Credit Card Fraud

The Contactless Generation

Kristin Paget

Chief Hacker, Recursion Ventures

kris@recursion.com

@KrisPaget

WHAT'S COMING UP?

- Contactless payments
  - What is EMV?
  - How does NFC fit in?
  - Threat vectors
  - Shielding inadequacy
  - Live fraud demo (x2!)
  - GuardBunny

CONTACTLESS PAYMENTS

- EMV: EuroPay, Mastercard, Visa
  - JCB and AmEx joined later
  - Europay bought by MasterCard in 2002
  - Defines standards for next-gen payments
    - “Contactless” in USA
    - “Chip and Pin” in Europe
    - Same standard, different communications
- NFC is a superset of “Contactless”
  - Same over-the-air protocol, additional security

DO YOU HAVE A CONTACTLESS CARD?

- You might be surprised...
- Two “universal” symbols aren't always present
- Other symbols are brand-specific

NFC AND CONTACTLESS PAYMENT ?

- NFC supports EMV-style contactless payment
  - We **BELIEVE** keys are stored securely
    In the NFC chip on the phone
  - Software reversing **SHOULD NOT** allow key recovery
- NFC application on the phone must be active
  - NFC is off when the screen is off (for Google Wallet)
  - PIN number required to unlock the NFC app
    With settable timeout
  - Explicit lock after use is possible
- Other than this, NFC is **IDENTICAL** to EMV
  - Arguably more secure, arguably just as vulnerable

CONTACTLESS SECURITY

- Cards are “secure”
  - JCOP smartcards are used
- Readers are “secure”
  - Again, secure microcontrollers and protected keys
- Protocol is “secure”
  - Strong encryption (?)
- “Secure” in this context means:
  - Cost of attack is larger than potential fraud gains
  - Keys can **ALWAYS** be extracted given adequate budget

IS THE PROTOCOL SECURE?

- Maybe, maybe not.
- There doesn't appear to be mutual auth.
  - http://nosedookie.blogspot.com/2011/06/reading-chase-visa-paypass-credit-cards.html
  - Read EMV cards from a non-EMV reader!
  - Do we get all the info? Not sure yet.
- **Some** data is available
- **Some** encryption is present
- More work is needed.

LEGACY PAYMENT INFRASTRUCTURE

- Payment terminals expect a “credit card number”
  - As well as other info: Customer name, CVV or other check digits
- Terminals always assume mag-stripes are used
  - Encryption is not supported
- Contactless payment readers have to work with this, so
  - A **secure** terminal...
  - ...speaks a **secure** protocol...
  - ...to a **secure** device...
  - ...and outputs a **plaintext** “card number”

CONTACTLESS FRAUD VECTOR

- Contactless readers are widely available
  - Around $100 on various sites
- Let the reader handle whatever crypto is there
  - Completely transparent to the terminal
- Harvest the card number
  - Data is output via serial port
- Write card data to magstripe
  - Use magstripe as a payment card

DOES THAT REALLY WORK?

DEMO 1: Making a payment

CONTACTLESS FRAUD LIMITATIONS

- Contactless “check digits” change
  - Unique check digits per-transaction
- Check digits are only used once
  - If re-presented, disable RFID token
- Check digits follow a sequence
  - If sequence is broken, disable RFID token
- Check digits are different than magstripe
  - If check digits don't match, disable RFID token
- Some cards (AmEx) use different numbers
  - One card number for magstripe, different number for RFID

DO THE PROTECTIONS WORK?

- Conducting multiple contactless transactions
  - Easy! Read the card multiple times.

    Only takes a **few seconds** per read
- Old-style card fraud:
  - One magstripe good for multiple transactions
- New-style card fraud:
  - Multiple contactless cards, one transaction each
- Contactless skimming is **far** easier than magstripe
  - Card never needs to leave the victims pocket

MULTIPLE TRANSACTIONS

Demo 2: Read many times

UPPING THE CONTACTLESS ANTENNA

- High-power readers are possible
  - Contactless range is typically *3-5 inches*
  - That's using milliWatts of RF power
- Contactless operates at 13.56MHz
- There's a Ham band at 14MHz
  - Slightly out-of-band amplifiers will work nicely
- High power is **easy** to obtain
  - Antennas and receivers are harder
- Theoretical range limit: At least tens of feet

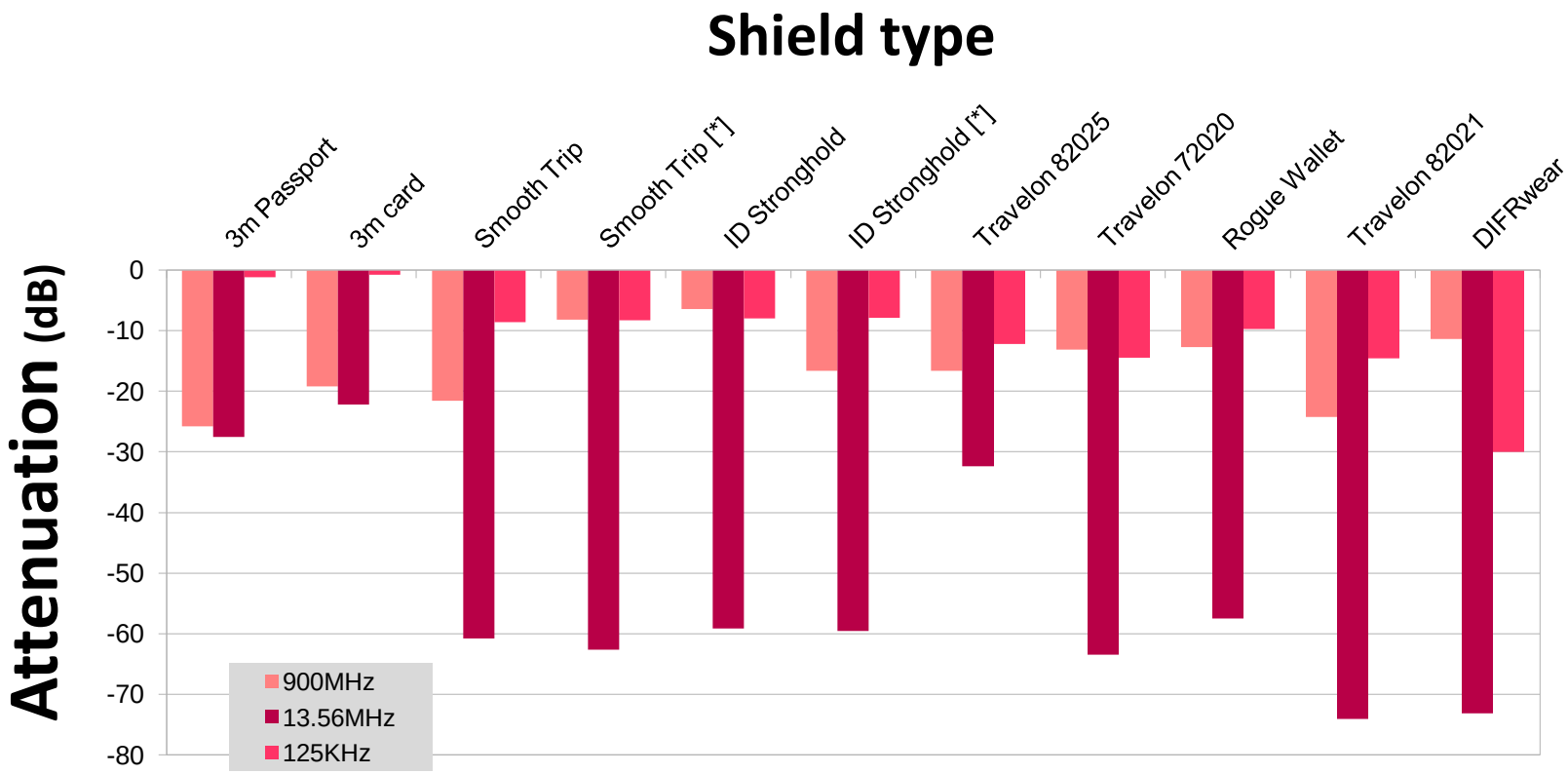
CONTACTLESS DEFENCES

- Passive “shields” or metallic wallets:
  - Only reduce the signal strength
    - This will not block a high-powered reader
- We lab-tested a dozen different passive shields
  - Reported for a large consumer magazine
- Significant inconsistency across samples, RFID bands
- No shielding standards exist
  - FIPS 201 is commonly cited, which simply says:

    “an electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information”

    *http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf (*page 8)

PASSIVE SHIELDS



PASSIVE SHIELDS: CONCLUSIONS

- No single product stood out as “The Best”
  - Different leaders in all 3 bands
- Crumpling can raise or lower performance
  - Could even depend on the RF band in use
- LOTS of variation on the market
  - @13.56MHz **-50dB** between best and worst!

    (That's **100,000x** for non-radio folks)
- Lack of standards mean lack of consistency
  - Recommend **NONE** of these products

SHIELDING FAILURES

Demo 3: 125KhZ

GUARD BUNNY™ : A BETTER SHIELD

- Passive shields don't work.
  - Too unpredictable, can be overpowered
- What about active shields?

- **GuardBunny™** has no CPU or memory
  - **LOWER**-power than the tag
- It generates similar modulation to the RFID tag
  - The reader can't tell us apart
- More power in, more power out!
  - VERY hard to overpower.

ACTIVE SHIELDING

Demo 4:

CAN YOU HAVE ONE?

- Currently made of discrete SMDs on PCB
  - Much more expensive than RFID tags :(
- Next step: **ASIC** production
  - Will make it cheaper & even lower-power
- Forecast: 6-9 months
  - Happy to talk to engineers or fab owners
  - (Or anyone else who can help us speed that up!)

QUESTIONS?

Kris@recursion.com

@KrisPaget