Internship Month 3
Project RFID Blocking
Rhombix Technologies
Intern: Syeda Fakiha
Internship Domain: Cybersecurity
Date of Report: August 2025

RFID Security — Threats, Tools & Defenses

Table of contents

1. Executive summary

RFID (Radio-Frequency Identification) and NFC (Near Field Communication) systems are widely deployed for payments, physical access, identity documents, transit cards, and supply-chain tracking. While designed for convenience, some RFID deployments — especially older or poorly implemented ones — are vulnerable to a range of attacks such as skimming, cloning, and relay attacks.

This project helps us assess how RFID systems work and the main threats and attacker capabilities, maps out commonly-seen attacks, and measures to be taken for better defense and mitigative controls you can deploy, and provides an ethically-sound test plan for evaluating a physical blocking solution (sleeve/wallet) and the overall system.

2. RFID fundamentals (how it works)

What RFID

RFID is a wireless technology that uses radio waves to communicate between a reader (interrogator) and a tag (transponder). Systems vary widely in frequency, power, protocol, and use case.

Key components:

- **Tag (or card):** Contains an antenna and an integrated circuit. Tags may be passive (powered by the reader's field), semi-passive, or active (battery-powered).
- **Reader (or interrogator):** Generates an electromagnetic field to power (for passive tags) and communicate with the tag. It decodes the tag's responses and forwards them to backend systems.
- **Backend/system:** Authentication, access control logic, payment or identity databases.

Frequencies:

- **Low Frequency (LF):** typically, ~125 kHz (common in older access control systems, animal IDs). Short-range, simple protocols.
- **High Frequency (HF):** 13.56 MHz (NFC and many contactless payment/access cards). Short range (a few centimeters to ~1 meter, depending on hardware).
- **Ultra-High Frequency (UHF):** ~860–960 MHz (used for supply-chain EPC tags; longer read ranges)

Passive vs active: Passive tags are prevalent in cards and fobs; they contain no battery and are powered by the reader's electromagnetic field. Passive tags typically have a short-read range and simpler functionality, which has security implications.

Protocols & standards (overview): ISO 14443 (used by many contactless payment cards and some access cards), ISO 15693 (vicinity cards), ISO 18000 series (UHF), and various proprietary formats. Some older chipsets used weak or proprietary cryptography and are therefore higher risk.

3. Common standards and real-world use cases

Payments: Contactless credit/debit cards and mobile wallets use strong backend security and tokenization layers, but implementations differ by vendor and region.

Access control: Employee badges and building access systems frequently use LF (125 kHz) or HF (13.56 MHz) cards. Some legacy systems rely on static identifiers and are weak.

Transit & identity: Transit cards, national ID, and passports may use RFID/NFC. Security varies from simple identifiers to cryptographically-backed secure elements.

Supply chain & inventory: UHF tags for inventory tracking have different security properties and are out of scope for the small-wallet blocking discussion but remain part of the broader RFID landscape.

4. Threat model & attacker capabilities

Typical attacker goals:

- Financial theft (unauthorized transactions)
- Unauthorized physical entry (cloning access badges)
- Tracking (identifying an individual by a unique tag)
- Data harvesting (reading sensitive data stored on tags)

Typical attacker capabilities:

- Carry small, portable readers/writers (some are consumer-grade)
- Use tools to emulate/tag responses or replay captured data
- Perform relay attacks by relaying signals between the victim tag and a legitimate reader
- Perform close-range skimming using concealed readers

Defenses should be proportionate to the attacker's capability you worry about.

5. Common types of attacks

This explains how attacks *work* at a high level so defenders can mitigate them. This does not provide operational instructions.

5.1 Skimming (eavesdropping/unauthorized read)

What: A rogue reader captures information broadcast by a tag when it comes within read range.

Why it matters: Some tags broadcast static, identifying data in plain text. This data can be used to clone weak systems or track a person if identifiers are persistent.

Defenses: Use shielding (sleeves), tokenization, limit exposed data, and ensure applications don’t store sensitive plaintext on tags.

5.2 Cloning

What: Attacker duplicates a tag’s data to create a working copy. Cloning depends on the protocol and whether the tag stores secrets or uses cryptography.

Why it matters: On systems where authentication is based solely on a static ID, cloning allows unauthorized access.

Defenses: Strong cryptographic mutual authentication in the reader–tag protocol, secure elements in cards, backend checks (e.g., challenge-response), and short-lived tokens.

5.3 Relay attacks (sometimes called "man-in-the-middle")

What: The attacker places a device near the victim’s tag that relays the radio exchange to a remote device positioned near a legitimate reader. The reader and tag believe they are communicating directly with each other.

Why it matters: Relay attacks can bypass proximity checks and are notable in research on car key and contactless payments. Even secure cryptography can be bypassed if authentication relies only on the presence of the tag.

Defenses: Distance bounding protocols (measure round-trip time), user interaction (press a button or enter PIN for transactions), disabling passive modes where feasible, and Faraday shielding when not intentionally using the card.

5.4 Replay attacks

What: Intercepting a valid message and replaying it later to gain access. Modern systems use nonces/challenges to prevent simple replay.

Defenses: Proper cryptographic challenge/response and session nonces.

5.5 Jamming & Denial-of-Service

What: Interfering with radio signals to prevent legitimate reading.

Why it matters: It may be used to cause failures or bypass checks that rely on reading tags at specific times.

Defenses: Redundancy, monitoring for RF anomalies, and physical checks.

5.6 Side-channel or implementation attacks

What: Exploiting weaknesses in the card's hardware or crypto implementation (e.g., weak random numbers, side-channel leakage).

Defenses: Use chips with well-reviewed secure elements and follow vendor security recommendations.

5.7 Physical/social attacks

What: Theft of the physical card, tailgating, social engineering to get a card close to a reader, or insider threats.

Defenses: Good physical security policies and user education.

6. Tools used in research and by attackers

Proxmark3 (research-grade tool): A widely used engineering tool for RFID/NFC research. It supports both low-frequency (125 kHz) and high-frequency (13.56 MHz) signals and is used by researchers to read, analyze, and test tag behavior. Because of its flexibility, it is a primary tool in academic and security-lab testing. (Note: programmatic cloning and exploitation steps are extra-sensitive and must not be performed against unauthorized systems.)

Flipper Zero (multi-tool): A portable, consumer-friendly multi-tool that supports a range of RF-related functions, including reading and emulating some types of 125 kHz and 13.56 MHz tags (capabilities vary by firmware and hardware revision). It is popular for benign tinkering and defensive testing, but also used by testers to demonstrate vulnerabilities.

Cheap USB RFID readers/writers & NFC-capable smartphones: Many inexpensive readers, and modern phones with NFC, allow reading and limited writing on compatible tags, useful for benign testing on owned tags.

Software-defined radios (SDRs): SDRs (e.g., Hack RF, RTL-SDR) enable flexible RF analysis across frequencies. They are powerful research tools but require advanced expertise.

Other kit & accessories: Antennas, test cards, lab power supplies, and shielding materials used for both defense and testing.

Legal & ethical note: These tools have legitimate uses (research, device development, IT asset recovery) but can be abused. Use tools only on your own equipment or where you have express authorization and follow a documented ethical testing policy.

7. Defensive measures (technical, physical, operational)

Defense should be layered: combine technical, physical, and process controls.

Defensive Measures (Technical, Physical, Operational)

Technical measures:
- Use encrypted RFID protocols (e.g., MIFARE DESFire, HID SEOS).
- Implement mutual authentication between reader and card.
- Regularly update firmware on RFID readers to patch vulnerabilities.

Physical measures:
- Use RFID-blocking sleeves, wallets, or Faraday cages to prevent unauthorized scans.
- Secure access control points physically to avoid tampering.

Operational measures:
- Limit the range and power of RFID readers.
- Train staff on RFID risks and social engineering attempts.
- Monitor for unusual access patterns in system logs.

8. Designing an Effective RFID-Blocking Sleeve (Practical, Defensive Guidance)

- Materials: Faraday fabric, copper mesh, or multiple layers of aluminum foil.
- Coverage: Ensure full enclosure around the card, no gaps at seams.
- Durability: Use sturdy outer layers (leather, PVC, or fabric) to protect the conductive core.
- Testing: Verify with multiple RFID frequencies (125 kHz & 13.56 MHz).

9. Incident Response: What to Do if You Suspect Compromise

1. Immediately disable compromised cards through issuer or IT department.
2. Replace with secure, encrypted RFID cards.
3. Review access logs for suspicious activity.
4. Report the incident to relevant authorities.
5. Educate affected parties on prevention measures.