Sensorless, Permissionless Information Exfiltration with Wi-Fi Micro-Jamming

ROM OGEN (ROMOG@POST.BGU.AC.IL)
OMER SHWARTZ (OMERSHV@POST.BGU.AC.IL)
KFIR ZVI (ZVIKF@POST.BGU.AC.IL)
YOSSI OREN (YOS@BGU.AC.IL)
BEN-GURION UNIVERSITY OF THE NEGEV, ISRAEL
“A covert listening device, more commonly known as a bug or a wire, is usually a combination of a miniature radio transmitter with a microphone. The use of bugs, called bugging, is a common technique in surveillance, espionage and police investigations. “ - Wikipedia
Previous Works

Farshteindiker et al. \cite{farshteindiker2016how} used a device’s gyroscope to exfiltrate data through a victim device.

A piezoelectric device causes interferences to the gyroscope sensor that are readable through a javascript running on the device.

\cite{farshteindiker2016how} Farshteindiker, Benyamin, Nir Hasidim, Asaf Grosz, and Yossi Oren. "How to Phone Home with Someone Else's Phone: Information Exfiltration Using Intentional Sound Noise on Gyroscopic Sensors." In WOOT. 2016.
Objectives

Develop and evaluate an exfiltration technique that maintains the advantages:

1. Covert
2. Permissionless
3. Long range

While reducing the limitations:

1. Need of physical contact with the victim
2. Power requirements
Our Contribution
"Covert channels through external interference."

Shah and Blaze [2] introduced the concept of an “interference channel”, which they defined as a “covert channel that works by creating external interference on a shared communications medium”

Interference Channel

The sender cannot communicate directly with the receiver.

The victim is an uninvolved, unknowing device performing normal communications.

The receiver is capable of receiving some output from the victim and has the ability to separate the benign data from the payload.

The malicious communication is hiding in plain sight.
Micro-Jamming

Many communication protocols, including 802.11, incorporate CCA (Clear Channel Assessment) mechanisms to maintain non-distr uptiveness.

By briefly jamming the radio channel, Wi-Fi frames and responses can be delayed for several milliseconds.
Micro-Jamming
Micro-Jamming
Micro-Jamming
Micro-Jamming
## Traditional Jamming vs Micro-Jamming

<table>
<thead>
<tr>
<th></th>
<th>Traditional Jamming</th>
<th>Micro-Jamming</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode of operation</td>
<td>Packet loss</td>
<td>Packet delay</td>
</tr>
<tr>
<td>Network layers affected</td>
<td>At least 1-2</td>
<td>Only layer 1</td>
</tr>
<tr>
<td>Required transmission power</td>
<td>Stronger than blocked signal</td>
<td>Minimum required for sensing</td>
</tr>
</tbody>
</table>
Test Setup - Active

- Victim Router
  - 2.462 GHz WiFi (channel 11)
  - $D_{AR}$
- Active Implant
  - 2.462 GHz $\mu$-Jam
  - $D_{AD}$
- Victim Device
Test Setup - Active
Test Setup - Active

ATMEGA256RFR2 Xplained Pro evaluation board

Keysight 33622A waveform generator

Tektronix RSA604 real-time signal analyzer
Results
Results
Results

Successful data transfer at rates of 40 bits-per-second with <10% error rate.
Effective to a range of 15+ meters, works through walls.
Found functional at low transmission powers of -17 dBm, or 20 microwatts.
Micro-Jamming Done Passively

When an antenna switches its impedance in a given frequency, it modulates reflecting any ambient radio signals while imposing a frequency shift.

Previous works\[3\] have used this phenomenon to shift one Wi-Fi channel to another while modulating data on top of it.

Using similar techniques, it is possible to jam a Wi-Fi channel using zero energy for transmission.

Test Setup - Passive

2.462 GHz WiFi (channel 11)

Victim Router I

D_{PR}

2.437 GHz WiFi (channel 6)

Victim Router II

D_{PS}

Passive Implant

2.462 GHz μ-Jam

D_{PD}

Victim Device
Test Setup – Passive
Test Setup – Passive

 ANALOG DEVICES

HMC190BMS8 / 190BMS8E

GaAs MMIC SPDT SWITCH
DC - 3 GHz

Typical Applications
The HMC190BMS8E is ideal for:
• MMDS & WirelessLAN
• Portable Wireless

Functional Diagram

Features
Low Insertion Loss: 0.4 dB
Ultra Small Package: MSOP8
High Input IP3: +56 dBm
Positive Control: 0V, 3V @ 0.1 µA

General Description
The HMC190BMS8E is a low cost SPDT switch in a 8-lead MSOP package. The switch can control signals from DC to 3 GHz. It is especially suited for low and medium power applications using positive control voltages. The two control voltages require a minimal amount of DC current, which is optimal for battery powered radio systems at 0.8, 1.8, and 2.4 GHz. The HMC190BMS8E provides exceptional third order intermodulation performance of +56 dBm. The design has been optimized for the small MSOP package, and maintains a VSWR of better than 1.2:1 up to 2 GHz. This device is the positive control MSOP8 packaged version of our HMC230AS8(E) negative control device.
### Traditional Jamming vs Micro-Jamming (cont’)

<table>
<thead>
<tr>
<th></th>
<th>Traditional Jamming</th>
<th>Micro-Jamming</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range vs transmission power</td>
<td>Small, must overcome existing signals</td>
<td>Large</td>
</tr>
<tr>
<td>Can be done passively?</td>
<td>Not effectively?</td>
<td>Demonstrated in the paper</td>
</tr>
<tr>
<td>Detectability</td>
<td>Shows in standard network logs</td>
<td>Hard to differentiate from noise</td>
</tr>
</tbody>
</table>
Demo
Conclusions

Micro-jamming was shown as an effective development over traditional jamming as a covert channel.

Using micro-jamming, an implant can transmit over longer distances and use less power than with traditional jamming.

In addition, micro-jamming allows for lower-profile exfiltration of data that is harder to detect without actively looking with the right equipment.
Thank You – Any Questions?

Rom Ogen (romog@post.bgu.ac.il)
Omer Shwartz (omershv@post.bgu.ac.il)
Kfir Zvi (zvikf@post.bgu.ac.il)
Yossi Oren (yos@bgu.ac.il)

Come see our live demo at the USENIX poster session!

https://iss.oy.ne.ro/Microjam