

COM-405: Mobile Networks

Lecture 11.1: Physical Layer Security Haitham Hassanieh



EPFL

SENS
Laboratory of SENSing
& Networking Systems

WIRELESS IMPLANTABLE MEDICAL DEVICES

Deep Brain
Neurostimulators



Cochlear Implants



Gastric
Stimulators



Cardiac Defibrillators/
Pacemakers



Foot Drop
Implants

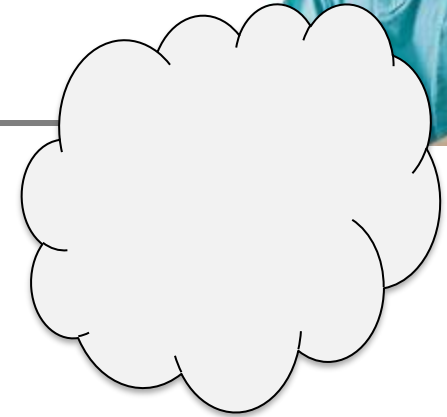


Insulin Pumps



Benefits of Wireless

- Easier communication with implant
- Remote monitoring



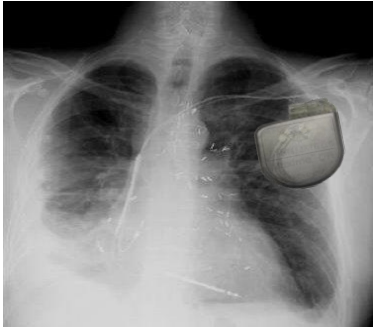
Benefits of Wireless

- Easier communication with implant
- Remote monitoring
 - Reduces hospital visits by 40% and cost per visit by \$1800
[Journal of the American College of Cardiology, 2011]

What about security?

Security Attacks

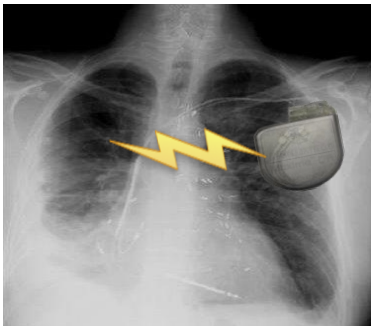
1) Passive attack: Eavesdrop on private data



Patient diagnosis,
vital signs

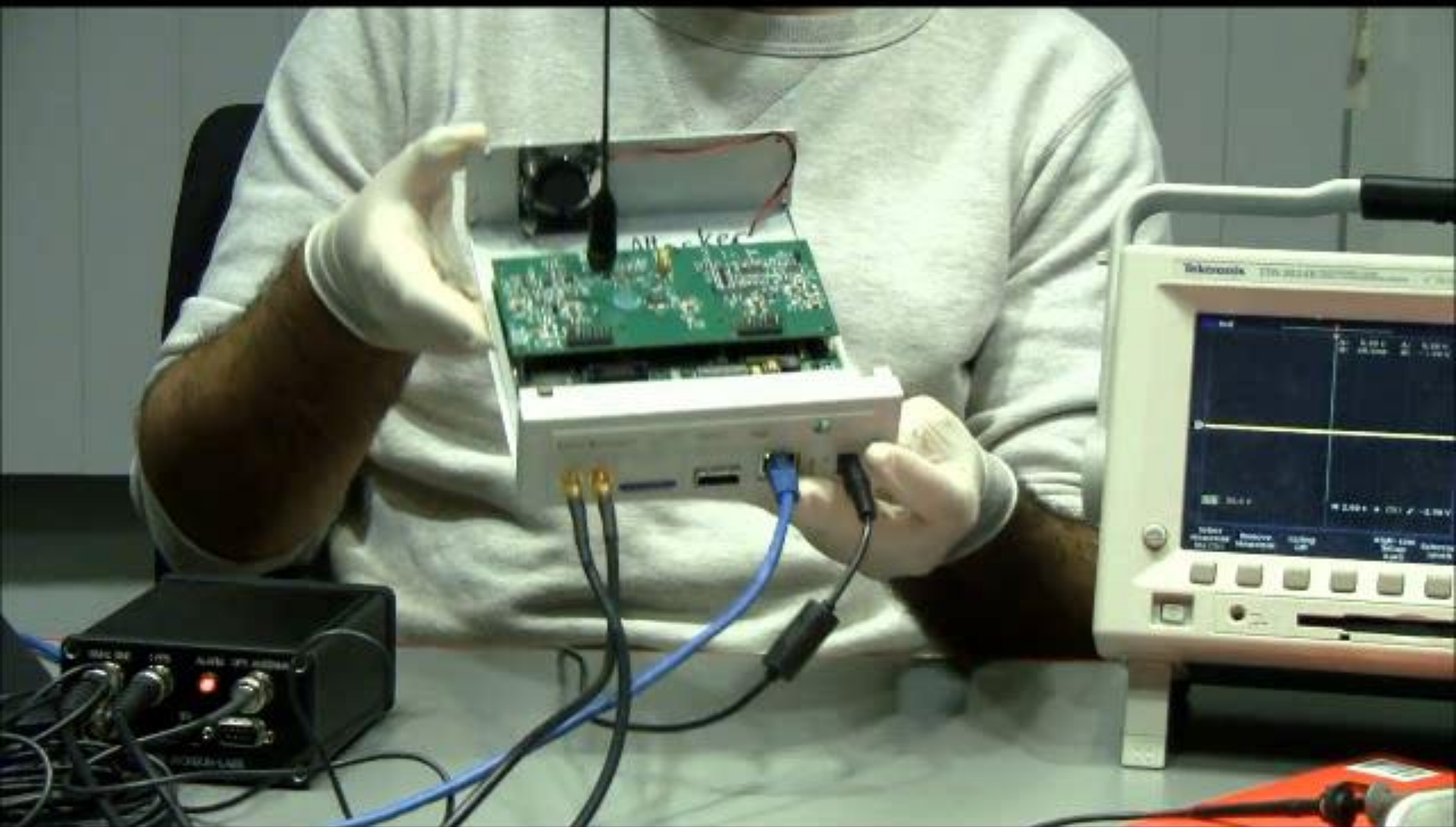


2) Active attack: Send unauthorized commands



Turn off therapies,
deliver electric shock





How Do We Protect Against Such Attacks?

Cryptography?

Problems with Adding Cryptography on Implants

- In emergencies, patient may be taken to a foreign hospital where doctors don't have the secret key
- Millions of patients already have implants with no crypto; would require surgery to replace

Ideally,

Ideally, secure implants **without modifying them**

Delegate security to an **external device**



- In emergencies, doctor turns external device off
- Helps people who already have implants

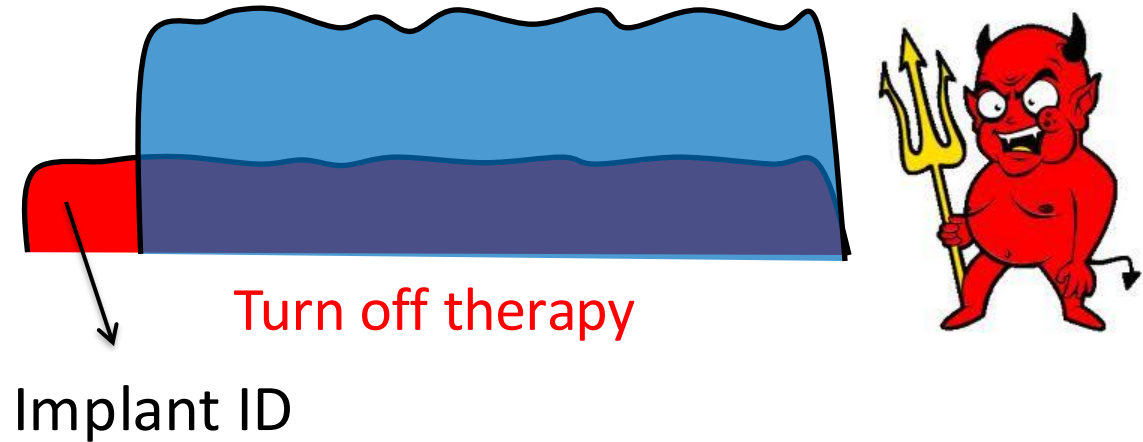
Solution Idea



Wireless Device

Shield Protects from Active Attacks

Shield Protects from Active Attacks



- Shield listens on medium
- Shield jams unauthorized commands

Implant protected from active attacks

But How to Protect from Passive Attacks?



Naïve Sol: Shield jams implant tx so attacker can't decode

How can we prevent eavesdropper from getting data while delivering data to doctor?

Analog one-time pad

Classic Approach: One-Time Pad

Encryption



Decryption

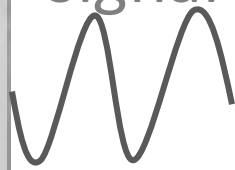


Only a node that has the key can decrypt

Protect from Passive Attacks: Analog One-Time Pad



Implant's
signal

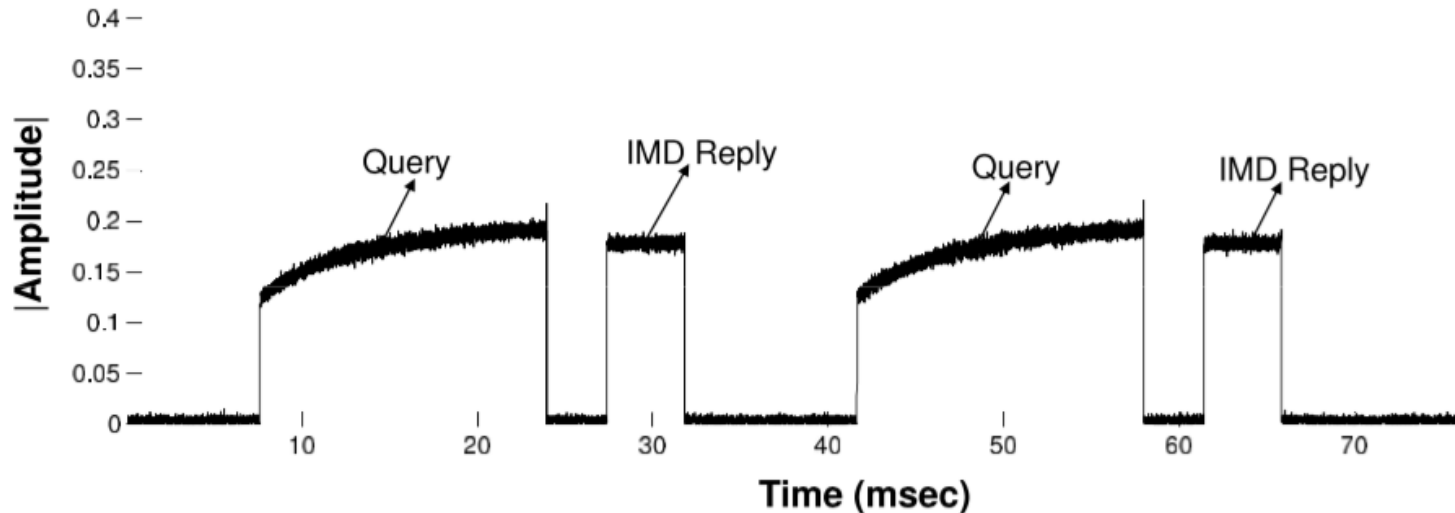


Random
Sum

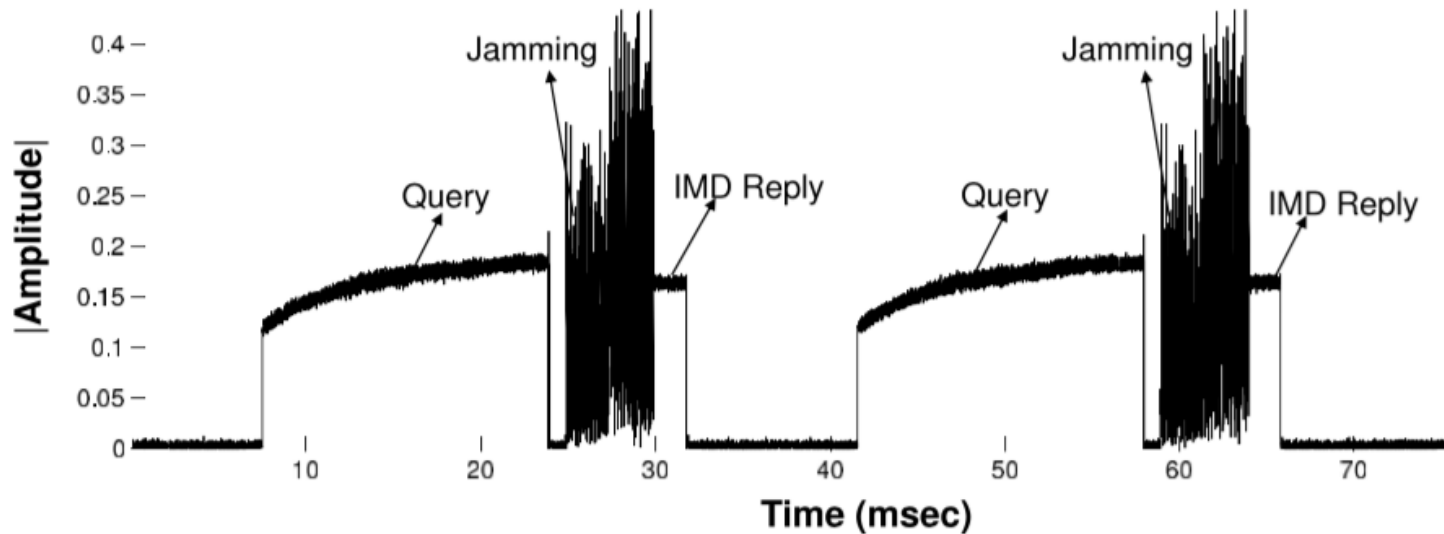


Jamming signal acts like the key in one-time pad

How Should the Jamming Signal Look like

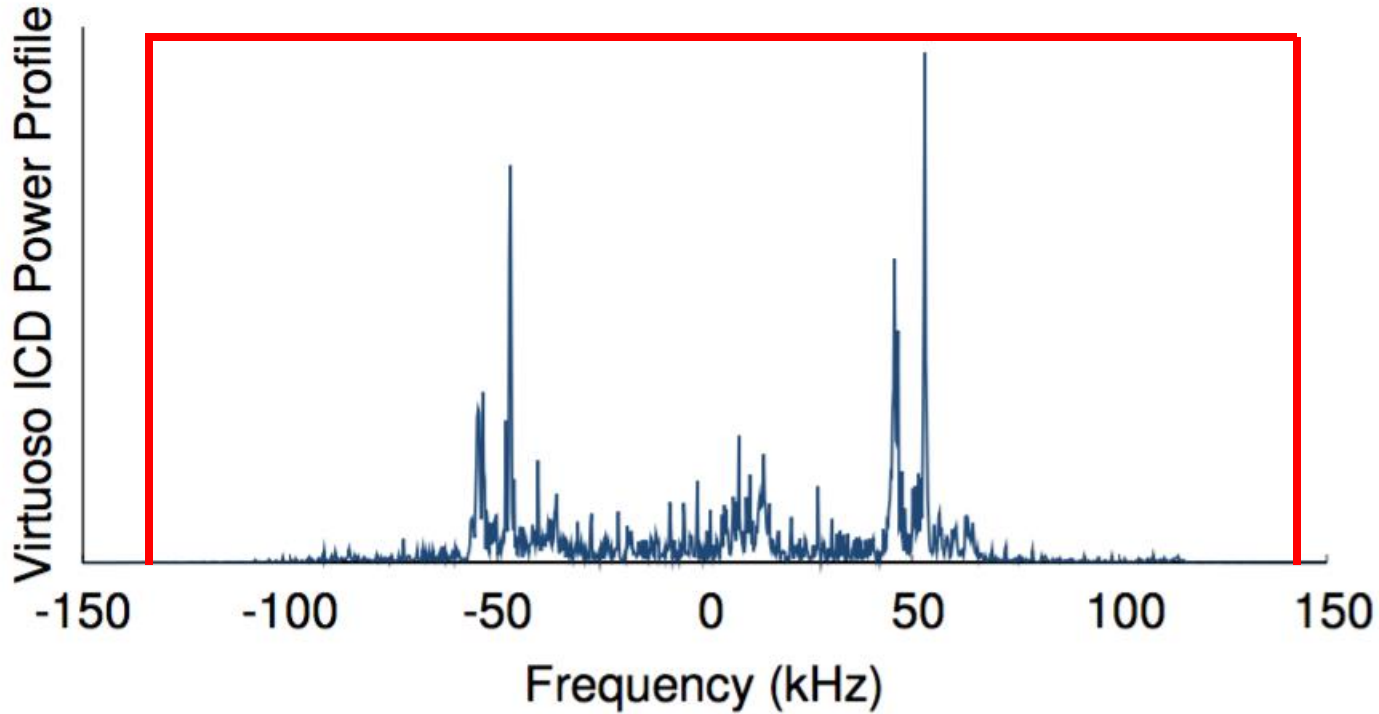


(a) Without jamming

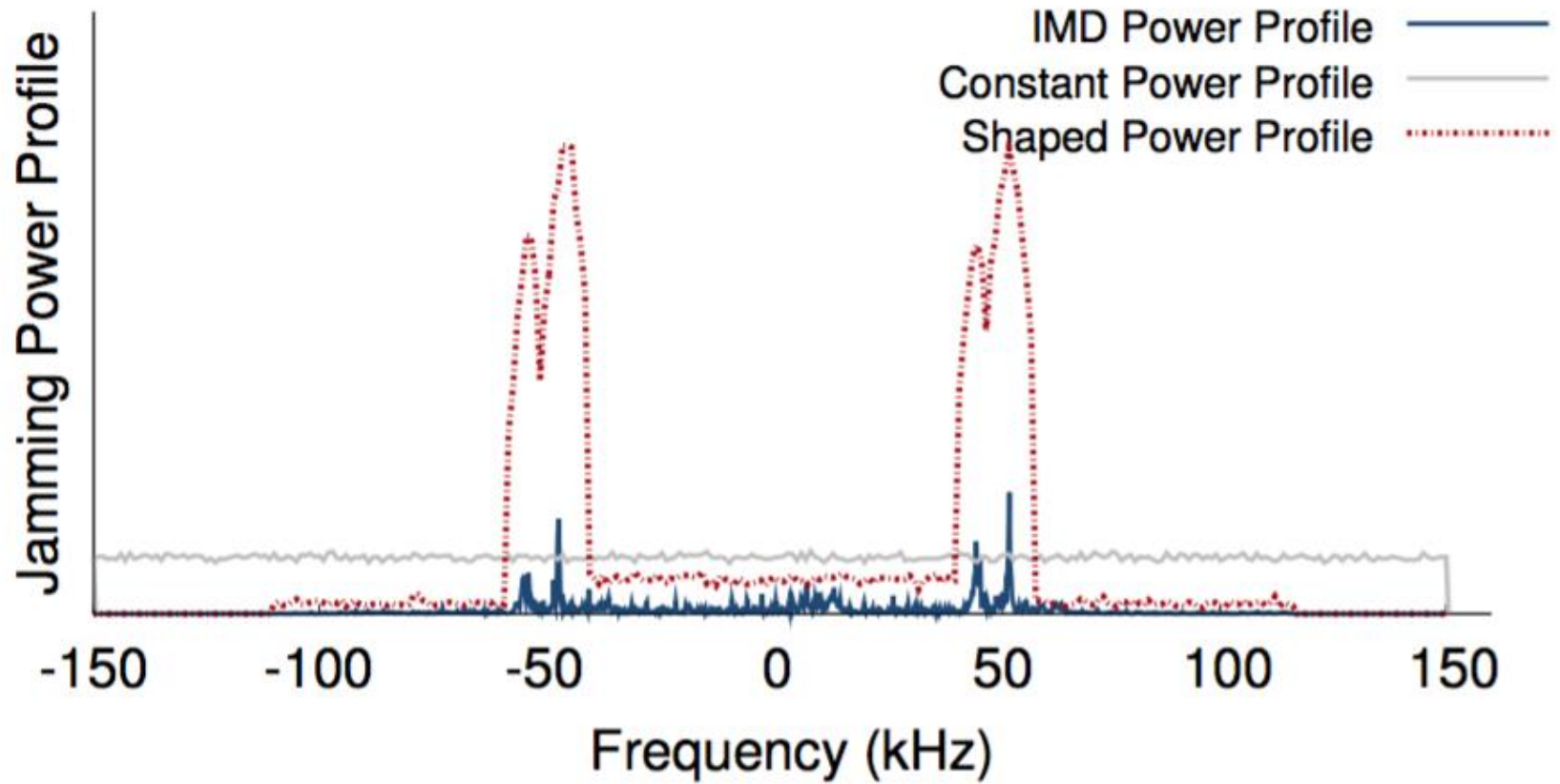


(b) With jamming

How could the Jamming Signal L_c look like

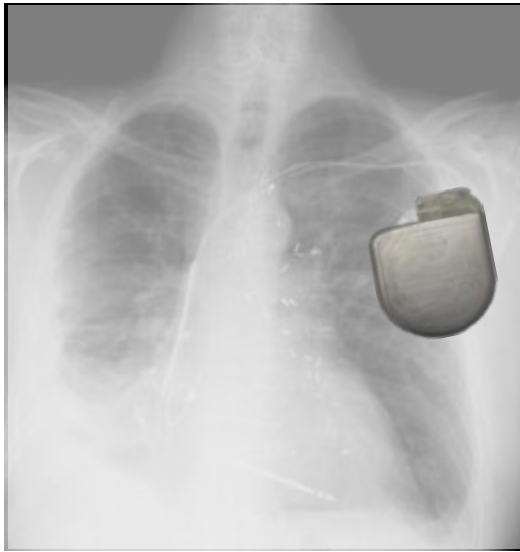


How Should the Jamming Signal Look like



Putting it together

Traditional System



Putting it together



Use encryption



Shield encrypts the implant data and forwards it to doctor

→ Shield acts as **proxy**

Shield simultaneously:

- Jams the implant's signal
- Decodes the implant's signal



Need radio that transmits and receives simultaneously, **i.e., a full-duplex radio**

RFIDs Are Used in Sensitive Applications



Access Control



Credit Cards



Passports



Pharmaceutical Drugs



Anti-Theft Car Immobilizers



Public Transportation

RFIDs Are Used in Sensitive Applications



Access Control

[SECRYPT'09, S&P'09
ESORICS'08, Usenix'08]



Credit Cards

[DefCon'13, ShmooCon'12,
DefCon'11, Usenix'05]



Passports

[DefCon'12, HackaDay'12,
BlackHat'06]



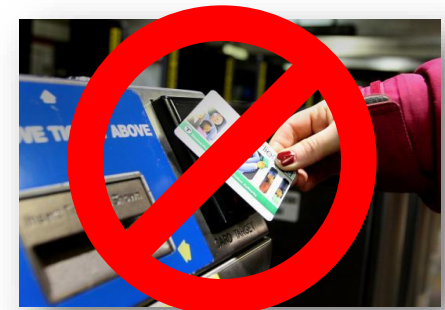
Pharmaceutical Drugs

[CCS'09, RFID'06]



Anti-Theft Car Immobilizers

[Usenix'12, Usenix'05]



Public Transportation

[Defcon'08, MIT'08,
S&P'09]

Hacking RFIDs for Dummies



www.nicolascourtois.com

www.nicolascourtois.com/MifareClassicHack.pdf

Mifare Classic Tool - MCT

https://play.google.com/store/apps/details?id=de.sysst.MifareClassicTool&hl=en

Wirelessly Hack unlock car without key-fob/

Live RFID Hacking System

www.openpcd.org/Live_RFID_Hacking_System

OpenPCD

Navigation Search Toolbox In other languages Views

Page Discussion View source History

Live RFID Hacking System

Bootable RFID Live Hacking System

The bootable Live RFID Hacking System contains a ready-to-use set of hacking tools for breaking and analyzing MIFARE Classic RFID cards and other well known card formats. It is built around PCSC-like, the CCID free software driver and librfic that gives you access to some of the most common RFID readers. See our tutorial video for a quick introduction on how to break MIFARE Classic RFID card keys using our Live RFID Hacking System.

This RFID Live Hacking System is superseded by our OpenPCD 2 reader with librfic support - you can download the latest ISO image here. This page is only kept for historical reasons.

The MF0C/MF0UK tools of the Live system won't work inside virtualization software like VMware as virtualization seems to break the timing requirements of the MIFARE Classic attack tools - please boot from the CD/DVD instead.

Our RFID hardware projects for RFID Security Analysis

OpenPCD 2 RFID Reader for 13.56MHz
OpenPCD RFID Emulator Project
OpenPCD Sniffer/Only 13.56MHz

Suggested RFID Reader for MIFARE Classic key recovery for this live system

Please use the ACR122U102 Tikitag RFID reader for MIFARE key extraction (v1.02) - later versions or compatible models could work, but some later firmware revisions (ACR122U207) seem to be crash while breaking MIFARE Classic with mf0c/mf0c. For normal use and known keys the other compatible readers should be fine though. Please send me a note if you successfully used another reader for key extraction using our Live CD. The Firmware version is shown when using mf0c.

Note for touchatag reader users

If the pcsc daemon balls out on a touchatag reader with:

```
00000012 ccid_usb.c:1981:ccid_check_firmware() Firmware (1.00) is bogus! Upgrade the reader firmware or get a new reader.
00000039 ifdHandler.c:1101:IFDCreateChannelByName() failed
00000025 ReaderFactory.c:398:RFInitialiseReader() Open Port 200000 failed
```

Just edit /usr/local/openpcd/lib/pcsc/drivers/Hd-ccid.bundle/Contents/info.plist - ifdDriverOptions and set key from 0x0000 to 0x0005 to disable version checking.

Checksums

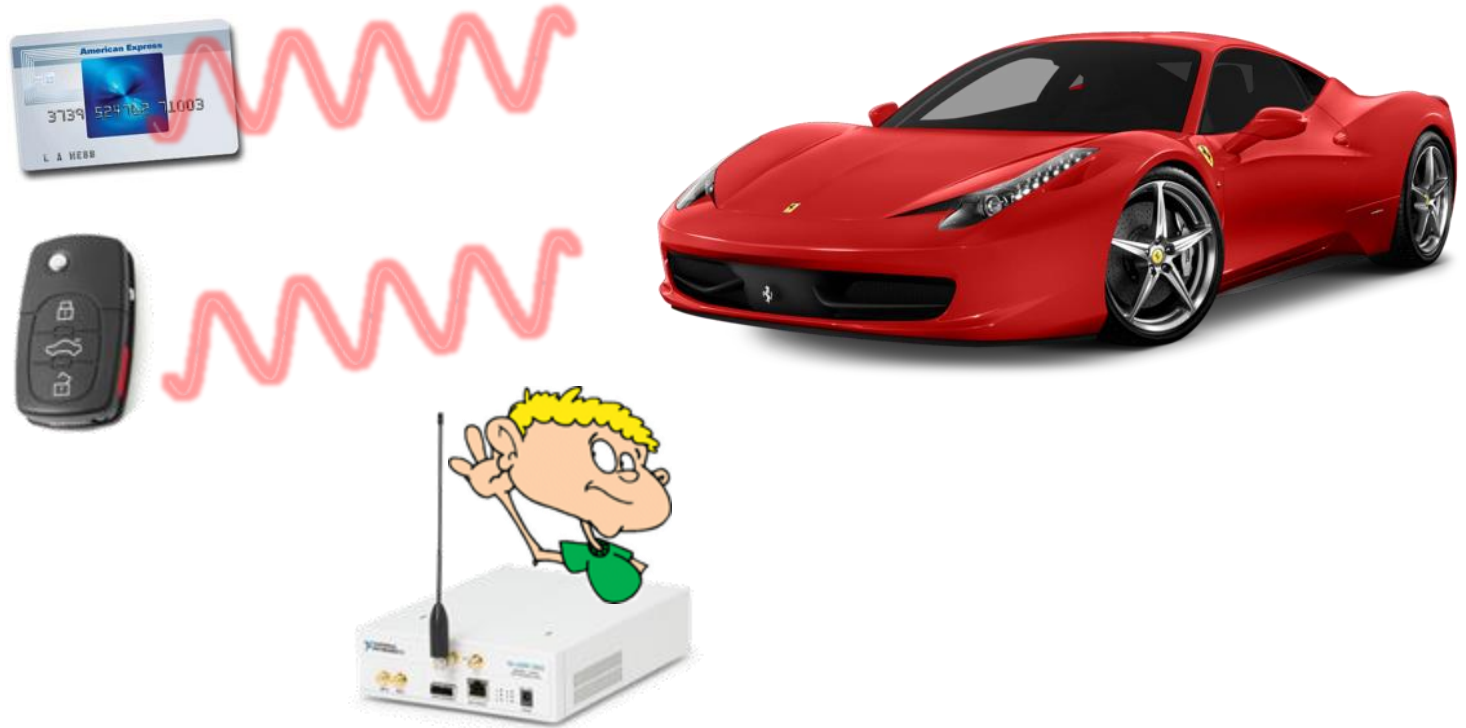
```
Fedora-15-x86_64-Live-RFID-v02.iso
SHA256: 793738eef8acc0cf348dd9a456356b7f22d07c066530bdf2968fce4654dbd2daa
MD5: c88f5c1f1c0a12c0b39f0c9e979750e
SHA1: d8549889590c38a7688e37e186689897f51ae2
```

Tools Installed

The most important tools are highlighted. The Fedora 15 based Live Desktop system runs GNOME 3 Desktop - just move your mouse cursor in the upper left corner to get a list of installed applications.

General Purpose Tools

Hacking RFIDs Simply By Eavesdropping



RFIDs adopt weak encryption protocols

Hacking RFIDs Simply By Eavesdropping

RFIDs adopt weak encryption protocols



Goal of RFID Industry: Dramatically reduce the power, size, and cost of RFIDs

Protect your RFID cards against active attacks

The screenshot shows an Amazon product page for a Flipside Wallets Men's RFID Blocking Flipside 3X Wallet. The browser address bar shows the URL: www.amazon.com/Flipside-Wallets-Blocking-Wallet-Stealth/dp/B00NLMZ2. The page features the Amazon Prime logo, a search bar with the text "rfid blocking wallet", and navigation links for "Shop by Department", "Haitham's Amazon.com", "Today's Deals", "Gift Cards", "Sell", and "Hello, Haitham Your Account". The product is displayed with a large image of the wallet open, showing a Visa card and cash. A vertical strip of smaller images is on the left. The product title is "Flipside Wallets Men's RFID Blocking Flipside 3X Wallet" with a 4.5-star rating and 117 customer reviews. The price is \$39.95 with Prime and free returns. The color is "Stealth". There are four color options shown: black, dark grey, red, and white. The product is "In Stock" and is sold by Flipside Wallets and fulfilled by Amazon. The page also includes a "Want it tomorrow" message with a 20-hour 41-minute deadline for same-day delivery.

Flipside Wallets Men's RFID Blocking Flipside 3X Wallet

★★★★☆ 117 customer reviews

Price: \$39.95 Prime & Free Returns. Details

Size: One Size Size Chart

Color: Stealth

\$39.95 Prime

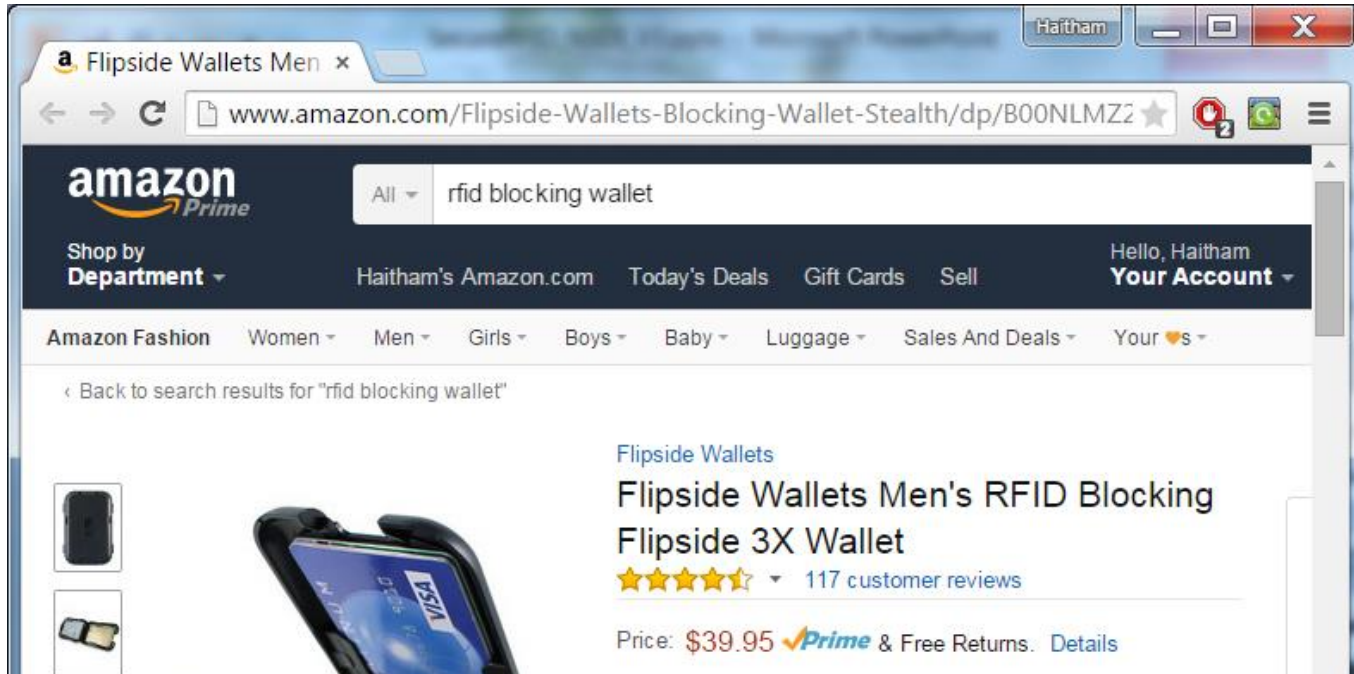
\$39.95 Prime

In Stock.

Sold by Flipside Wallets and Fulfilled by Amazon. Gift-wrap available.

Want it tomorrow, May 3 to 02139? Order within 20 hrs 41 mins and choose Same-Day Delivery at checkout.

Protect your RFID cards against active attacks

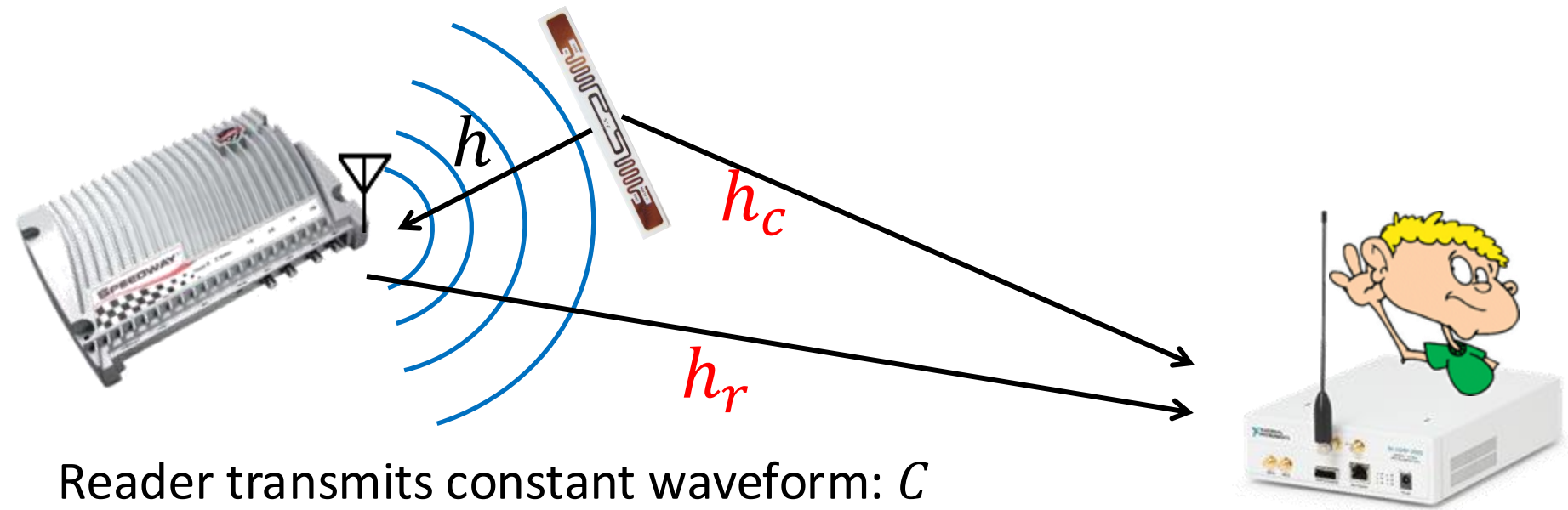


Most attacks demonstrated by eavesdropping



Need solution for eavesdropping that works with existing RFIDs

RFID Communication



Reader transmits constant waveform: C

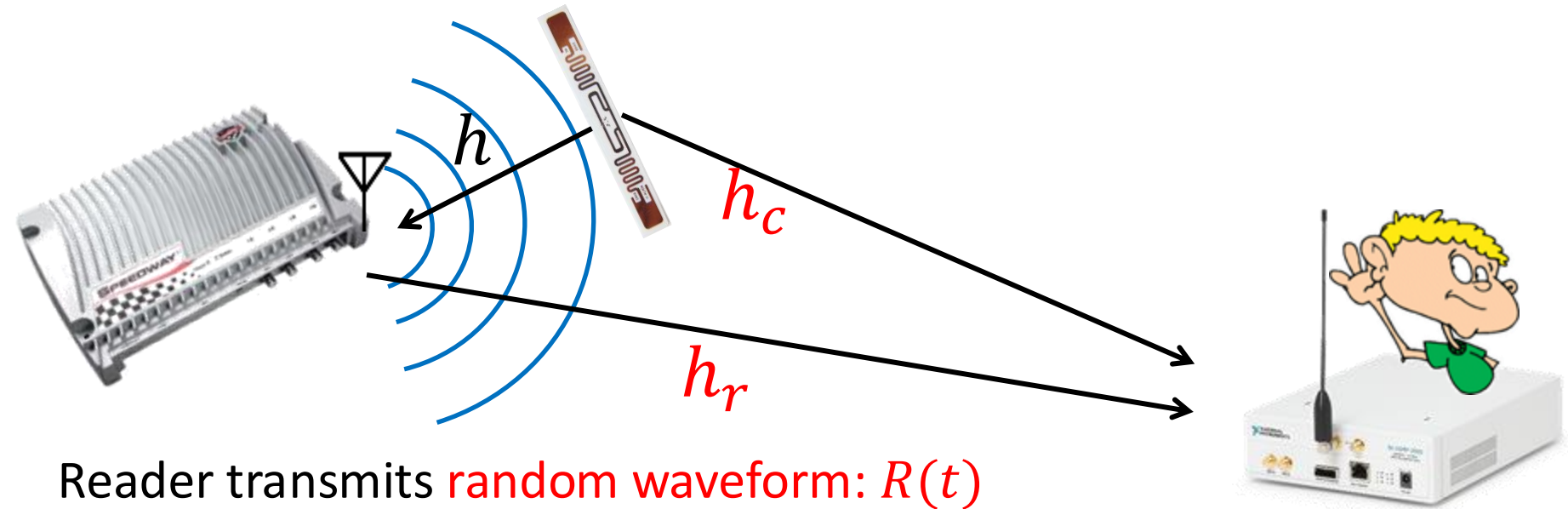
RFID reflects the reader's signal using ON-OFF switch

Reader receives (full-duplex) : $h \times C \times bits$

Eavesdropper receives: $h_r \times C + h_c \times C \times bits$

Replace constant waveform C with a random waveform $R(t)$

RF-Cloak Solution



Reader transmits **random waveform: $R(t)$**

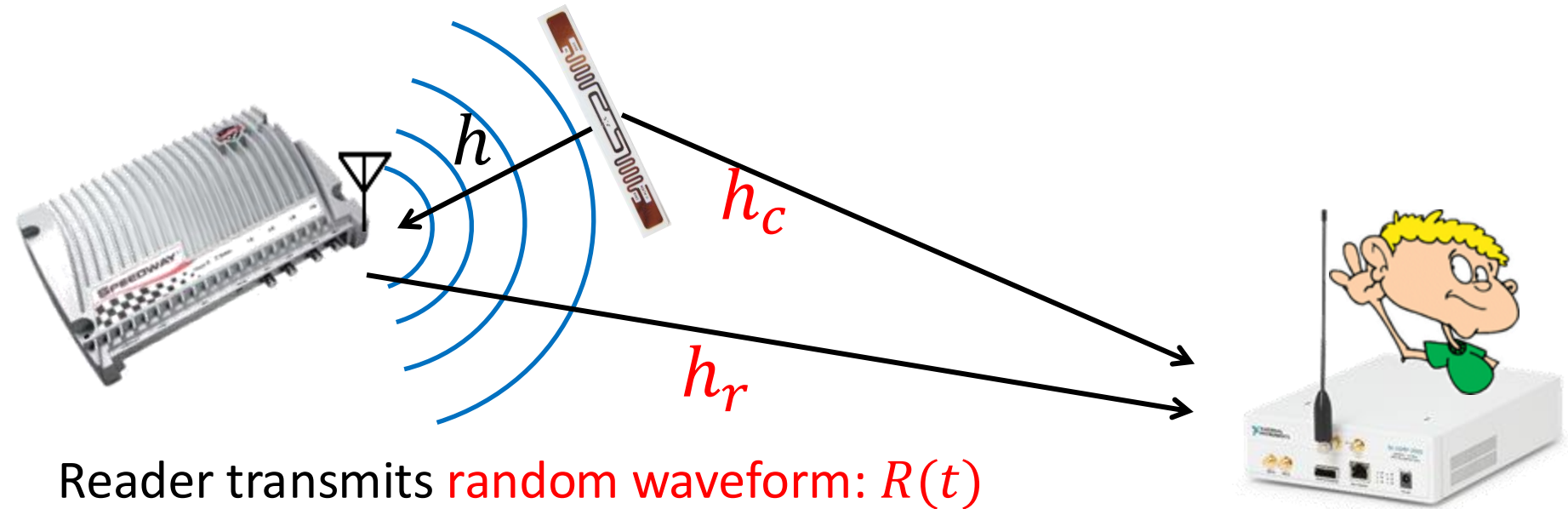
RFID reflects the reader's signal using ON-OFF switch

Reader receives (full-duplex): $h \times R(t) \times bits$

Eavesdropper receives: $h_r \times R(t) + h_c \times R(t) \times bits$

Replace constant waveform C with a random waveform $R(t)$

RF-Cloak Solution



Reader transmits **random waveform: $R(t)$**

RFID reflects the reader's signal using ON-OFF switch

Reader receives (full-duplex): **$h \times R(t) \times bits$**

Eavesdropper receives: **$h_r \times R(t) + h_c \times R(t) \times bits$**

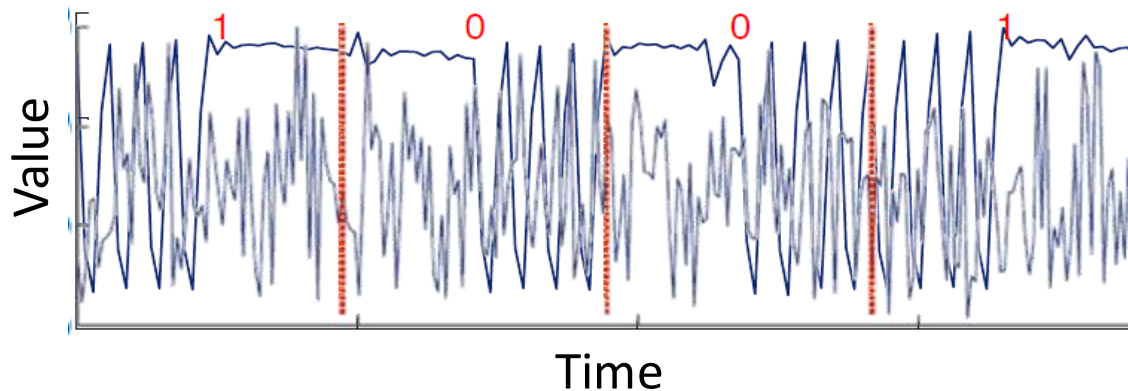
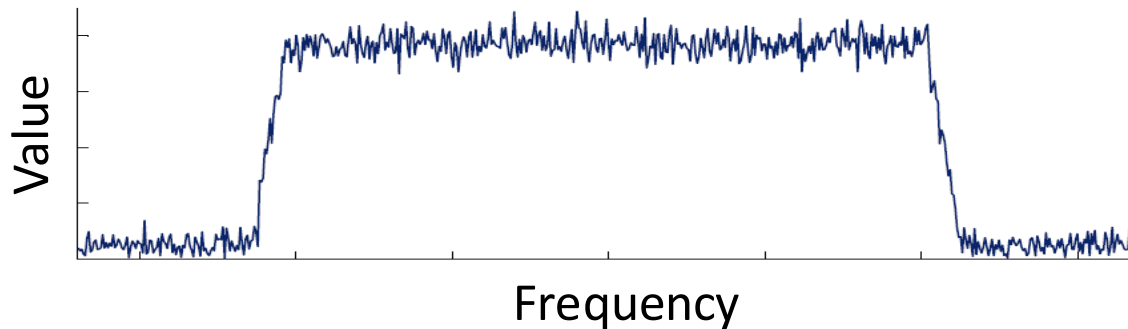
Reader knows $R(t) \rightarrow$ Can decode

Eavesdropper doesn't know $R(t) \rightarrow$ Cannot decode

RF-Cloak: Randomizing the Reader's Signal

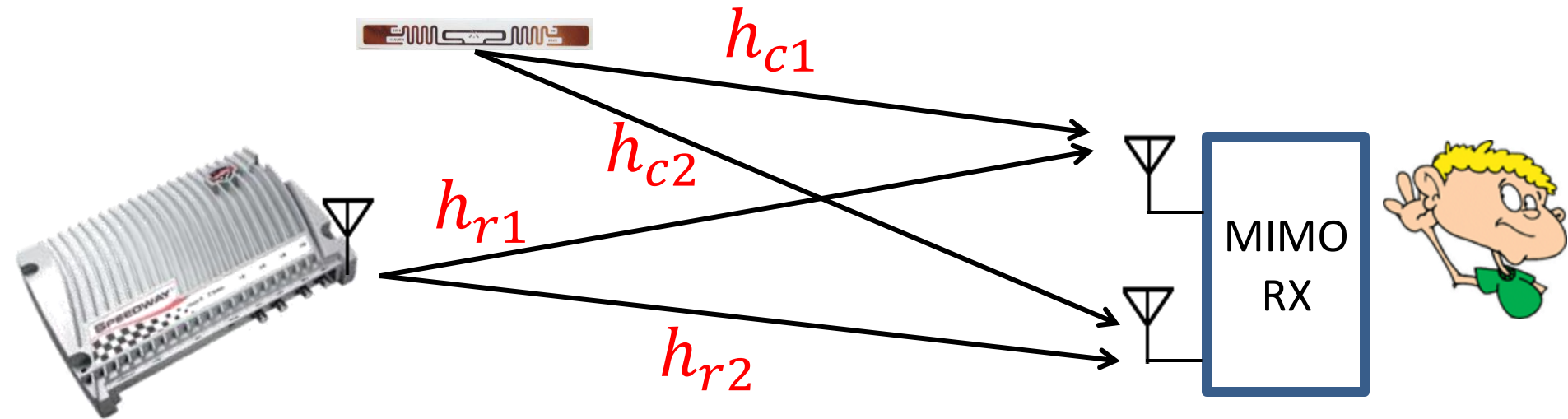
Random waveform:

- Must change as fast as any transition in the RFID signal
 - has same bandwidth as RFID signal
- Must be indistinguishable from white noise i.e. flat frequency profile
 - samples taken from complex Gaussians



What if the attacker has multi-antenna
MIMO capability?

MIMO Eavesdropper



Reader transmits random waveform: $R(t)$

Eavesdropper receives:

$$1^{\text{st}} \text{ receiver: } Y_1(t) = h_{r1} \times R(t) + h_{c1} \times R(t) \times \text{bits}$$

$$2^{\text{nd}} \text{ receiver: } Y_2(t) = h_{r2} \times R(t) + h_{c2} \times R(t) \times \text{bits}$$

$$\frac{Y_1(t)}{Y_2(t)} = \frac{h_{r1} + h_{c1} \times \text{bits}}{h_{r2} + h_{c2} \times \text{bits}}$$

MIMO Eavesdropper

MIMO Eavesdropper can eliminate the random waveform and decode the RFID bits.

Reader transmits random waveform: $R(t)$

Eavesdropper receives:

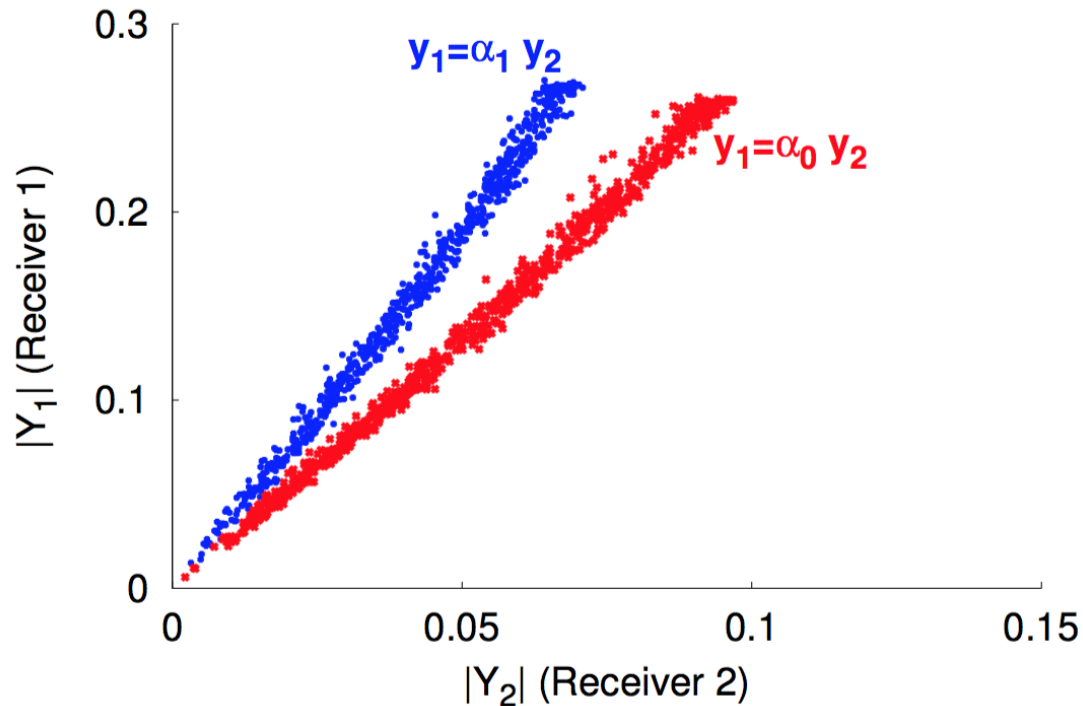
$$1^{\text{st}} \text{ receiver: } Y_1(t) = h_{r1} \times \cancel{R(t)} + h_{c1} \times \cancel{R(t)} \times \text{bits}$$

$$2^{\text{nd}} \text{ receiver: } Y_2(t) = h_{r2} \times \cancel{R(t)} + h_{c2} \times \cancel{R(t)} \times \text{bits}$$

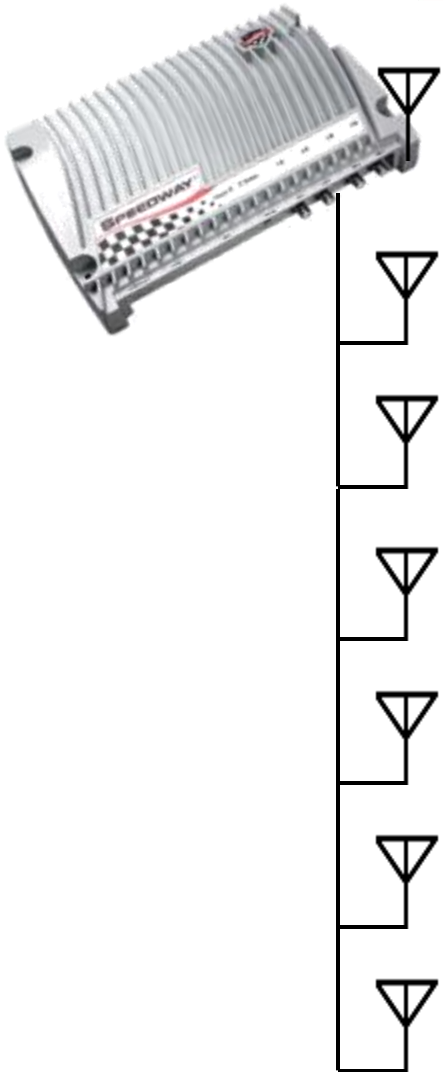
$$\frac{Y_1(t)}{Y_2(t)} = \frac{h_{r1} + h_{c1} \times \text{bits}}{h_{r2} + h_{c2} \times \text{bits}}$$

MIMO Eavesdropper

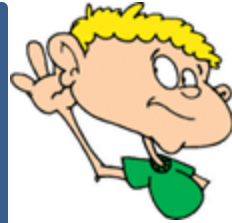
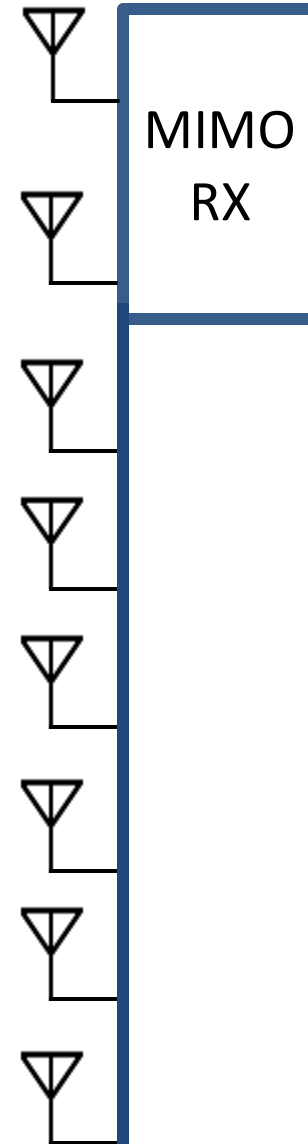
$$\left\{ \begin{array}{l} \frac{h_{r1} + h_{c1}}{h_{r2} + h_{c2}} \text{ if bit} = 1 \\ \frac{h_{r1}}{h_{r2}} \text{ if bit} = 0 \end{array} \right.$$



RF-Cloak vs MIMO Eavesdropper



Antenna War!

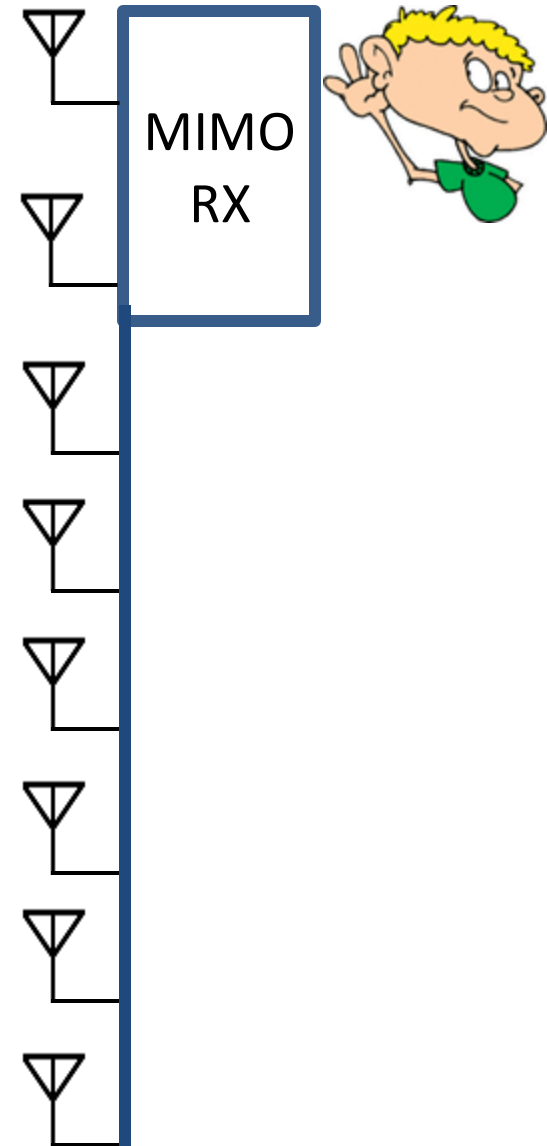


RF-Cloak vs MIMO Eavesdropper

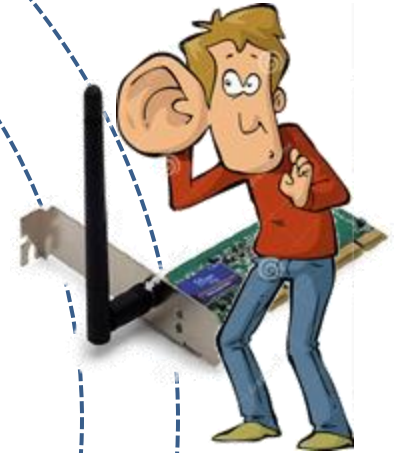


RF-Cloak combines antenna motion and rapid antenna switching

→ Emulate a very large number of fast changing antennas



Eavesdropping is a longstanding problem!



No way to regulate or know who is listening on the wireless channel!

Defense Against Eavesdropping: Encryption

Encryption breaks due to security loopholes.

Low power devices employ weak or no encryption.

Vulnerability in WPA2
[SIGSAC'17]



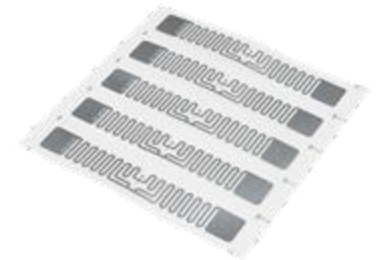
Side Channel Attacks

[CRYPTO'14, CHES'15, CCS'16, RSA'16, MobiCom'15]



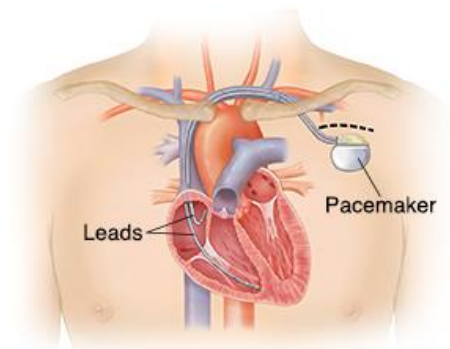
Ultra-Low Power RFIDs

[S&P'09, CCS;09, Usenix'12, Defcon'13, NSDI'15]



Medical Implants

[S&P'10, SIGCOMM'11]



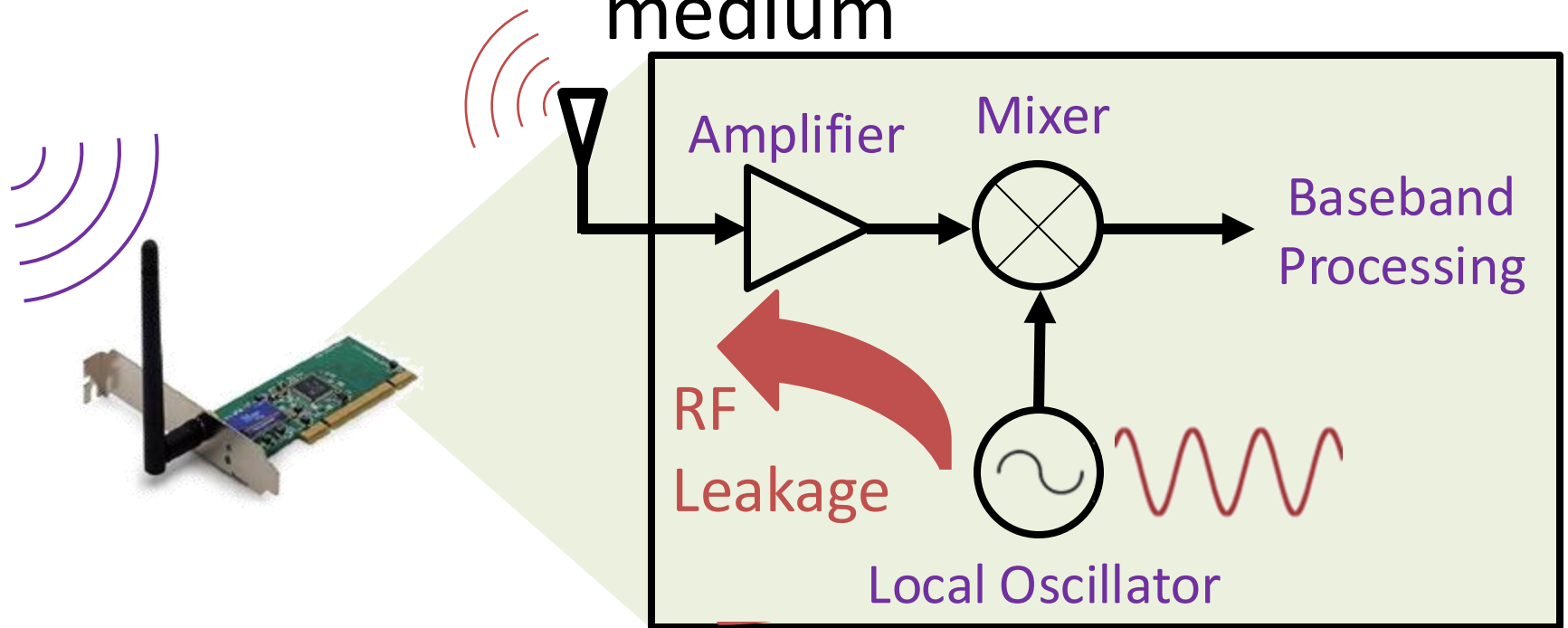
Can we detect the hidden presence of
wireless eavesdroppers?

Ghostbuster



- A system that can reliably detect an eavesdropper in the presence of ongoing transmissions.
- Does not require any modifications to current transmitters and receivers.
- Implemented and empirically tested against SDR & WiFi cards based eavesdroppers.

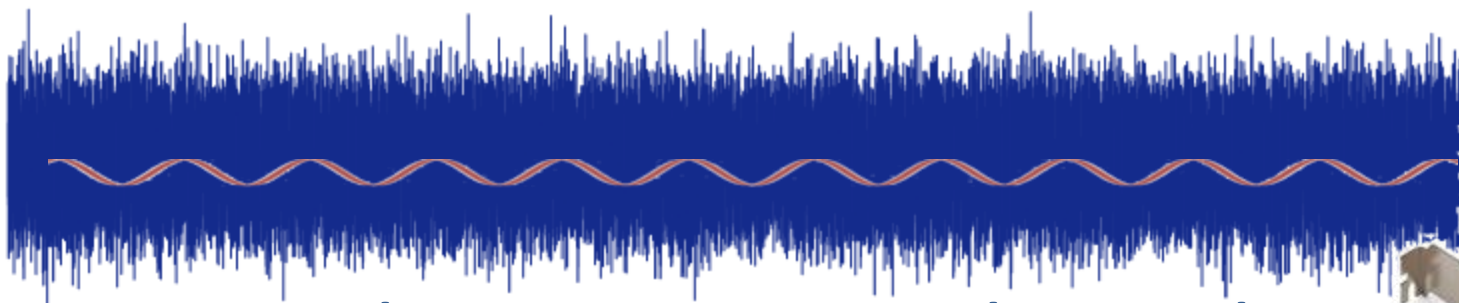
Key Observation: Even passive receivers leakage RF signals on to the wireless medium



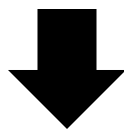
Eavesdropper's Digital Receiver

Receiver's oscillator creates a sinusoid signal at the carrier frequency of operation





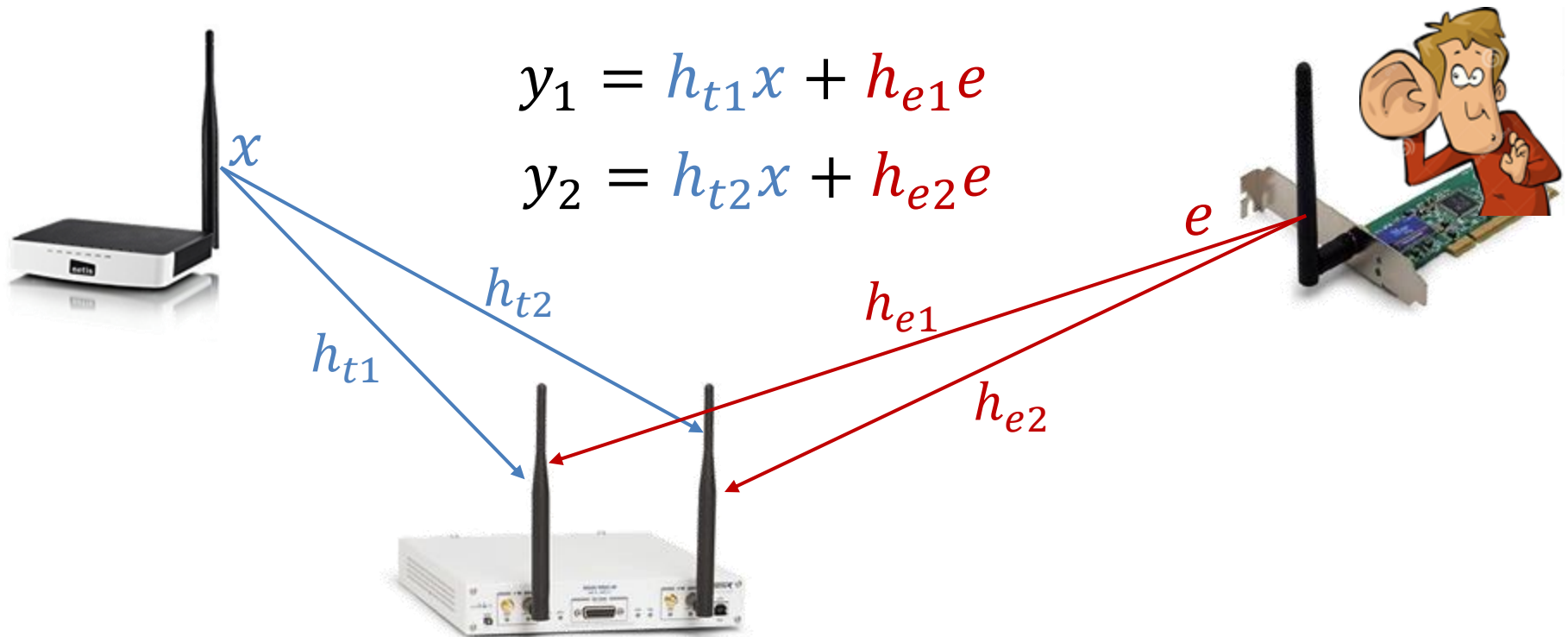
RF Leakage is extremely weak:
buried under noise floor



Hard to detect with today's receivers

Ghostbuster

Null On Going Transmissions using MIMO



$$y_1 = h_{t1}x + h_{e1}e$$

$$y_2 = h_{t2}x + h_{e2}e$$

$$y_1 - \frac{h_{t1}}{h_{t2}} y_2 = \left(h_{e1} - \frac{h_{t1}}{h_{t2}} h_{e2} \right) e$$

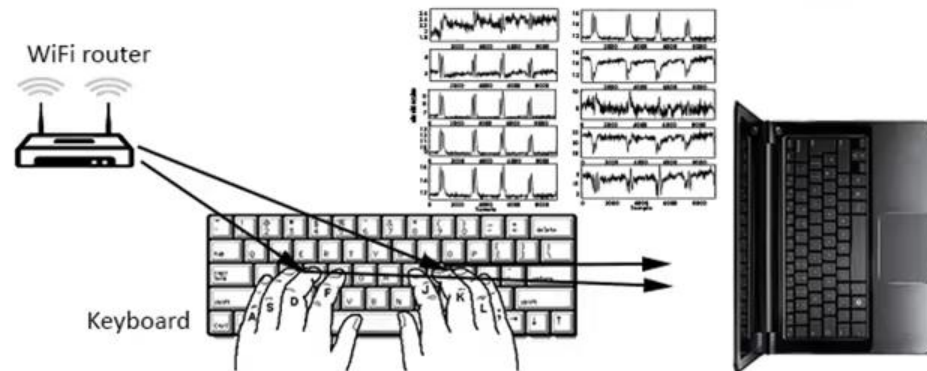
In the presence of ongoing transmissions & other receivers.

Estimated Number of Receivers

	0	1	2	3	4	≥ 5
0	97.97%	0.68%	0.68%	0%	0.68%	0
1	2.16%	96.55%	1.01%	0.29%	0	0
2	0	2.8%	95.43%	1.47%	0.15%	0.15%
3	0	0.29%	3.74%	91.81%	3.16%	1.01%
4	0	0	0.29%	7.61%	89.94%	2.16%

Actual Number of Receivers

Wi-Key



Acoustic Eavesdropping through Wireless Vibrometry

Teng Wei[†], Shu Wang[†], Anfu Zhou^{†}, Xinyu Zhang[†]*

*[†]Department of Electrical and Computer Engineering
University of Wisconsin - Madison*

^{}Institute of Computing Technology
Chinese Academy of Sciences*

MOBICOM 2015