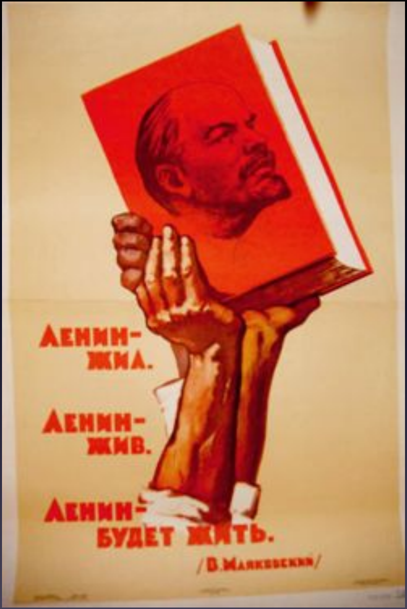
Strange and Radiant Machines in the PHY Layer

Travis Goodspeed   Sergey Bratus

Neighbors for the Liberation of Weird Machines

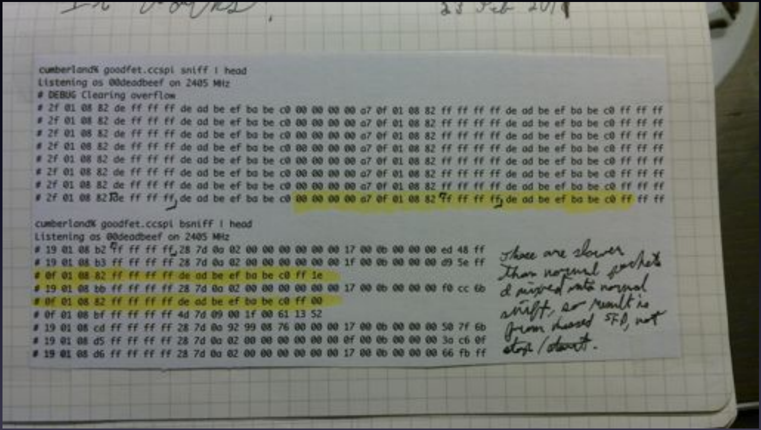
April 12, 2012


ЛЕНИН-
ЖИЛ.
ЛЕНИН-
ЖИВ.
ЛЕНИН-
БУДЕТ ЖИТЬ.
/В. МАЯКОВСКИЙ/

DEMOTIVATORS.RU
Это Сибирь, детка

Introduction

Introduction

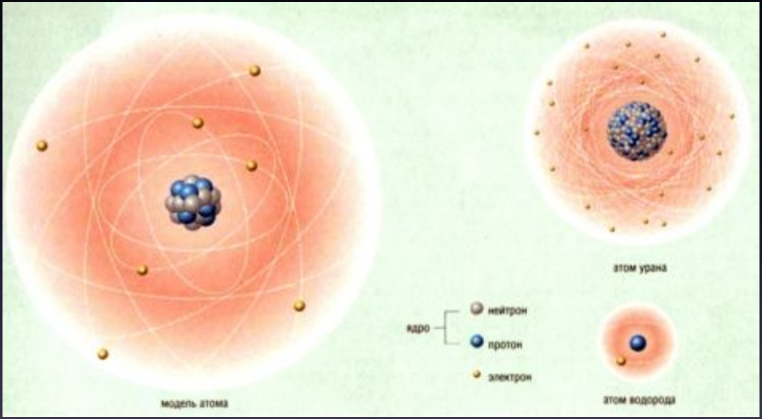


It Works, 23 Feb 2011

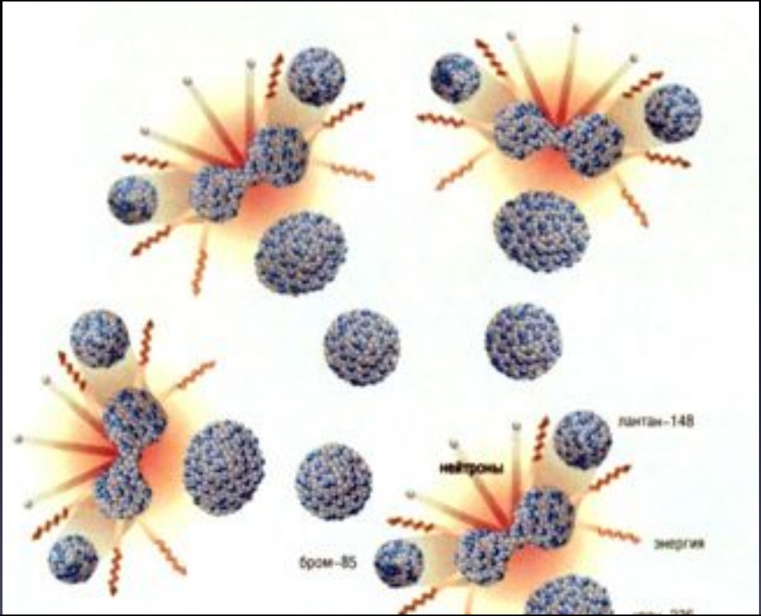
```
cumberland% goodfet.ccspi sniff | head
Listening as 00deadbeef on 2405 MHz
# DEBUG Clearing overflow
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff 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

cumberland% goodfet.ccspi bsniff | head
Listening as 00deadbeef on 2405 MHz
# 19 01 08 b2 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 ed 48 ff
# 19 01 08 b3 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 1f 00 0b 00 00 00 d9 5e ff
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 1e
# 19 01 08 bb ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 f0 cc 6b
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 00
# 0f 01 08 bf ff ff ff ff 4d 7d 09 00 1f 00 61 13 52
# 19 01 08 cd ff ff ff ff 28 7d 0a 92 99 08 76 00 00 00 17 00 0b 00 00 00 50 7f 6b
# 19 01 08 d5 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 0f 00 0b 00 00 00 3a c6 0f
# 19 01 08 d6 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 66 fb ff
```

These are slower
Than normal packets
& mixed into normal
sniff, so result is
from shared SFD, not
stop/start.

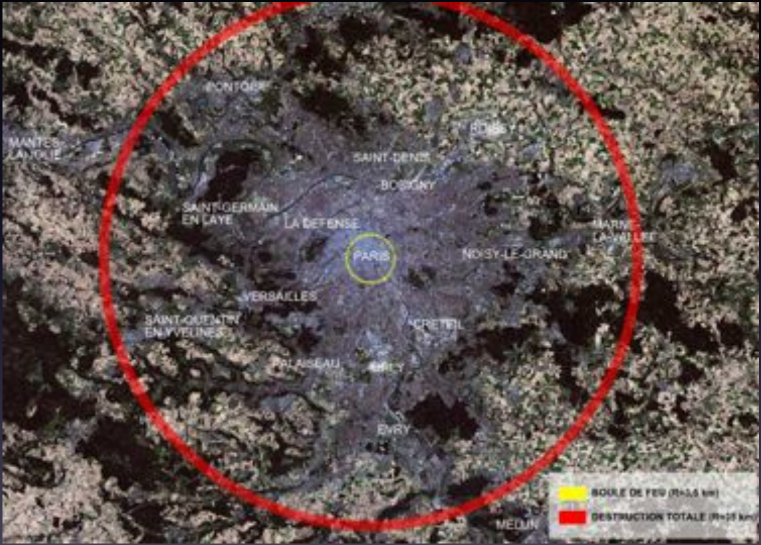
Introduction



Introduction



Introduction



🟨 BOULE DE FEU (R=3,6 km)

🟥 DESTRUCTION TOTALE (R=25 km)

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.

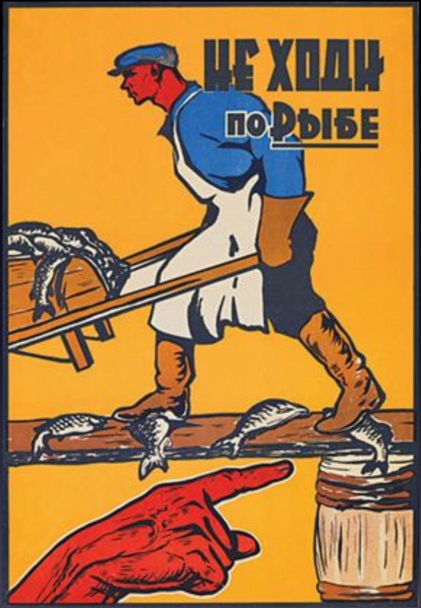
- Heap Feng Shui to control heap alignment.
- Jit Spraying to produce shellcode in executable region.
- Return-Oriented-Programming to repurpose existing code.

- 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

ПРЯЧЬ
ВОЛОСЫ

КИРПИЧ
УКЛАДЫВАЙ
ПРАВИЛЬНО
25
рядов

Осторожно
при натяжке
проводов

НЕ ОБТИРАЙ
БАРАБАН
НА ХОДУ

НЕ ЗАГРОМОЖДАЙ
РАБОЧЕГО МЕСТА

СМОТРИ
ПОД
НОГИ

НЕ ПРОВЕРЯЙ ПАЛЬЦЕМ
есть ли
напряжение

НЕ
ПРОХОДИ
ПОД
ТРАНСМИССИОННЫМ
ВАЛОМ

СТАВЬ
ПОДРУЧНИК
БЛИЖЕ
К КАМНЮ
НЕправильно
правильно

НАВЕРХУ
РАБОТАЮТ
НЕ
СТОЙ
ПОД МАЧТОЙ

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 *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.

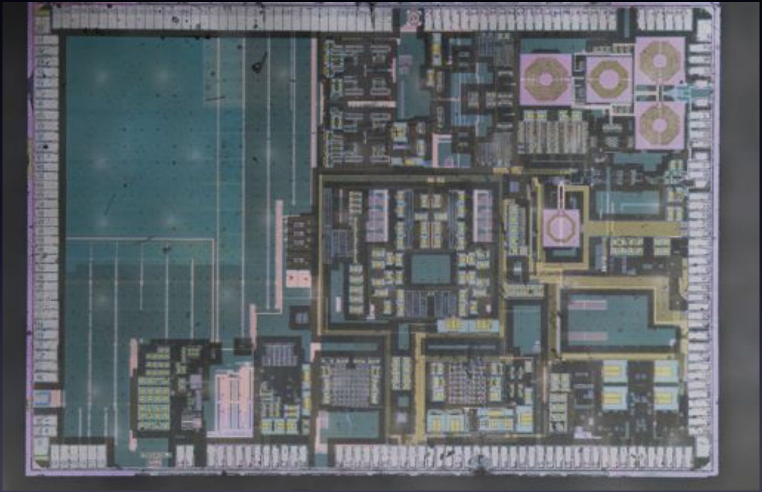
Radiant Machines

- 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.

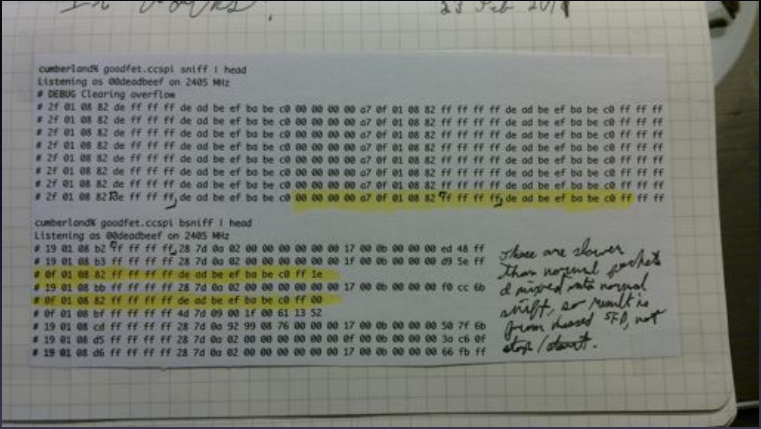
Radiant Machines

- 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



Packet in Packet



```
cumberland% goodfet.ccspi sniff | head
Listening as 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

cumberland% goodfet.ccspi bsniff | head
Listening as 00deadbeef on 2405 MHz
# 19 01 08 b2 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 ed 48 ff
# 19 01 08 b3 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 1f 00 0b 00 00 00 d9 5e ff
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 1e
# 19 01 08 bb ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 f0 cc 6b
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 00
# 0f 01 08 bf ff ff ff ff 4d 7d 09 00 1f 00 61 13 52
# 19 01 08 cd ff ff ff ff 28 7d 0a 92 99 08 76 00 00 00 17 00 0b 00 00 00 50 7f 6b
# 19 01 08 d5 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 0f 00 0b 00 00 00 3a c6 0f
# 19 01 08 d6 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 66 fb ff
```

These are slower than normal packets & mixed into normal sniff, so result is from shared SFD, not stop/start.

Radiant Machines of Packet in Packet

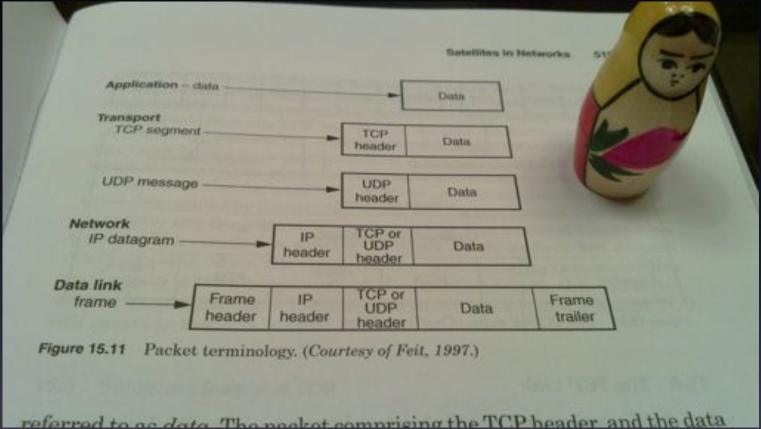
- The OSI Model gives attacker control of *inside* of packet.
- Radio receivers suffer false positives, false negatives.

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 in Packet



Satellites in Networks 51

Application – data → Data

Transport
TCP segment → TCP header | Data

UDP message → UDP header | Data

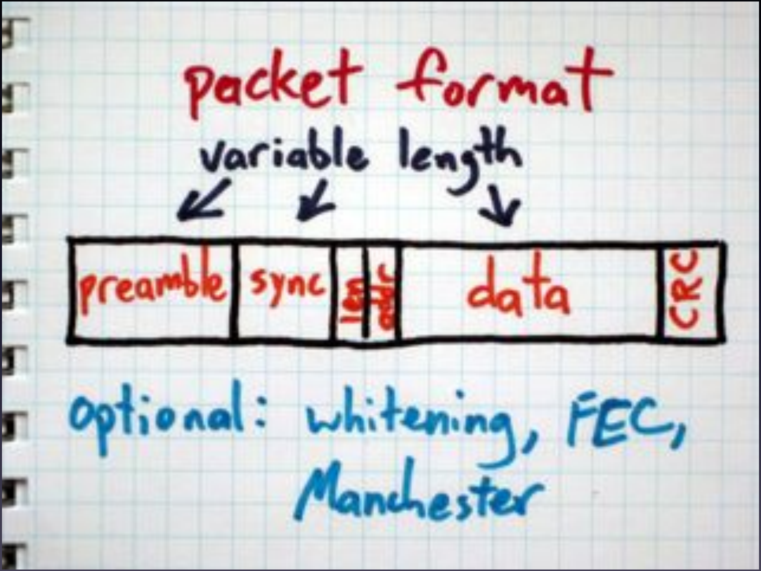
Network
IP datagram → IP header | TCP or UDP header | Data

Data link
frame → Frame header | IP header | TCP or UDP header | Data | Frame trailer

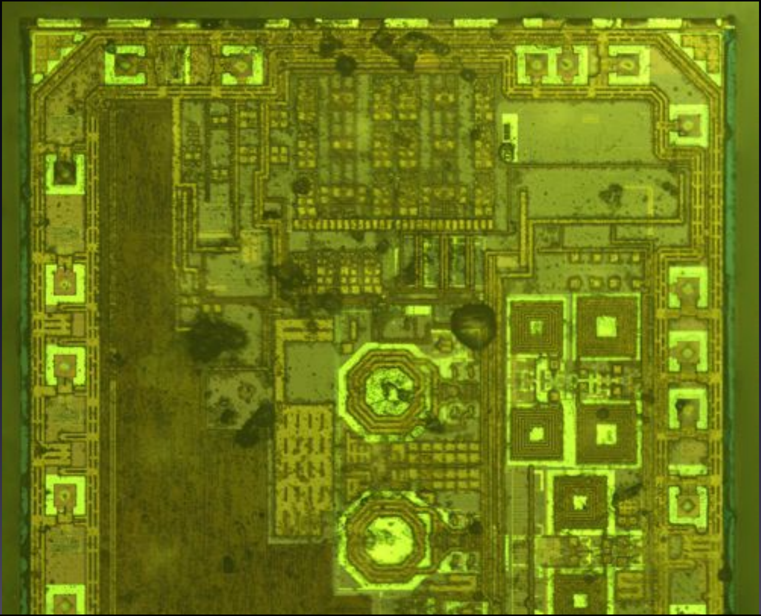
Figure 15.11 Packet terminology. (*Courtesy of Feit, 1997.*)

referred to as *data*. The packet comprising the TCP header and the data

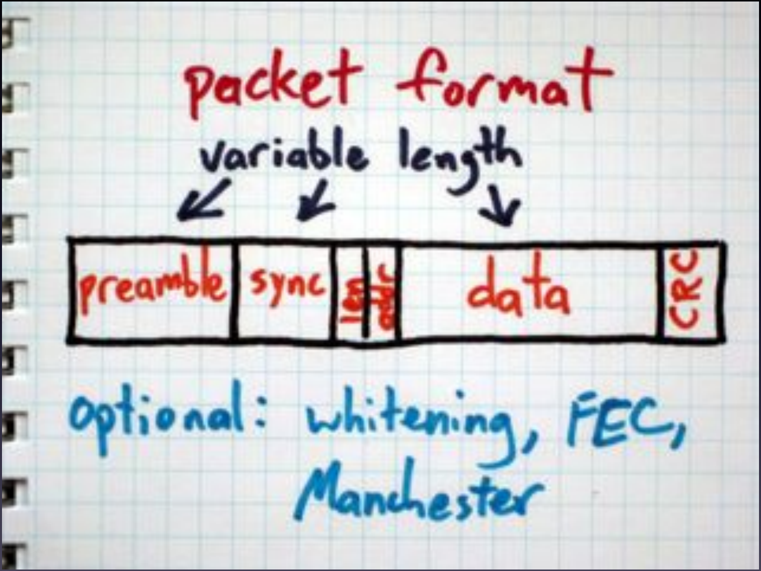
Packet in Packet



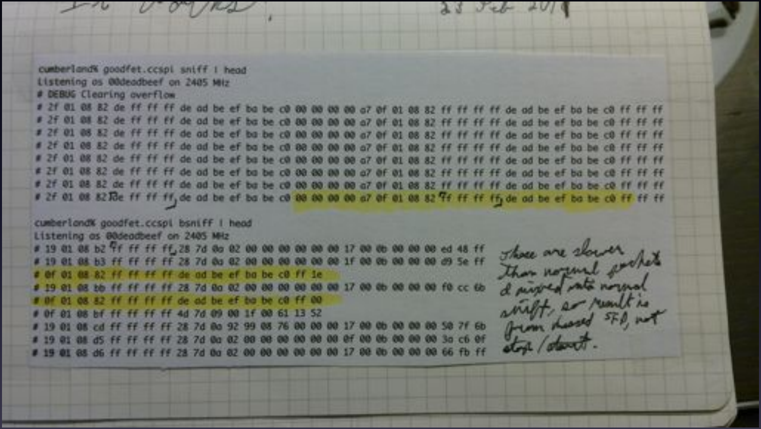
Packet in Packet



Packet in Packet



Packet in Packet

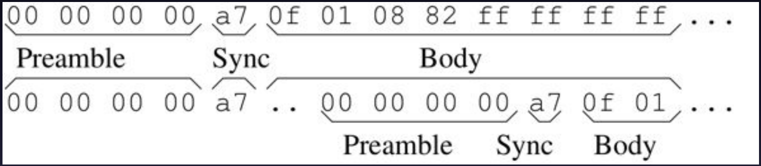


[illegible] 23 Feb 201

```
cumberland% goodfet.ccspi sniff | head
Listening as 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

cumberland% goodfet.ccspi bsniff | head
Listening as 00deadbeef on 2405 MHz
# 19 01 08 b2 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 ed 48 ff
# 19 01 08 b3 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 1f 00 0b 00 00 00 d9 5e ff
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 1e
# 19 01 08 bb ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 f0 cc 6b
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 00
# 0f 01 08 bf ff ff ff ff 4d 7d 09 00 1f 00 61 13 52
# 19 01 08 cd ff ff ff ff 28 7d 0a 92 99 08 76 00 00 00 17 00 0b 00 00 00 50 7f 6b
# 19 01 08 d5 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 0f 00 0b 00 00 00 3a c6 0f
# 19 01 08 d6 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 66 fb ff
```

These are slower
than normal packets
& mixed into normal
sniff, so result is
from [illegible] SFD, not
stop/start.

Packet in Packet



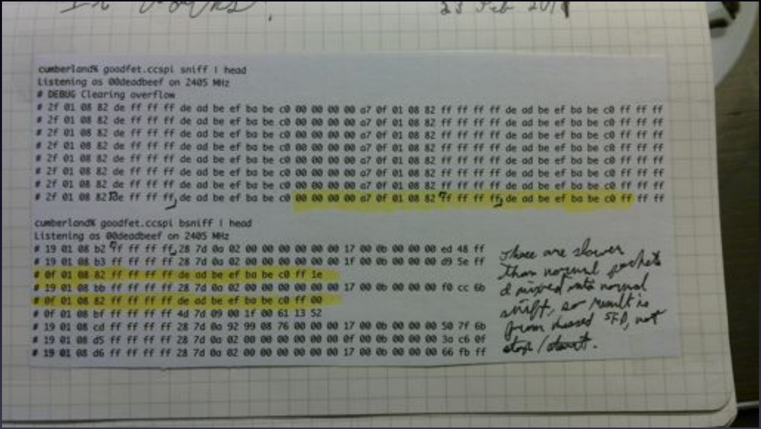
```
00 00 00 00 a7 0f 01 08 82 ff ff ff ff ...
```

Preamble Sync Body

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

Preamble Sync Body

Packet in Packet



It works! 23 Feb 2011

```
cumberland% goodfet.ccspi sniff | head
Listening as 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

cumberland% goodfet.ccspi bsniff | head
Listening as 00deadbeef on 2405 MHz
# 19 01 08 b2 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 ed 48 ff
# 19 01 08 b3 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 1f 00 0b 00 00 00 d9 5e ff
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 1e
# 19 01 08 bb ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 f0 cc 6b
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 00
# 0f 01 08 bf ff ff ff ff 4d 7d 09 00 1f 00 61 13 52
# 19 01 08 cd ff ff ff ff 28 7d 0a 92 99 08 76 00 00 00 17 00 0b 00 00 00 50 7f 6b
# 19 01 08 d5 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 0f 00 0b 00 00 00 3a c6 0f
# 19 01 08 d6 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 66 fb ff
```

These are slower
than normal packets
& missed into normal
sniff, so result is
from shared SFD, not
stop/start.

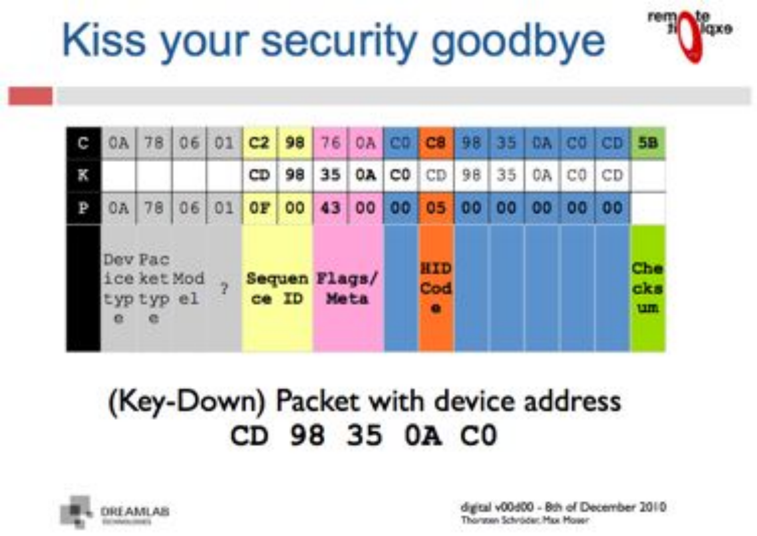
Radiant Machines of Packet in Packet

- 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

C	0A	78	06	01	C2	98	76	0A	C0	C8	98	35	0A	C0	CD	5B
K					CD	98	35	0A	C0	CD	98	35	0A	C0	CD	
P	0A	78	06	01	0F	00	43	00	00	05	00	00	00	00	00	
	Device type	Packet type	Model	?	Sequence ID		Flags/ Meta			HID Code						Checksum

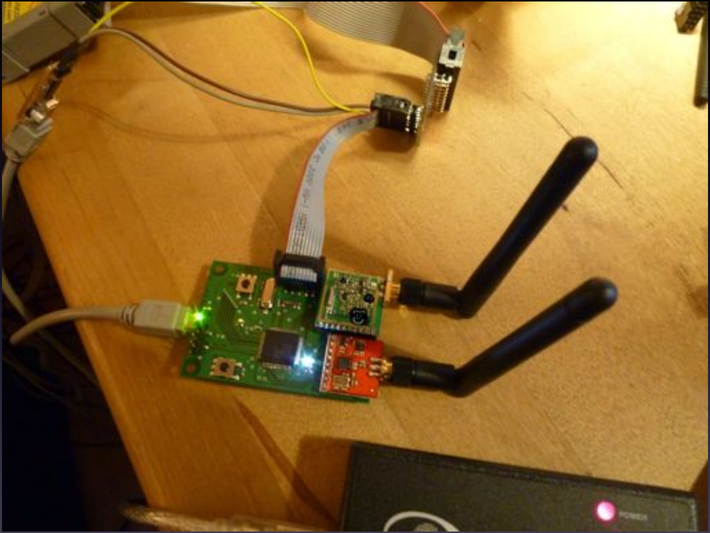
(Key-Down) Packet with device address

CD 98 35 0A C0

DREAMLAB

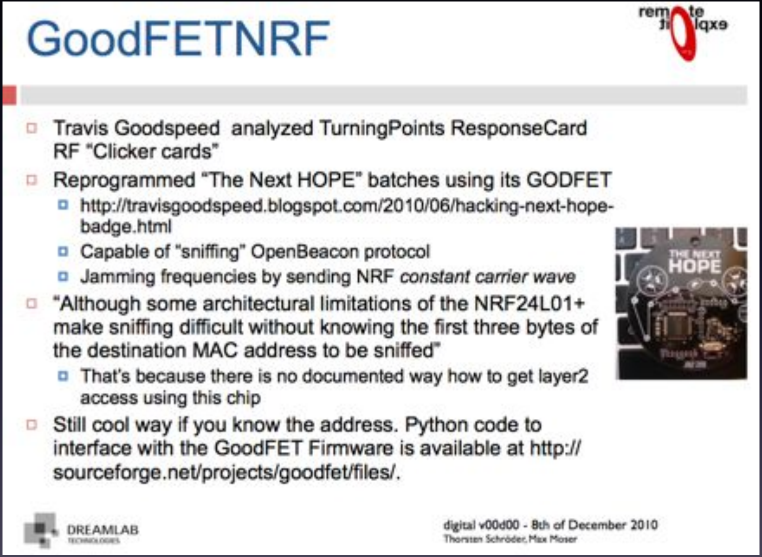
digital v00d00 - 8th of December 2010
Thorsten Schröder, Max Moser

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
  - http://travisgoodspeed.blogspot.com/2010/06/hacking-next-hope-badge.html
  - 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/.

digital v00d00 - 8th of December 2010
Thorsten Schröder, Max Moser

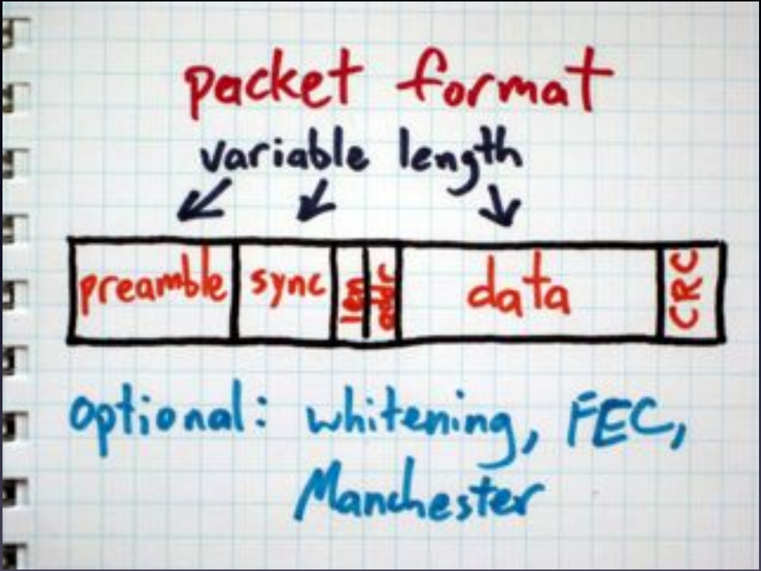
Packet Out of Packet

- Keykeriki needed custom hardware to sniff at 2Mbps.
- Couldn’t match in hardware because SYNC is unknown.

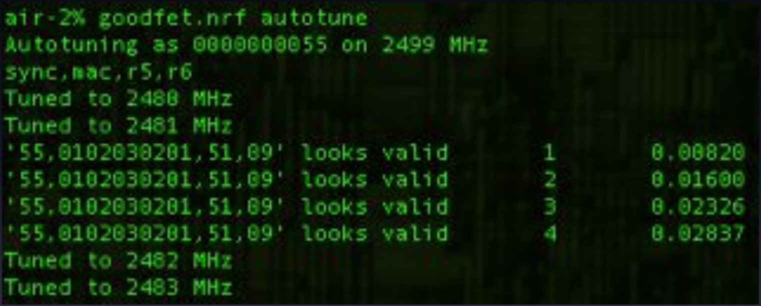
- With a trick similar to PIP, we can do it on cheap hardware.
- First, cause false-positive matches *before* the packet.
- Second, disable the CRC.

Packet Out of Packet

Packet Out of Packet



Packet 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
```

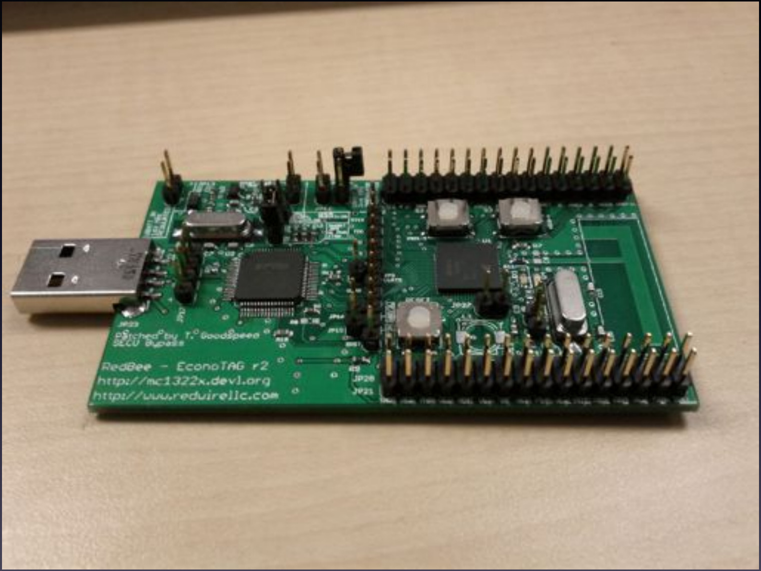
Packet Out of Packet

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.

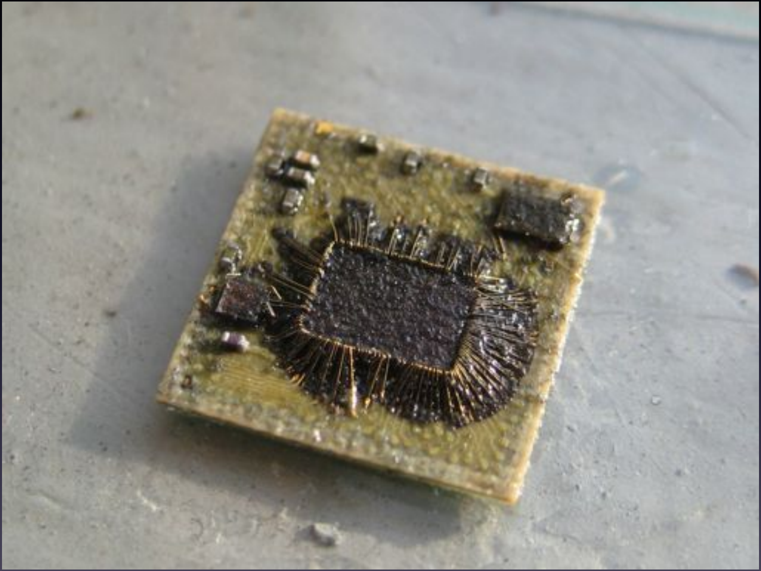
Power Supply Attacks



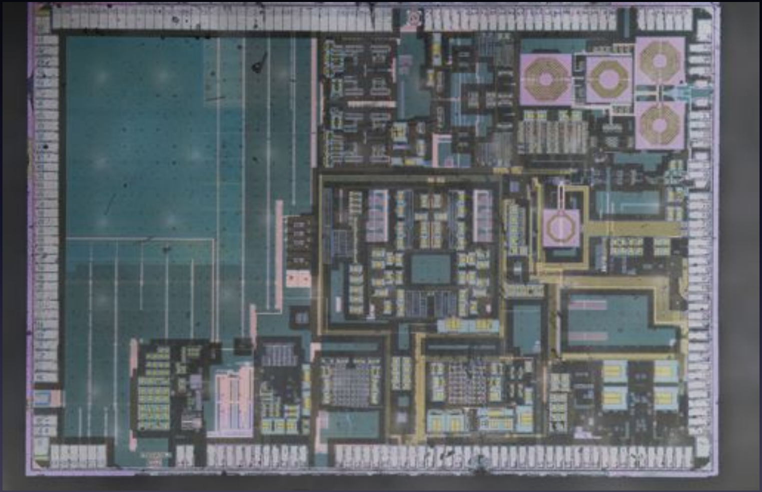
Radiant Machines in Power Supplies

- Flash has different voltage tolerances than RAM or ROM.
- Regions of a chip have different power supplies.

Power Supply Attacks



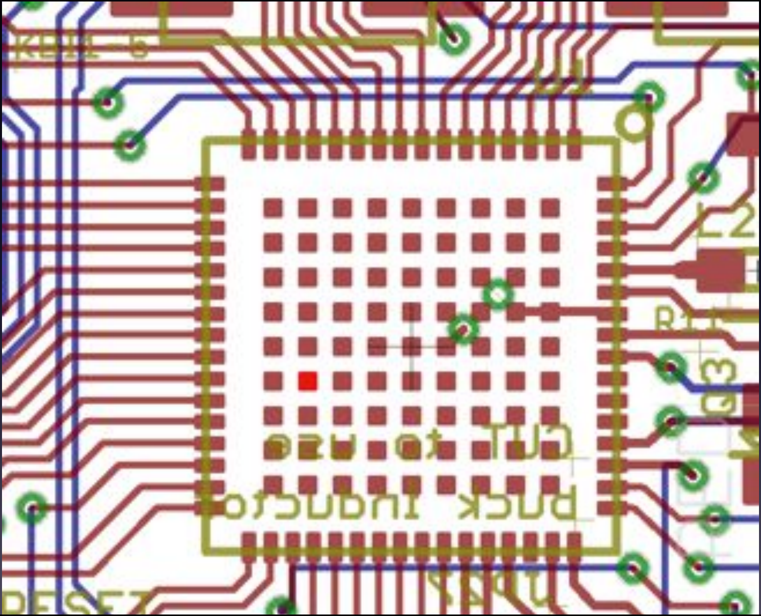
Power Supply Attacks



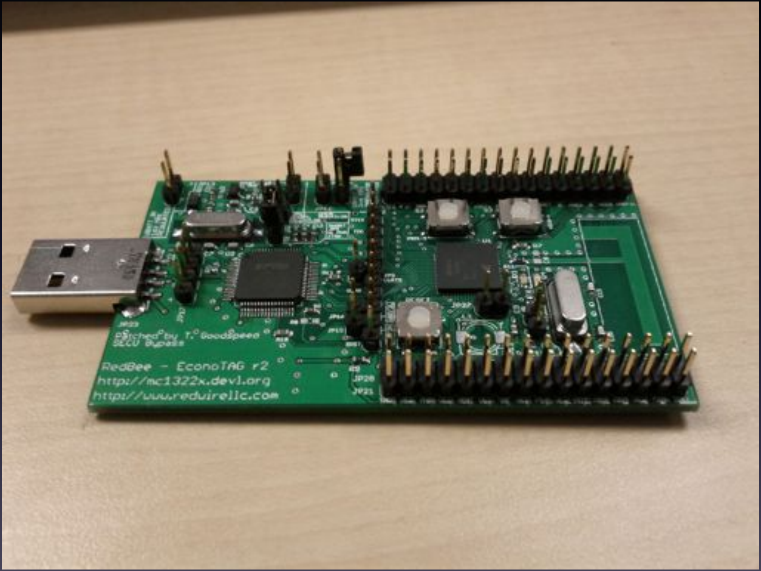
Power Supply Attacks

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