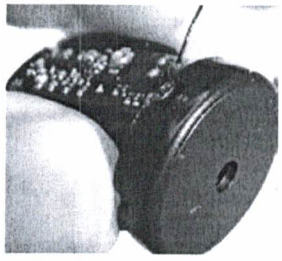
Physical examination and professional-quality hidden camera detectors offer two methods of finding a camera: either they look for that glint from the lens (much like using a flashlight or smartphone), or they detect RF broadcasts from a wireless camera. To make visually finding a hidden camera easier, detectors use multiple flashing LED lights or lasers to help light up camera lenses.[6]

Physical search

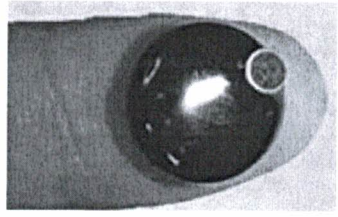
Each target area was examined for several types of threats during this inspection phase. We were looking for hidden microphones, suspicious wiring, concealed radio transmitters, modified communications or power equipment, InfraRed heat, and susceptibility to the laser. Although "bugs" can be battery operated, the audio or video time would be limited to hours or days depending on the activity. Most "bugs" receive power from an existing power supply in the house, including but not limited to wall sockets, light switches, lights, and other plug-in devices.

Photos of some eavesdropping devices

Wall and Glass Spy



Bug invisible transmitter



UHF Spy Bug - Mini Spy Audio Bug

Real Life examples of located "bugs."

A personal debugging story.

A retired FBI agent colleague asked me to assist them with an electronic sweep for a major athletic franchise in a Tampa Florida hotel. They had ongoing sensitive contract negotiations and needed to ensure the room was "clean" (bug-free). I traveled from my Daytona Beach office and was greeted by the client and the security team. The hotel room was an open space area with a large conference table and a king size bed just a few feet away. I began my TSCM process sweep, and after carefully sweeping all areas (closets, alcoves, ceilings, vents, etc.), I advised the team that the area, at first blush, looked clean to me. I began my visual, physical search – looking and touching all areas. I searched the floors, under the tables, the bed and backboard, and then under the bed.

Moreover, I also removed the mattress protector at the foot of the bed. I recall thinking this was the closest point to the conference table where the conversation and the negotiations would occur. As I closely scanned the immediate area, I observed a wire with a microphone attached to a Radio Shack mini recorder. As a seasoned tech, I turned the recorder off, put it into an evidence envelope, labeled and sealed it, and secured it as evidence. Upon completing the sweep, I checked with the front desk to see if the room had been rented and to whom after my client departed. Did anyone rent this room prior or after the occupant left?

Conclusion

Our job as debugging sleuths is to execute techniques to detect, neutralize, and exploit technical surveillance technologies and hazards that permit unauthorized access to or removal of information. We have made advances over time and have come a long way from the birth of the oscilloscope. Today, seasoned debuggers can often visually find transmitting devices without the use of technological means during their initial survey sweep. However, when you put the power of today's electronic technology in the hands of a seasoned debugging sleuth, it helps make an extremely potent cocktail.

Over the years, these seasoned debugging experts have helped businesses safeguard important formulas, assisted companies in keeping sensitive information confidential, aided corporate executives in keeping contract negotiations confidential, and helped business owners save money and worry. Investigative sleuths would be wise to study up on the art and science of debugging and put the pedal to the metal and turn their beam of inquiry toward this exciting and lucrative business specialty!

When looking for a TSCM specialist, look first for experience. Then identify if they have certification and training on the equipment they use. PI

References:

1. https://www.ojp.gov/ncjrs/virtual-library/abstracts/electronic-surveillance-and-countermeasures
2. https://technologystories.org/reversing-the-whispering-gallery-of-dionysius-a-short-history-of-electronic-surveillance-in-the-u-s
3. https:/www.encyclopedia.com/social-sciences-and-law/electronic-surveillance
4. https://learn.sparkfun.com/tutorials/how-to-use-an-oscilloscope/all
5. 5. EDN NETWORK -Perform five common debug tasks with an oscilloscope https://www.edn.com/perform-five-common-debug-tasks-with-an-oscilloscope/
6. Retired Special Agent F.B.I U. S Department of Justice Larry Gould, FLORIDA INVESTIGATIVE SERVICES Larry Gould, P.I., B.A.I. https://www.facebook.com/FISDetectives/

John M Gaspar, MMBA, M.S, CFE, BAI, CSI is current president of the Florida Association of Private Investigators (FAPI), former president of the Society of Professional Investigators (SPI), past chairman of (BAI) Board Accredited Investigator, retired NYPD Major Case Squad Detective, retired FCSO Detective Supervisor in Charge of the Economic Crime Division, Retired FCSO Administrator: Professional Standards, Director of FLA-PAC Police Accreditation/ CALEA National Recognition, & Director of Training, Florida Department of Law Enforcement instructor, professor, academy instructor, program lead Human Diversity instructor, Master Crime Scene, Technical Surveillance Counter Measures (TSCM) investigator, forensic hypnotist, and Florida licensed private investigator. He is the President of All Florida Investigations & Forensic Services, Inc., Keiser University Academic Dean & department program coordinator for CSI, retired Daytona State College adjunct professor, and FDLE instructor. In addition to numerous articles in *PI Magazine*, John's published and co-published works with Dr. Anthony Luizzo include:

1. *Fraud Magazine* November/December 2013 Volume 28 the "Shutter Bug case" ($800,000 Construction Fraud Scheme).
2. Published study on Forensic Hypnosis & Memory Recall -NYPD
3. Applying the Theory of Learned Helplessness to Psychological Development of Street Prostitutes Thesis published work Nova University
4. ACFE article "*The Shutter Bug Fraud Case*"

Anthony Luizzo, Ph.D., CFE, CST, PI (RET. NYPD) is a Certified Fraud Examiner, Certified Security Trainer, and a Licensed Master Locksmith. His former positions include Police Officer / Detective Specialist - New York City Police Department, Director Security Programs – New York City Office of Economic Development and Business Services, Corporate Director Loss Prevention Bureau – New York City Health & Hospitals Corporation, CEO/President L.C. Security Consulting Group, board of directors, Accufacts Pre-employment Screening (public company), board of advisors, Vault Verify, LLC. He has published dozens of articles on security management and administration, fraud prevention, forensic accounting, interviewing and interrogation, forensics, crime scene management, and background screening. Industry Recognition: Listed as a Noteworthy LOSS PREVENTION EXECUTIVE CONSULTANT BY MARQUIS WHO'S WHO. He is a frequent contributor to *PI Magazine*.

Publications:

1. Book co-author: *Healthcare Security: Solutions for Management, Operations & Administration* - Publisher: Rutledge / Taylor & Francis Group - ISBN 978103210549-9 (2022)
2. Training manual co-author: *Fraud Auditing A Complete Guide;* Foundation for Accounting Education & NYS Society of Certified Public Accountants (1992 - Rev. 1995)
3. Authored dozens of articles speaking to: hospital security, proactive crime control planning, security survey design, fraud examination, forensics, criminalistics, background screening, interviewing, forensic hypnosis, and crime scene management.