Contactless Threats to FIPS 201 Systems

Dan Bailey, RFID Solutions Architect

RSA Laboratories

RSA SECURITY®

Confidence Inspired™

Acknowledgements

- NIST has done a tremendous amount of great work in a very short period of time!
- It’s difficult to adequately express the gratitude we all hold for your work in *keeping us all safe*.
- RSA Security would like to thank the General Services Administration, the Office of Management and Budget, and the Department of Commerce and NIST for hosting today’s event in particular for the opportunity to expand on some of the comments we submitted on the draft FIPS 201 document

FIPS 201 and Card Threats

- Let’s focus on two basic threats to card-based identification systems:
  - **Cloning**, where the attacker produces an unauthorized copy of a legitimate credential
  - **Tracking/Targeting**, where the attacker targets or tracks the movements of an individual
- FIPS 201 provides different protections against these threats when applied to the contact or contactless interface.
- The contact interface gets a public-private keypair and certificate.
- The contactless interface is prohibited from using these, probably because of power and range issues

RSA
SECURITY

Contact Cloning Threat

- **Threat:** An attacker attempts to copy a legitimate card and use the copy to fool a contact reader
- **Difficulty:** Low. Modest technical skills are required to read and write to cards using commodity equipment.
- **Mitigation:** But the attacker **doesn't know the card's private key**. It cannot be exported and the card provides physical protection to meet FIPS 140-2 Level 3 requirements. This fact will be detected by PACS-High.

Contactless Cloning Threat

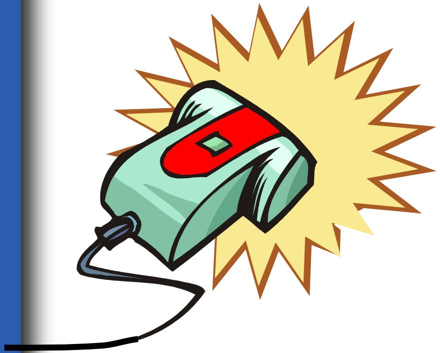
- **Threat:** An attacker attempts to copy a legitimate card and use it to fool a contactless reader
- **Difficulty:** Low. Commodity equipment, modest skills
- **Mitigation:** The CHUID can be read by anyone. Additional protections are optional only. The standard says:

  …agencies may choose to supplement this basic functionality with storage for a local authentication key and support for a corresponding set of cryptographic operations

  As we understand it, that means agencies can deploy systems with cards that are **easily cloned**

Contactless Cloning Threat

Attacker reads CHUID and injects in fake card



The legitimate reader can't tell the difference!

Contactless Range

- ISO 14443 devices are designed to reliably operate at a range of 15cm.
- But attackers aren't looking for 99+% read rate. Reading 1% of cards passing by a busy street corner could be good enough for an attacker
- Press reports* suggest an attacker can read a 14443 device at a **range of up to 30 feet**.
  - Experts suggest a briefcase-size device can read at a range of 3 feet
  - DHS spokeswoman confirms a range of several feet.
- These ranges suggest attackers able to conceal large antennas could conduct a lot of surreptitious scanning

EETIMES

THE INDUSTRY SOURCE FOR ENGINEERS & TECHNICAL MANAGERS WORLDWIDE

- ***Tests reveal e-passport security flaw**

Contactless Cloning Threat

- **Conclusion:** Relying on only the CHUID - as in PACS-Low - provides very little security
  - Akin to an ATM card with no PIN or a username without a password
- Agencies may optionally implement a local authentication key on the card for a challenge-response protocol
- Perhaps this should be **mandatory**!

Contact Tracking/Targeting Threat

- How is tracking/targeting mitigated on the contact interface?
- A contact card is explicitly inserted into a reader by a user
- This simple act does the following:
  - — Requires intentionality on the part of the user
  - — Requires some simple but effective forms of reader authentication
    - Location (physical and contextual)
    - Appearance (logo, design cues)
    - Social (everyone else is using it)
    - History (I put my card in it yesterday when I came to work)
- We trust these factors every day to authenticate ATMs!

Contactless Threat

- **Threat:** An attacker attempts to track or target a cardholder using the contact interface
- **Difficulty:** Low. It's all commodity equipment.
- **Mitigation:** None. Page 25 says:

  The PIV CHUID shall be accessible from both the contact and contactless interfaces of the PIV card without card activation.

  As we understand it, that means **without user knowledge or consent**, an off-the-shelf reader can obtain the CHUID.

What Does an Attacker Learn?

- An attacker who gets a cardholder’s CHUID over the cotnactless interface can learn **facts about the cardholder:**
  - The cardholder is a Federal employee or contractor
  - Agency affiliation
  - Position sensitivity
  - FASC-N, including Person Identifier. Note the earlier SEIWG-012 used the cardholder’s Social Security Number as the Person Identifier
  - Patterns of physical movements, especially in high-threat areas

What Does an Attacker Gain?

- What could an attacker do with this data?
  - Intrusive targeted marketing. Retailers near Federal facilities could compile **dossiers** on customers who are Federal employees
  - Targeting for **terrorist acts**. The CHUID could allow terrorists to target individuals or agencies with **Improvised Explosive Devices** (IEDs)
    - Yahya Ayyash, bomb maker for Hamas, was killed this way
- HSPD-12 specifies a card that “is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation”

What Can We Do?

1. The contactless interface could **authenticate the reader.** This solution reduces range and increases time in field.

   — Essentially, we'd be requiring **card activation** before the CHUID is accessible over the contactless interface

   — **Step 1:** User supplies card-specific PIN to reader (as in 4.1.6.1).

   - Reader presents PIN to card and card reveals its key ID.

   — **Step 2:** Use a challenge-response protocol between card and reader (4.1.6.2).

   - Reader uses key ID to determine the card's unique local key
   - Reader and card prove key knowledge to each other
   - Then card reveals CHUID.

What Else Can We Do?

2. Enable the contactless interface only while the cardholder is **pressing a “button”** on the card. MasterCard has piloted such cards.
3. Allow an authenticated contact reader to **switch off** the contactless interface with software commands. An authenticated contact reader could later switch the interface back on. This solution requires careful coordination among readers.
4. Instruct cardholders to store cards in a **foil-lined bag** when not in use. This approach is cumbersome at best.
5. **Replace the CHUID** with a random identifier. These numbers would populate the “Authorized FASC-N List” instead of their actual counterpart. Note this approach **does not prevent tracking or cloning** and only modestly protects cardholder identity.

An Active Research Area

- Privacy and security in RFID and contactless systems is a very active research area.
- Designing a privacy-preserving reader auth. protocol - easily implemented on a contactless interface - is a tough problem.
- In a few years’ time, battery-assisted contactless cards may be available which could do **robust crypto** such as public-key
- The continuing miniaturization of electronics could lead to **new form factors** that are smaller or more convenient
- We encourage the DoC and NIST, OMB, and GSA to track these emerging technologies so future versions of the standard can provide the best protection possible for our Federal workers

Questions?

Dan Bailey

RFID Solutions Architect, RSA Laboratories

http://www.rsasecurity.com/go/rfid

dbailey at rsasecurity dot com

+1 781 515 7253

RSA SECURITY