

# Security for Smart Tags

Kevin Fu, Wayne Burleson (UMass Amherst);  
Ari Juels (RSA Labs); Adam Stubblefield (JHU)

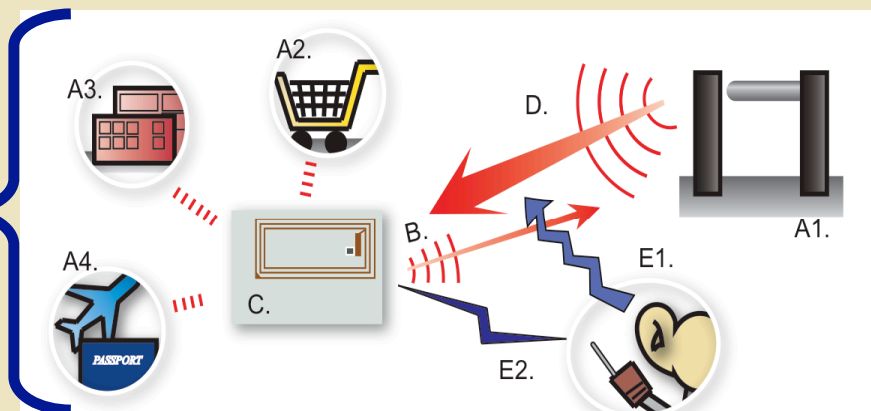
rfid-cusp.org



## RFID Security and Privacy: Threats & Approaches

### Problem

SmartTag-enabled devices lack basic protection for security and privacy.



A **SmartTag** (C) is a nomadic device often without a local power source and with minimal computation and storage. **SmartTag readers** (A1-4) both interrogate and wirelessly power tags to facilitate sporadic network connectivity. Unique constraints for SmartTags include asymmetric signal strengths (D), passive **eavesdropping** of reader signals (E1), and active eavesdropping by surreptitiously energizing a non-consenting tag (E2). Security-sensitive applications include public transit (A1), e-commerce (A2), building entry (A3), and e-passports (A4) where shared tags interact with network resources via untrusted readers.

### Approach

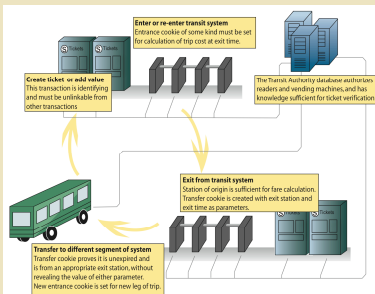
- Build secure applications, protocols, and hardware for RFID systems relying on untrusted components.
- Analyze the security of deployed RFID systems.

### Result 1: Privacy for Public Transit

- Unlinkable transfers
- Variable rate fare structure
- Revocable untrusted readers

### Result 2: RFID Credit Card Analysis

- Personal information leaked
- Cross contamination of non-RFID
- 20 million cards in circulation



Overview of transit system architecture in an imaginary subway. The Smart Tag reader sets a cookie on a passenger's tag to keep track of fares. When the passenger exits, the cookie is replaced with a new transfer token, anonymizing the passenger's path.



A homemade credit card emulator. The low-cost device consisting of a Gumstix embedded Linux system and analog circuitry demonstrates that many deployed RFID credit cards are susceptible to replay attacks.

### References

- "Cryptanalysis of two lightweight RFID authentication schemes." PerSec Workshop, 2007.
- "Vulnerabilities in first-generation RFID-enabled credit cards." Financial Cryptography, 2007.
- "Researchers see privacy pitfalls in no-swipe credit cards." The New York Times, 2006.
- "The security implications of VeriChip cloning." Journal of the American Medical Informatics Association (JAMIA), 2006.
- "Privacy for public transportation." Workshop on Privacy Enhancing Technologies (PET), 2006.
- "Collaborative monitors of embedded system security." 1st International Workshop on Embedded Systems Security, 2006.

### Students

- Hee-Jin Chae
- Benessa Defend
- Thomas S. Heydt-Benjamin
- Dan Holcomb
- Lang Lin
- Josh Mason
- Sam Small