Catching Bugs
Detecting and Locating Hostile Recording Devices to Secure Sensitive Information

Each year, corporations lose billions of dollars from illegal espionage and intellectual property theft. A portion of this theft is done through the use of illegal devices, or bugs, which record and transmit sensitive or confidential information back to a listening post. A widely cited report from the US State Department suggests that hundreds of millions of dollars worth of bugs are installed into US corporations with the goal of stealing proprietary information.

While figures are difficult to verify, this number is likely increasing significantly. The widespread availability of low-cost, easily obtainable, and powerful audio and video devices has made it simple for nearly anyone to acquire and deploy these devices into government offices, secure facilities, corporate boardrooms, hotel rooms, or homes.

Illegal bugs also represent a serious threat to national security, law enforcement, government operations, and personal privacy. Technical surveillance countermeasures (TSCM) is a critical component of maintaining physical security, controlling the flow of information, and keeping operations safe from internal and external threats.

In response to these trends, TSCM professionals require a solution that is capable of detecting hostile signals, monitoring the signal of interest for further analysis, and locating the source of the signal for removal.

The Challenge

Though historically most bugs recorded audio only, today’s bugs are able to record and transmit high quality audio and video while being small enough to be hidden in common objects, such as office supplies, light fixtures, telephone jacks, and even children’s toys. As a result, they are often difficult to detect without experienced professionals and high quality equipment.

Similarly, users conducting TSCM activities face unique challenges compared to other spectrum monitoring applications. In most cases, operators are unsure what types of signals to look for, or if a signal is even present at all. They need a strong understanding of the baseline signal environment and the ability to quickly identify hostile signals before information is lost.

Finally, as devices and hostile actors have become more sophisticated, many are able to avoid detection during traditional sweeps. For example, many bugs now transmit signals intermittently, at low power, and at various frequencies, making them difficult to detect during regular working hours when sweeps would typically be conducted.

QUICK FACTS

The widespread availability of low-cost and powerful bugs has increased the threat of illegal surveillance activities.

The ThinkRF™ Surveillance System is a complete TSCM system that enhances traditional bug sweeping through continuous, 24/7 monitoring of facilities.

High performance TSCM software applications and omni/directional antennas allow professionals to demodulate signals and locate bugs more quickly and effectively.
The ThinkRF Surveillance System is designed for bug detection in difficult indoor environments, such as large corporate office buildings, government facilities, and other secure locations. It consists of a software-defined spectrum analyzer with up to 27 GHz frequency range, 100 MHz real-time bandwidth, and 28 GHz/s sweep rate. The hardware is driven by the appropriate software application on a laptop along with suitable antennas consisting of omni-directional and optional directional antennas.

The system enhances the performance of traditional TSCM techniques by providing continuous, 24/7 monitoring. Combined with a high sweep rate, advanced triggers, and powerful TSCM software, users can detect infrequent, short duration, and frequency hopping signals with a higher probability and locate them to remove the source.

The Surveillance System enables all interference and bug detection procedures. Users can:

- Conduct full spectrum scans
- Distinguish between friendly and hostile signals
- Create databases and signal libraries
- Monitor the signal of interest
- Demodulate the signal if required
- Locate the source

The system incorporates:

- ThinkRF R5550 or R5750 Real-Time Spectrum Analyzers
- Laptop
- IP Networks for Multi-Sensor Deployments
- Kestrel TSCM® Professional Software
- Omni/Directional Antennas
- Handheld Cases

Benefits of the ThinkRF Surveillance System

- Increases the probability of detection through continuous monitoring of the spectrum environment
- Enhances the ability of TSCM professionals to locate bugs beyond traditional sweeps
- Allows users to create a signal library, record data for post analysis, and generate reports
The Results

Through the use of in-place and roaming sensors, TSCM professionals can go beyond traditional bug sweeps and ensure the security of the facilities they operate in. With continuous monitoring of the spectrum environment, users can detect, locate, and remove illegal bugs faster in order to reduce the risk of information being lost to malicious actors. As a result, companies can protect confidential business transactions and intellectual property and governments can maintain control over national security and law enforcement operations.

ABOUT THINKRF

ThinkRF is the leader in software-defined spectrum analysis platforms that monitor, detect and analyze complex waveforms in today’s rapidly evolving wireless landscape. By providing more flexibility, greater coverage, increased functionality and better ROI, ThinkRF solutions are ideal for regulatory and intelligence monitoring, telecom deployment optimization and RF application development. With open APIs and proven integrations, ThinkRF offers the only compact and networkable spectrum analyzer that can be deployed without a PC and the best price to performance on the market. Founded in 2006, ThinkRF is headquartered in Ottawa, Canada with offices and partners globally.

For more information, visit www.thinkrf.com, contact info@thinkrf.com or on Twitter, LinkedIn and YouTube.