Categorizing RFID Privacy Threats with STRIDE

Dale R. Thompson, Jia Di, Harshitha Sunkara, and Craig Thompson

University of Arkansas
CSCE Dept.
311 Engineering Hall
Fayetteville, AR 72701

{drt, jdi, hsunkar, cwt}@uark.edu

ABSTRACT

Privacy threats by radio frequency identification (RFID) are categorized using the security-oriented STRIDE model. Categorizing the privacy threats with STRIDE identifies potential strategies for mitigating them. Preliminary results for preventing tracking using universal re-encryption are presented.

1. INTRODUCTION

A pervasively networked information society is our destiny. Cell phones, GPS, enhanced 911 services, toll passes, loyalty retail cards, face recognition algorithms, and many databases all contain personally identifiable data [1], [2]. Now being mass deployed in the retail industry, radio frequency identification (RFID) enables objects and individuals to be automatically identified with a no-contact, non-line-of-sight, and invisible system. It provides benefits such as visibility into the retail supply chain to track and locate containers, pallets, cases, and items. RFID is the vanguard of mass deployment of sensors in a networked society – a coming Internet of Things where everything is alive – that is, where common objects (including those that are inanimate and abstract) can have individual identities, memory, processing capabilities, and the ability to communicate and sense, monitor, and control their own behaviors [3].

Individually and integrated, all these technologies can provide huge benefits to society. But they also pose invasive new threats to rights, privacy of individuals, and security of organizations. Privacy advocates are concerned that the supply chain RFID system that retailers are building to track items can be used to profile and track individuals [4]. The Total Information Awareness (TIA) program proposed by DARPA had its funding eliminated by Congress because of privacy concerns – but that begs the question of how to provide privacy assurance technologies since our society is developing ever more information awareness technology. Privacy principles based on fair information practices discussed in [9] need to be incorporated into these technologies. We need to understand and quantize the threats and their severity, and to develop and deploy privacy and security mechanisms, systemic architectures, and regulations that keep pace.

An RFID system consists of readers, printers, tags, middleware, communication networks, and databases [5], [6]. A tag contains a unique serial number and is attached to objects so that a reader can automatically identify the object with a wireless signal by querying the tag, obtaining the serial number, and looking it up in a database. A large number of attributes about the object can be referenced with this serial number.

The first step in building a system that protects the privacy of individuals is to understand the threats. Threats are potential events that cause a system to respond in an unexpected or damaging way. Privacy threats include exposing personally identifiable data.

RFID has at least the following three privacy threats that need to be addressed: tracking, hotlisting, and profiling [7]. Limiting or preventing tracking the location of individuals is a high priority item. Hotlisting is used by an attacker to single out certain individuals because of the items they possess. Profiling is identifying the items an individual has in their possession. Categorizing privacy threats as tracking, hotlisting, and profiling is useful for understanding the threats. However, we want to categorize the privacy threats into categories that map directly into strategies for mitigating them. In this work, the focus is on threats to privacy by RFID and the privacy threats are categorized using STRIDE [8].

2. STRIDE THREAT MODEL

The STRIDE threat model has been used in the design of secure software systems [8] and applied to security threats to RFID [5], [6], but not privacy threats by RFID. STRIDE is an acronym for six threat categories that are listed below.

- **Spoofing identity**. Spoofing occurs when an attacker successfully poses as an authorized user of a system.
- **Tampering with data**. Data tampering occurs when an attacker modifies, adds, deletes, or reorders data.
- **Repudiation**. Repudiation occurs when a user denies an action and no proof exists to prove that the action was performed.
- **Information disclosure**. Information disclosure occurs when information is exposed to an unauthorized user.
- **Denial of service**. Denial-of-service denies service to valid users. Denial-of-service attacks are easy to accomplish and difficult to guard against.
- **Elevation of privilege**. Elevation of privilege occurs when an unprivileged user or attacker gains higher privileges in the system than what they are authorized.

General mitigation techniques for each category in the STRIDE model are listed in Table 1.

3. STRIDE APPLIED TO PRIVACY

Example privacy threats by RFID are categorized using STRIDE and are listed below.

- Spoofing identity
    - An attacker replaces an authorized reader with their reader and reads the tags of an individual without the individual's authorization.
- Tampering with data
    - An attacker modifies the tag in a passport to contain the serial number associated with another individual.
- Repudiation
    - The government says it will not track, hotlist, or profile individuals using tags but they do.
- Information disclosure
    - An attacker tracks an individual determining where an individual is located and where they have been by the tags carried by an individual being read at multiple locations.
- Denial of service
    - An attacker deletes or modifies the serial number in an RFID-enabled passport preventing or delaying the individual from entering the country.
- Elevation of privilege
    - An attacker modifies the serial number on a RFID-enabled passport to be a citizen in good standing instead of a criminal.

4. PREVENTING TRACKING USING A MIXNET

One way to prevent tracking (information disclosure) is to periodically change the serial number of a tag to a random or untraceable number. Universal re-encryption [10] using ElGamal encryption was implemented in Java. In universal re-encryption, the serial number and added information on a tag is encrypted with a public key. Then security agents (specialized readers) that do not have knowledge of the public or private key re-encrypt the contents; however, the user with the private key can still decrypt the tag's serial number.

Table 1. Mitigation techniques for each category in the STRIDE model [8]

Category	**Techniques**
Spoofing identity	Appropriate authentication, Protect secrets, Don't store secrets
Tampering with data	Appropriate authentication, Hashes, Message authentication codes, Digital signatures, Tamper-resistant protocols
Repudiation	Digital signatures, Timestamps, Audit trails
Information disclosure	Authorization, Privacy-enhanced protocols, Encryption, Protect secrets, Don't store secrets
Denial of service	Appropriate authentication, Appropriate authorization, Filtering, Throttling, Quality of Service
Elevation of privilege	Run with least privilege

5. FUTURE WORK

Future work on privacy architectures that use middleware, network, and hardware techniques to provide privacy assurance is planned. The plan is to incorporate the implemented universal re-encryption software into one or more readers or into existing middleware that control readers. A physical implementation of RFID systems, hardware, including both readers and tags, has significant impact on RFID privacy and security. Research on designing innovative hardware circuits against non-invasive attacks for RFID systems is planned.

6. REFERENCES

[1] Sarma, S. A history of the EPC. *RFID: Applications, Security, and Privacy*. Garfinkel, S., and Rosenberg, B., Eds. Addison-Wesley, Upper Saddle River, NJ, 2006, 37-55.

[2] Perrin, S. RFID and global privacy policy. *RFID: Applications, Security, and Privacy*. Garfinkel, S., and Rosenberg, B., Eds. Addison-Wesley, Upper Saddle River, NJ, 2006, 57-81.

[3] Thompson, C. Everything is alive. *IEEE Internet Computing*, (Jan./Feb. 2004).

[4] Weinberg, J.. RFID, privacy, and regulation. *RFID: Applications, Security, and Privacy*. Garfinkel, S., and Rosenberg, B., Eds. Addison-Wesley, Upper Saddle River, NJ, 2006, 83-97.

[5] Chaudhry, N., Thompson, D. R., and Thompson, C. *RFID Technical Tutorial and Threat Modeling, ver. 1.0*. Technical Report, CSCE Dept., University of Arkansas, Fayetteville, Arkansas, 2005. Available: http://csce.uark.edu/~drt/rfid

[6] Thompson, D. R., Chaudhry, N., and Thompson, C. W. RFID security threat model. In *Proceedings Acxiom Laboratory for Applied Research (ALAR) Conf*. Conway, Arkansas, Mar. 3, 2006.

[7] Karthikeyan, S., and Nesterenko, M. RFID security without expensive cryptography. In *Proceedings ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*. Alexandria, VA, Nov. 2005, 63-67.

[8] Howard, M., and LeBlanc, D. *Writing Secure Code, 2nd ed*. Microsoft Press, Redmond, WA, 2003.

[9] Langheinrich, M. Privacy by design—Principles of privacy-aware ubiquitous systems. In *Proceedings Ubicomp*. Atlanta, GA, Oct. 2001.

[10] Golle, P., Jakosbsson, M, Juels, A., and Syverson, P. Universal re-encryption for mixnets. *Lecture Notes in Computer Science*, (2004), 163-178.