

RF-Cloak: Securing RFID Cards Without Modifying them

Haitham Hassanieh

Jue Wang, Dina Katabi, Tadayoshi Kohno



Massachusetts
Institute of
Technology



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

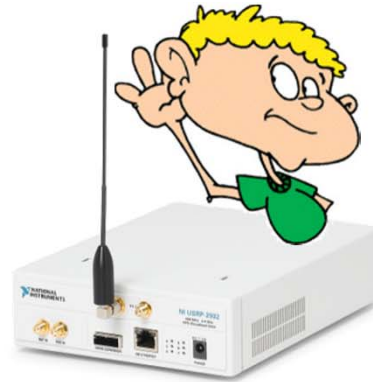
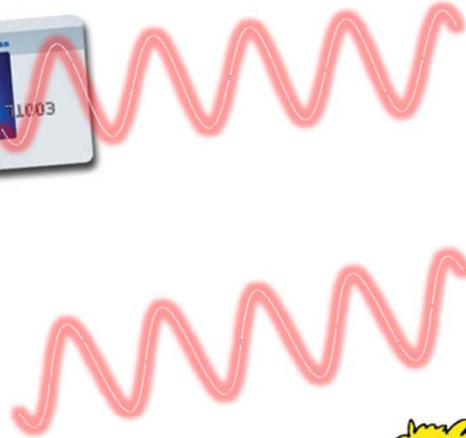
[Defcon'08, MIT'08,
S&P'09]

Hacking RFIDs for Dummies



The screenshot shows a web browser with several tabs open. The main content area displays a page titled "Live RFID Hacking System" from the website "OpenPCD". The page includes a navigation menu, a search bar, and a main heading "Live RFID Hacking System". Below the heading, there is a sub-heading "Bootable RFID Live Hacking System" and a paragraph of text describing the system. A yellow box highlights a note: "This RFID Live Hacking System is superseded by our OpenPCD 2 reader with libnfc - you can download the latest ISO image here. This page is only kept for historical reasons." Below this, there is a section titled "Our RFID hardware projects for RFID Security Analysis" with a list of links: "OpenPCD 2 RFID Reader for 13.56MHz", "OpenPICC RFID Emulator Project", and "OpenPICC SnifferOnly 13.56MHz". Another section titled "Suggested RFID Reader for MIFARE Classic key recovery for this live system" provides instructions on using the ACR122U102 Tikitag RFID reader. A "Note for touchatag reader users" section contains a code block with error messages: "0000012 ccid_usb.c:901:ccid_check_firmware() Firmware (1.00) is bogus! Upgrade the reader firmware or get a new reader.", "0000039 ifohandler.c:181:IPDwCreateChannel() failed", and "0000015 readerfactory.c:990:RFInitializeReader() Open Port 20000 failed". Below the code block, there is a note: "just edit /usr/local/openpcd/libpcc/drivers/lib-ccid.bundle/Contents/Info.plist - ifDriverOptions and set key from 0x0000 to 0x0005 to disable version checking." The page also includes a "Checksums" section with a list of hashes for various ISO images, such as "Fedora-15-x86_64-Live-RFID-v02.iso". At the bottom, there is a "Tools Installed" section and a "General Purpose Tools" section.

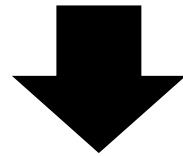
Hacking RFIDs Simply By Eavesdropping



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

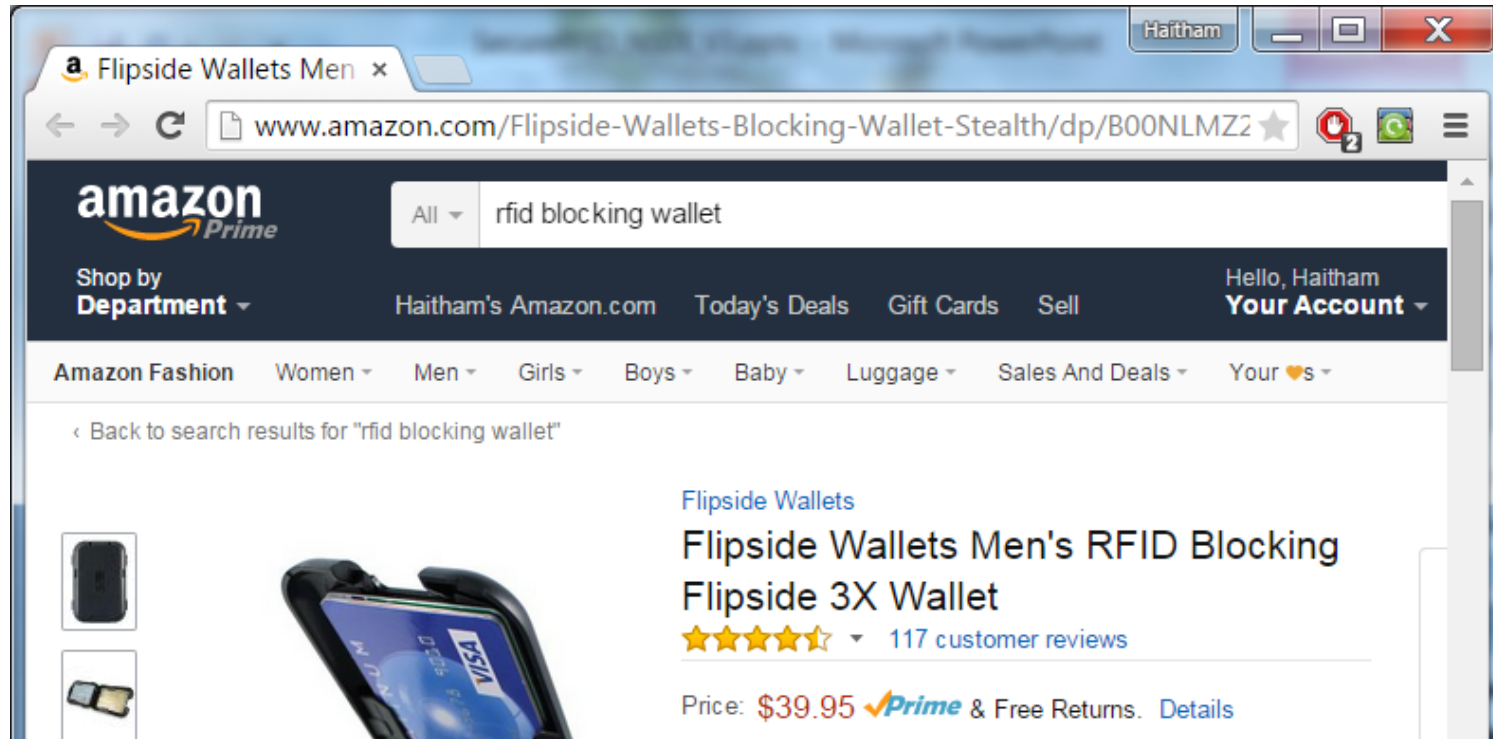
The screenshot shows a web browser window with the Amazon website. The address bar displays the URL: www.amazon.com/Flipside-Wallets-Blocking-Wallet-Stealth/dp/B00NLMZ2. The page features the Amazon Prime logo and a search bar containing the text "rfid blocking wallet". Navigation links include "Shop by Department", "Haitham's Amazon.com", "Today's Deals", "Gift Cards", "Sell", and "Hello, Haitham Your Account". A secondary navigation bar lists categories like "Amazon Fashion", "Women", "Men", "Girls", "Boys", "Baby", "Luggage", "Sales And Deals", and "Your ♥s".

The main content area shows search results for "rfid blocking wallet". The primary product is the "Flipside Wallets Men's RFID Blocking Flipside 3X Wallet". The product image shows a black wallet open, revealing a blue Visa card and a stack of US dollar bills. A vertical strip of smaller images on the left allows for zooming in on the product. Below the main image is a heart icon and the text "Roll over image to zoom in".

The product details include the brand "Flipside Wallets", the title "Flipside Wallets Men's RFID Blocking Flipside 3X Wallet", a star rating of 4.5 stars from 117 customer reviews, and a price of \$39.95 with Prime and free returns. The size is listed as "One Size" and the color as "Stealth". A color selection area shows three options: black (selected), dark grey, and red, each with a price of \$39.95 and Prime eligibility. A white option is also visible below.

The status is "In Stock", sold by Flipside Wallets and fulfilled by Amazon. A delivery notice states: "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



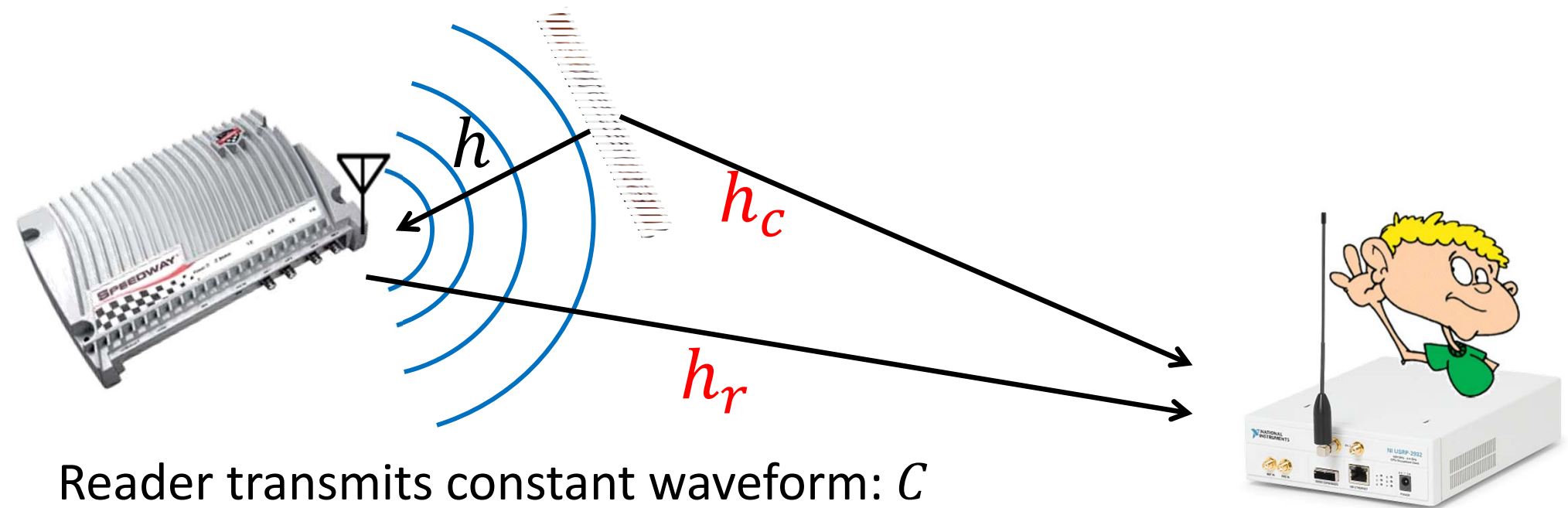
Need solution for eavesdropping that works with existing RFIDs

RF-Cloak

System that protects RFIDs against eavesdropping attacks

- Does not require any modification to the RFID cards
- Protects against a wide range of attackers including multi-antenna MIMO eavesdroppers
- Theoretically proven the security guarantees
- Implemented the system and empirically demonstrated its benefits

RFID Communication



Reader transmits constant waveform: C

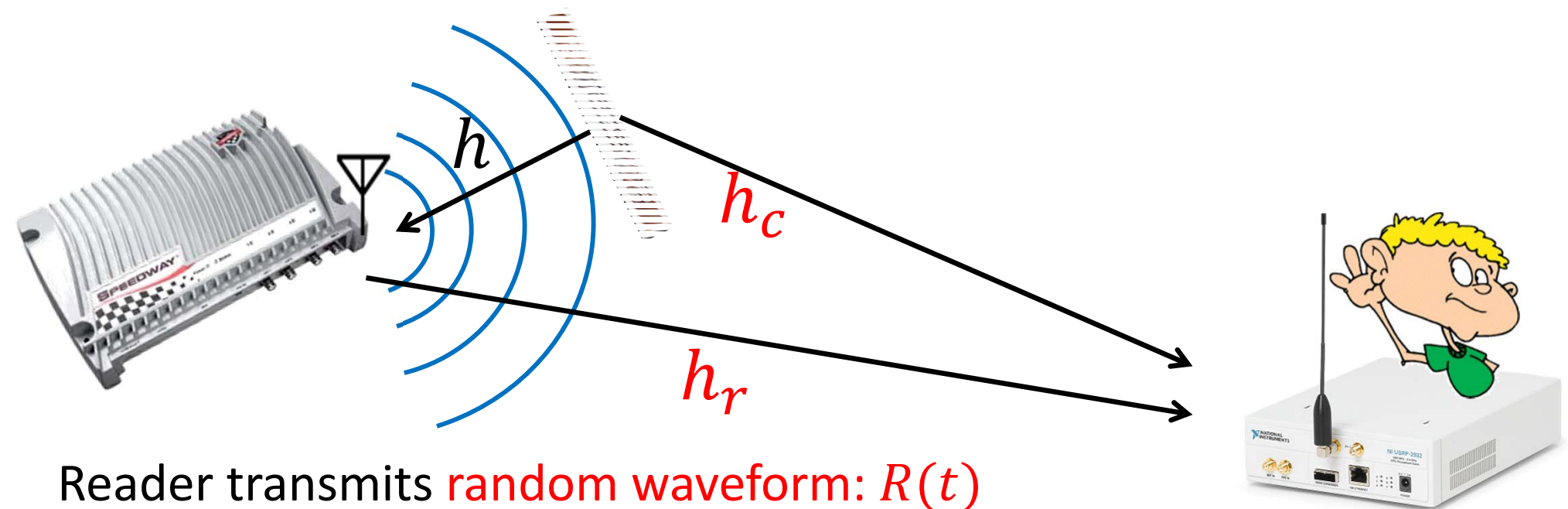
RFID reflects the reader's signal using ON-OFF switch

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: $R(t)$**

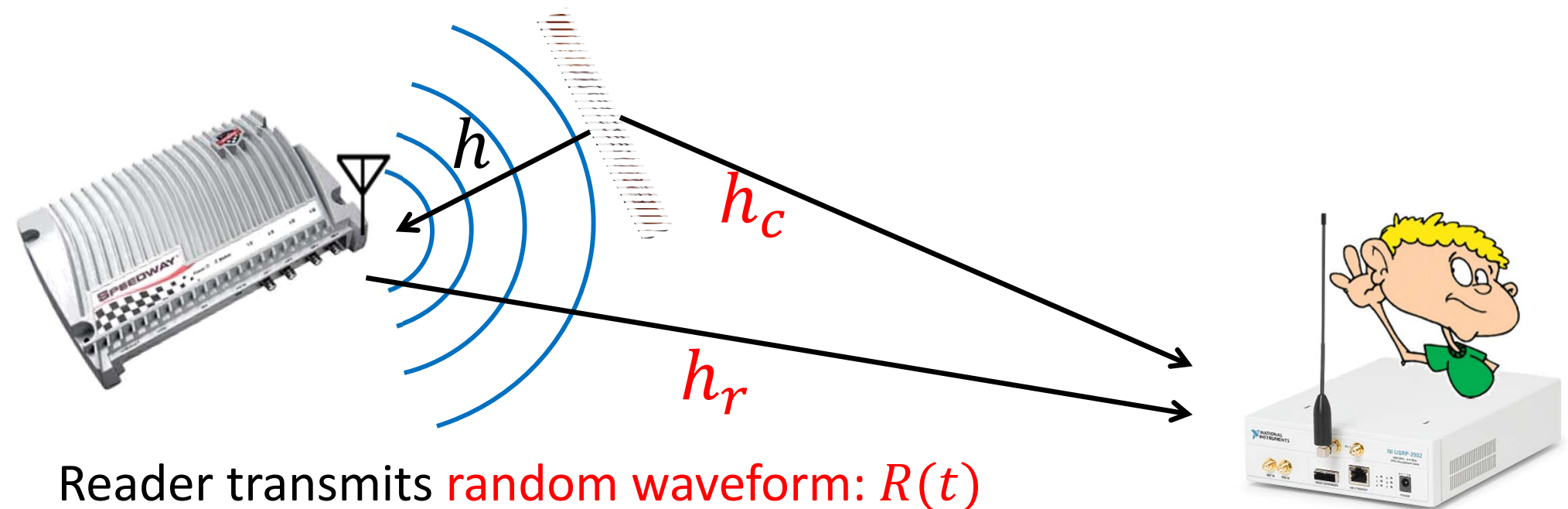
RFID reflects the reader's signal using ON-OFF switch

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

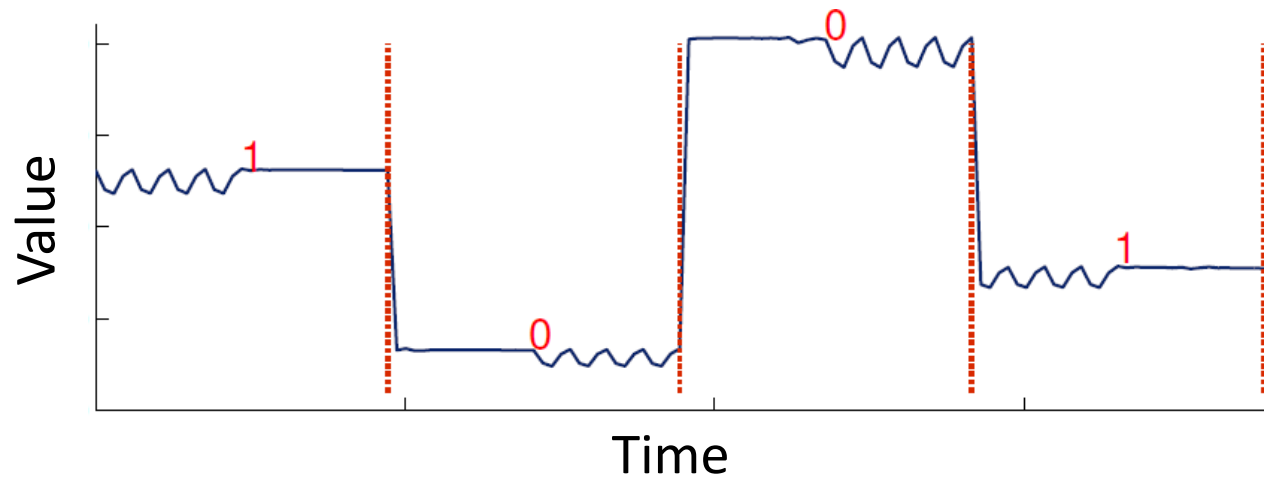
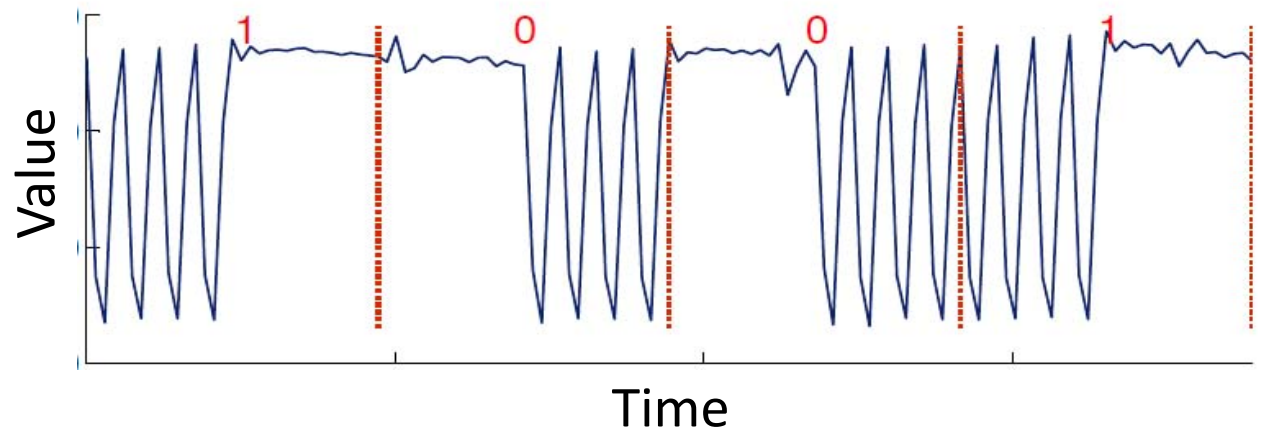
Reader knows $R(t) \rightarrow$ Can decode

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

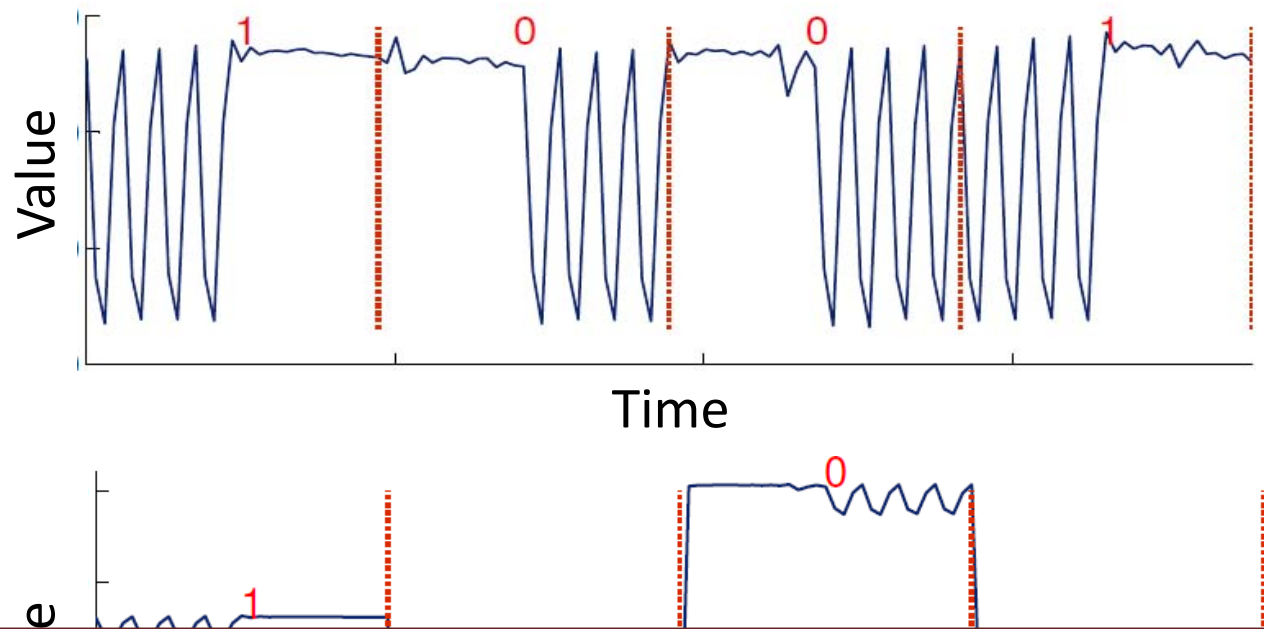
RFID Signal:



RF-Cloak: Randomizing the Reader's Signal

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

RFID Signal:

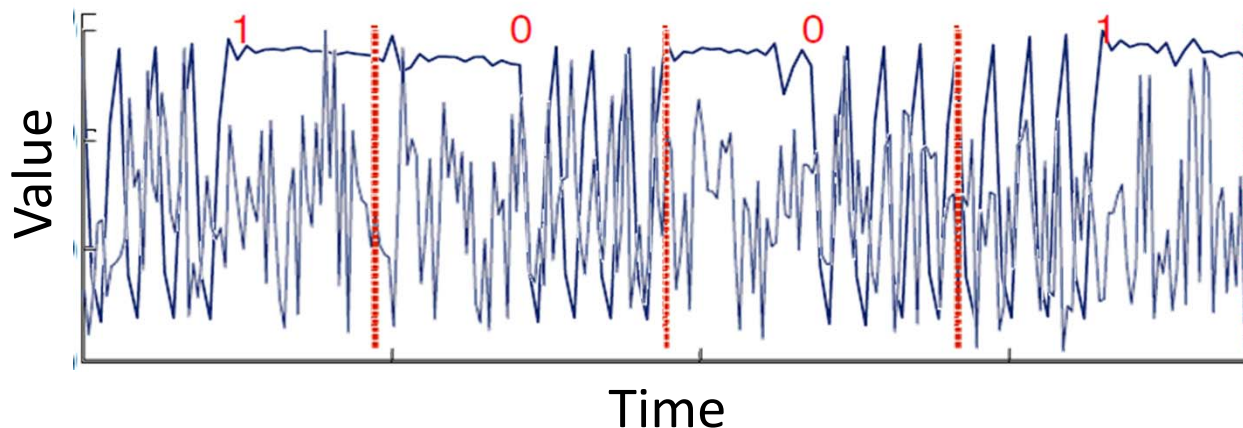
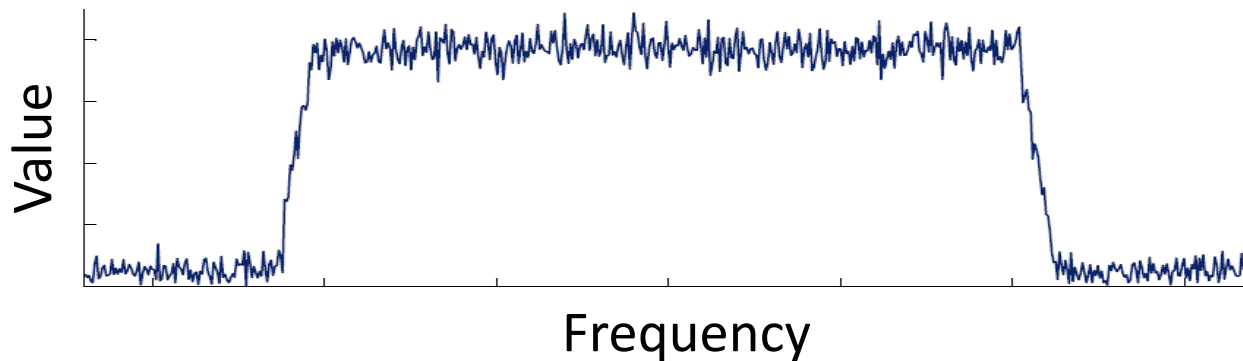


Random waveform must destroy internal signal patterns of the bits

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



RF-Cloak: Randomizing the Reader's Signal

Threat model:

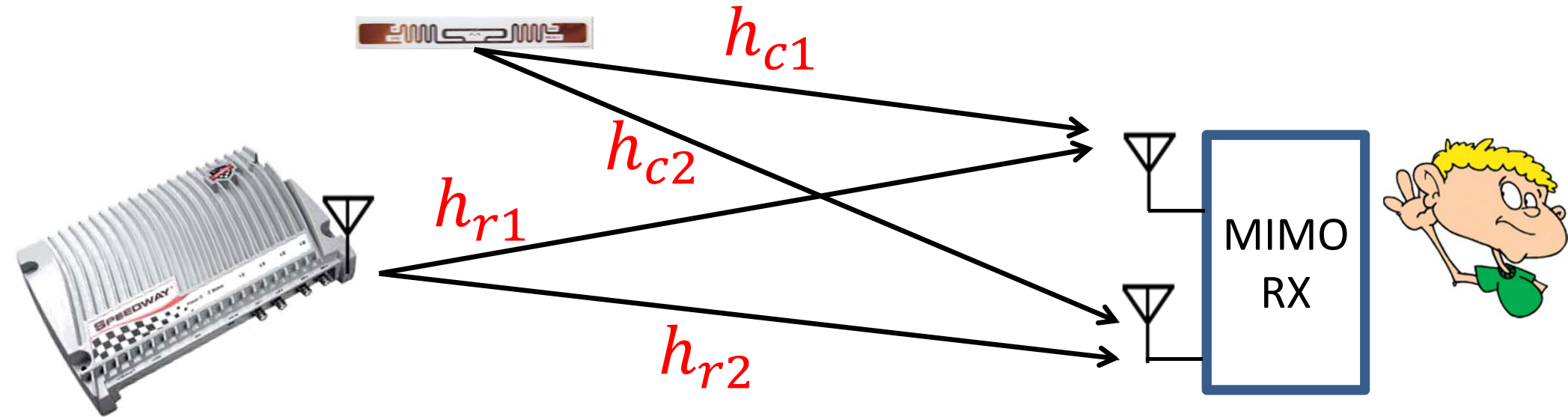
Single antenna eavesdropper using the optimal decoder

Guarantee: (informally restated)

Theorem 1: Using RF-Cloak's random signal $R(t)$, an eavesdropper will not be able to distinguish a 0 bit from a 1 bit which is no better than a random guess

What if the attacker has multi-antenna
MIMO capability?

MIMO Eavesdropper



Reader transmits random waveform: $R(t)$

Eavesdropper receives:

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

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

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

MIMO Eavesdropper

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

Reader transmits random waveform: $R(t)$

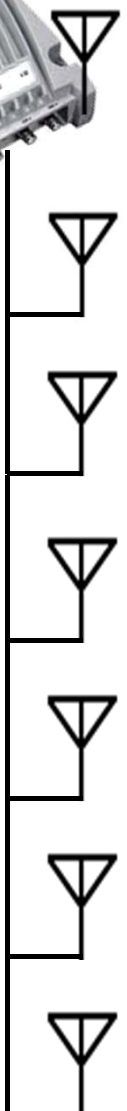
Eavesdropper receives:

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

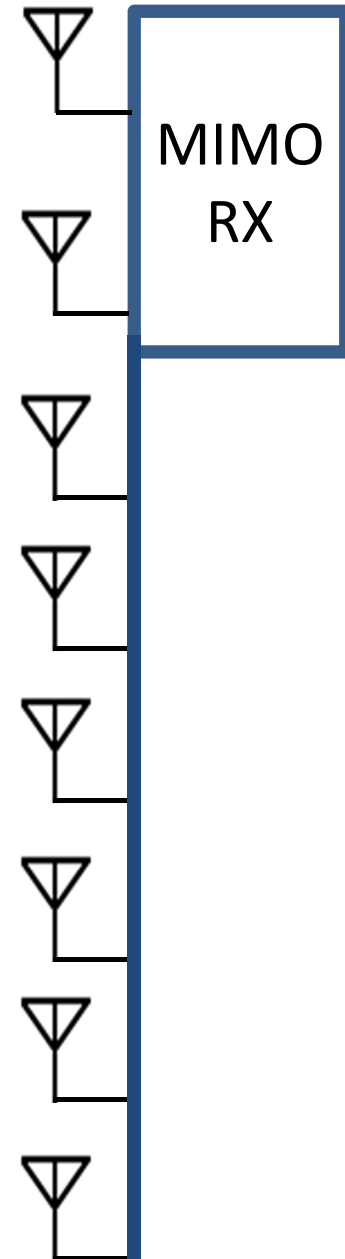
$$2^{\text{nd}} \text{ receiver: } Y_2(t) = h_{r2} \times \cancel{R(t)} + h_{c2} \times \cancel{R(t)} \times \text{bits}$$

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

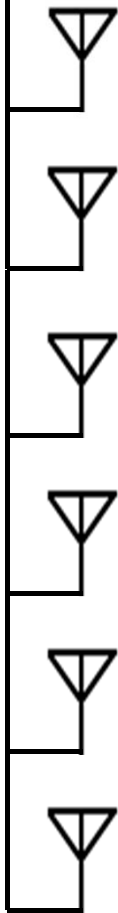
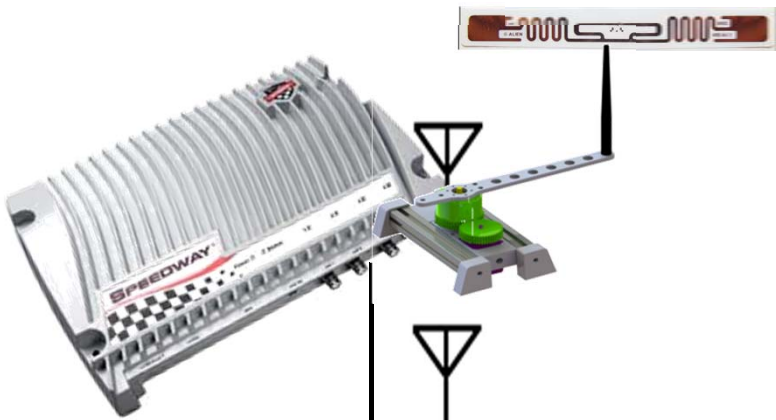
RF-Cloak vs MIMO Eavesdropper



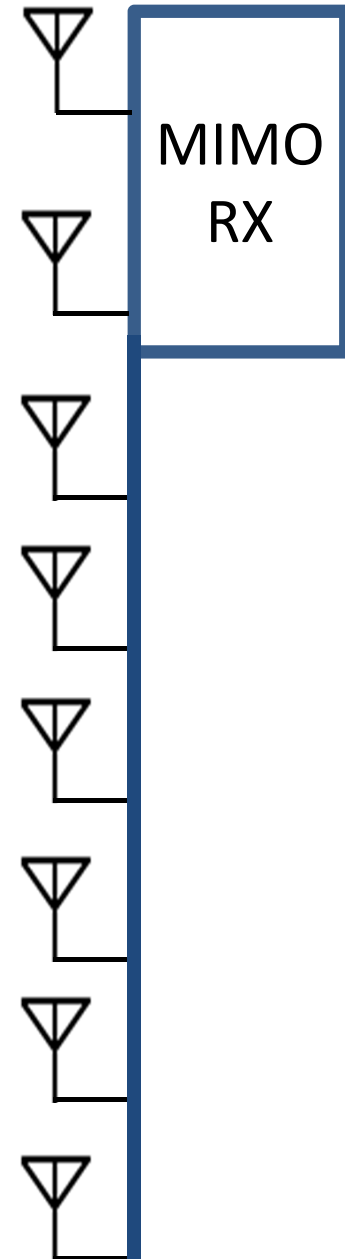
Antenna War!



RF-Cloak vs MIMO Eavesdropper



Antenna War!

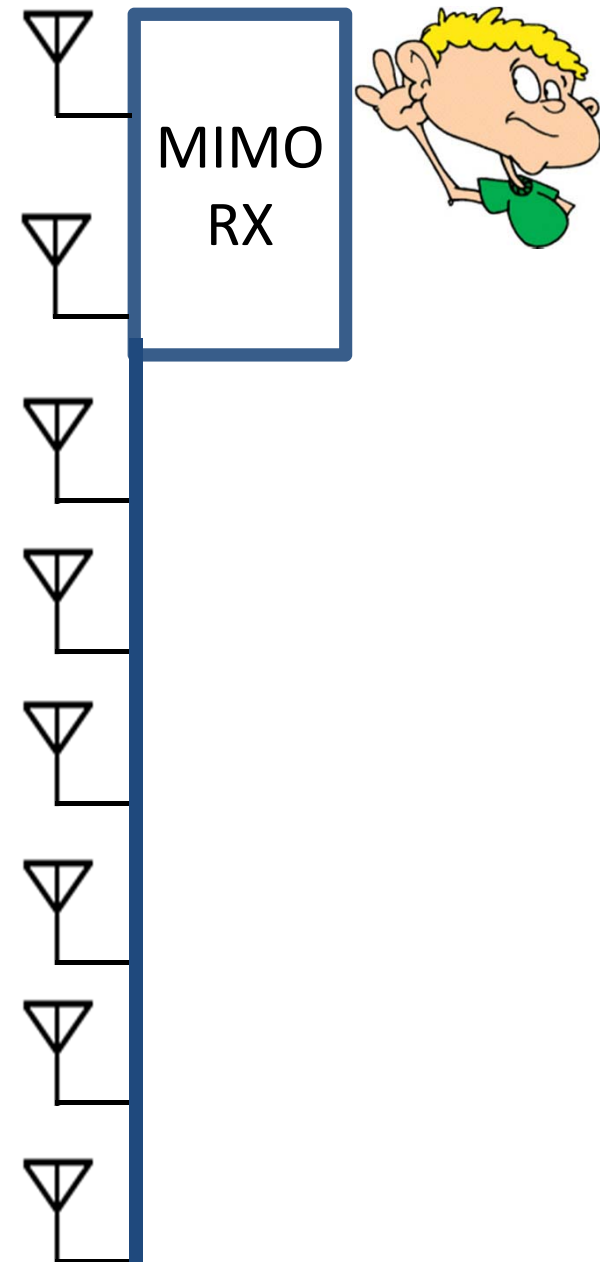


RF-Cloak vs MIMO Eavesdropper



RF-Cloak combines antenna motion and rapid antenna switching

→ Emulate a very large number of fast changing antennas



RF-Cloak vs MIMO Eavesdropper

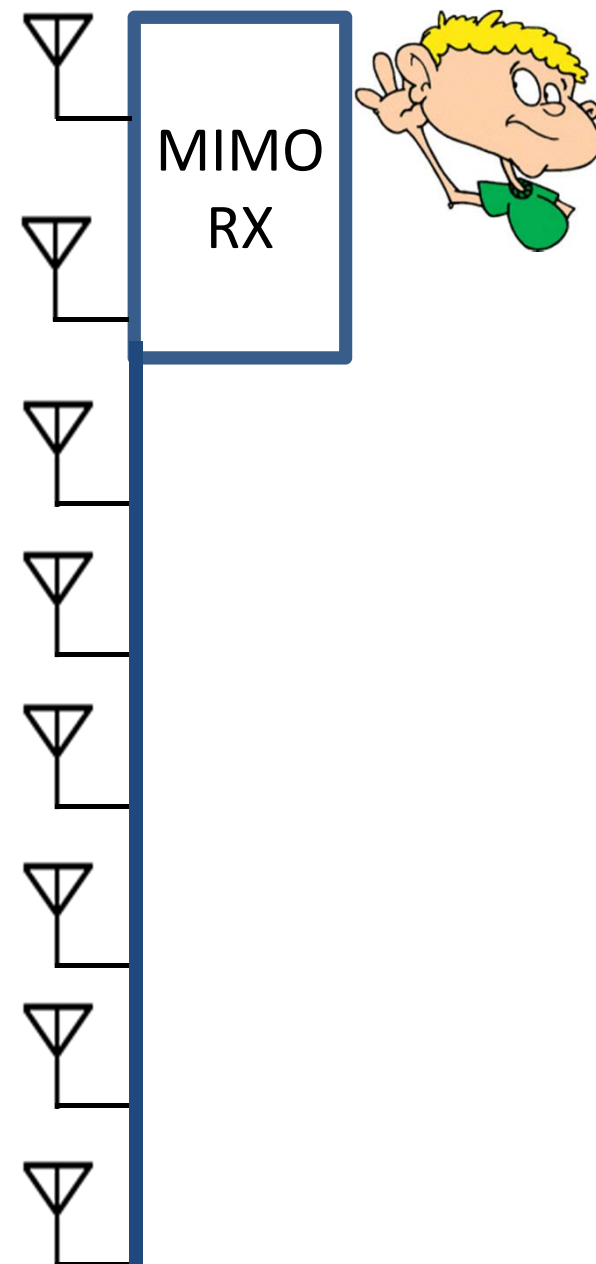


- Channels to eavesdropper change very fast → Cannot separate RFID signal from Reader signal

→ Cannot decode

- Reader (full duplex) → Only receives reflection from RFID

→ Can decode



RF-Cloak: Randomizing the Wireless Channel

Threat model:

Multi-antenna MIMO eavesdropper using the optimal decoder.

Guarantee: (informally restated)

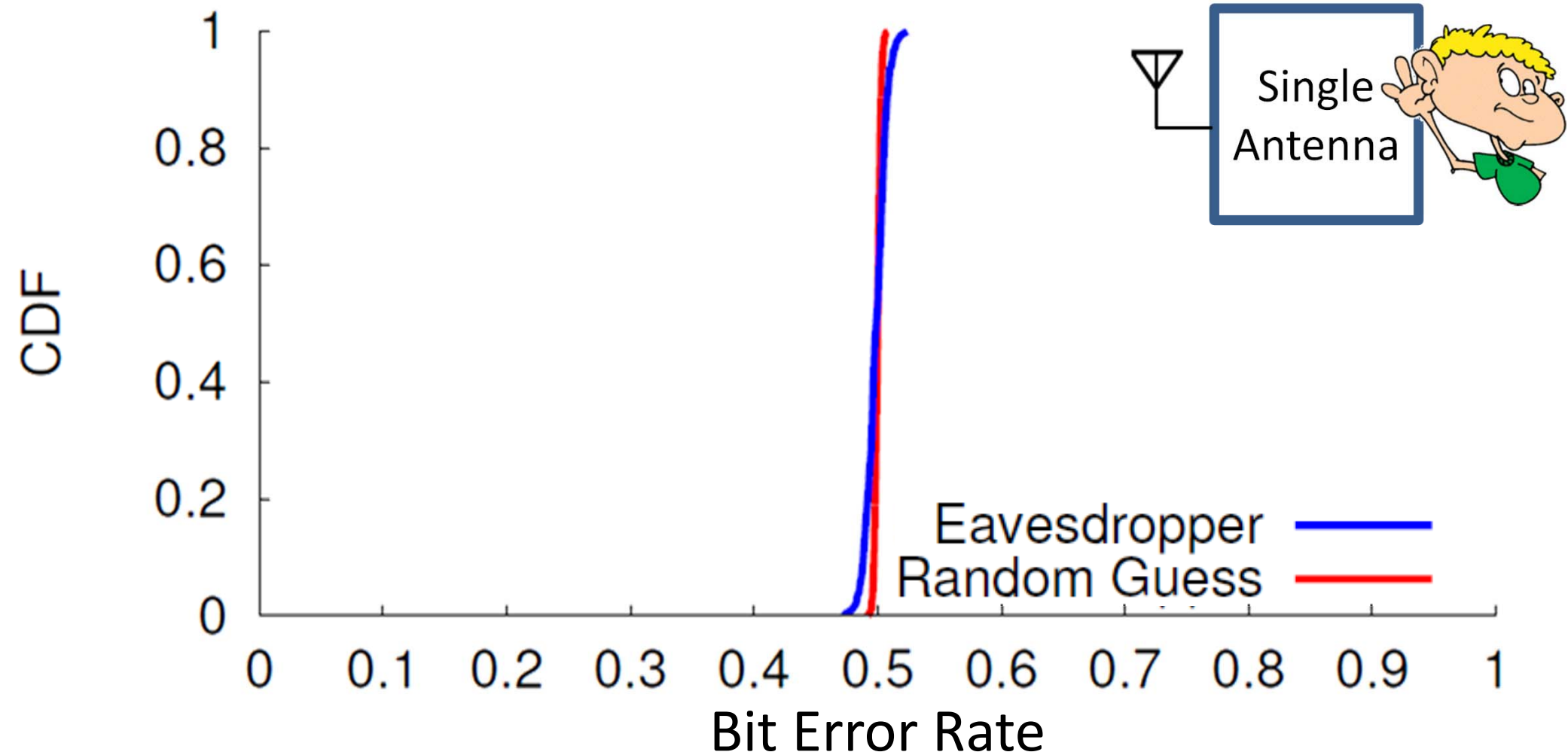
Theorem 2: Using RF-Cloak's channel randomization, a MIMO eavesdropper will not be able to distinguish a 0 bit from a 1 bit which is no better than a random guess

Evaluation

- Implemented RF-Cloak on USRP N210 software radios and combined it with a 1725 rpm motor and ADG904R RF switches.
- Evaluated it against different types of commercial RFID cards
- Evaluation metric : Bit error rate (BER)

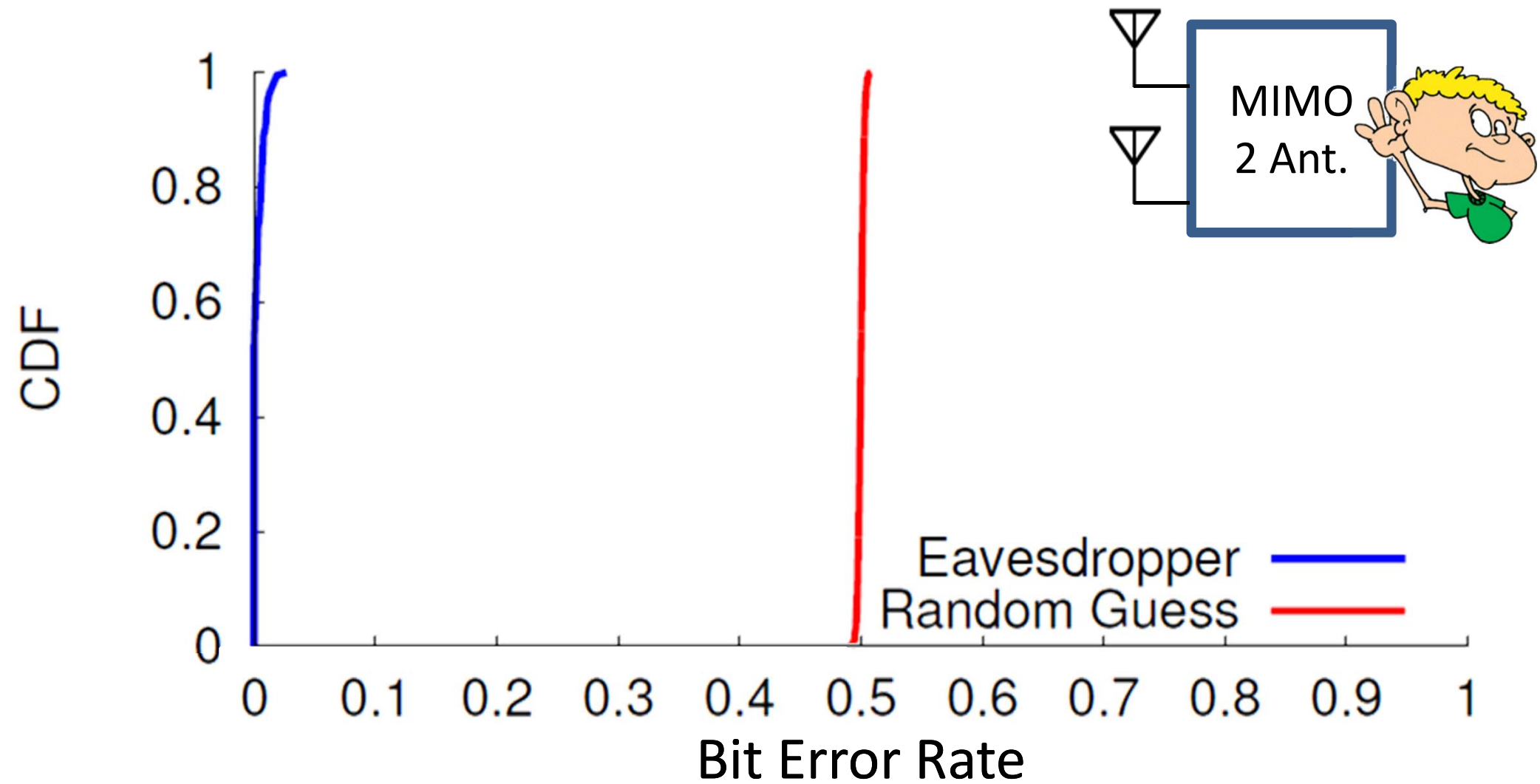


RF-Cloak Random Waveform vs Single Antenna Eavesdropper



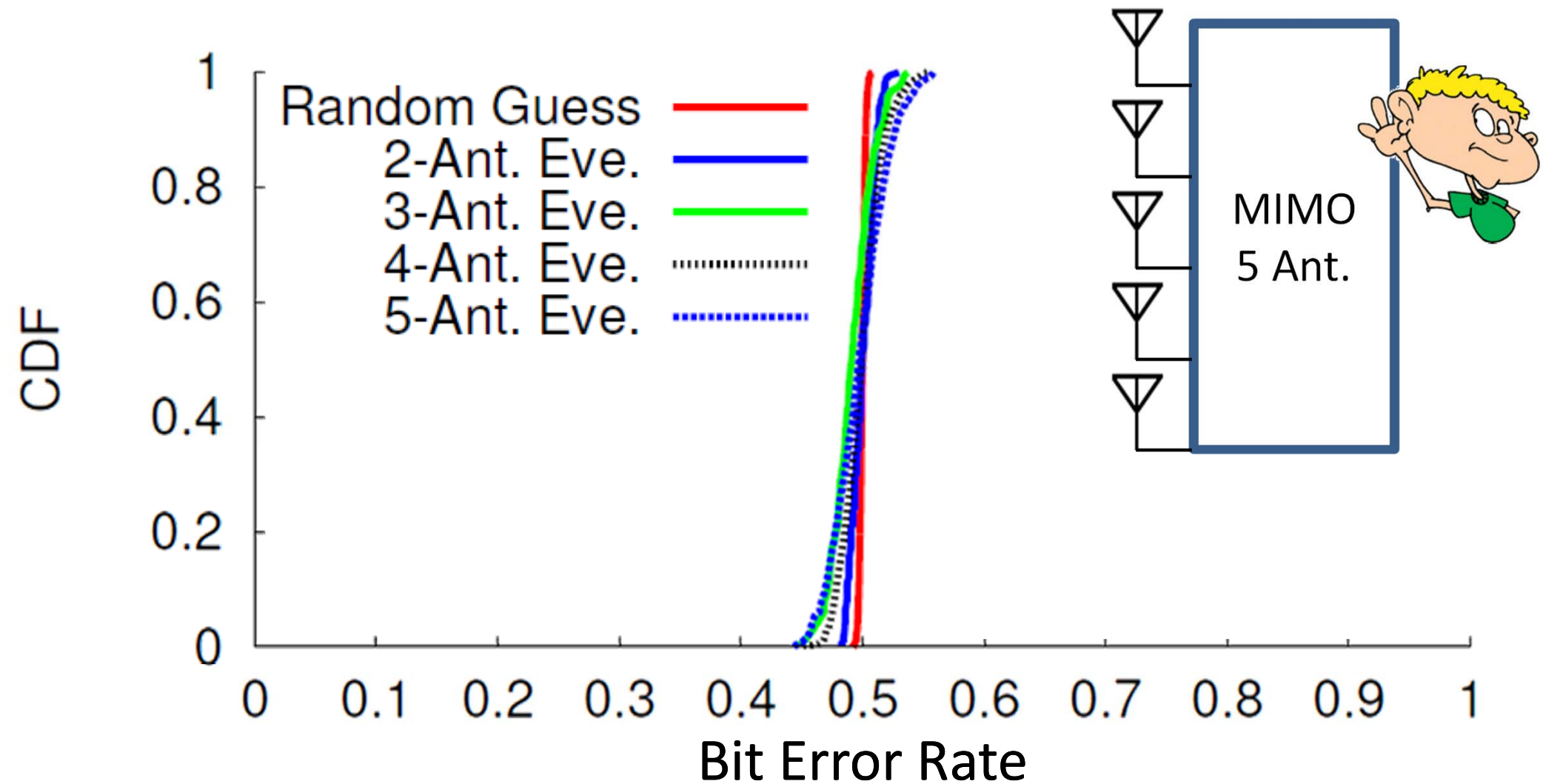
Eavesdropper has mean BER of 0.498 with std. dev. 0.008
→ Very close to a random guess

RF-Cloak Random Waveform vs Two Antenna MIMO Eavesdropper



A two-antenna MIMO eavesdropper can correctly decode the RFID bits

RF-Cloak Channel Randomization vs MIMO Eavesdropper



RF-Cloak can prevent a MIMO eavesdropper from decoding the RFID's data

Related Work

- **Physical layer security:**

[JCM'07, TCOM'13, SIGCOMM'11, Oakland'13, ICC'12, INFOCOM'11, MobiSys'13, SIGCOMM'13, MobiSys'14]

- **Securing RFIDs against eavesdropping:**

[CHES'07, RFIDSec'11, CARDIS'06, JRSC'12, PerCom'07]

- **Moving antennas:**

[SIGCOMM'14, MOBICOM'14, HOTNETS'14, MOBICOM'13, SIGCOM'13, HotMobile'12, ISJ'14]

Conclusion

- RF-Cloak is the first system that can protect deployed RFIDs against eavesdropping without any modification to the RFID
- RF-Cloak is the first system that can hide the signal from MIMO attacker with many antennas even when the reader has no MIMO capability.
- RF-Cloak provides a defense in depth solution.