Strange and Radiant Machines in the PHY Layer

Travis Goodspeed  Sergey Bratus

Neighbors for the Liberation of Weird Machines

April 12, 2012
Это Сибирь, детка
Introduction
Introduction
Introduction
Introduction
Phrack 49:19

• `strcat()` overwrite the return pointer.
• `foo()` returns to the wrong place.
• Some of the string is executed as code.
Nowadays, you need more tricks.

- Heap Feng Shui to control heap alignment.
- Jit Spraying to produce shellcode in executable region.
- Return-Oriented-Programming to repurpose existing code.
Nowadays, you need more tricks.

• Heap Feng Shui to control heap alignment.
• Jit Spraying to produce shellcode in executable region.
• Return-Oriented-Programming to repurpose existing code.

• None of these are useful in isolation.
• None of these were useful in 1996.
• All of these are useful in 2012.
Fingerprinting to Attack Hardware

- Just like software, hardware has bugs.
- Unlike software, these bugs are poorly understood.
- Document everything strange, find what’s useful later.
НЕ СНИМАЙ НОГОЙ ПРИВОДНОГО РЕМНЯ
не ходи
по рыбе
Кирпич укладывай

Правильно

25 Радио 6
Не загромождай рабочего места
НЕ ПРОХОДИ ПОД ТРАНСМИССИЙНЫМ ВАЛОМ
СТАВЬ ПОДРУЧНИК БЛИЖЕ К ХАМНЮ
НЕПРАВИЛЬНО
ПРАВИЛЬНО
Fingerprinting to Attack Hardware

- Just like software, hardware has bugs.
- Unlike software, these bugs are poorly understood.
- Document everything strange, find what’s useful later.
Strange and Radiant Machines

- Strange Machines:
  - Might not be useful.
  - ANYTHING and EVERYTHING unexpected qualifies.
Strange and Radiant Machines

- Strange Machines:
  - Might not be useful.
  - ANYTHING and EVERYTHING unexpected qualifies.

- Radiant Machines:
  - Were useful *once* in writing *one* exploit.
  - Most of these seem useless out of context.
Radiant Machines

- The OSI Model gives attacker control of *inside* of packet.
Radiant Machines

- The OSI Model gives attacker control of \textit{inside} of packet.
- Radio receivers suffer false positives, false negatives.
Radiant Machines

- The OSI Model gives attacker control of *inside* of packet.
- Radio receivers suffer false positives, false negatives.
- Instructions have maximum clock frequencies.
The OSI Model gives attacker control of *inside* of packet.
Radio receivers suffer false positives, false negatives.
Instructions have maximum clock frequencies.
Flash has different voltage tolerances than RAM or ROM.
Radiant Machines

- The OSI Model gives attacker control of *inside* of packet.
- Radio receivers suffer false positives, false negatives.
- Instructions have maximum clock frequencies.
- Flash has different voltage tolerances than RAM or ROM.
- Regions of a chip have different power supplies.
PHY-Layer Exploits
cumberland% goodfet.csspi sniff i head
Listening on 00deadbeef on 2405 MHz
# DEBUG Clearing overflow
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff

There are slower than normal packets are sent faster normal shift as result is from header lost not stop/start.
• The OSI Model gives attacker control of *inside* of packet.
• Radio receivers suffer false positives, false negatives.
• The OSI Model gives attacker control of *inside* of packet.
• Radio receivers suffer false positives, false negatives.

• For the Zigbee/802.15.4 implementation,
• Packets length may vary.
• The same symbol set is used for payload and headers.
Packet in Packet

Figure 15.11 Packet terminology. (Courtesy of Feit, 1997.)
Packet in Packet

Packet format

variable length

$preamble \quad sync \quad \frac{g}{3} \quad data \quad CRC$

Optional: whitening, FEC, Manchester
Packet in Packet
Packet in Packet

packet format

variable length

preamble sync data CRC

Optional: whitening, FEC, Manchester
cumberland% goodfet.cspl sniff 1 head
Listening on 00deadbeef on 2405 MHz
# DEBUG Clearing overflow
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff

There are shorter than normal packets.
I suspect rate normal
shifts as result is
given handshades not
to catch.

Goodspeed/Bratus HES2012  PHY Layer Exploits  35
Packet in Packet

```
00 00 00 00 a7 0f 01 08 82 ff ff ff ff ff...

Preamble  Sync  Body

00 00 00 00 a7 .. 00 00 00 00 a7 0f 01 ...

Preamble  Sync  Body
```
Radiant Machines of Packet in Packet

- The OSI Model gives attacker control of *inside* of packet.
- Radio receivers suffer false positives, false negatives.
- For the Zigbee/802.15.4 implementation,
  - Packets length may vary.
  - The same symbol set is used for payload and headers.
Packet Out of Packet
### Packet Out of Packet

#### Kiss your security goodbye

<table>
<thead>
<tr>
<th>C</th>
<th>OA</th>
<th>78</th>
<th>06</th>
<th>01</th>
<th>C2</th>
<th>98</th>
<th>76</th>
<th>OA</th>
<th>CO</th>
<th>C8</th>
<th>98</th>
<th>35</th>
<th>OA</th>
<th>CO</th>
<th>CD</th>
<th>5B</th>
</tr>
</thead>
<tbody>
<tr>
<td>K</td>
<td>CD</td>
<td>98</td>
<td>35</td>
<td>OA</td>
<td>C0</td>
<td>CD</td>
<td>98</td>
<td>35</td>
<td>OA</td>
<td>C0</td>
<td>CD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P</td>
<td>OA</td>
<td>78</td>
<td>06</td>
<td>01</td>
<td>0F</td>
<td>00</td>
<td>43</td>
<td>00</td>
<td>00</td>
<td>05</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td></td>
</tr>
</tbody>
</table>

Dev Pac ket Mod ty typ el e

Sequence ID Flags/ Meta

HID Code

Checksum

(Key-Down) Packet with device address:

CD 98 35 0A C0
Packet Out of Packet

Keykeriki 2.0, http://www.remote-exploit.org/
Max Moser and Thorsten Schroeder
Packet Out of Packet

GoodFETNRF

- Travis Goodspeed analyzed TurningPoints ResponseCard RF “Clicker cards”
- Reprogrammed “The Next HOPE” batches using its GODFET
  - Capable of “sniffing” OpenBeacon protocol
  - Jamming frequencies by sending NRF constant carrier wave
- “Although some architectural limitations of the NRF24L01+ make sniffing difficult without knowing the first three bytes of the destination MAC address to be sniffed”
  - That’s because there is no documented way how to get layer2 access using this chip
- Still cool way if you know the address. Python code to interface with the GoodFET Firmware is available at http://sourceforge.net/projects/goodfet/files/.

- DREAMLAB TECHNOLOGIES

Digital v00d00 - 8th of December 2010
Thorsten Schröder, Max Moser
• Keykeriki needed custom hardware to sniff at 2Mbps.
• Couldn’t match in hardware because SYNC is unknown.

• With a trick similar to PIP, we can do it on cheap hardware.
• First, cause false-positive matches before the packet.
• Second, disable the CRC.
Packet Out of Packet
Packet Out of Packet

Packet format

variable length

preamble sync data CRC

Optional: whitening, FEC, Manchester
Packet Out of Packet

```
air-2% goodfet.nrf autotune
Autotuning as 0000000055 on 2499 MHz
sync,mac,r5,r6
Tuned to 2480 MHz
Tuned to 2481 MHz
'55,0102030201,51,09' looks valid 1 0.00820
'55,0102030201,51,09' looks valid 2 0.01600
'55,0102030201,51,09' looks valid 3 0.02326
'55,0102030201,51,09' looks valid 4 0.02837
Tuned to 2482 MHz
Tuned to 2483 MHz
```
Radiant Machines of POOP

- Radio receivers suffer false positives, false negatives.
- For the MSKB implementation,
- Address length is arbitrary on the receiver.
- Checksums can be disabled.
- The preamble is predictable.
- Preamble damage is not fatal to reception.
Power Supply Attacks
Radiant Machines in Power Supplies

- Flash has different voltage tolerances than RAM or ROM.
- Regions of a chip have different power supplies.
Power Supply Attacks
Power Supply Attacks
Power Supply Attacks
Power Supply Attacks
Power Supply Attacks
Power Supply Attacks
Radiant Machines in Power Supplies

- Flash has different voltage tolerances than RAM or ROM.
- Regions of a chip have different power supplies.
Other Vulnerabilities
Read the Fucking Papers

• Packets in Packets:
Orsen Welles’ In-Band Signaling Attack for Digital Radios
http://packetsinpackets.org/
Read the Fucking Papers

- Packets in Packets:
  Orsen Welles’ In-Band Signaling Attack for Digital Radios
  http://packetsinpackets.org/

- Promiscuity is the NRF24L01+’s Duty
  http://travisgoodspeed.blogspot.com/
Read the Fucking Papers

- Packets in Packets: Orsen Welles’ In-Band Signaling Attack for Digital Radios
  http://packetsinpackets.org/
- Promiscuity is the NRF24L01+’s Duty
  http://travisgoodspeed.blogspot.com/
- Freescale MC13224 Memory Extraction
  http://travisgoodspeed.blogspot.com/
Read the Fucking Papers

- Packets in Packets: Orsen Welles’ In-Band Signaling Attack for Digital Radios  
  http://packetsinpackets.org/
- Promiscuity is the NRF24L01+’s Duty  
  http://travisgoodspeed.blogspot.com/
- Freescale MC13224 Memory Extraction  
  http://travisgoodspeed.blogspot.com/
- Language-Theoretic Security  
  http://langsec.org/
Questions