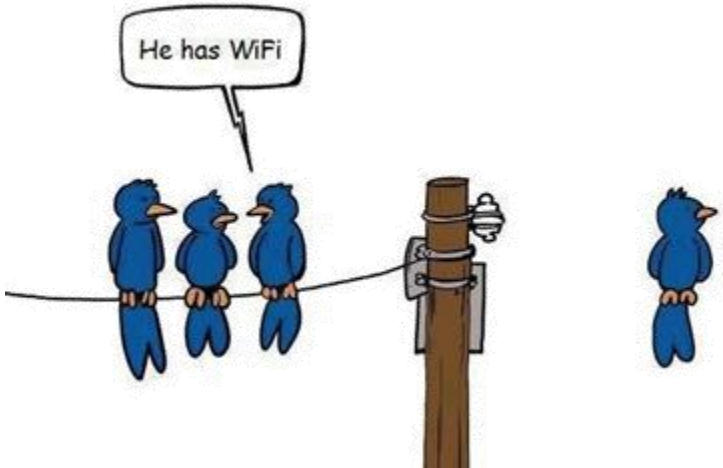
COM-405: Mobile Networks

Lecture 11.1: Physical Layer Security

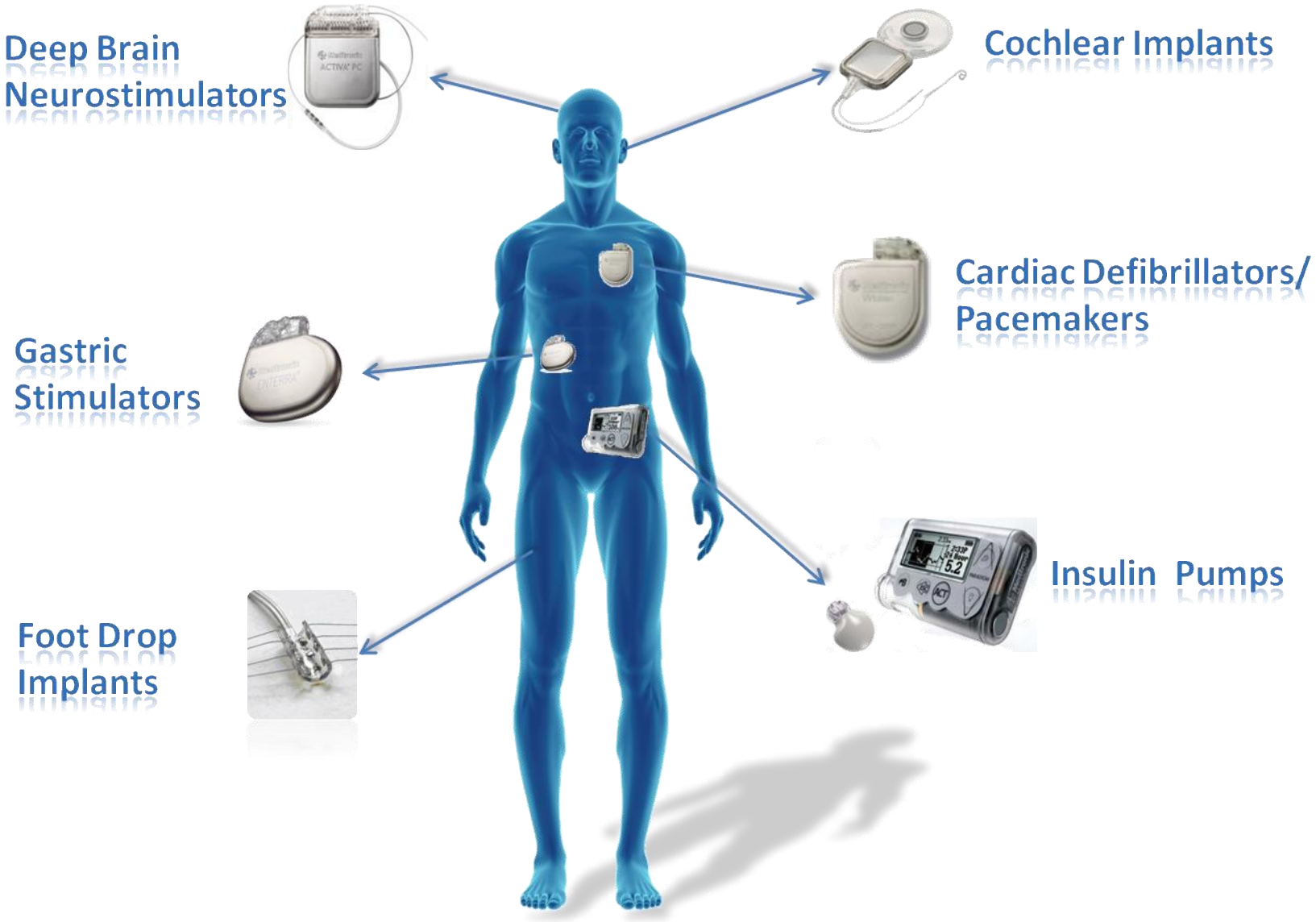
Haitham Hassanieh



EPFL

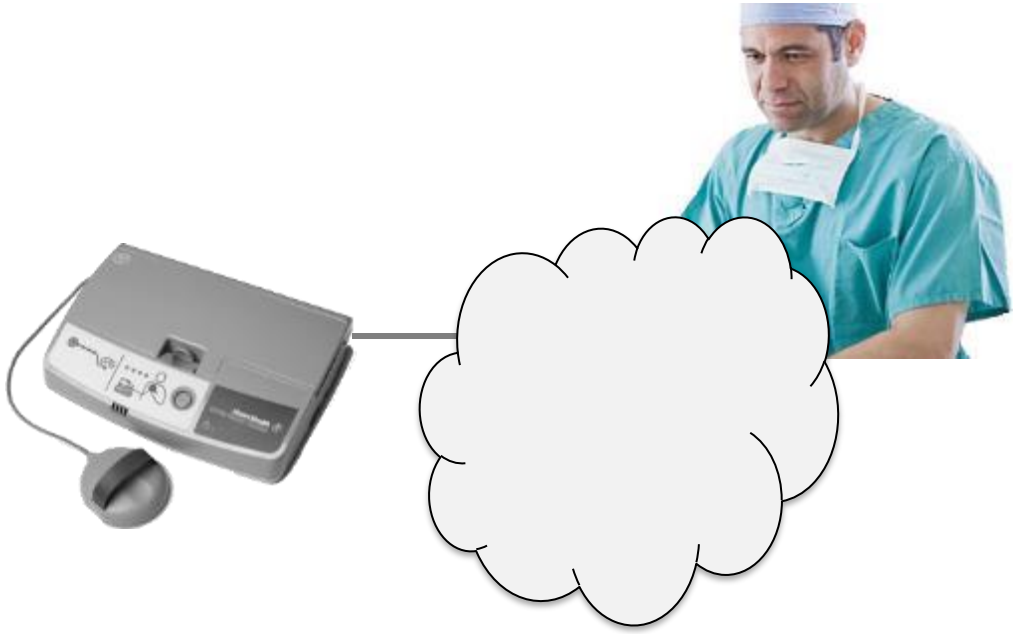
Laboratory of SEnsing
& Networking Systems

WIRELESS IMPLANTABLE MEDICAL DEVICES



Benefits of Wireless

- Easier communication with implant
- Remote monitoring



Benefits of Wireless

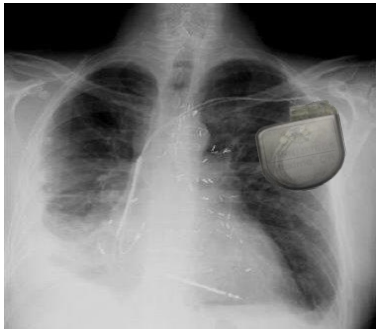
- Easier communication with implant
- Remote monitoring
  - ➢ Reduces hospital visits by 40% and cost per visit by $1800

[Journal of the American College of Cardiology, 2011]

What about security?

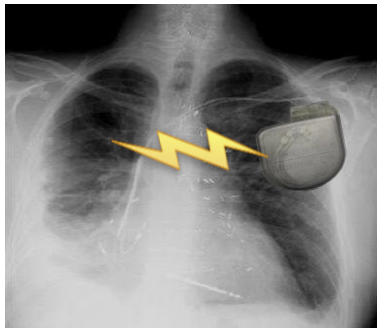
Security Attacks

1) Passive attack: Eavesdrop on private data

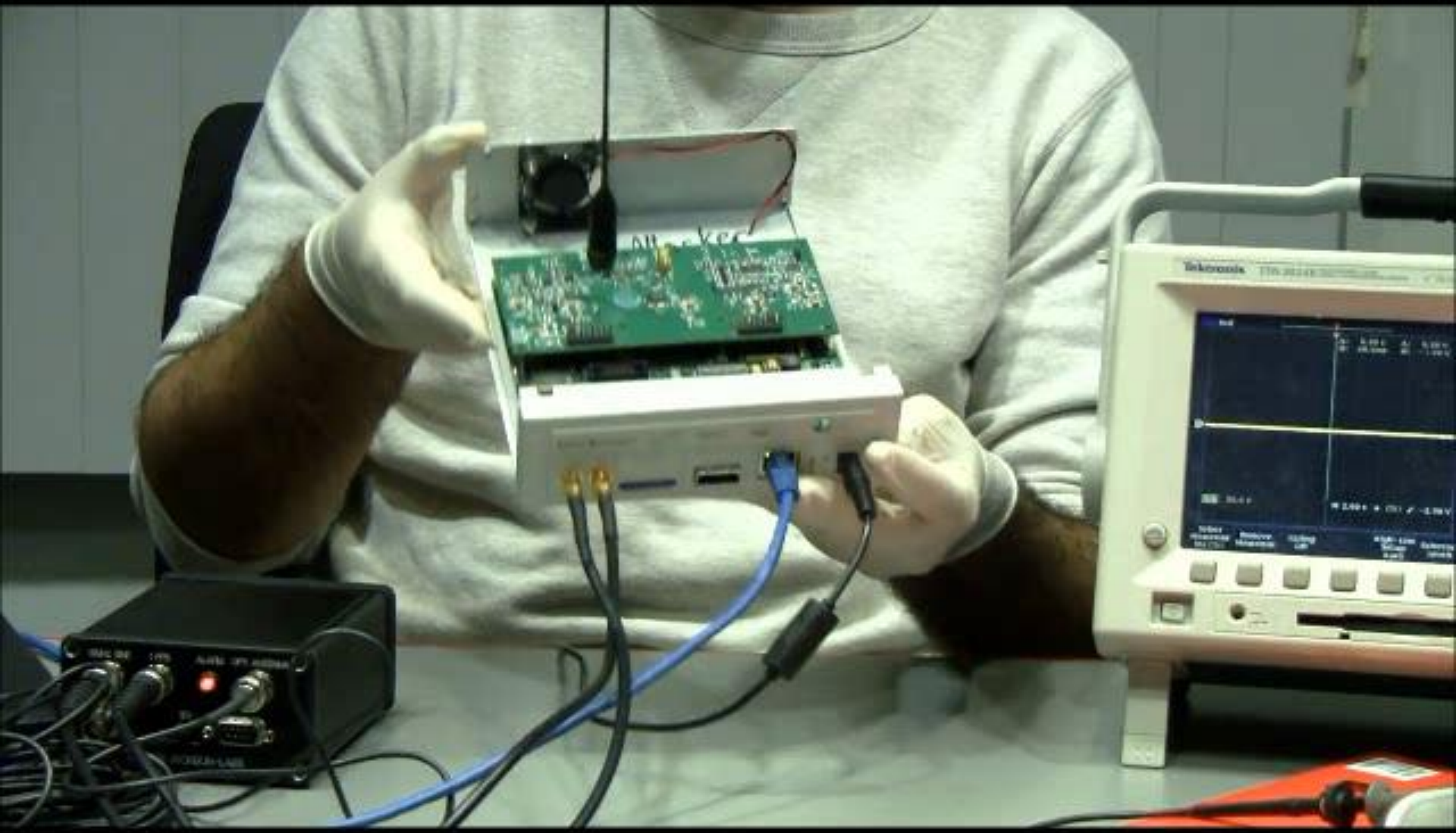


Patient diagnosis,
vital signs

2) Active attack: Send unauthorized commands



Turn off therapies,
deliver electric shock


Tektronix

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

Message Key ***Encrypted Message***

Decryption

Encrypted Message Key *Message*

Only a node that has the key can decrypt

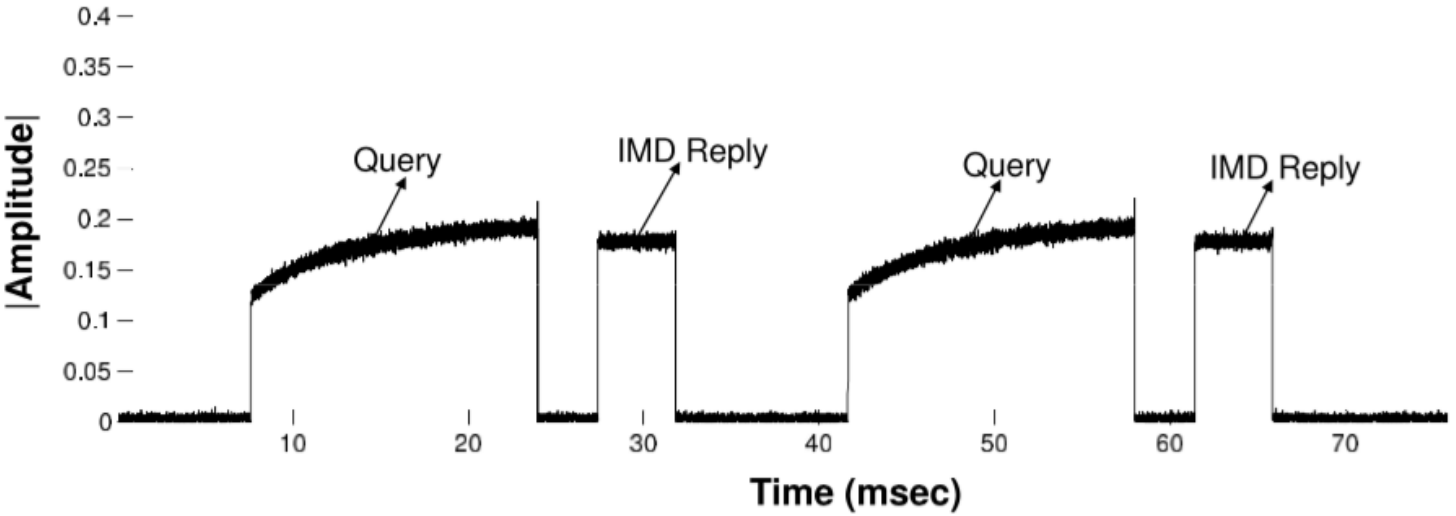
Protect from Passive Attacks: Analog One-Time Pad

Implant's signal

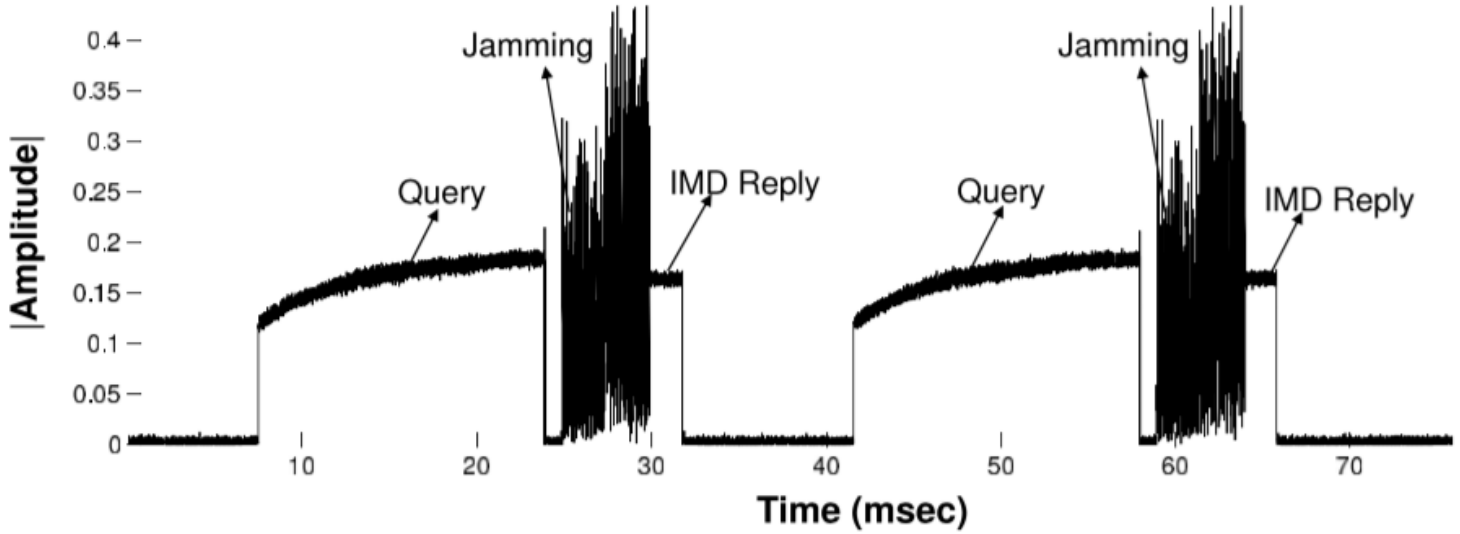
Random Sum

Jamming signal acts like the key in one-time pad

How Should the Jamming Signal Look like

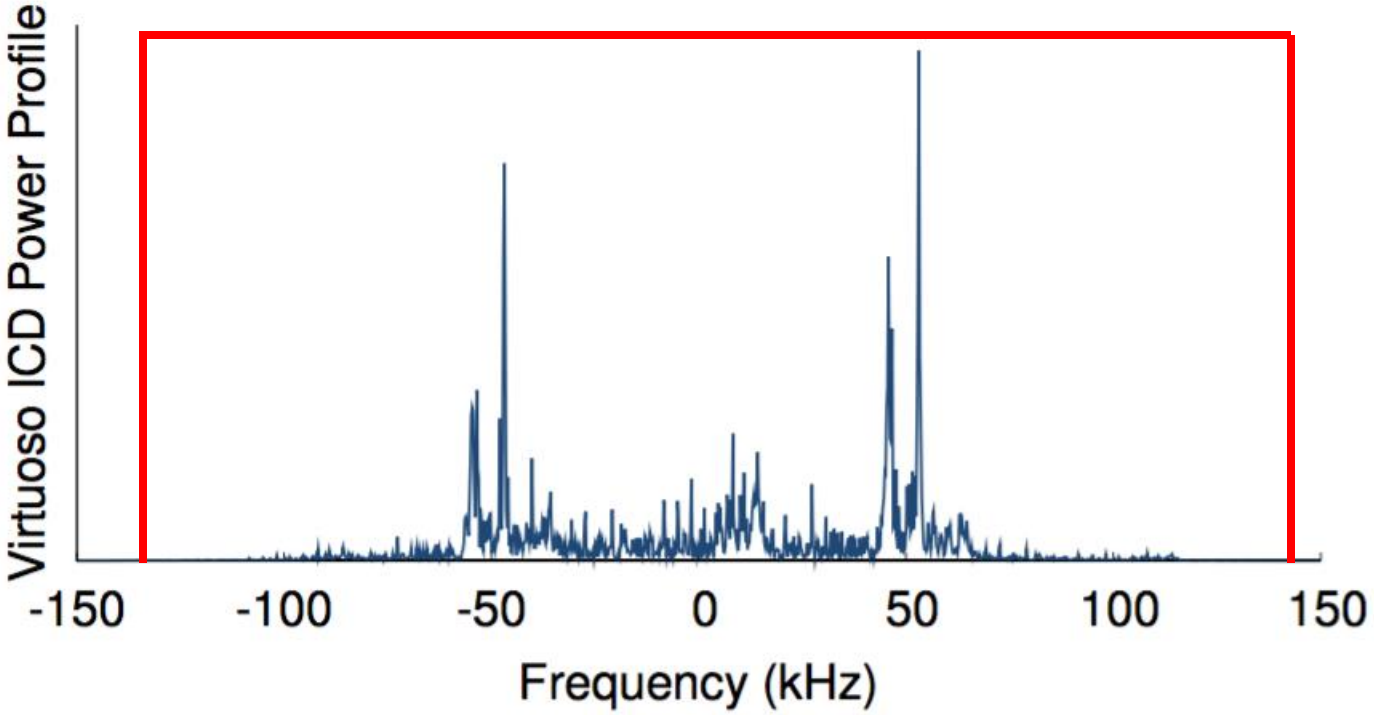


(a) Without jamming

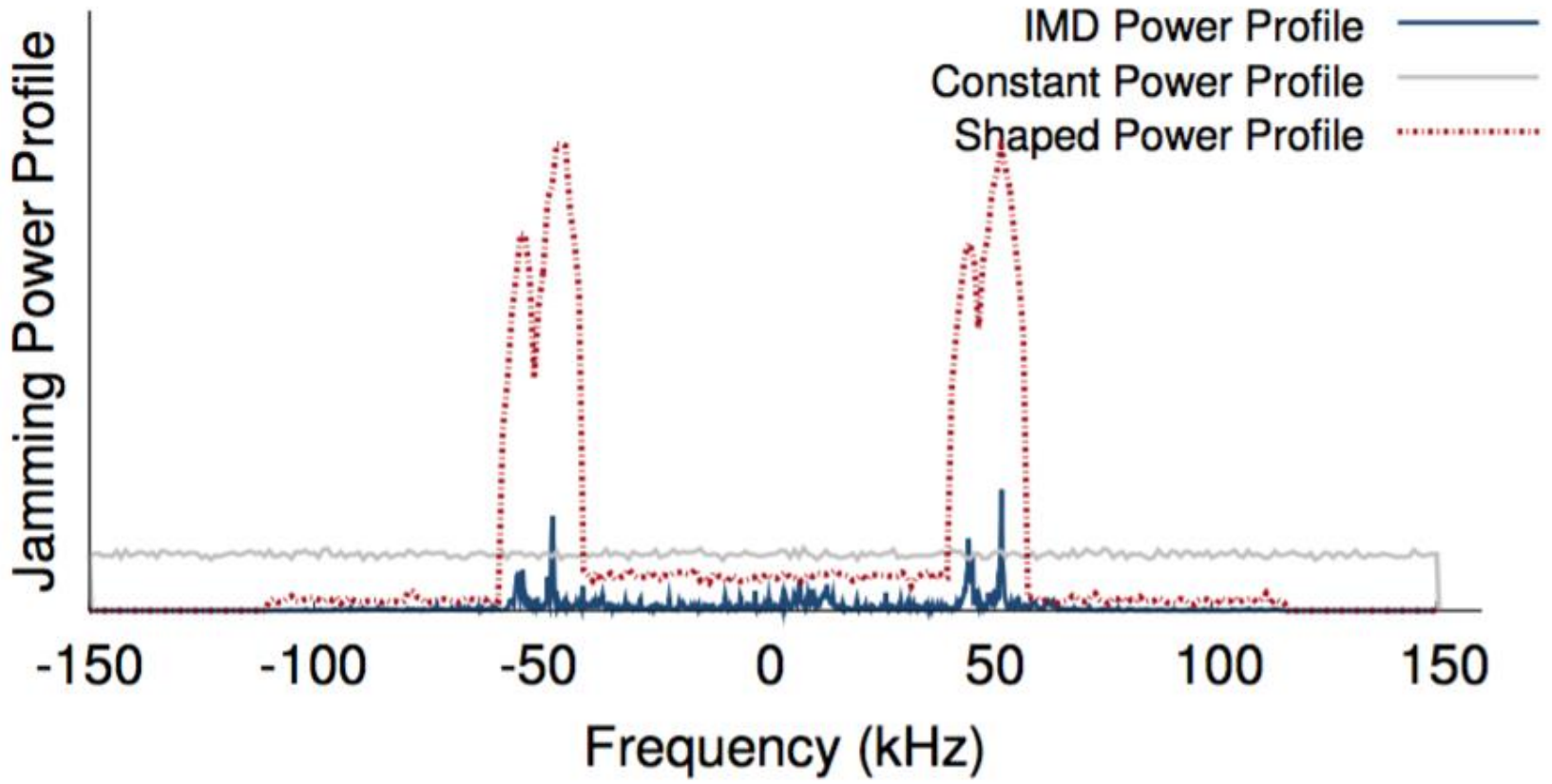


(b) With jamming

How ould the Jamming Signal Lc 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

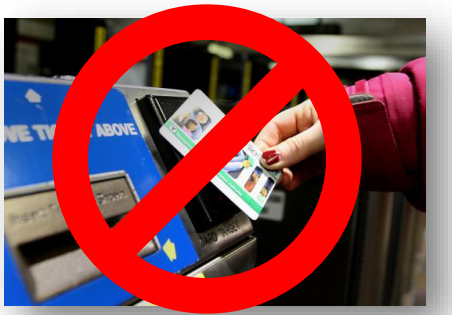
Access Control
[SECRYPT'09, S&P'09 ESORICS'08, Usenix'08]

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

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

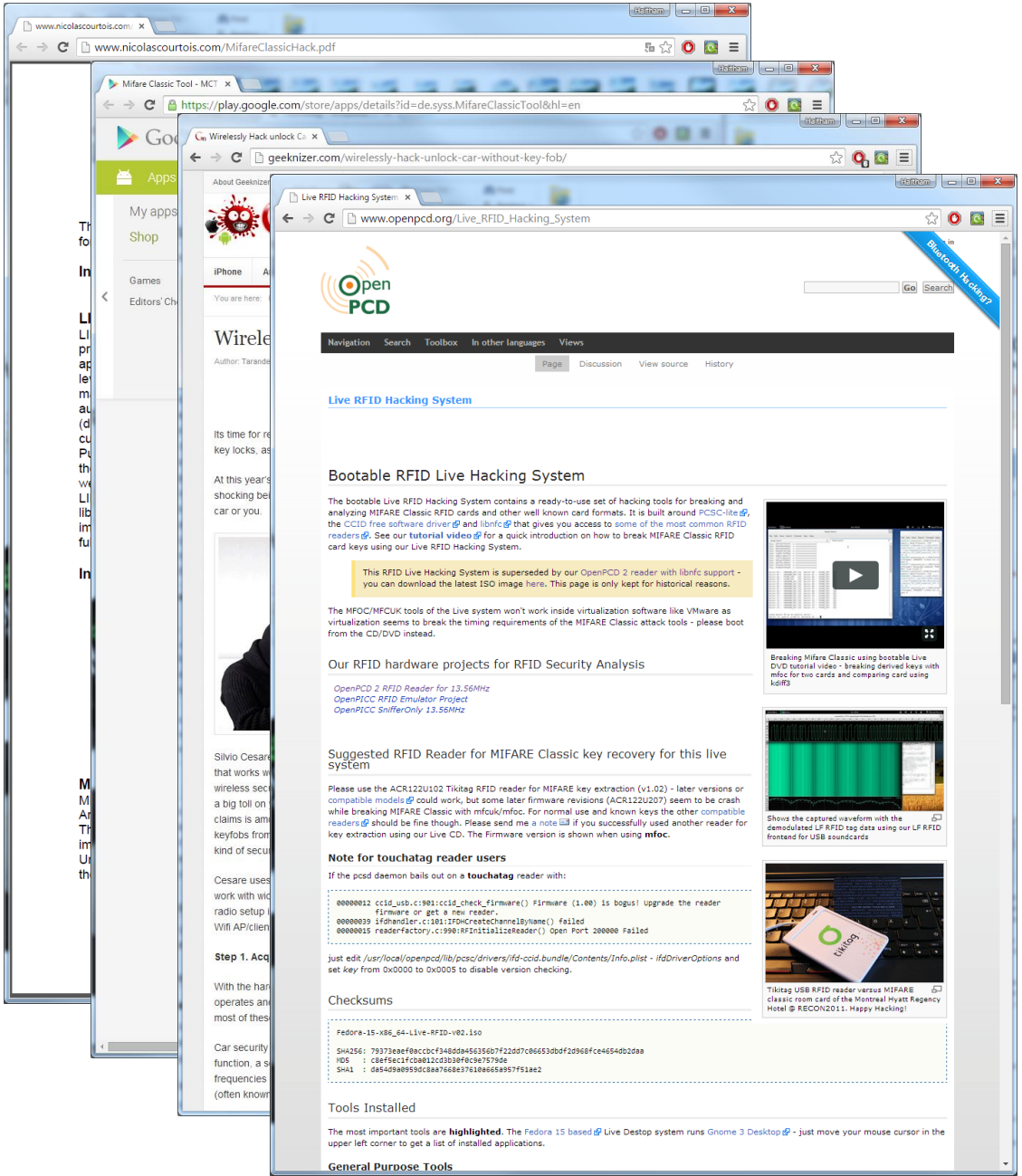
Pharmaceutical Drugs
[CCS'09, RFID'06]

Anti-Theft Car Immobilizers
[Usenix'12, Usenix'05]

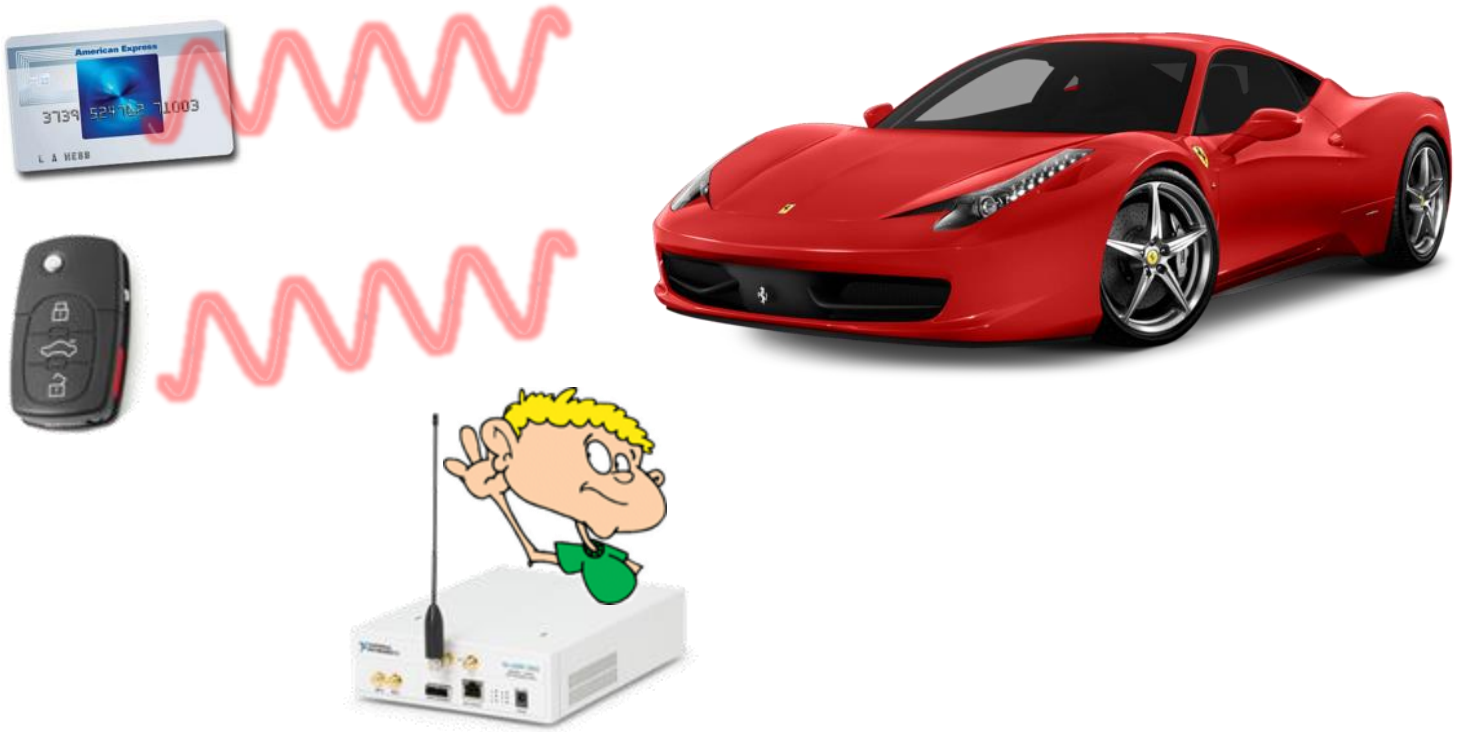


Public Transportation
[Defcon'08, MIT'08, S&P'09]

Hacking RFIDs for Dummies



Hacking RFIDs Simply By Eavesdropping



RFIDs adopt weak encryption protocols

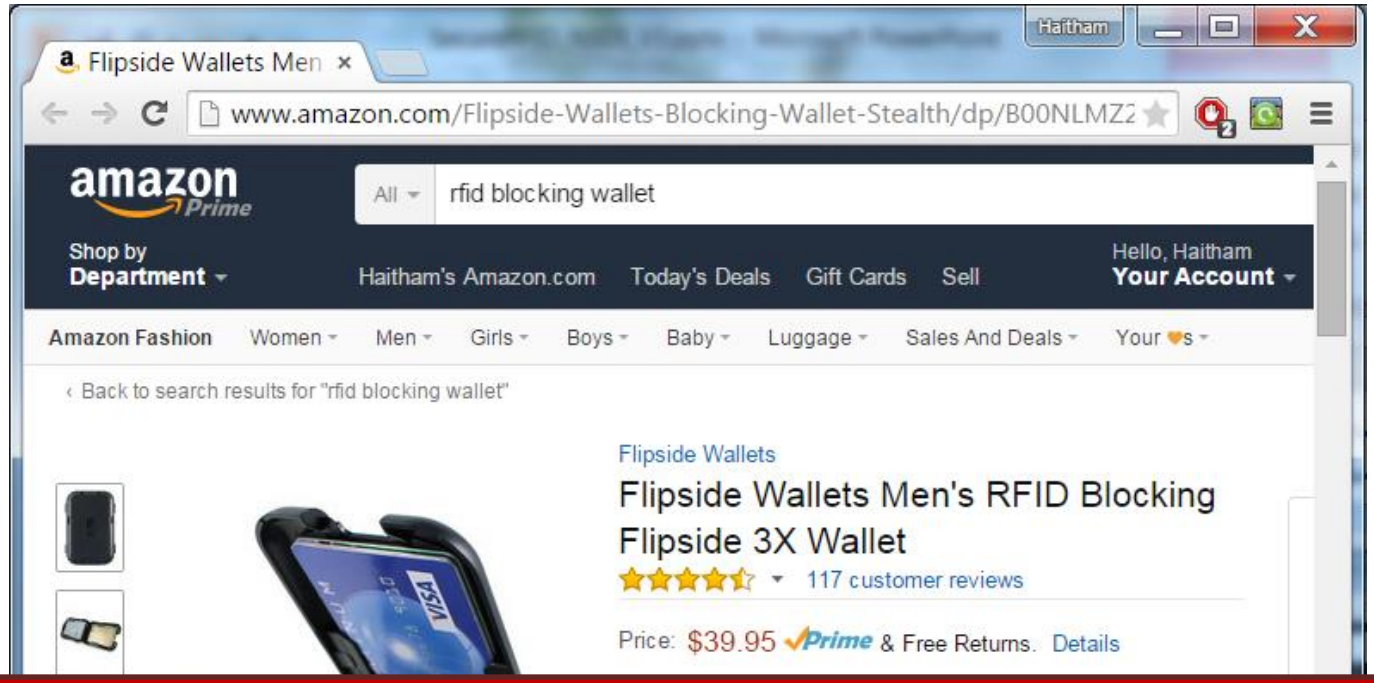
Hacking RFIDs Simply By Eavesdropping

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

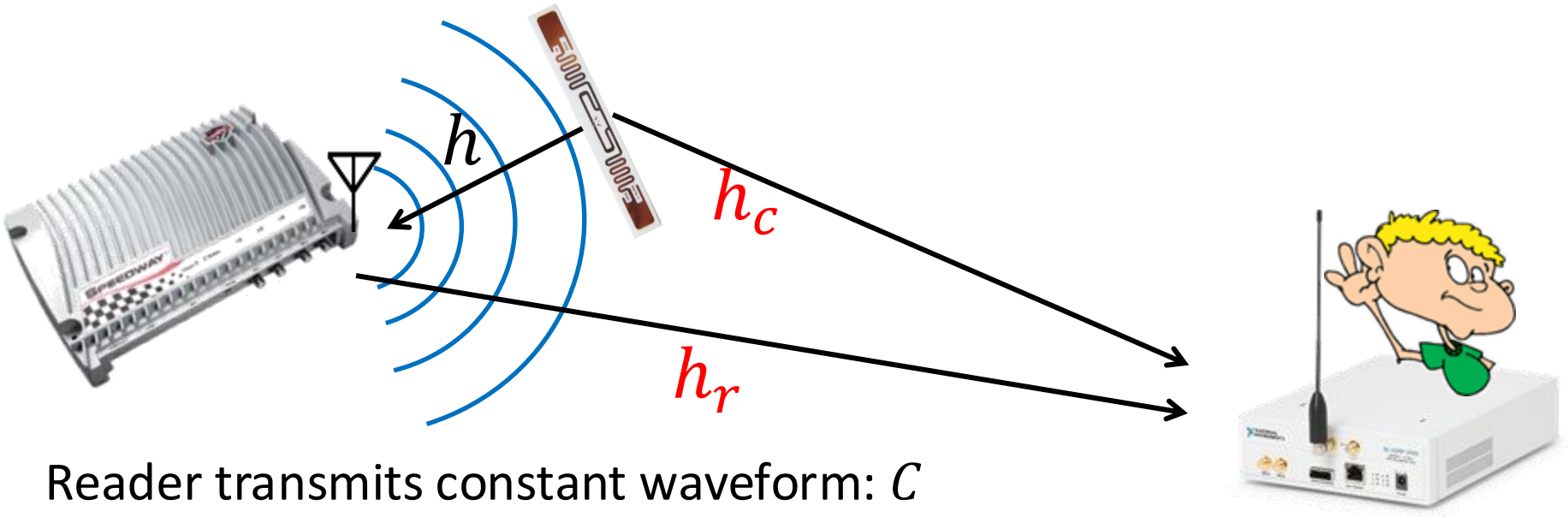
Protect your RFID cards against active attacks



Most attacks demonstrated by eavesdropping

Need solution for eavesdropping that works with existing RFIDs

RFID Communication



Reader transmits constant waveform: C

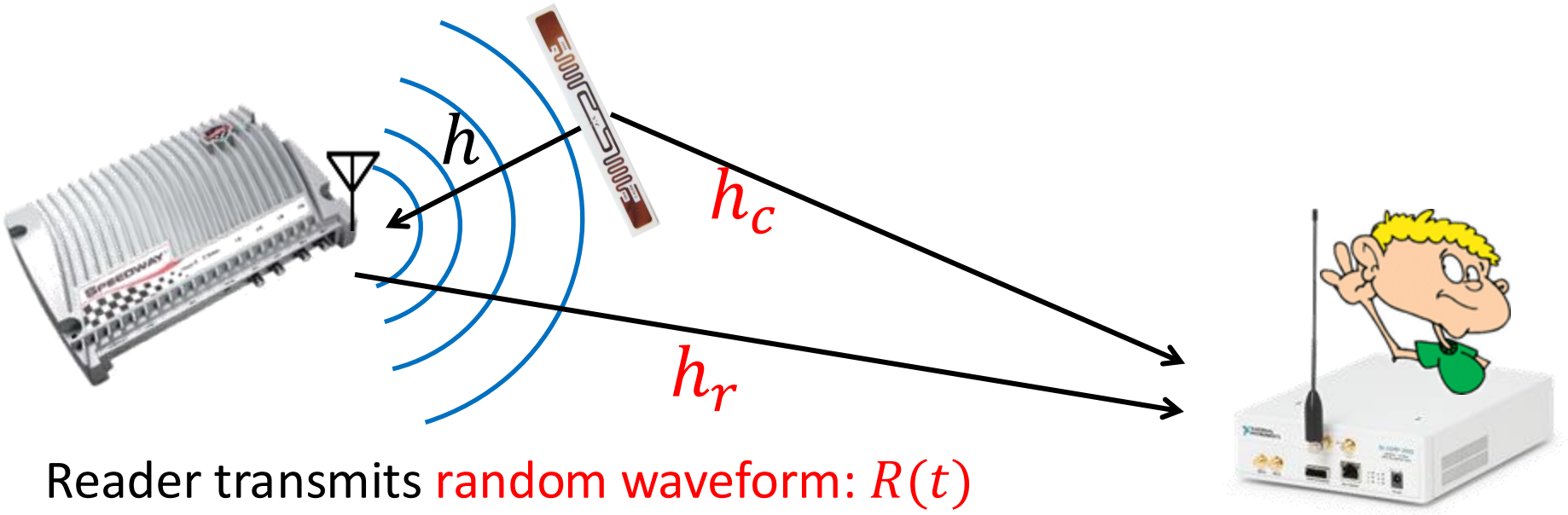
RFID reflects the reader's signal using ON-OFF switch

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: $R(t)$

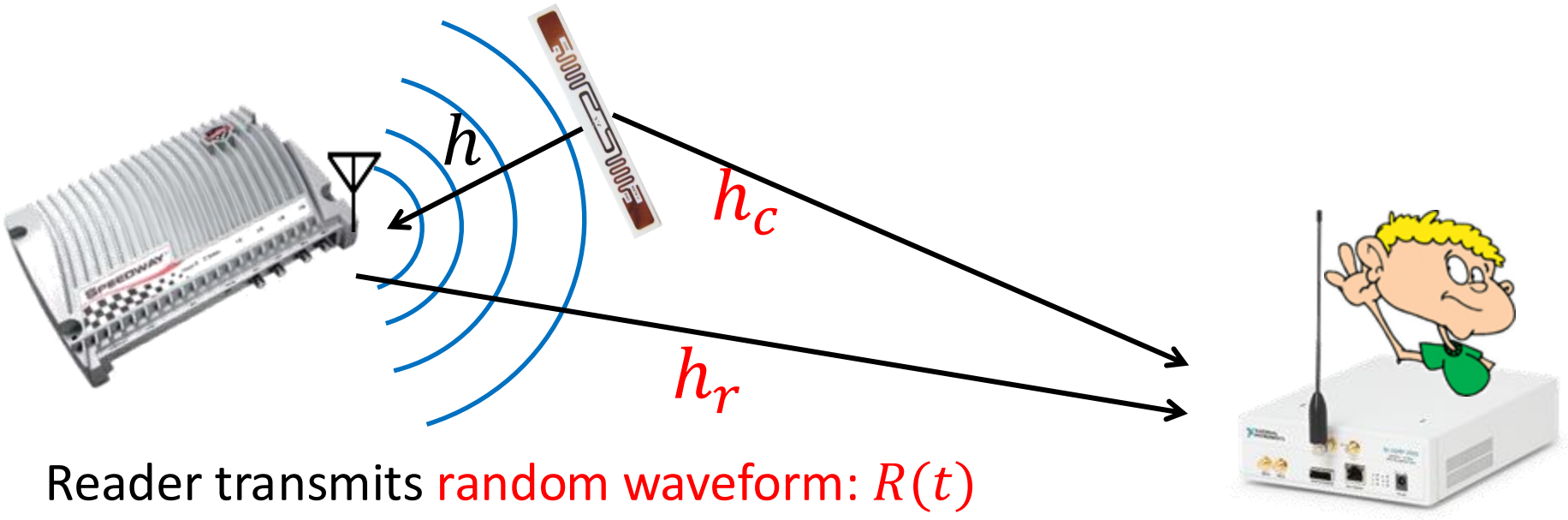
RFID reflects the reader's signal using ON-OFF switch

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

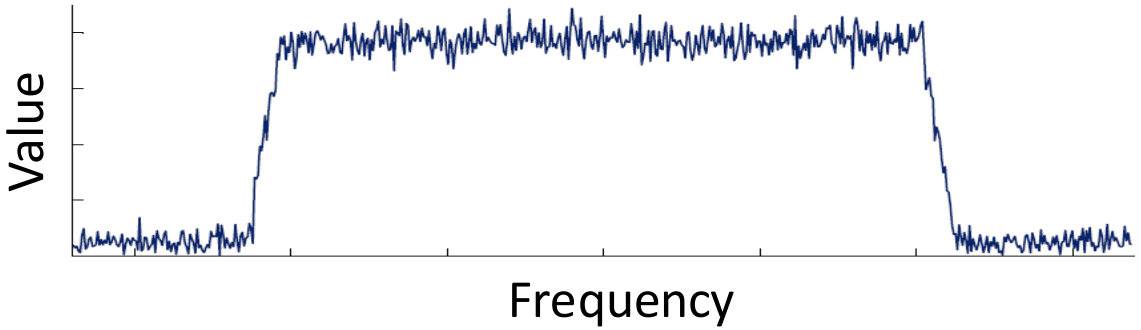
Reader knows $R(t)$→ Can decode

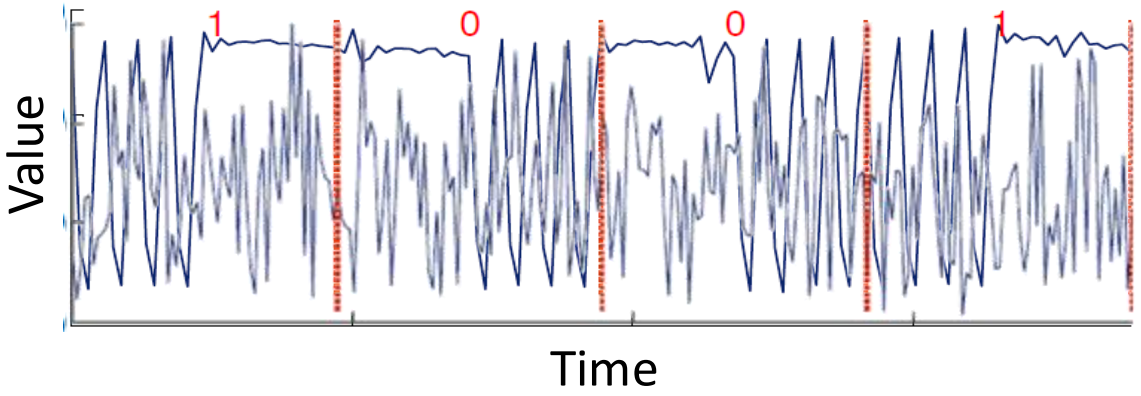
Eavesdropper doesn't know $R(t)$→ Cannot decode

RF-Cloak: Randomizing the Reader's Signal

Random waveform:

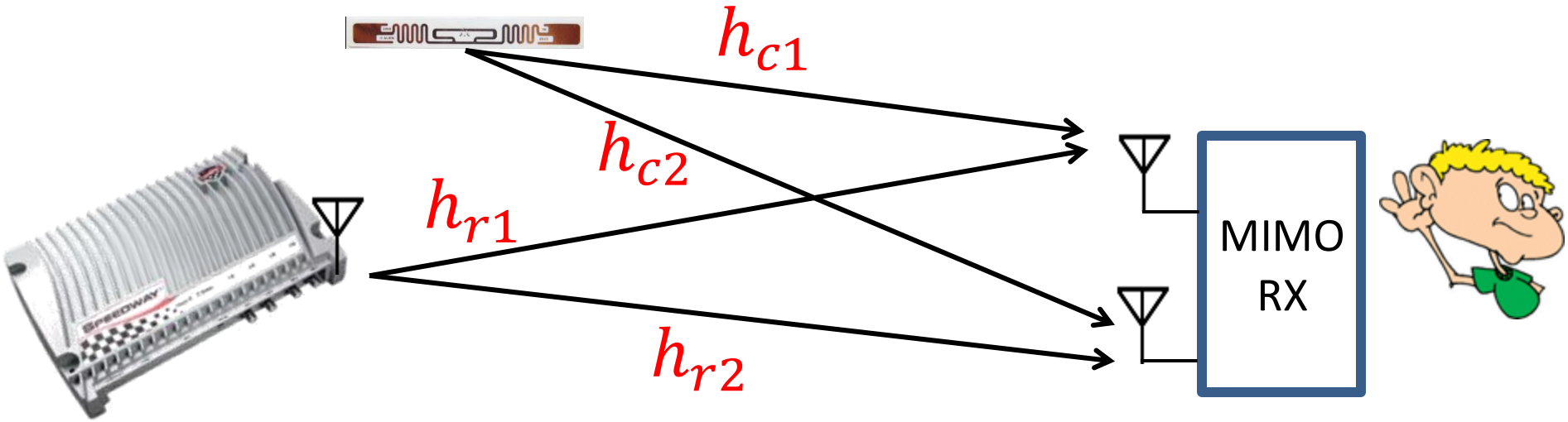
- Must change as fast as any transition in the RFID signal
  → has same bandwidth as RFID signal
- Must be indistinguishable from white noise i.e. flat frequency profile
  → samples taken from complex Gaussians





What if the attacker has multi-antenna MIMO capability?

MIMO Eavesdropper



Reader transmits random waveform: $R(t)$

Eavesdropper receives:

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

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

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

MIMO Eavesdropper

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

Reader transmits random waveform: $R(t)$

Eavesdropper receives:

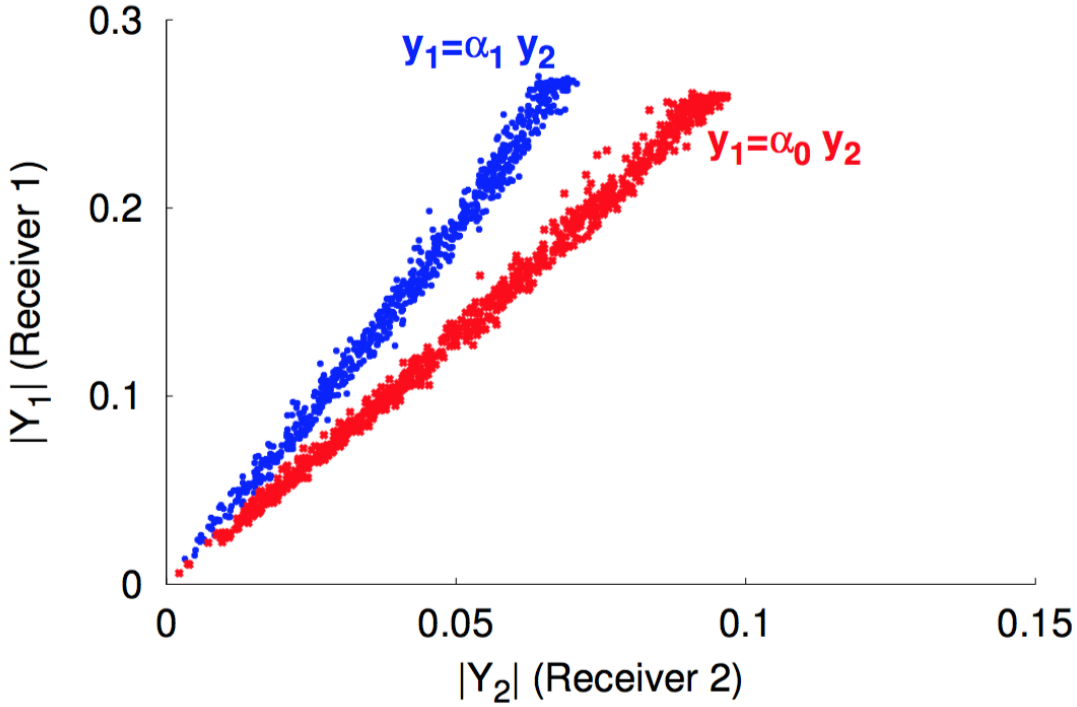
1st receiver: $Y_1(t) = h_{r1} \times \cancel{R(t)} + h_{c1} \times \cancel{R(t)} \times bits$

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

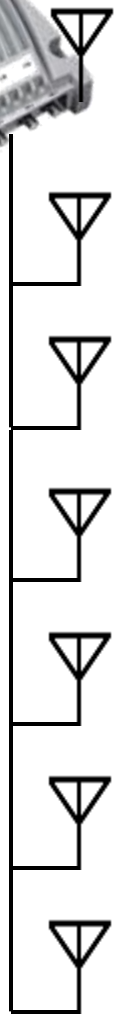
$$\frac{Y_1(t)}{Y_2(t)} = \frac{h_{r1} + h_{c1} \times bits}{h_{r2} + h_{c2} \times bits}$$

MIMO Eavesdropper

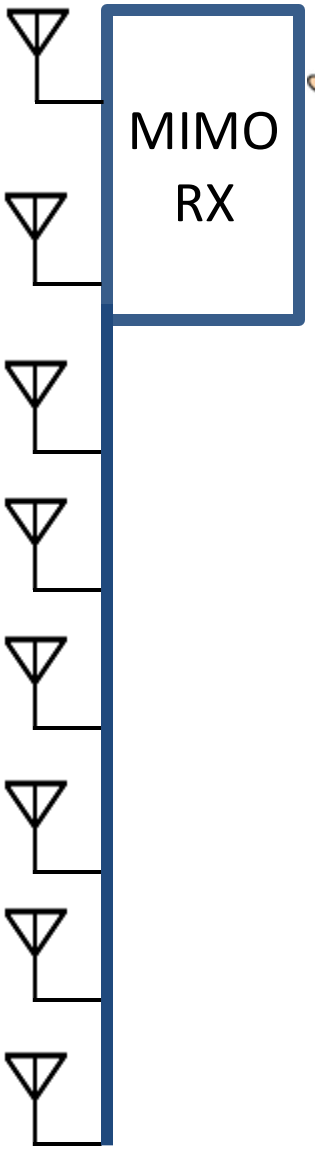
$$\begin{cases} \dfrac{h_{r1} + h_{c1}}{h_{r2} + h_{c2}} & if\ bit = 1 \\ \dfrac{h_{r1}}{h_{r2}} & if\ bit = 0 \end{cases}$$



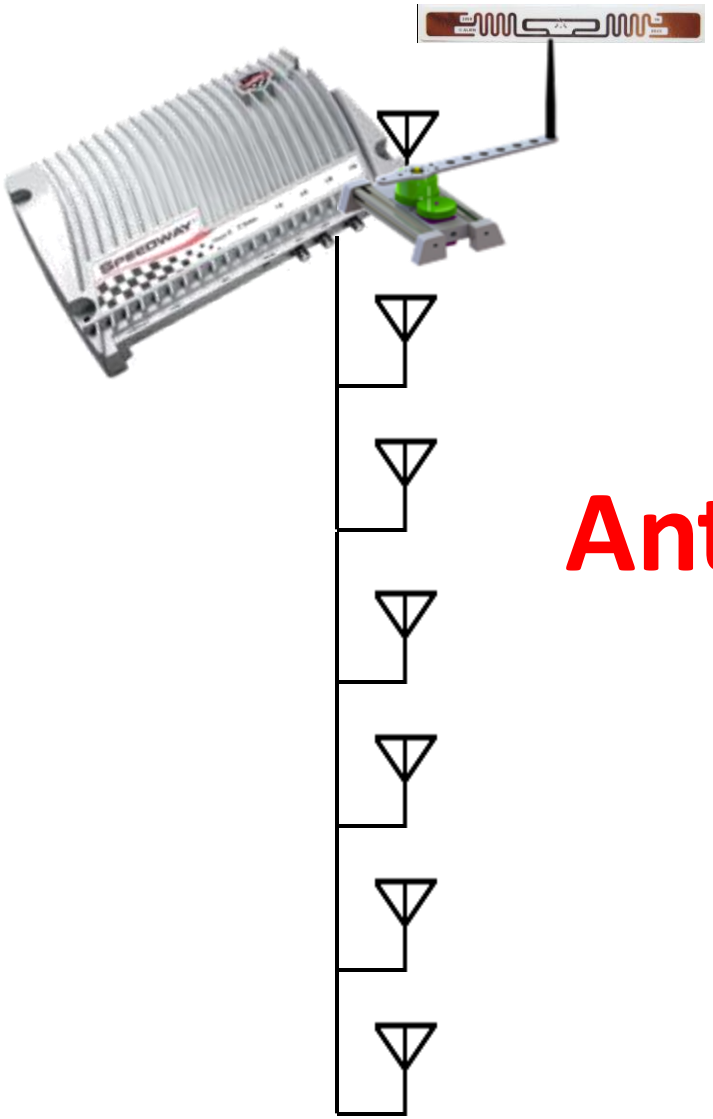
RF-Cloak vs MIMO Eavesdropper



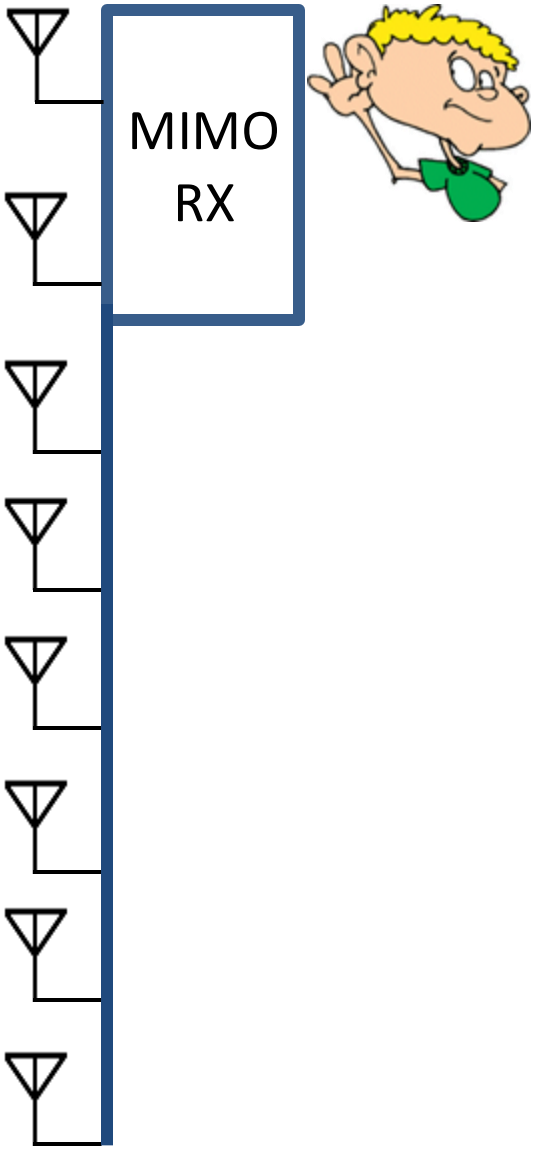
Antenna War!



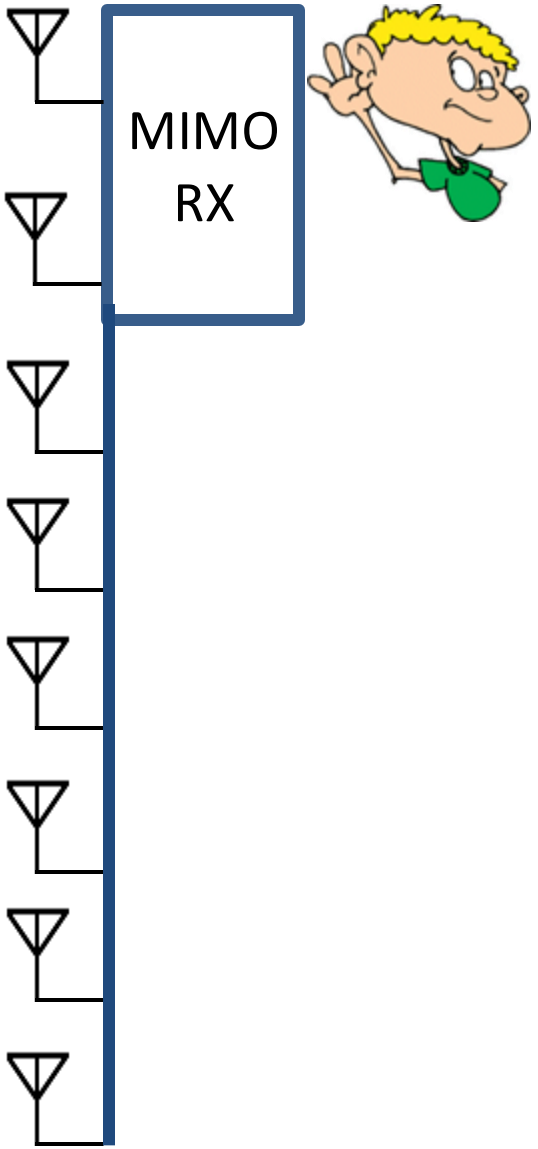
RF-Cloak vs MIMO Eavesdropper



Antenna War!



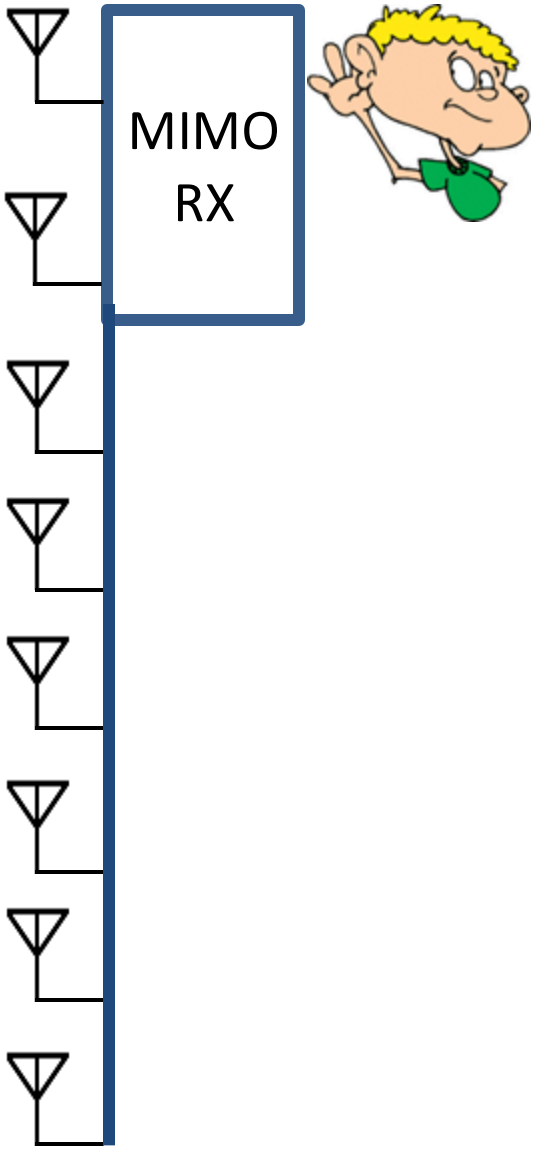
RF-Cloak vs MIMO Eavesdropper



RF-Cloak combines antenna motion and rapid antenna switching

→ Emulate a very large number of fast changing antennas

RF-Cloak vs MIMO Eavesdropper

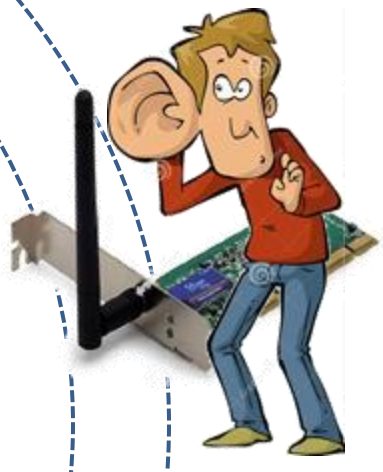


- Channels to eavesdropper change fast → Cannot separate RFID signal from Reader signal

- **Rotation → Periodic signal**
- **Motion → Slow**

→ Randomly switch between moving 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.

Vulnerability in WPA2
[SIGSAC'17]

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

Low power devices employ weak or no encryption.

Ultra-Low Power RFIDs
[S&P'09, CCS;09, Usenix'12, Defcon'13, NSDI'15]

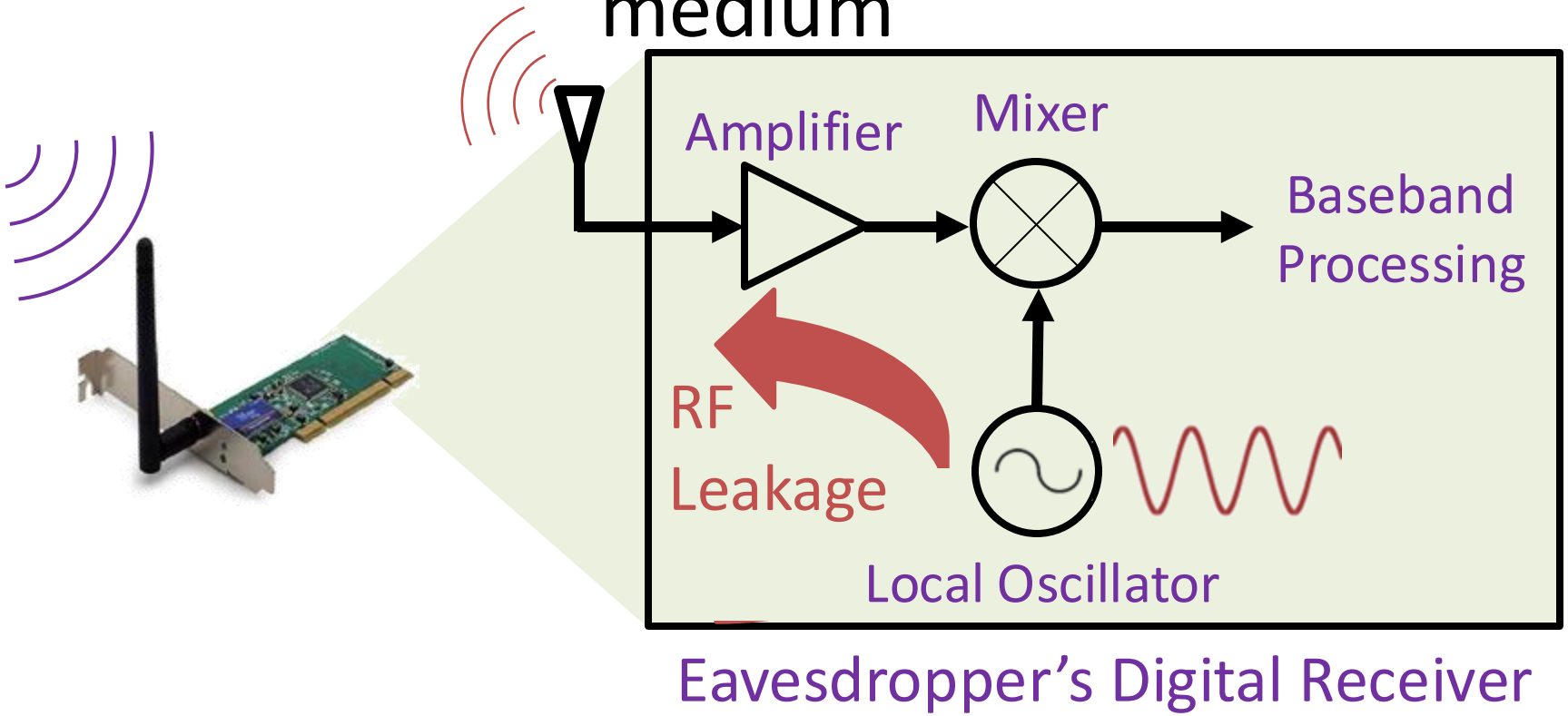
Medical Implants
[S&P'10, SIGCOMM'11]

Can we detect the hidden presence of wireless eavesdroppers?

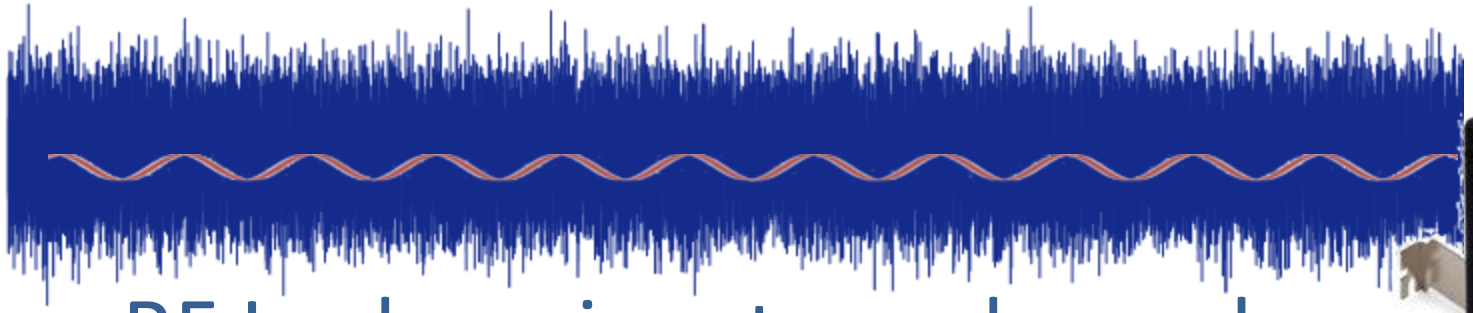
Ghostbuster

- 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.

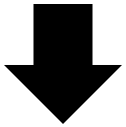
Key Observation: Even passive receivers leakage RF signals on to the wireless medium



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



RF Leakage is extremely weak:
buried under noise floor



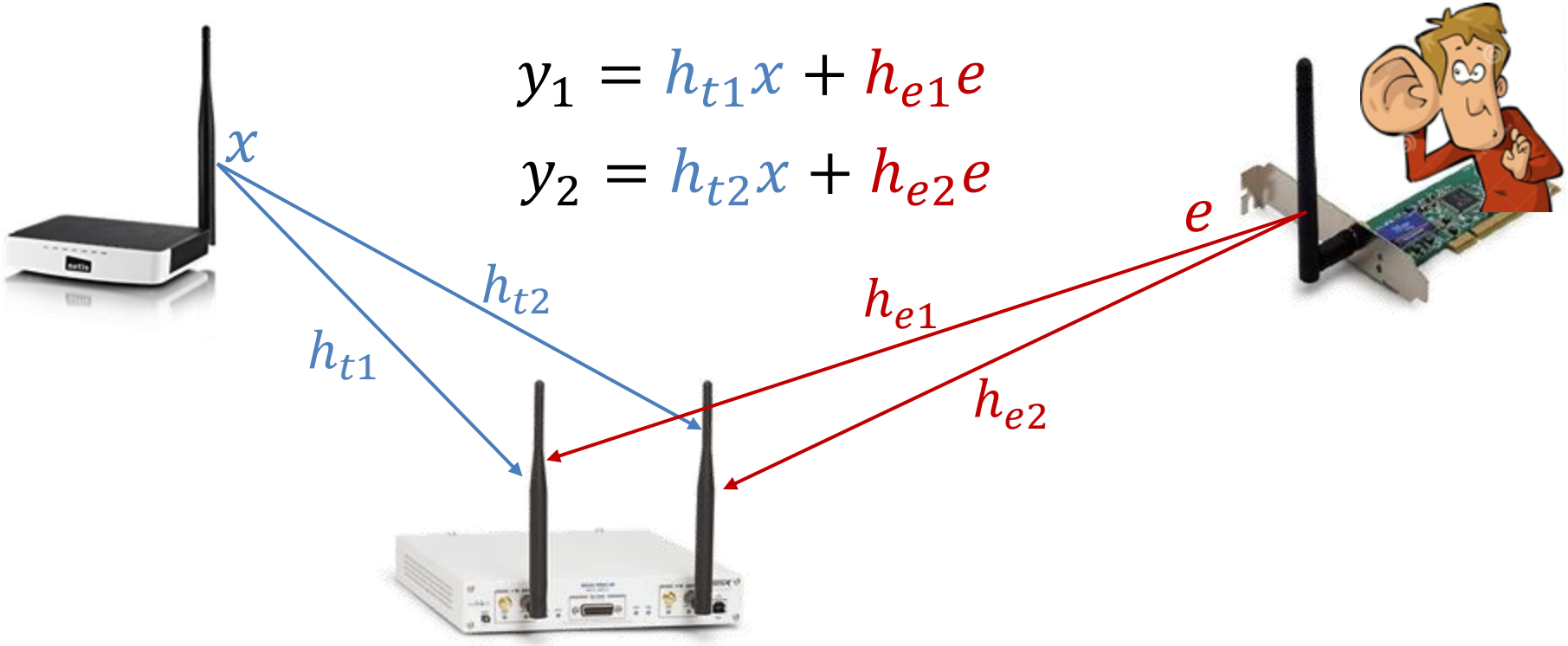
Hard to detect with today's receivers

Ghostbuster

Null On Going Transmissions using MIMO

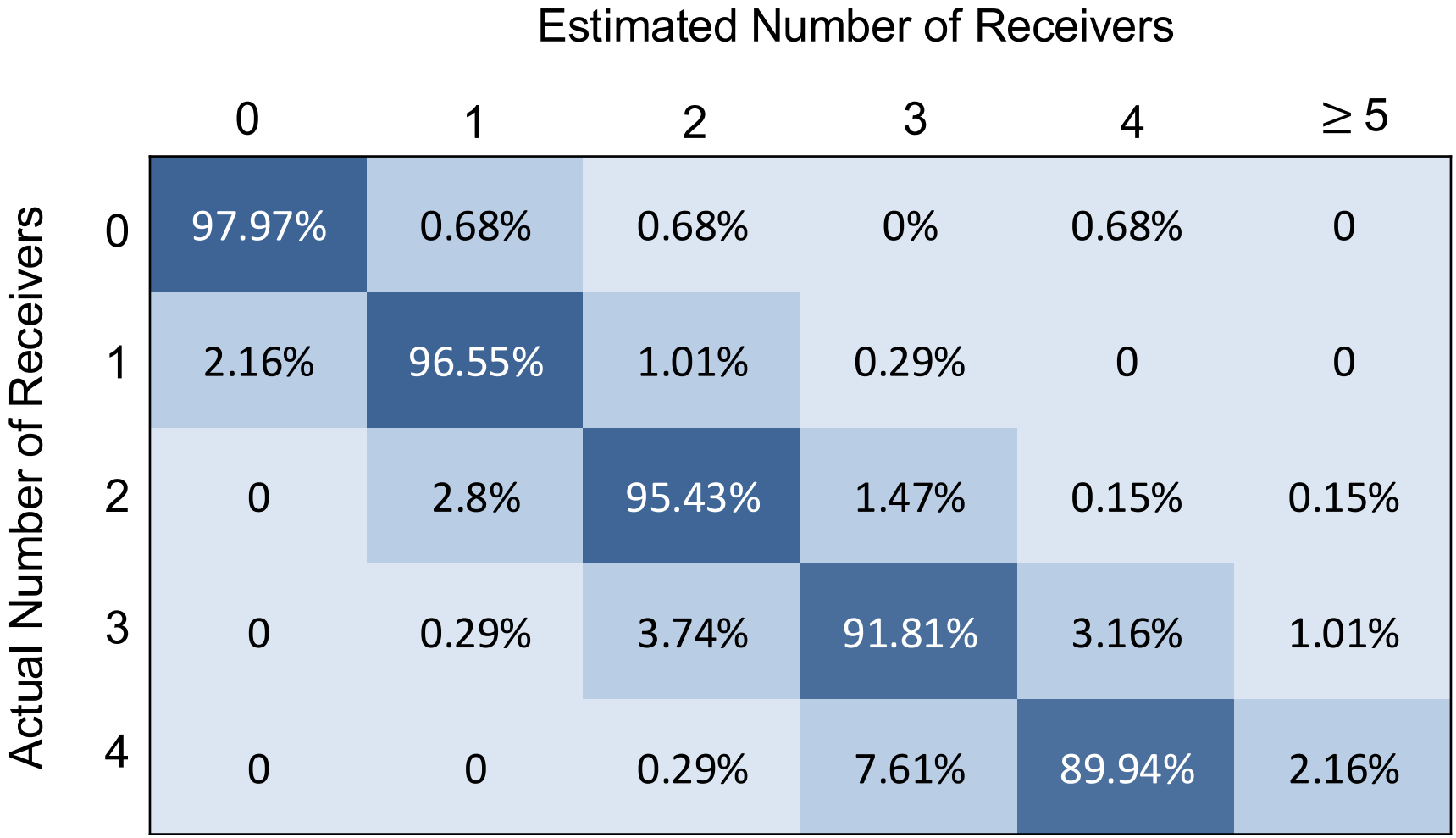
$$y_1 = h_{t1}x + h_{e1}e$$

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

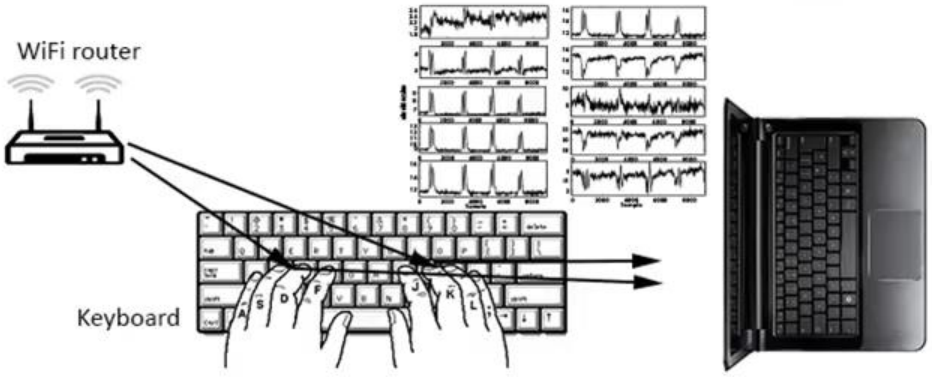


$$y_1 - \frac{h_{t1}}{h_{t2}} y_2 = \left(h_{e1} - \frac{h_{t1}}{h_{t2}} h_{e2} \right) e$$

In the presence of ongoing transmissions & other receivers.



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