Types of Bugs and Wiretapping

Bugging

A “bug” is a device placed in an area to intercept and transmit communications to a listening post. The eavesdropper can be nearby or far away, depending on the type of bug used. Bugs fall into five main categories: Acoustic, Ultrasonic, RF, Optical, and Hybrid.

• Acoustic Bugs: These involve direct interception using simple devices like a glass, stethoscope, or rubber tube. They can exploit sound leakage through windows, ventilation structures, or other soft spots.

• Ultrasonic (VLF) Bugs: These convert sound into an audio signal above the range of human hearing, which is then intercepted and converted back to audio nearby. They use audio pressure waves instead of creating a radio signal.

• RF (Radio Frequency) Bugs: The most common type, RF bugs use a radio transmitter placed in an area or device. These are easy to detect with the right equipment but difficult to trace back to the installer.

• Optical Bugs: These convert sound or data into optical pulses or beams of light. Though rarely used and expensive, they are easy to detect. An example is an active or passive laser listening device.

• Hybrid Bugs: These combine various techniques from the categories above to create a versatile eavesdropping device.

Wiretapping

Wiretapping involves intercepting communications by tapping into wires or other conductors. This method is preferred for high-quality intelligence and minimizing detection risk. Wiretaps are categorized into four types: Hardwired, Soft, Record, and Transmit.

• Hardwired Wiretap: Involves gaining physical access to a wire and attaching a second set of wires to bridge the signal to a secure location. This type is commonly used by law enforcement but can be traced back to the observation post if discovered.

• Soft Wiretap: This modifies the software of a phone system, either at the telephone company or within a business PBX. Popular among law enforcement and intelligence agencies, it is easier to find on a PBX but harder in the phone company’s system.

• Recording Wiretap: A simple tape recorder or digital recorder wired into a phone line. This is easy to find during a Technical Surveillance Counter Measures inspection and is commonly used by amateurs.

• Transmit Wiretap: Involves an RF transmitter connected to a wire, often with a microphone. This type is popular but increases the risk of detection due to the RF energy produced. The risk of detection can be mitigated by utilising a burst transmitter (sending compressed recordings in short timeframes at unusual time periods).

Detecting wiretaps requires significant expertise and specialized equipment. Simple bug detectors or spy shop gadgets are insufficient. TSCM specialists use advanced instruments to perform sensitive measurements.

Families of Bugs

- Free Space Emission:
- Acoustic/Audible Pressure Waves
- Acoustic/Ultrasonic Pressure Waves
- Optical/Invisible Light (UV, etc.)
- Optical/Visible Light
- Optical/Invisible Light (Infrared, etc.)
- RF Transmission (Various frequency ranges)
- Free Space - Magnetic
- Conducted Emission:
- Audible (Voice Frequency)
- Ultrasonic
- Video
- Current Carrier (AC Mains, Phone, CATV, etc.)
- Radio Frequency (AC/Mains Devices, waveguide, etc.)
- Fiber Optic

Other Types of Covert Eavesdropping Activities

- Intelligence:
- Counter-Counterintelligence (Counter-TSCM)
- Counterintelligence (TSCM)
- Active (Classic Spying, Heavy Bugging)
- Passive (Primarily Listen, Minor Bugging)
- Active (Wiretaps, Body wires, etc.)
- Passive (Cellular Phone/Beeper Monitoring)
- Management (Video and/or GPS in work vehicles, wireless microphones)
- Organised Crime (Illegal Surveillance Activities)
- Private Investigators
- Amateur/Private Individual (e.g. domestic violence; family law)