NICScatter: Backscatter as a Covert Channel in Mobile Devices

Zhice Yang\textsuperscript{1,2}, \textbf{Qianyi Huang}\textsuperscript{2}, Qian Zhang\textsuperscript{2}  
\textsuperscript{1}SIST, ShanghaiTech University  
\textsuperscript{2}CSE, Hong Kong University of Science and Technology
Is Our Data Safe Enough?
Information Leakage under Isolation

Incident Signal

Victim

Reflected Signal

Attacker
Covert Communication through Backscatter

NICScatter: backscatter through commercial NICs

System vulnerabilities in smartphone and Linux notebook
Backscatter Basics

Incident Signals

Reflected Signals

Backscatter Transmitter

Impedance Switching Circuits
Backscatter through Commercial NICs
BCM 1045 Wi-Fi NIC

Vector Network Analyzer
## NICScatter Efficiency

<table>
<thead>
<tr>
<th>Model</th>
<th>Off State</th>
<th>On State</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM1045, ant1</td>
<td>12.4+j14.4</td>
<td>106.9-j9.8</td>
</tr>
<tr>
<td>Intel5300, ant1</td>
<td>119.0+j137.0</td>
<td>80.3+j66.8</td>
</tr>
<tr>
<td>Intel5300, ant2</td>
<td>54.3+j122.7</td>
<td>57.7+j78.4</td>
</tr>
</tbody>
</table>

- **Incident Signal**

- **Reflected Signal**

-6 dB
## NICScatter Efficiency

<table>
<thead>
<tr>
<th>Model</th>
<th>Off State</th>
<th>On State</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM1045, ant1</td>
<td>12.4+j14.4</td>
<td>106.9-j9.8</td>
</tr>
<tr>
<td>Intel5300, ant1</td>
<td>119.0+j137.0</td>
<td>80.3+j66.8</td>
</tr>
<tr>
<td>Intel5300, ant2</td>
<td>54.3+j122.7</td>
<td>57.7+j78.4</td>
</tr>
</tbody>
</table>

**Incident Signal**

-18 dB

**Reflected Signal**
Reflection Diversities

Intel 5300

Atheros AR9285
Reflection Diversities

On Off Position Modulation (OOPM)
Latency Diversities

![Graph showing execution delay for different kernels and devices]

- Up delay on kernel 4.4.0-31
- Down delay on kernel 4.4.0-31
- Up delay on kernel 3.19.0-25
- Down delay on kernel 3.19.0-25

Devices:
- AR9285
- AR9380
- BCM1045
- Intel 5300
Latency Diversities

On Off Position Modulation (OOPM)

Delay (second)

0.2
0.15

- Up delay on kernel 4.4.0-31
- Down delay on kernel 4.4.0-31
- Up delay on kernel 3.19.0-25
- Down delay on kernel 3.19.0-25

0.5s
How to Hide the Communication?
RFKILL Subsystem

Network Manager

rfkill unblock

/dev/rfkill

uevent

rtnetlink

IEEE80211_open

*driver* _start

*driver* _stop

rfkill block

rfkill core

cfg80211

mac80211

WNIC driver

HARDWARE

on

off

KERNEL

userspace

netlink socket

IEEE80211_stop

cfg80211_rfkill_set_block

# file: rfkill
# owner: root
# group: netdev
user::rw-
user: testu:rw-
group::rw-
mask::rw-
other::r--

HARDWARE

rfkill

unblock

block
Android App Permissions

• Dangerous Permissions
  • READ_CALENDAR, CAMERA, READ_SMS, READ_CALL_LOG ...

• Normal Permissions
  • SET_ALARM, SET_TIME_ZONE, ...
  
  CHANGE_WIFI_STATE
Attack Scenario

- Receiver
- Victim
- Helper

Diagram:
- Helper to Receiver: $d_2$ (150cm)
- Helper to Victim: $d_1$ (65cm)
- Victim to Receiver: $d_3$
Attack Scenario

N210

Incident Signal

HP Elitebook 8530P

SNR (dB) vs. Distance (cm)
Attack Scenario

- N210
- Incident Signal
- Galaxy S2

Graph:
- SNR (dB) vs. Distance (cm)
  - Distance (cm): 2, 4, 6, 8, 10, 12, 14, 16, 18, 20
  - SNR (dB): -6, -4, 0, 2, 4, 6, 8, 10, -4, -6
Attack Scenario

TPLink 4300

Ref: HP Elitebook 8530P

RSSI

CSI

HP Elitebook 8530P
Limitations and Discussion

• Communication Distance
  • SINR, NIC Models, Antenna Gain, etc.
    ➢ Interference Cancellation

• Date Rate
  • Software: NIC Driver, Hardware: On-off processing logic
    ➢ Fast impedance change

• Possible Applications
  • Cross Protocol Communication, Wireless Sensing, etc.
Thank you!
Backup Slides
On-o Position Modulation (OOPM)
Transmission Time of Sensitive Information

<table>
<thead>
<tr>
<th>Data</th>
<th>bits</th>
<th>Laptop@30cm</th>
<th>USRP@90cm</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>48</td>
<td>49 sec</td>
<td>54 sec</td>
</tr>
<tr>
<td>Plain Password</td>
<td>64</td>
<td>1.09 min</td>
<td>1.20 min</td>
</tr>
<tr>
<td>MD5</td>
<td>128</td>
<td>2.18 min</td>
<td>2.40 min</td>
</tr>
<tr>
<td>GPS Coordinate</td>
<td>128</td>
<td>2.18 min</td>
<td>2.40 min</td>
</tr>
<tr>
<td>SHA1 Hash</td>
<td>160</td>
<td>2.72 min</td>
<td>3.00 min</td>
</tr>
<tr>
<td>Disk Encryption Key</td>
<td>256</td>
<td>4.35 min</td>
<td>4.80 min</td>
</tr>
</tbody>
</table>
Receiving Range