MIT Proximity Card Vulnerabilities

Josh Mandel, Austin Roach, Keith Winstein

{jmandel, aroach, keithw}@mit.edu

CSAIL, Radio Society, SIPB

Introduction

- We analyzed MIT proximity card and magstripe encoding, built long-range prox reader and card mimic.
  - Can proximity cards be read remotely?
  - How far away?
  - Can we copy a proximity card?
  - Can we steal TechCASH by reading a proximity card?

Introduction

- We analyzed MIT proximity card and magstripe encoding, built long-range prox reader and card mimic.
  - Can proximity cards be read remotely?
    Yes.
  - How far away?
  - Can we copy a proximity card?
  - Can we steal TechCASH by reading a proximity card?

Introduction

- We analyzed MIT proximity card and magstripe encoding, built long-range prox reader and card mimic.
  - Can proximity cards be read remotely?
    Yes.
  - How far away?
    Several feet.
  - Can we copy a proximity card?
  - Can we steal TechCASH by reading a proximity card?

Introduction

- We analyzed MIT proximity card and magstripe encoding, built long-range prox reader and card mimic.
  - Can proximity cards be read remotely?
    Yes.
  - How far away?
    Several feet.
  - Can we copy a proximity card?
    Yes. System uses passive authentication, not challenge-response.
  - Can we steal TechCASH by reading a proximity card?

Introduction

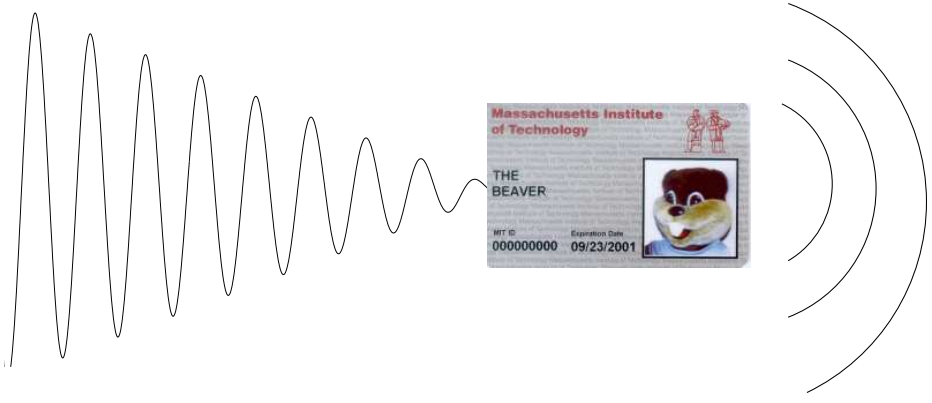
- We analyzed MIT proximity card and magstripe encoding, built long-range prox reader and card mimic.
  - Can proximity cards be read remotely?
    Yes.
  - How far away?
    Several feet.
  - Can we copy a proximity card?
    Yes. System uses passive authentication, not challenge-response.
  - Can we steal TechCASH by reading a proximity card?
    Yes. Card data is not encrypted. Prox card ID can be converted to magstripe.

Recommendations

- Don’t use prox card for monetary transactions or high-security areas. Remove from nuclear reactor.
- Split magstripe ID and prox ID. Don’t depend on Indala FlexSecur to keep magstripe ID secret.
- Recall issued proximity cards and rewrite magstripes.
- Incorporate local experts in procurement process.
- Instead of prox readers, consider magstripe readers or prox readers with PIN keypad.

Findings: Reading the Card

- Card is powered by 125 kilohertz sine wave.
- Card responds with AM broadcast of bits.
- Broadcast can be received with modified AM radio or oscilloscope.



"1011100010101101..."
"1011100010101101..."
"1011100010101101..."
"1011100010101101..."

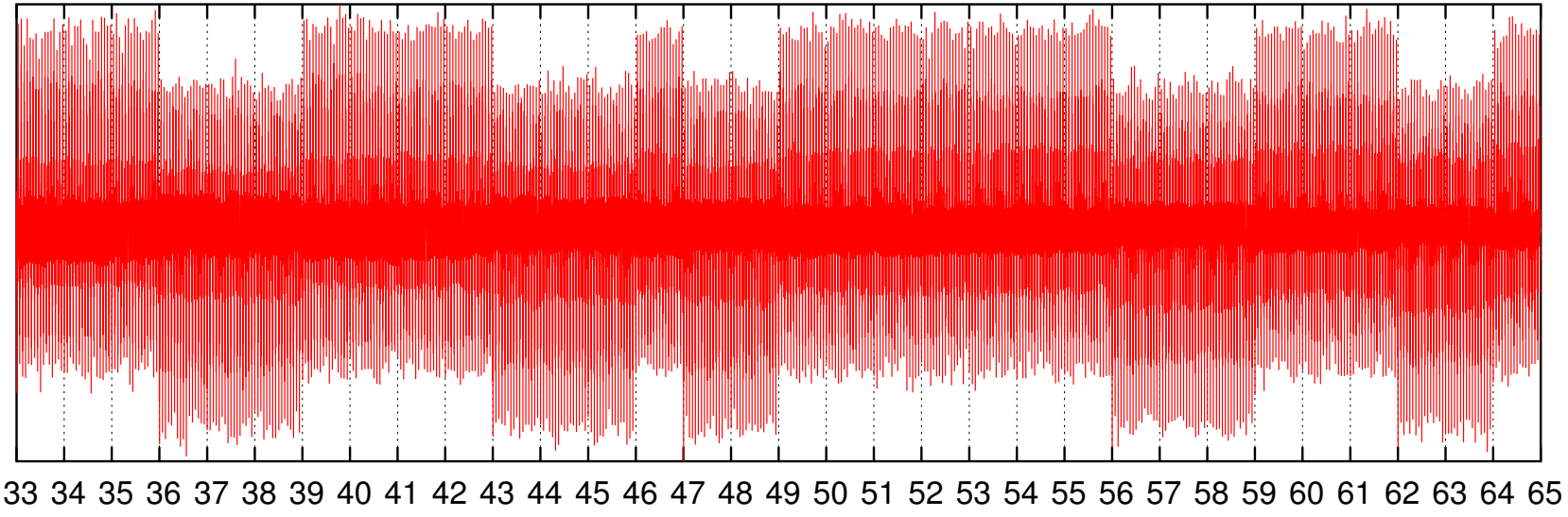
125 kilohertz (in)

AM broadcast (out)

Findings: Card Contents

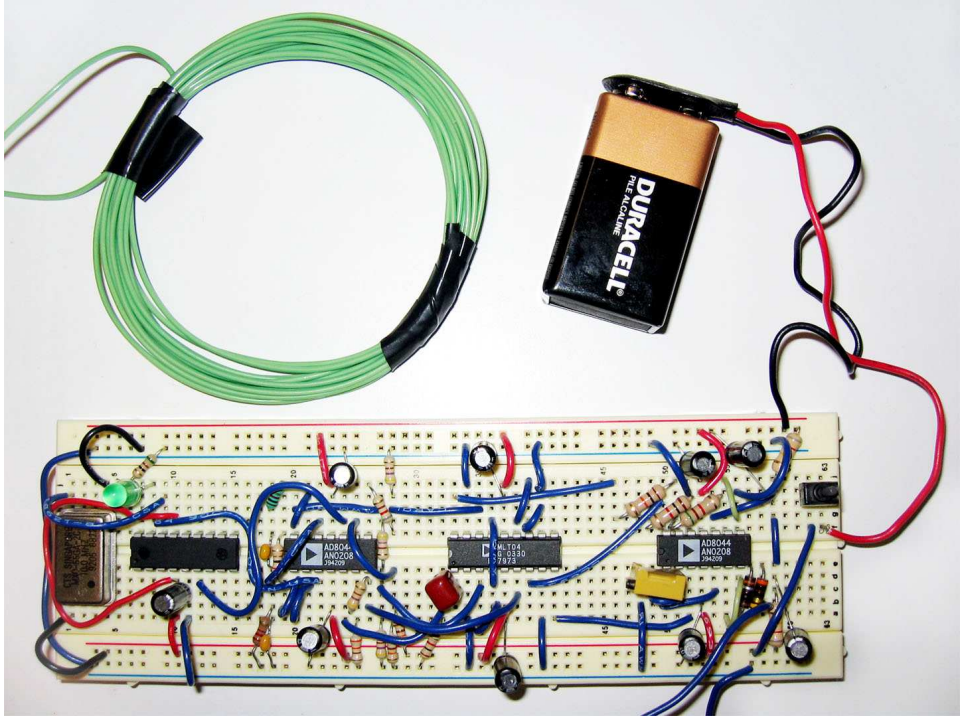
- Card broadcasts 224 bits and repeats over and over.
- 30 zeros + 22 constant + 172 user bits = 224 total bits
- Of 172 user bits, only 32 vary among cards we have seen. Rest are constant.

- Example broadcast (Austin's card):



Findings: Mimicking a Card

- If we record the broadcast and replay it to a door, does the door open?
- To find out, we built an AM transmitter for $30.



- Result: door opens. (Building 4 piano lab.)

Findings: Card Security

- System does not use active authentication. Card is just a string of 32 ones and zeros.

Findings: Card Security

- System does not use active authentication. Card is just a string of 32 ones and zeros.
- System is not challenge-response. Card sends exact same 32 bits each time.

Findings: Card Security

- System does not use active authentication. Card is just a string of 32 ones and zeros.
- System is not challenge-response. Card sends exact same 32 bits each time.
- Card is easy to read from close range. Just need wire and 6.002 lab equipment.

Findings: Card Security

- System does not use active authentication. Card is just a string of 32 ones and zeros.
- System is not challenge-response. Card sends exact same 32 bits each time.
- Card is easy to read from close range. Just need wire and 6.002 lab equipment.
- Card is easy to mimic. Just record AM broadcast, and replay it.

Findings: Card Security

- System does not use active authentication. Card is just a string of 32 ones and zeros.
- System is not challenge-response. Card sends exact same 32 bits each time.
- Card is easy to read from close range. Just need wire and 6.002 lab equipment.
- Card is easy to mimic. Just record AM broadcast, and replay it.
- AM transmitter costs $30 to build. This is cheaper than magstripe writer, which costs about $250.

Findings: Reading Range

- If card is close enough to reader, user can be tracked and card copied. This is less secure than magnetic stripes, which require physical possession to copy.
- How close is close enough?
- So far, our receiver works two feet away.
- Future: we think five feet is realistic.
- Tradeoff between time and range. Longer time spent reading yields longer range.

Findings: Indala FlexSecur

- Reader and mimic let us copy proximity card, track users.
- Can they also steal a TechCASH account? Only with magnetic stripe.
- Proximity card's 32 bits appear to contain a transformed version of 9-digit magstripe ID, encoded with Indala's FlexSecur "data encryption."

Findings: Indala FlexSecur

- Reader and mimic let us copy proximity card, track users.
- Can they also steal a TechCASH account? Only with magnetic stripe.
- Proximity card's 32 bits appear to contain a transformed version of 9-digit magstripe ID, encoded with Indala's FlexSecur "data encryption."
- FlexSecur is actually just addition and rearrangement, not encryption.

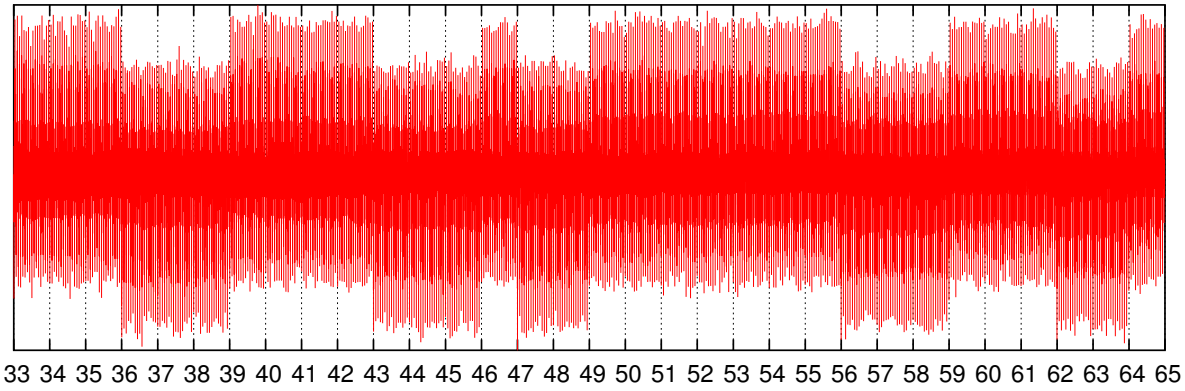
Findings: Decoding FlexSecur

- We collected magstripes and prox IDs from 8 people.
- Similar prox IDs produce similar magstripes.
- Tried to find patterns to predict magstripe from prox ID.
- Took 10 hours to find the encoding:

Findings: Decoding FlexSecur

- We collected magstripes and prox IDs from 8 people.
- Similar prox IDs produce similar magstripes.
- Tried to find patterns to predict magstripe from prox ID.
- Took 10 hours to find the encoding:
  - Rearrange prox ID bits, then add key, to produce magstripe ID.
  - Key is the same for each card we tested.
  - To find key, just *subtract* prox ID (rearranged) from magstripe ID on any card.

Findings: FlexSecur Demo



Prox: 1 0 0 1 0 0 1 0 0 0 1 0 0 1 1 0 1 0 0 0 0 0 0 1 0 0 1 0 0 1 0 1

XOR

Rearranged: 1 1 1 0 0 1 0 0 0 0 1 0 0 1 1 0 1 0 0 0 0 0 0 1 0 0 1 0 0 1 0 1

Key: 1 1 0 0 1 0 1 0 1 0 0 0 0 0 1 1 1 0 0 0 1 0 0 1 0 1 1 1 1 1 1 0

XOR

Result: 0 0 1 0 1 1 1 0 1 0 1 0 0 1 0 1 0 0 0 0 1 0 0 0 0 1 0 1 1 0 1 1

= *782567515 in binary*

Magstripe: 782567515 -- 8016 -- 050630-782567515-00(15)(11)

Recommendations

- Don’t use prox card for monetary transactions or high-security areas. Remove from nuclear reactor.
- Split magstripe ID and prox ID. Don’t depend on Indala FlexSecur to keep magstripe ID secret.
- Recall issued proximity cards and rewrite magstripes.
- Incorporate local experts in procurement process.
- Instead of prox readers, consider magstripe readers or prox readers with PIN keypad.