Protect from eavesdropping with 24/7 RF Audio/Video

2017 TSCM Project Proposal
# Table of Contents

1. Background --- page: 3
2. Audio Eavesdropping Techniques --- page: 4
3. Video Eavesdropping Techniques --- page: 5
4. Laser Eavesdropping Techniques --- page: 6
5. 24/7 TSCM Block Diagram --- page: 7
6. Features --- page: 8
7. TSCM System Transmission Method and Action --- page: 9
8. The Stealth DX 24/7 Audio Signal Surveillance --- page: 10 ~ 12
9. The Stealth DX 24/7 Video Signal Surveillance --- page: 13 ~ 16
10. Oath of Confidentiality --- page: 17
Background

As much more developed wiretapping techniques are introduced across the world, more engaged security solutions are demanded against different types of wiretapping attacks.

Government agencies, information security departments, as well as major companies operate real time eavesdropping surveillance systems for secured areas and implement detailed security inspection periodically to meet the high standards of security management for additional possible attacks.

GTG proposes the state of art security management solutions that enable immediate identification upon detection as high level of management of this more engaged security system operation.

We have broken the stereotypes that RF signal detection has to deal with complex spectrum analysis – clients can identify audio signal like a FM radio, video signal like a TV display.
Audio Eavesdropping Techniques

Technological Trend

The main point of current eavesdropping techniques is that wiretapping is done so secretly that it prevents the other party even from recognizing the attack. Remotely controlling functional switches is very frequently observed and there have been advances such as using a micro repeater in a close distance by having higher frequency range or lowering transmitter output. Audio demodulation has been digitalized as well.

Solutions

- Increase the frequency range of monitoring units and receiving sensitivity.
- Conduct a detailed measurement of security for secured areas periodically since digital modulation can’t be demodulated.
Video Eavesdropping Techniques

Technological Trend

Advanced illegal recording devices have been introduced in various forms such as button holes or nail heads. Subminiature microphones that help camera video transmission include modulated audios are now embedded and companies are being threatened. Cameras in a frequency range of 5.8 GHz is also introduced in the market as video eavesdropping frequency use has been increased.

Solutions

- Operating a eavesdropping monitoring unit that can detect both audio and video in a frequency range of 5.8 GHz is the best solution.
- A frequency range of 5.8 GHz is a very crucial item that should be included in periodic measurement of security.
Laser Eavesdropping Techniques

Technological Trend

This method eavesdrops the target's communications by releasing laser beams on window glasses and demodulating tiny vibrations into audible voices on a returning beams.

Since infiltration into the targeted building is not required for this method, the victim does not realize attacks.

Solutions

Masks audios in tiny vibrations by having random noises on window glasses so that the attacker can't analyze the eavesdropped audios.
24/7 TSCM Block Diagram

Audio Monitoring

Video Monitoring

PC

Internet / LAN

The Stealth DX

Transducers

Up to 1,000 units

The Stealth DX

Omni Speakers

Hidden Camera

Bug

Laser Audio Surveillance
## Features

<table>
<thead>
<tr>
<th>Name</th>
<th>The Stealth DX RF Detector with Real Time Remote Monitoring Capability</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main Features</strong></td>
<td></td>
<td>- Storage of all audio and video event signals. Search report function.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Expansion of channel and output as the result of increase in laser wiretapping devices in the market.</td>
</tr>
<tr>
<td><strong>Audio:</strong></td>
<td></td>
<td>- Wireless eavesdropping and monitoring surveillance</td>
</tr>
<tr>
<td>* like a radio (in less than 15 seconds, approx.700 sq ft.)</td>
<td></td>
<td>- Prevention of wiretapping in laser and concrete</td>
</tr>
<tr>
<td>* storage of event signal, SMS alert</td>
<td></td>
<td>- Noise Generation Channel: 2 CH</td>
</tr>
<tr>
<td><strong>Video:</strong></td>
<td></td>
<td>* Transducer - snapping wire surveillance</td>
</tr>
<tr>
<td>* like a TV (in less than 15 seconds, approx.700 sq ft.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* storage of event signal, SMS alert</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Country of Origin</strong></td>
<td>Republic of Korea</td>
<td></td>
</tr>
<tr>
<td><strong>Manufacturer</strong></td>
<td>Global TSCM Group, Inc.</td>
<td></td>
</tr>
</tbody>
</table>

**Remark**

One-year warranty
# TSCM System Transmission Method and Action

<table>
<thead>
<tr>
<th>Transmission Method</th>
<th>Current Equipment</th>
<th>New Equipment</th>
<th>Video Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A list of dozens of suspicious signals detected in the whole frequency range will appear and spectrum analysis will identify if it is audio or video signals. Demodulation will then identify it as an illegal signal or not. Each event frequency needs to be verified and eliminated, causing a considerable amount of time.</td>
<td>Detected suspicious signals will be sent to central monitoring site via internet and the central monitoring site will decide if it is illegal signal just by directly listening to the audio or by checking its origin, time, or frequency. It does not require signal analysis process such as spectrum. It enables prompt and accurate decision making and counteraction.</td>
<td>Detected suspicious video signals will be compressed and sent to the central monitoring site via internet, where monitoring staff will check the video in a pop up display and verify if it is illegal or not.</td>
</tr>
<tr>
<td>Action</td>
<td>Inquire a security company or conduct a detailed security measures for the area with existing professional equipment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remark</td>
<td>Spectrum Analyzing</td>
<td>Audio Demodulation</td>
<td>Video Demodulation</td>
</tr>
</tbody>
</table>
The Stealth DX RF Detector with 24/7 Real Time Remote Monitoring Capability

Audio Signal Surveillance

The Stealth DX, the RF eavesdropping monitoring module which installed in the information security area such as the office, conference room or residence of the politics, financial and big business CEO and entertainer, can monitor the area in 24/7 to be ready to grasp any illegal attempt of RF eavesdropping activity. When any suspected activity is grasped, an alert with the detected RF audio signal is transmitted to the central control center in real time to be analyzed whether they are harmful activities. The client or security personnel will be immediately informed about on-going illegal activity to prevent any damage from important information outflow and privacy leakage.

They can send a real time SMS to the client’s mobile phone when the Stealth FX detects any suspicious RF signal.
The Stealth DX  RF Detector with 24/7 Real Time Remote Monitoring Capability

Main Features
- Detects RF audio signal and output as actual audio like a radio
- Introduces random number program for laser wiretapping prevention - generates interceptive signals
- SMS alert
- Transducer - snapping wire surveillance
  ***more features will be introduced in the future
  (trespasser alert, or having 5 ports for updates such as CO2 sensor)

Specification
- Wireless eavesdropping surveillance
- Sweeping Time: less than 15 seconds
- Frequency Range
  20MHz-6GHz
- Receiving Mode : WFM, FM, AM, FHSS, etc.

- Preventing Laser Eavesdropping
- Noise Generator – 2 CH Random White Noise
- Transmission via: Internet, LAN
- Transmitting Data: ID, Frequency, Time, etc.
Transducer / TRN-600

Introduction

- Attached on window glasses, it generates random noises in order to act against laser eavesdropping activities.

- Manipulates voices to be inaudible or delays decoding when a third party tries to eavesdrop indoor communications by releasing laser beams from the outside.

Specification

- Connecting Jack
  
  RJ 11 6 pin

- Size
  
  Diameter: Approx. 60mm
  Height: Approx. 24mm

- Weight
  
  Approx. 50g
Video Signal Surveillance

Summary

This is the most advanced video eavesdropping monitoring equipment that enables security management by having illegally installed camera videos or audio signals submitted to central monitoring center 24/7 in real time or by directly witnessing at the site.

It does not require the process of spectrum analysis to verify the existence of specific video signal - it can be identified and watched immediately like a TV display and improves the work productivity of monitoring or security.

A high receiving sensitivity of 6.0GHz will easily detect the most advanced spy camera signal of 5.8GHz.

This module installed in a number of different secured sites will send suspicious audio and video signals to the central monitoring center in real time. The main site will monitor up to 1,000 client signals simultaneously in a single monitor display.
Major wiretapping frequency ranges used across the world are stored and can control the monitoring according to specified levels for each frequency use.

Analyzing frequency signal

Can remotely adjust setting value of devices installed in meeting rooms.
The Stealth DX RF Detector with 24/7 Real Time Remote Monitoring Capability

Wireless Video Features

- Wideband wireless video signal detection and immediate watch/transmission
- Wideband internet network or internal LAN network
- Control management

Specification

- Detecting Method: VIDEO SWEEP
- Major wiretapping frequency range inspection
  Demodulation: 900MHz-3GHz, 5GHZ-6GHz (more than 99% in major frequency range)
  Detection: 20MHz – 6GHz
- Sweeping time: less than 15 seconds
- Receiving Mode: NTSC, PAL / SECAM, AUDIO
- Transmitting network: Internet, LAN
PC Monitoring Display On a Remote Site(Video)

1. Display of central monitoring center when there is no any suspicious signal.

2. A camera video is detected at 1 area of VIP room or meeting room protected under GTG solutions.

3. A video signal is reported with a pop-up display.

4. All issues have been resolved and the display goes back to normal display.
Oath of Confidentiality

We hereby acknowledge that no information collected during this project will be leaked to a third party under any circumstances without approval or permission from the clients. We will take the full legal responsibility in the events of such leakage.

※ Project includes the following but are not limited to: security measures, surveillance, preventing system operation, or inquiries and consultation.

Received from:
Name (print)
Signature
Date

Received by:
Name (print)
Signature
Date