

# ECE 598HH: Advanced Wireless Networks and Sensing Systems

Lecture 16: Security  
Haitham Hassanieh

# WIRELESS IMPLANTABLE MEDICAL DEVICES

Deep Brain  
Neurostimulators



Cochlear Implants



Gastric  
Stimulators



Cardiac Defibrillators/  
Pacemakers



Foot Drop  
Implants

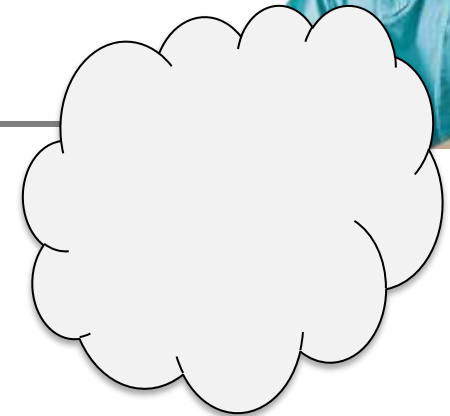


Insulin Pumps



# 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

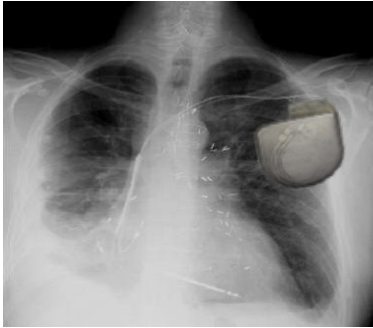
*[Journal of the American College of Cardiology, 2011]*

What about security?



# Security Attacks

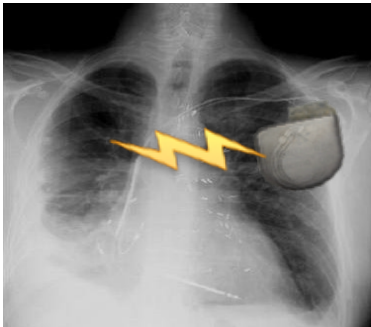
## 1) Passive attack: Eavesdrop on private data



Patient diagnosis,  
vital signs

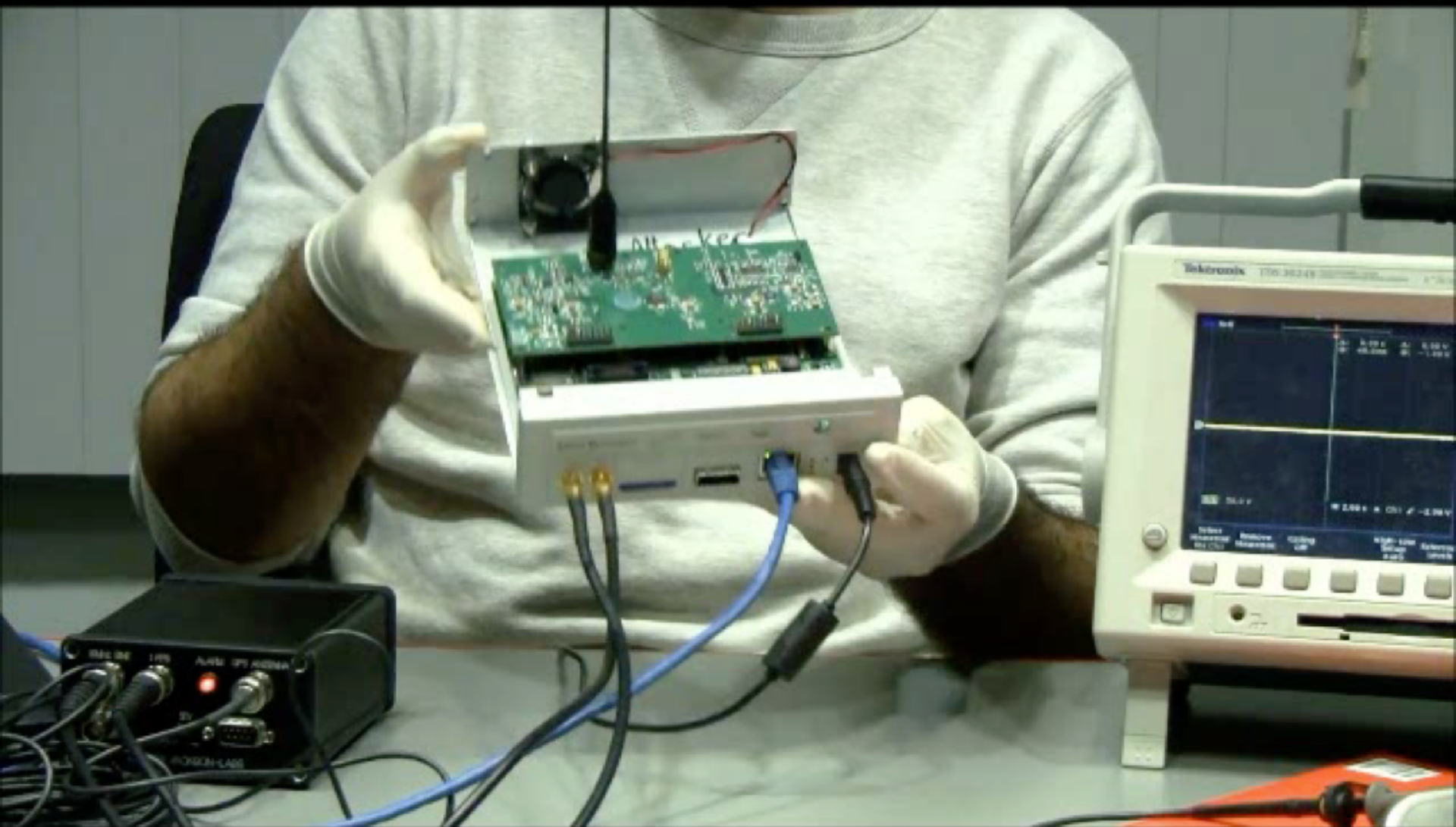


## 2) Active attack: Send unauthorized commands



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

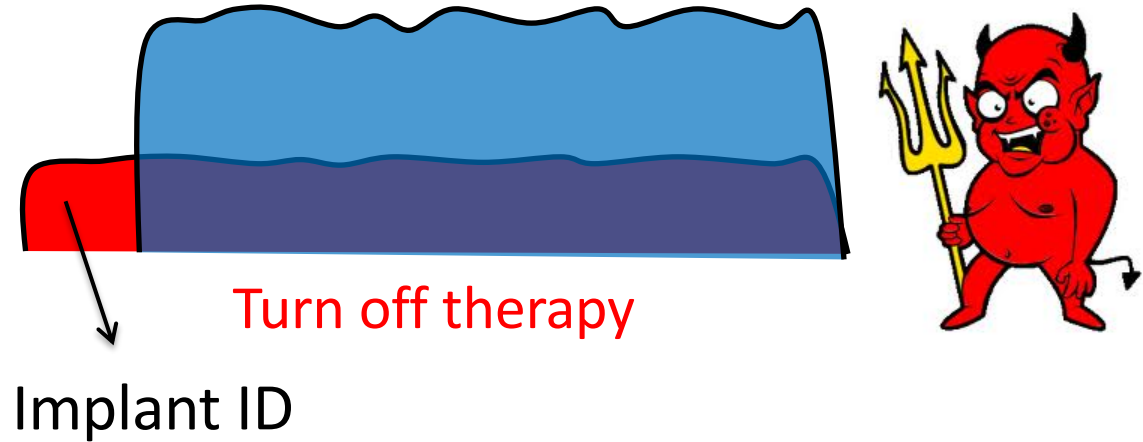


Wireless Device

# 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

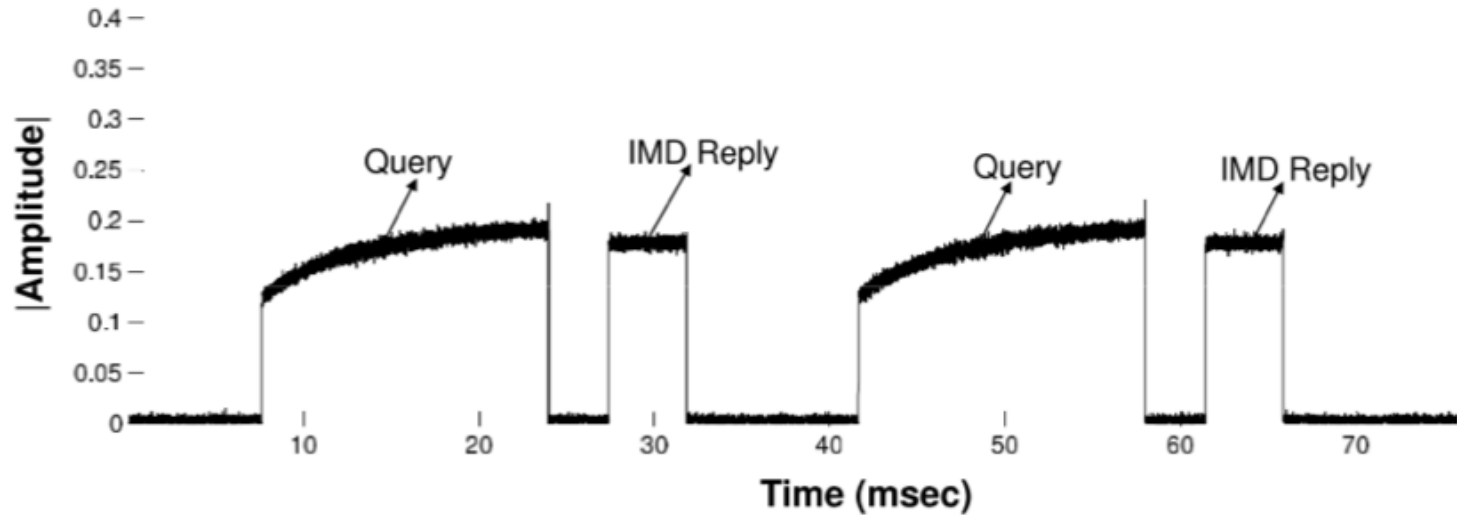


Random  
Sum

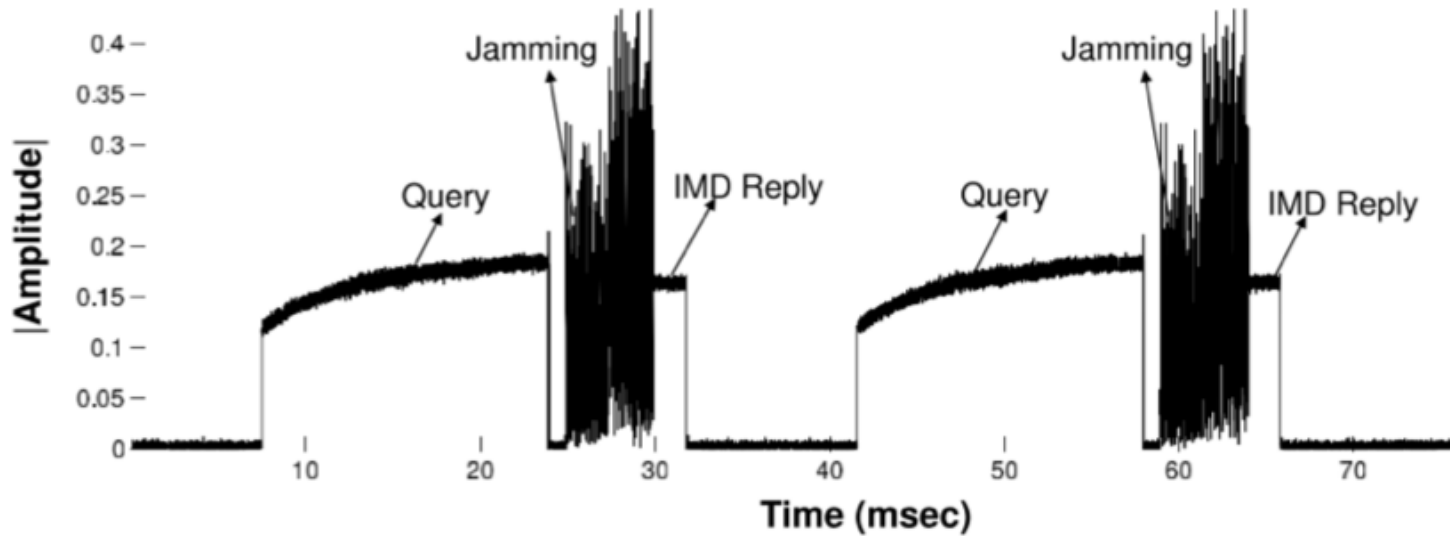


Jamming signal acts like the key in one-time pad

# How Should the Jamming Signal Look like

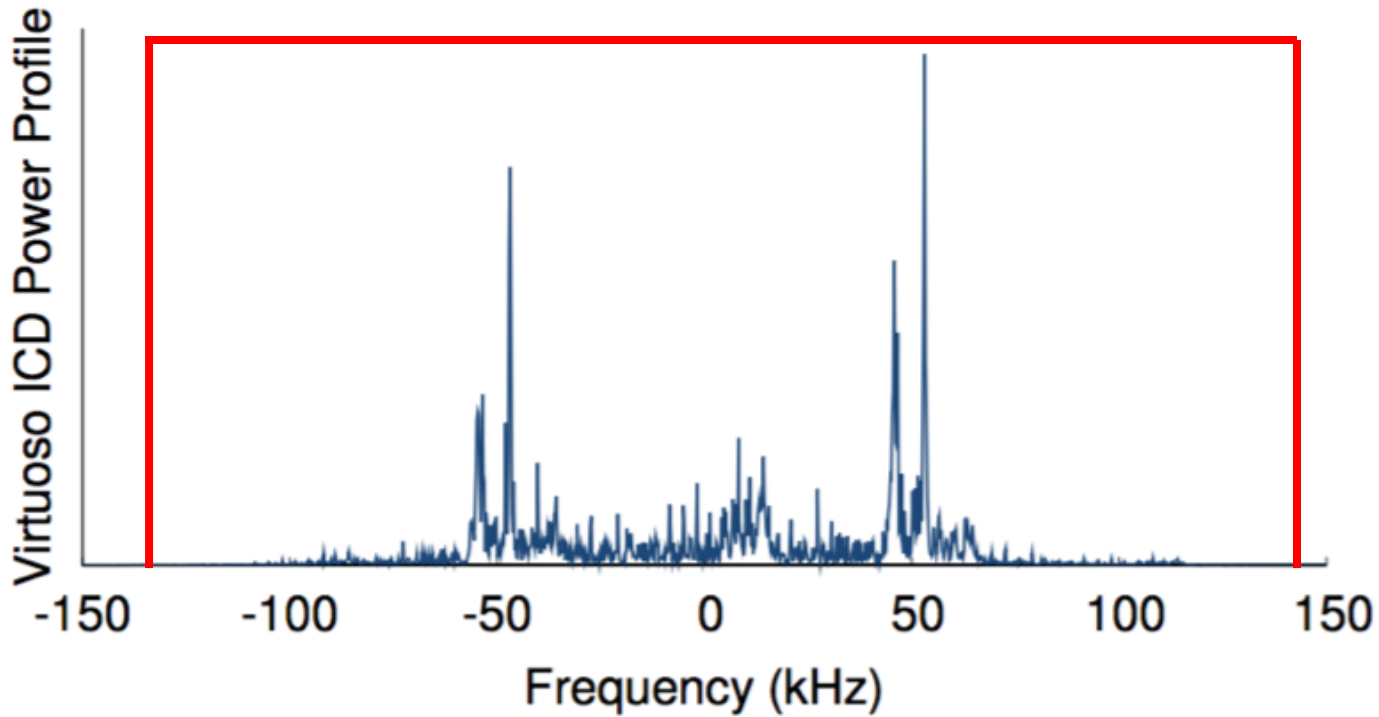


(a) Without jamming

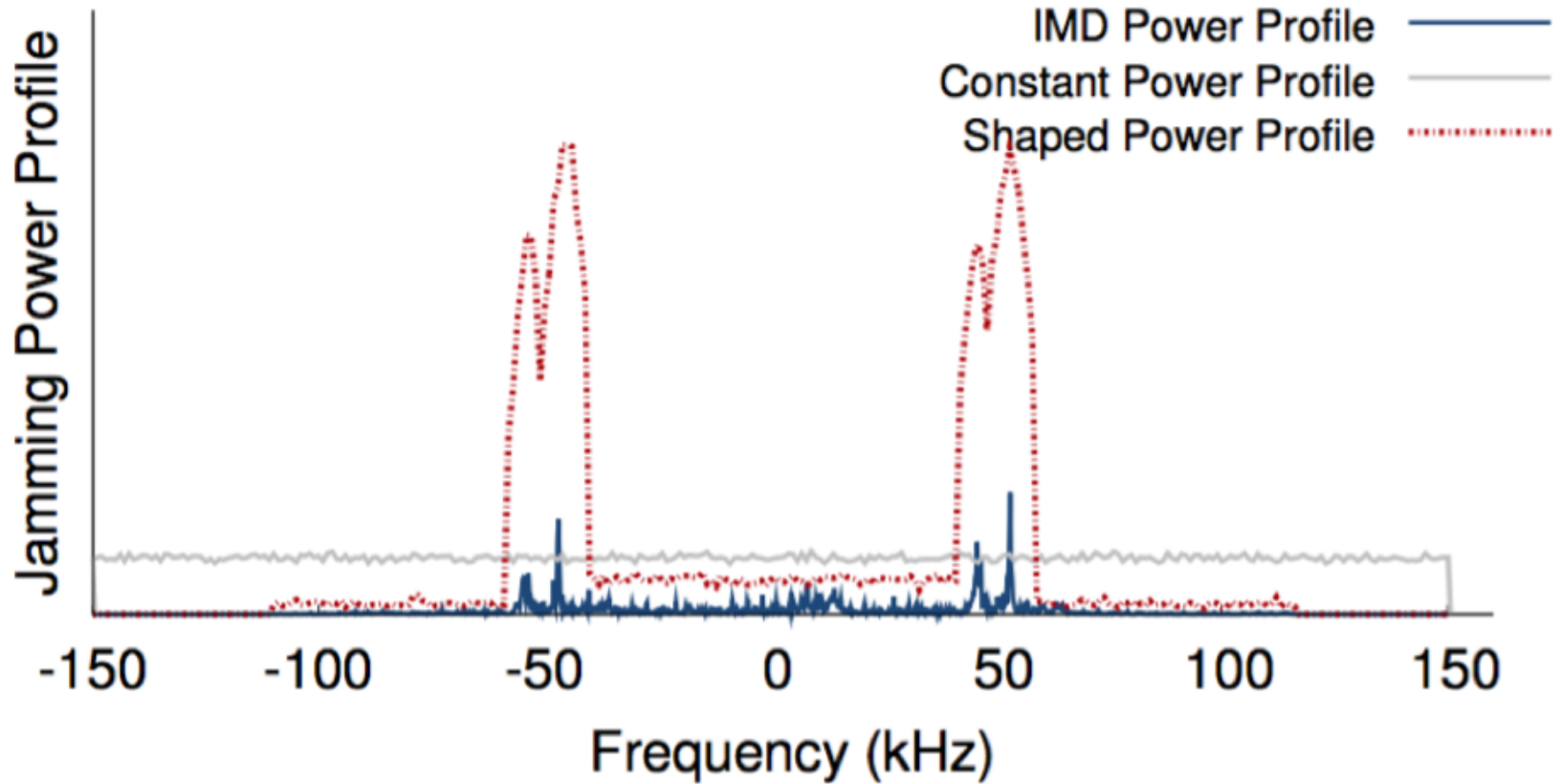


(b) With jamming

# How could the Jamming Signal $L_c$ look like



# How Should the Jamming Signal Look like



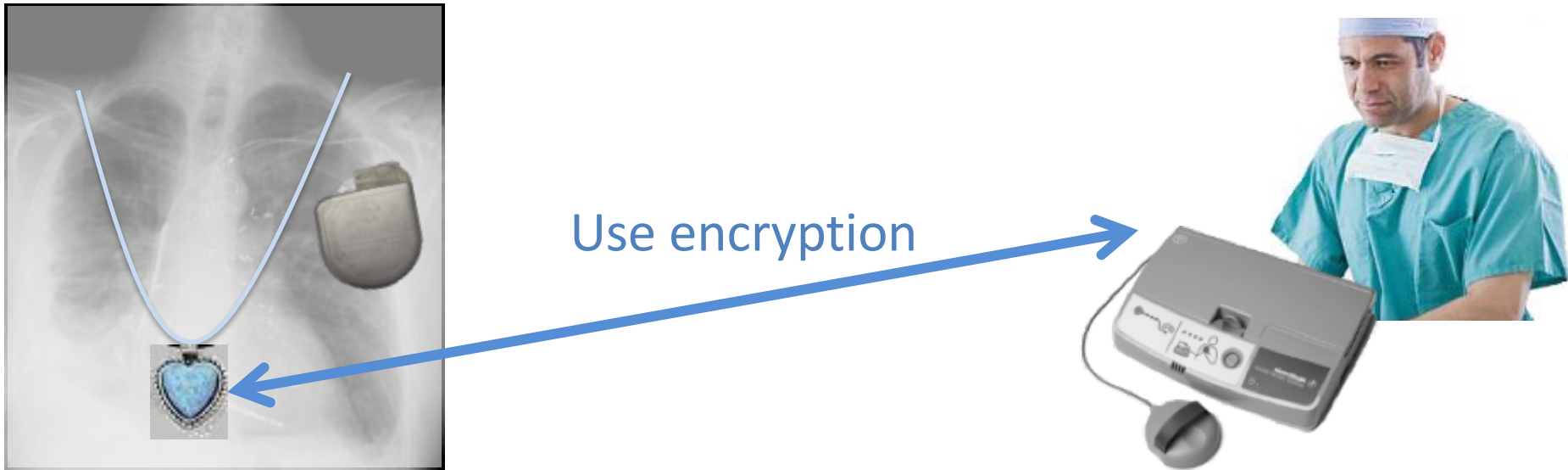
# Putting it together

## Traditional System





# Putting it together



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**

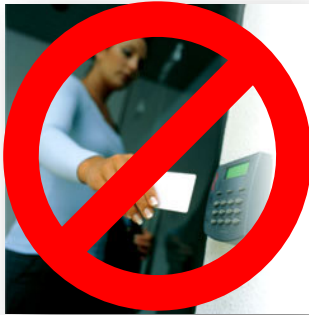


**Anti-Theft Car Immobilizers**



**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



**Live RFID Hacking System**

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-lite, 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 SnifferOnly 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 mf0uk/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 bails 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:181:IFDCreateChannelByName() failed
00000015 readerfactory.c:398:RFInitialiseReader() Open Port 200000 failed
```

just edit `/usr/local/openpcd/lib/pcsc/drivers/ff-ccid_bundle/Contents/info.plist - #DriverOptions` and set key from 0x0000 to 0x0005 to disable version checking.

#### Checksums

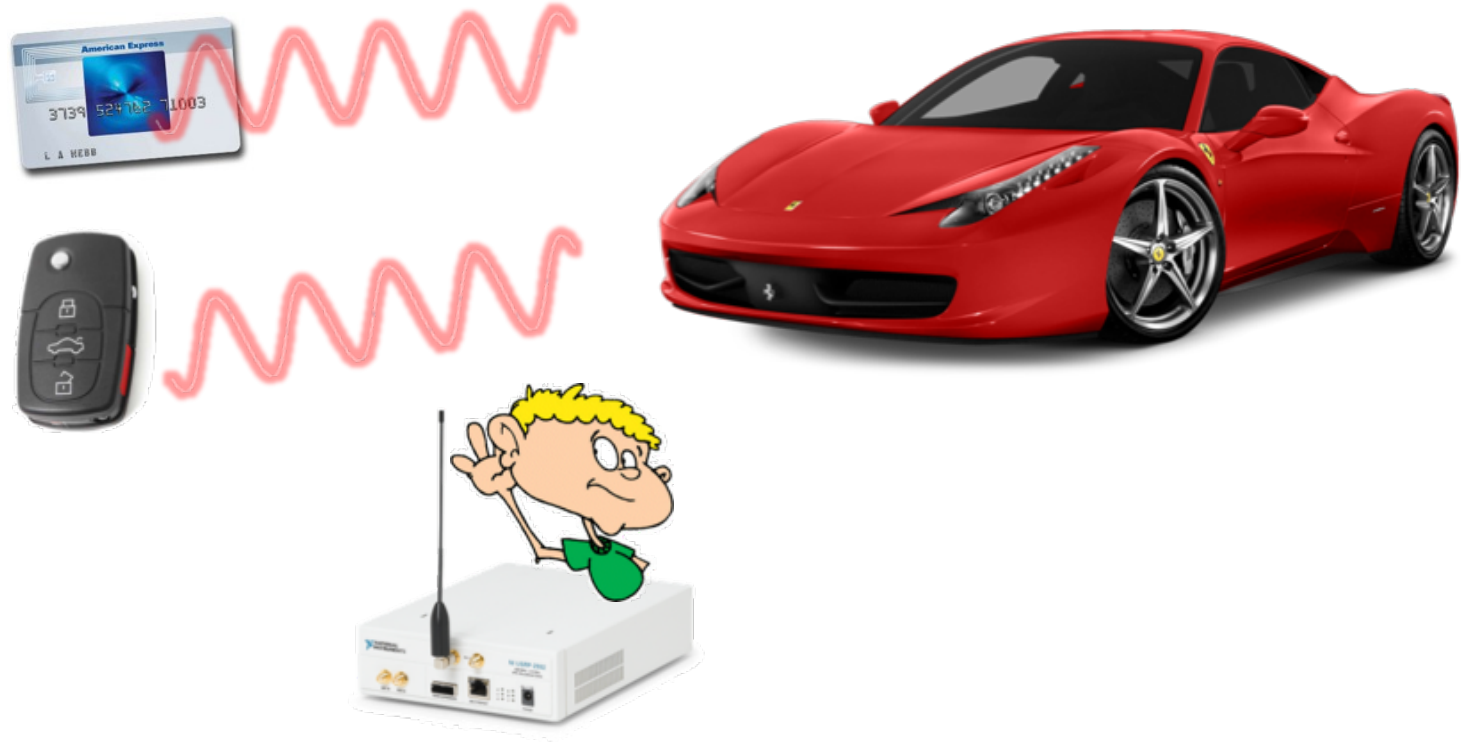
```
Fedora-15-x86_64-Live-RFID-v02.iso
SHA256: 79373eeef8accbf348bd9d46536b7f22d07c86653dbdf2968fce454dbd2da
MD5 : c8a5fac1fcb812c30309f9c9e979796
SHA1 : d854d989596c8a7668e37618a6658957f51ae2
```

#### 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.

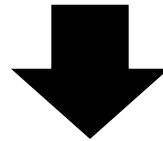
#### General Purpose Tools

# Hacking RFIDs Simply By Eavesdropping



RFIDs adopt weak encryption protocols

# Hacking RFIDs Simply By Eavesdropping



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

**RFIDs adopt weak encryption protocols**



# Protect your RFID cards against active attacks

The screenshot shows a web browser window with the Amazon website. The search bar contains "rfid blocking wallet". The product page displays the "Flipside Wallets Men's RFID Blocking Flipside 3X Wallet" for \$39.95. The product is shown in a large image, with a smaller image showing it open and containing a Visa card and cash. The page also shows a list of color options (black, grey, red, white) and a "In Stock" status. The browser window title is "Flipside Wallets Men" and the URL is "www.amazon.com/Flipside-Wallets-Blocking-Wallet-Stealth/dp/B00NLMZ2".

amazon Prime

Shop by Department

Haitham's Amazon.com Today's Deals Gift Cards Sell

Hello, Haitham Your Account

Amazon Fashion Women Men Girls Boys Baby Luggage Sales And Deals Your

Back to search results for "rfid blocking wallet"

Flipside Wallets

### 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

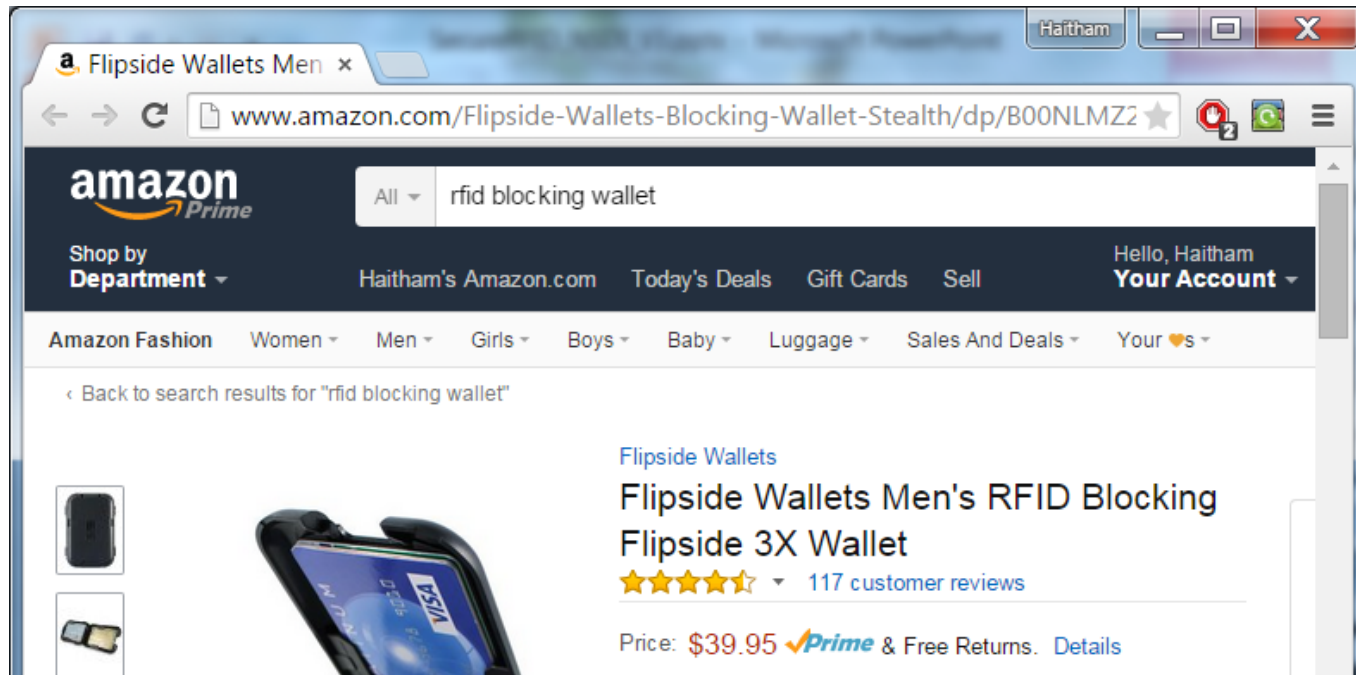
In Stock.

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

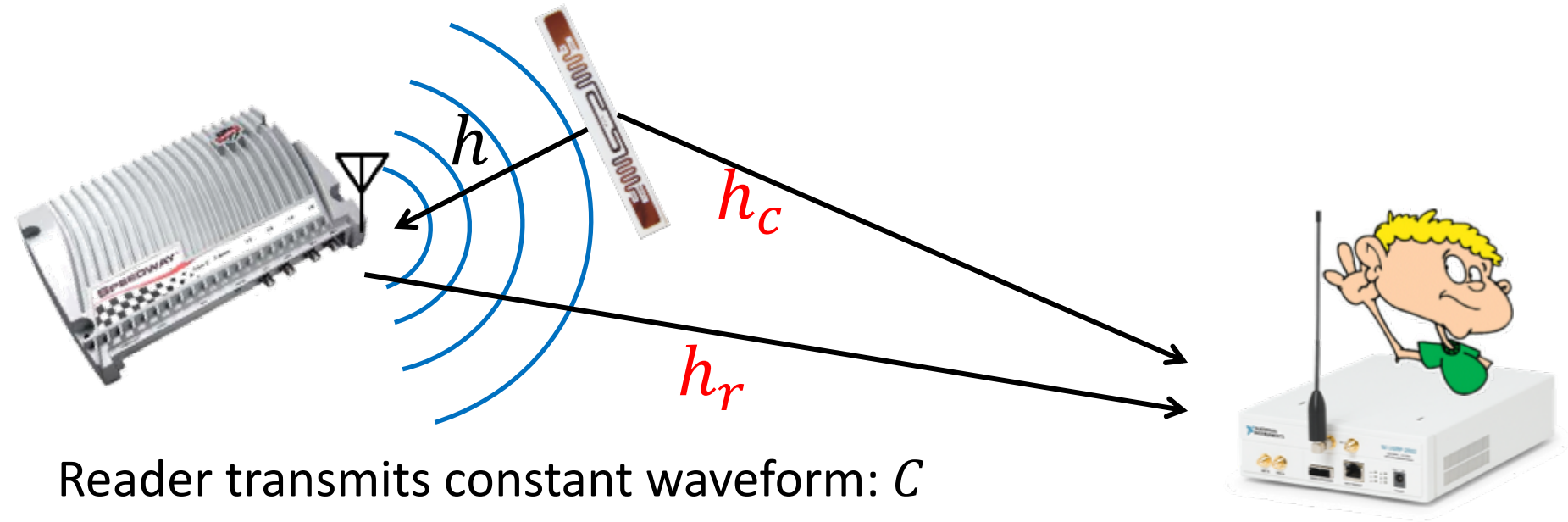


**Most attacks demonstrated by eavesdropping**



**Need solution for eavesdropping that works with existing RFIDs**

# RFID Communication



Reader transmits constant waveform:  $C$

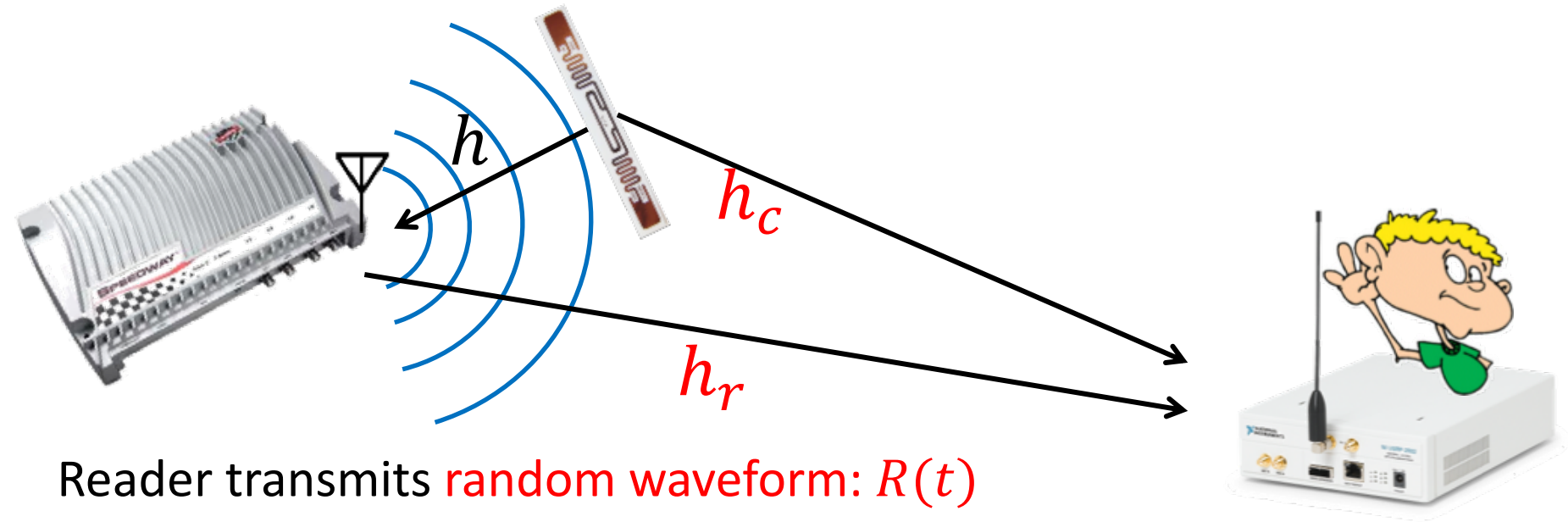
RFID reflects the reader's signal using ON-OFF switch

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:  $R(t)$**

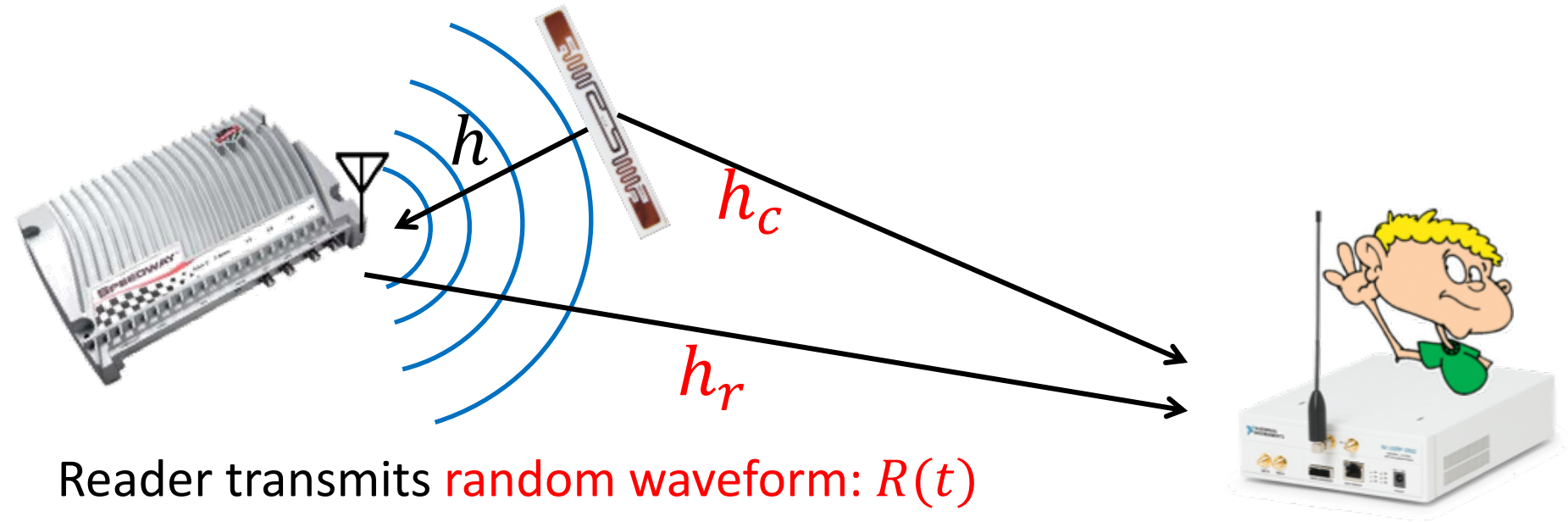
RFID reflects the reader's signal using ON-OFF switch

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

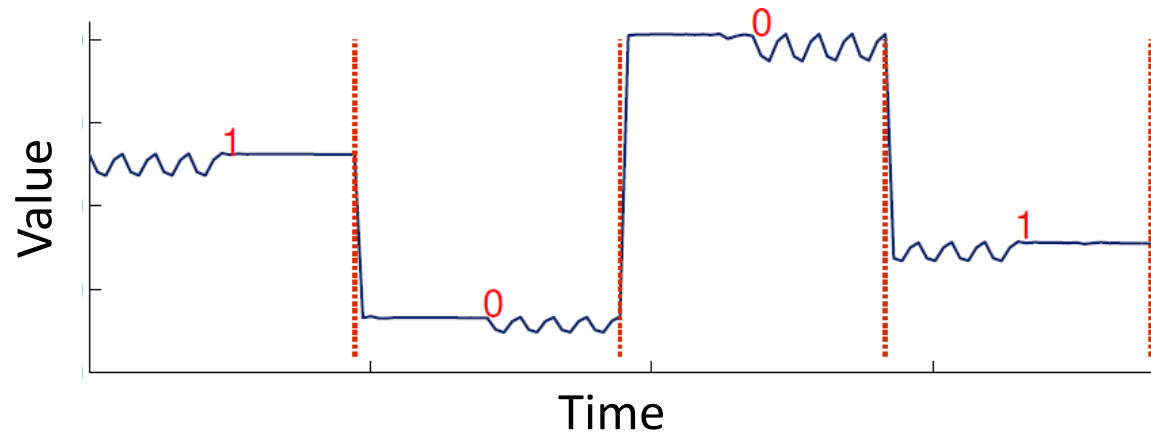
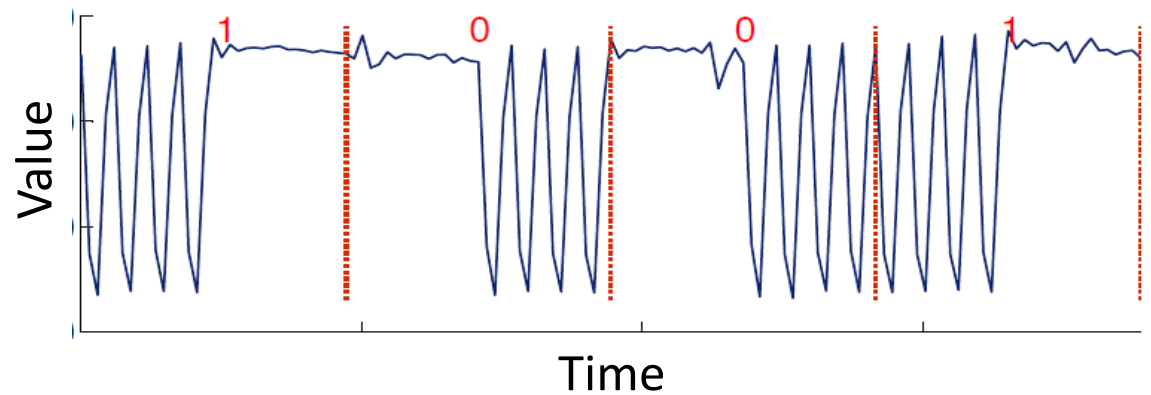
**Reader knows  $R(t) \rightarrow$  Can decode**

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

# RF-Cloak: Randomizing the Reader's Signal

- Random waveform acts like a one-time pad on the air  
→ Naïve solution: Multiply each bit with random number

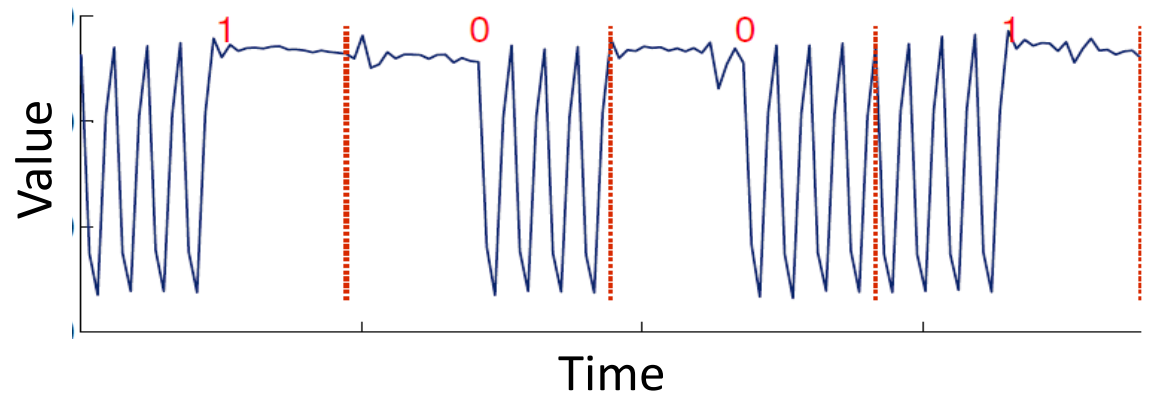
**RFID Signal:**



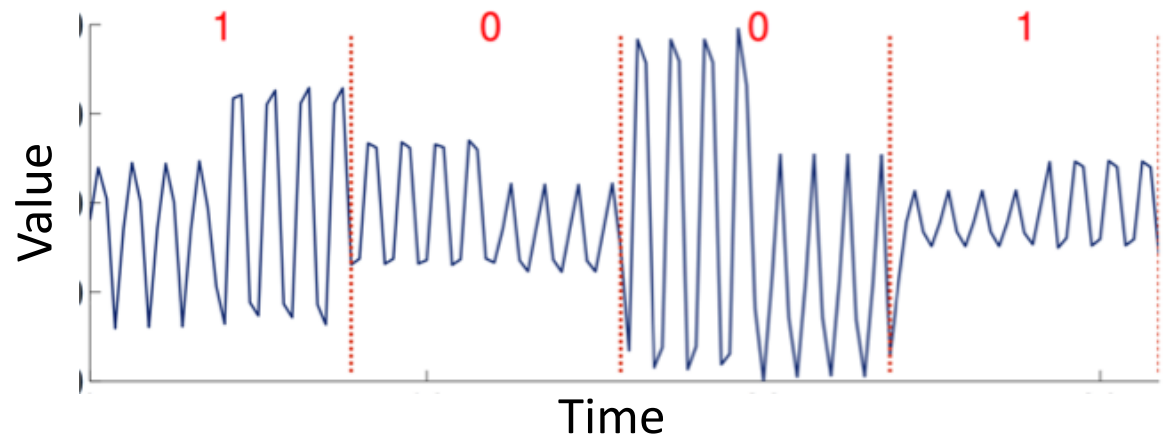
# RF-Cloak: Randomizing the Reader's Signal

- Random waveform acts like a one-time pad on the air

**RFID Signal:**



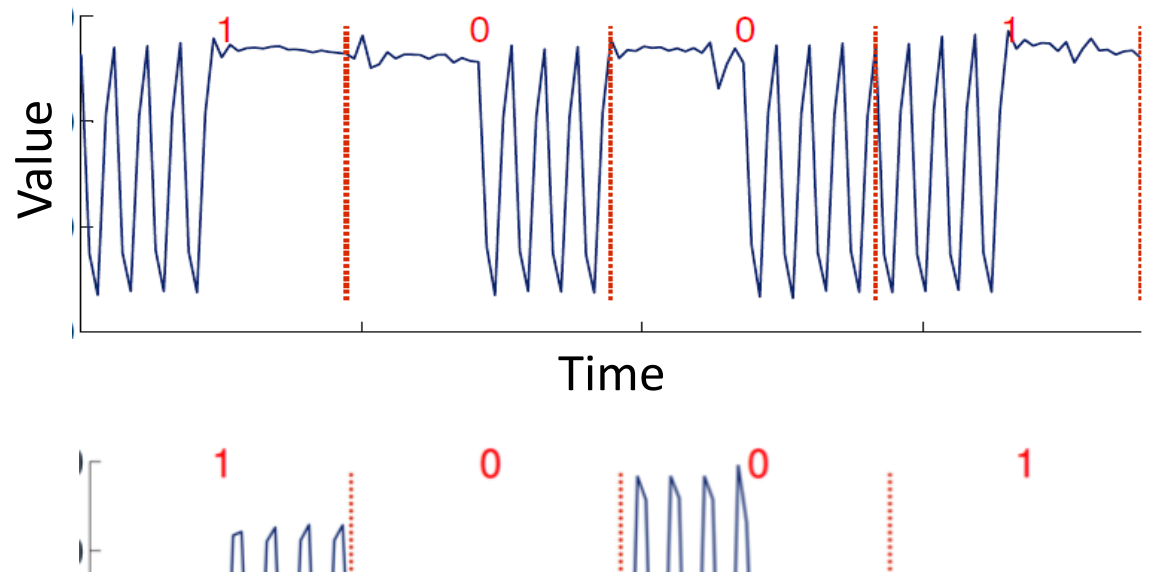
**Noisy Reader:**



# RF-Cloak: Randomizing the Reader's Signal

- Random waveform acts like a one-time pad on the air

**RFID Signal:**

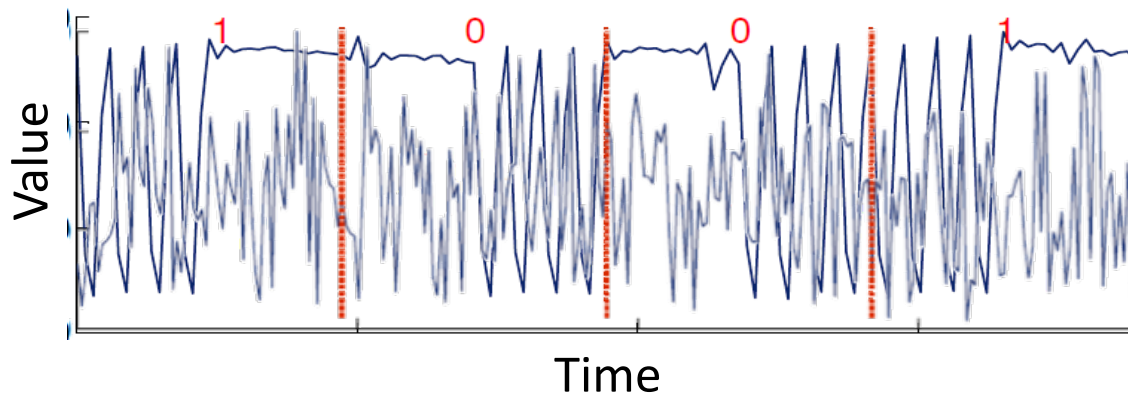
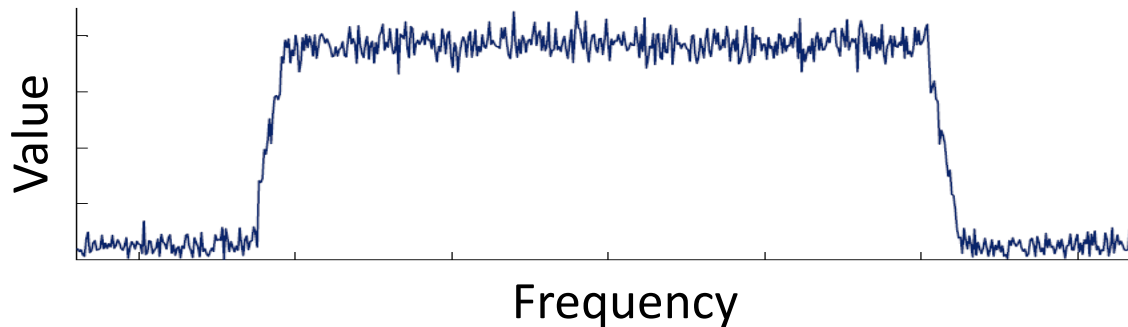


Random waveform must destroy internal signal patterns of the bits

# RF-Cloak: Randomizing the Reader's Signal

Random waveform:

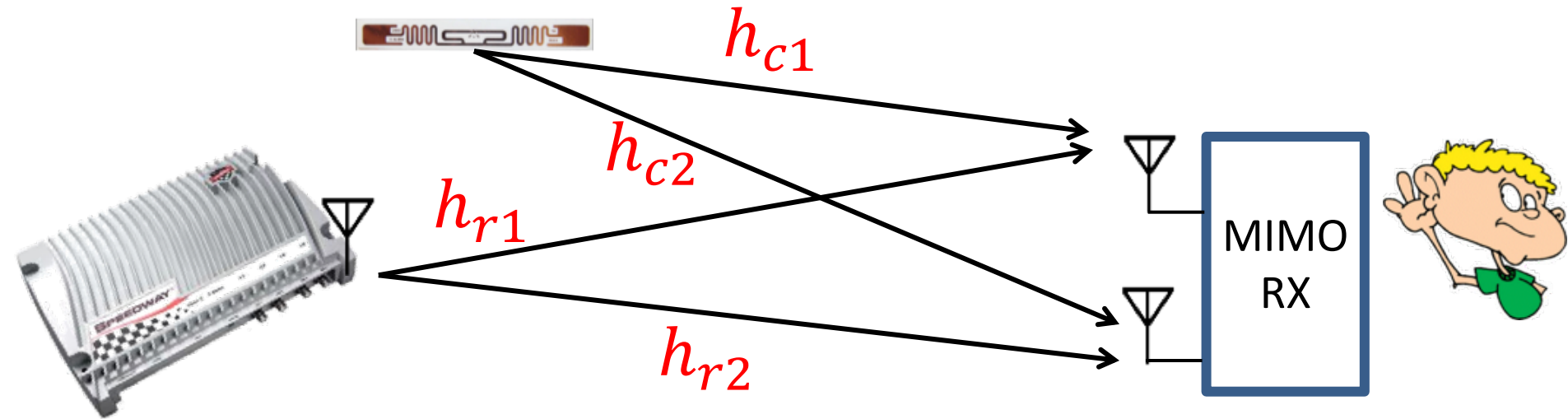
- Must change as fast as any transition in the RFID signal  
→ has same bandwidth as RFID signal
- Must be indistinguishable from white noise i.e. flat frequency profile  
→ samples taken from complex Gaussians





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:

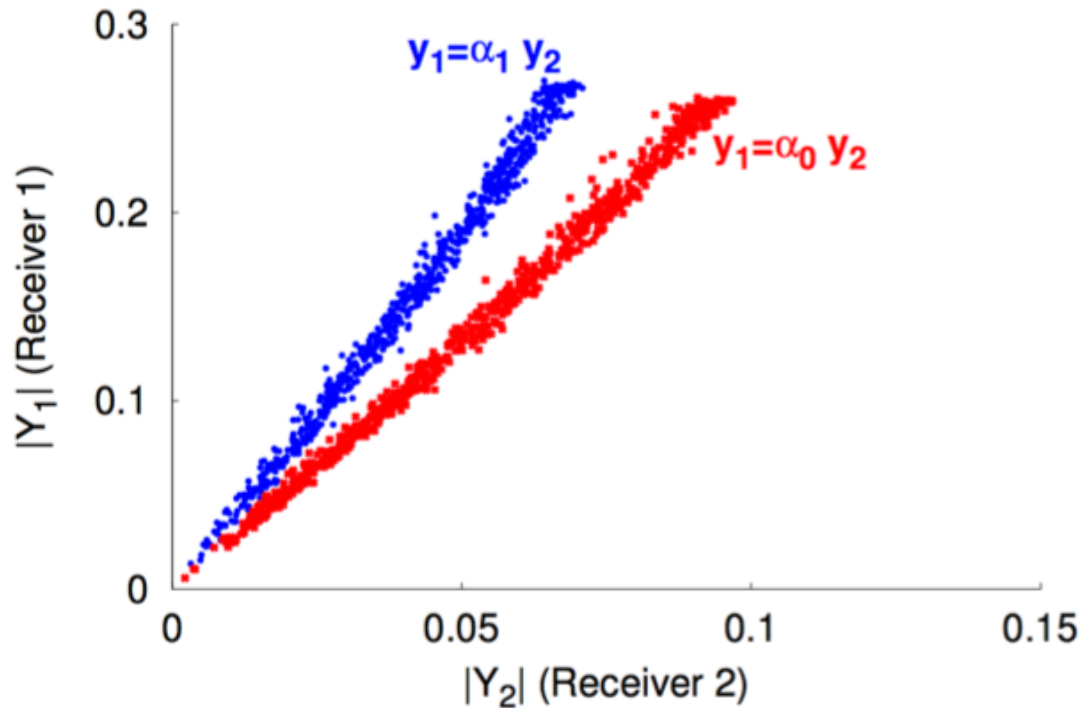
$$1^{\text{st}} \text{ receiver: } Y_1(t) = h_{r1} \times R(t) + h_{c1} \times R(t) \times \text{bits}$$

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

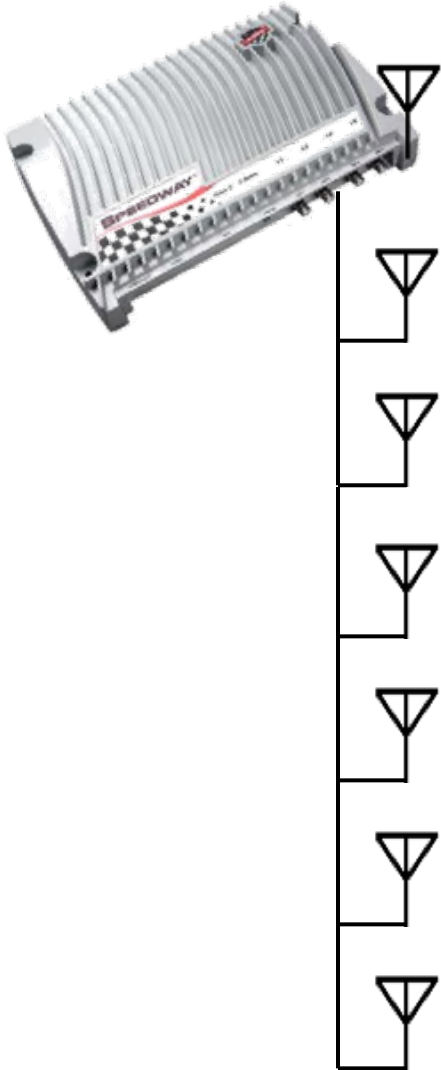
$$\frac{Y_1(t)}{Y_2(t)} = \frac{h_{r1} + h_{c1} \times \text{bits}}{h_{r2} + h_{c2} \times \text{bits}}$$

# MIMO Eavesdropper

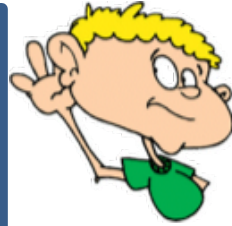
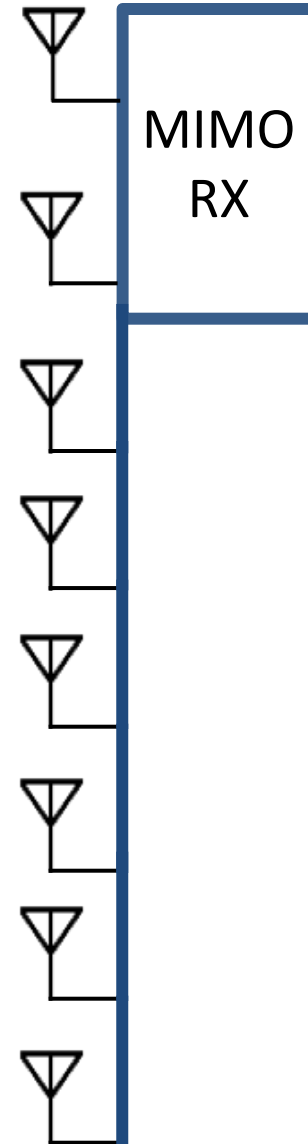
$$\left\{ \begin{array}{l} \frac{h_{r1} + h_{c1}}{h_{r2} + h_{c2}} \text{ if bit} = 1 \\ \frac{h_{r1}}{h_{r2}} \text{ if bit} = 0 \end{array} \right.$$



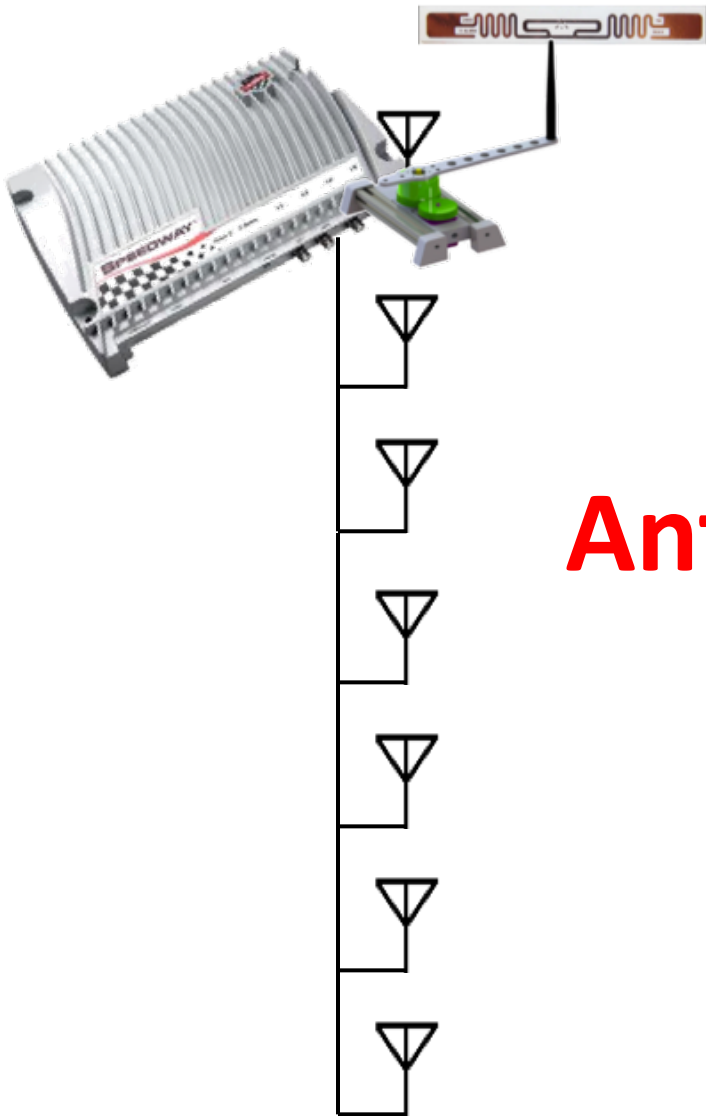
# RF-Cloak vs MIMO Eavesdropper



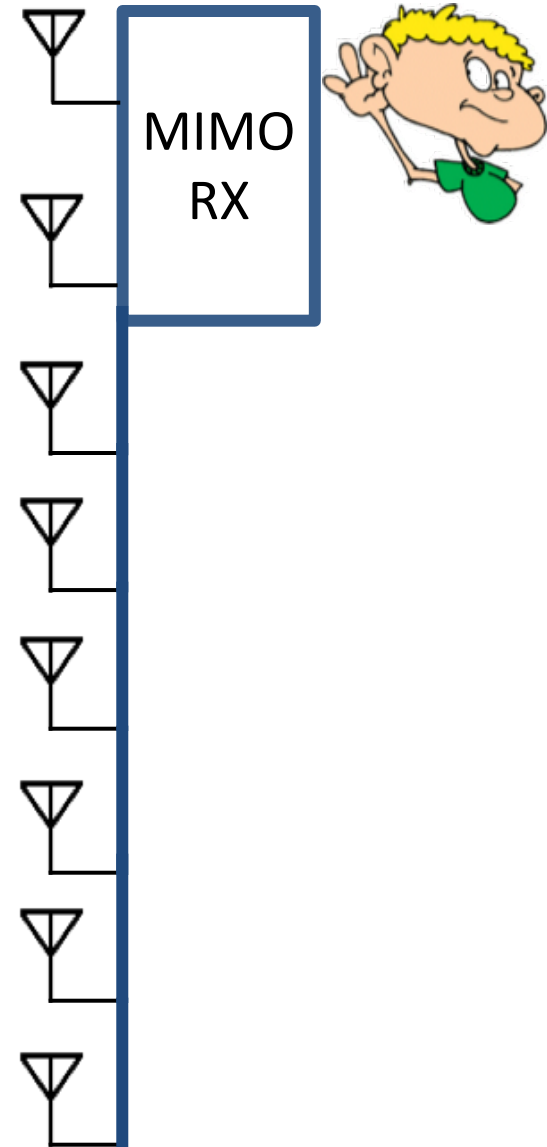
**Antenna War!**



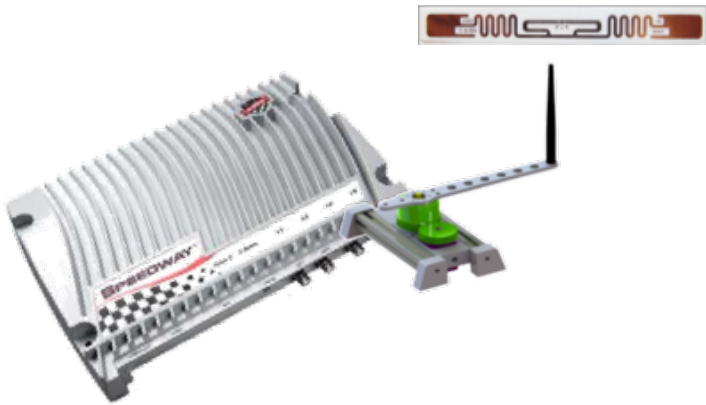
# RF-Cloak vs MIMO Eavesdropper



**Antenna War!**

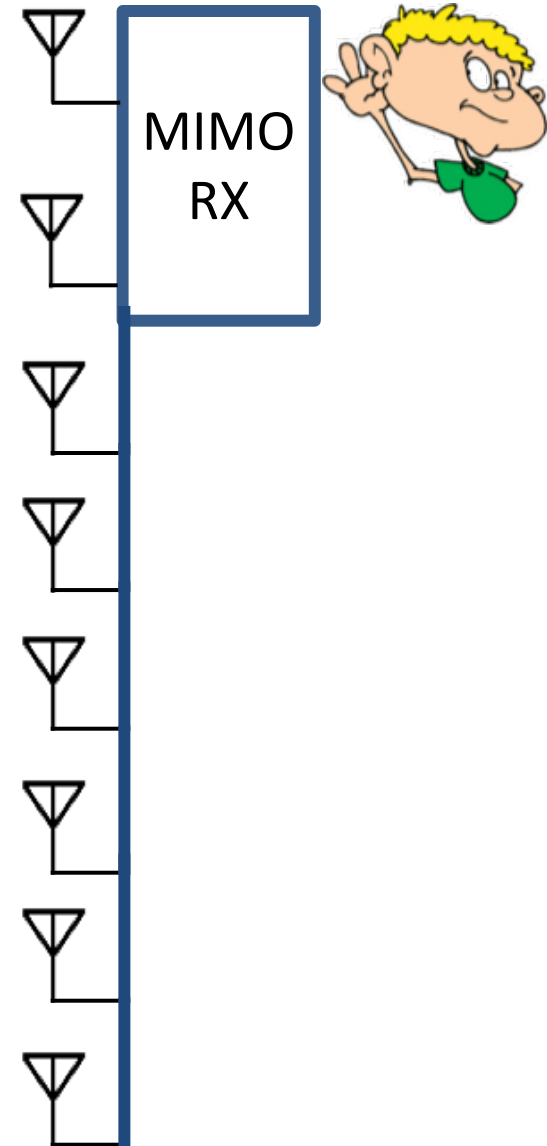


# RF-Cloak vs MIMO Eavesdropper



**RF-Cloak combines antenna motion  
and rapid antenna switching**

**→ Emulate a very large number of  
fast changing antennas**

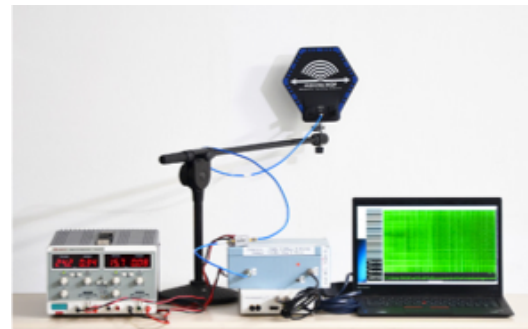
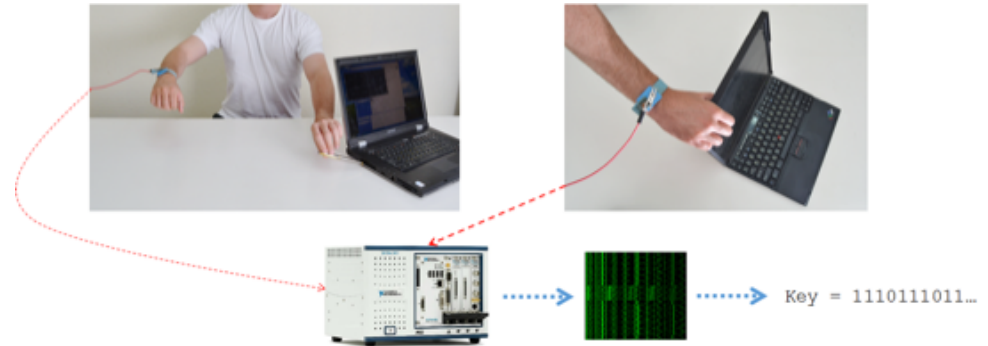






# Side Channel Attacks

Leakage from: acoustic, EM, RF, ... render crypto protocols insecure → **Extract secret keys from side channels!**



# Information Leakage in Side Channels

- Keystroke Recognition
  - Smart Watch Sensors

# MoLe: Motion Leaks through Smartwatch Sensors

He Wang, Ted Tsung-Te Lai, Romit Roy Choudhury  
University of Illinois at Urbana-Champaign


# Information Leakage in Side Channels

- Keystroke Recognition
  - Smart Watch Sensors
  - Audio on your phone



**DAISY**

Data Analysis and Information Security Lab



# Snooping Keystrokes with mm-level Audio Ranging on a Single Phone

Jian Liu<sup>†</sup>, Yan Wang<sup>†</sup>, Gorkem Kar<sup>#</sup>, Yingying Chen<sup>†</sup>,  
Jie Yang<sup>‡</sup>, Marco Gruteser<sup>#</sup>

<sup>†</sup>*Dept. of ECE, Stevens Institute of Technology, USA*

<sup>#</sup>*Winlab, Rutgers University, USA*

<sup>‡</sup>*Dept. of CS, Florida State University, USA*

**MobiCom 2015**

Paris, France  
Sep. 9 – 11, 2015



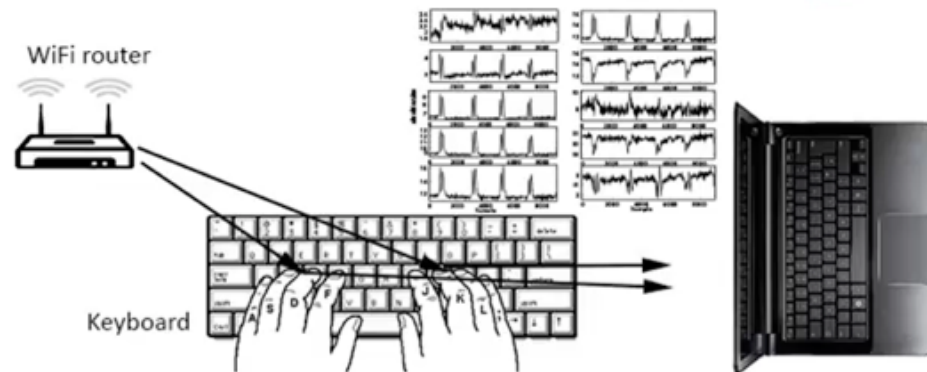
THE  
FLORIDA STATE  
UNIVERSITY

THE STATE UNIVERSITY OF NEW JERSEY  
**RUTGERS**

# Information Leakage in Side Channels

- Keystroke Recognition
  - Smart Watch Sensors
  - Audio on your phone
  - Wireless Signals

# Wi-Key



# Information Leakage in Side Channels

- Keystroke Recognition
  - Smart Watch Sensors
  - Audio on your phone
  - Wireless Signals
- Audio Eavesdropping
  - Video Camera



# **The Visual Microphone: Passive Recovery of Sound from Video**

**Abe Davis  
Michael Rubinstein  
Neal Wadhwa  
Gautham J. Mysore  
Fredo Durand  
William T. Freeman**

# Information Leakage in Side Channels

- Keystroke Recognition
  - Smart Watch Sensors
  - Audio on your phone
  - Wireless Signals
- Audio Eavesdropping
  - Video Camera
  - Phone Sensors

# Listening through a Vibration Motor

Nirupam Roy, Romit Roy Choudhury  
UIUC

MobiSys 2016



# Information Leakage in Side Channels

- Keystroke Recognition
  - Smart Watch Sensors
  - Audio on your phone
  - Wireless Signals
- Audio Eavesdropping
  - Video Camera
  - Phone Sensors
  - Wireless Signals

# Acoustic Eavesdropping through Wireless Vibrometry

*Teng Wei<sup>†</sup>, Shu Wang<sup>†</sup>, Anfu Zhou<sup>\*†</sup>, Xinyu Zhang<sup>†</sup>*

*<sup>†</sup>Department of Electrical and Computer Engineering  
University of Wisconsin - Madison*

*<sup>\*</sup>Institute of Computing Technology  
Chinese Academy of Sciences*

MOBICOM 2015