

# Ownership Transfer of RFID Tags based on Electronic Fingerprint

Senthilkumar Chinnappa Gounder Periaswamy, Dale R. Thompson, and Jia Di

Department of Computer Science and Computer Engineering, University of Arkansas, Fayetteville, Arkansas, USA

**Abstract**—Pervasive computing devices such as radio-frequency identification (RFID) tags and wearable computing devices will require ownership transfer. Ownership transfer is a method to transfer a device to a new owner which prevents the previous owner from querying or interacting with the device. It should provide forward security in which no information about the device’s past operation or past owner can be derived if the security of the device is compromised in the future. Most proposed ownership transfer techniques are based on changing stored secrets of the device using cryptographic algorithms and authentication protocols. In this work, we propose to transfer ownership by permanently changing the physical attributes of a device to a new but unpredictable value. These physical attributes are like an electronic fingerprint. Results of a proof-of-concept experiment are presented in which one attribute of a RFID tag is changed to a new value thus altering the electronic fingerprint.

**Keywords:** RFID, Security, Privacy, Ownership transfer, Identification, Authentication.

## 1. Introduction

RADIO frequency identification (RFID) is one type of a pervasive computing device. An RFID system consists of readers, printers, tags, middleware, communication networks, management systems, and databases [1] [2]. The tag is a miniature chip containing information with an affixed radio antenna. 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.

RFID systems should have the ability to perform ownership transfer in which the new owner can read the tag but the previous owner cannot [3-6]. Ownership transfer could occur anywhere in the supply chain such as from the manufacturer to the distributor, from the retail store to the consumer, or from one individual to another individual. Once ownership transfer occurs, a future compromise of the tag should not aid in the identification of the tag’s past

interactions [5]. This feature is called “forward security” in the literature [4], although there is debate on whether this is an accurate term [5]. In [5], it is proposed that a compromised tag that has all of its information revealed should neither aid in the identification of the tag’s past interactions nor aid in the identification of the tag’s future interactions.

In the literature, ownership and ownership transfer are performed by the owner and tag managing shared secrets. The tag’s past interactions are commonly protected by using a hash function to update the secret assuming that the function is not reversible [4] [5]. Another choice is to use symmetric encryption to update the secret [3] [6]. In [3], a shared tree of secrets is used for both ownership transfer and time-limited delegation although [5] argues that the ownership transfer in [3] is time-limited delegation because the backend server maintains control of the tag and a reader can only read the tag a certain number of times. An anonymous ownership transferring mechanism is proposed in [6].

A much stronger form of ownership transfer is proposed in [5]. They extend the ownership transfer method in [7] and [8] such that the compromise of the tag and its secrets at a point in time does not aid in the identification of the tag’s past or future interactions. They use the hashing of secrets to protect the past interactions and periodically refresh the secrets in the tag to protect the future interactions.

The military pioneered electronic fingerprinting technology by using it during the Second World War to authenticate communication signals and to track enemy troop movement [9]. The technology involved measuring several unspecified parameters and characterizing them to produce a fingerprint of the device.

Electronic fingerprinting is used on cellular networks by Corsair Communications to reduce cloning fraud [10]. The company has successfully deployed their system known as PhonePrint in base stations of cellular operators. PhonePrint is a combination of hardware and software that characterizes and creates a fingerprint of all the handsets that ask for service [10]. The fingerprint, which is stored in a database, is used for further authentications of services. There is little technical detail available on this technique due to the proprietary nature of the work.

Researchers in [11] could remotely fingerprint an Ethernet card by exploiting small, microscopic deviations in the hardware that manifest themselves as differences in clock skew. They measured the clock skew by monitoring the differences in TCP timestamps, ICMP timestamp reply messages or periodic activities. They used Fourier transform on the arrival timestamps to infer the clock skew. Their results were consistent even when the device was connected to the Internet at multiple locations and via different access technologies.

Fingerprinting of the transient portion of the signal was used in an approach for intrusion detection of Bluetooth networks by [12]. The transient is the turn-on portion of the signal. They extracted fifteen attributes from the amplitude, frequency and phase components of the transient and used k-means clustering to create a fingerprint. After creating the fingerprint, the Hotelling's  $T^2$  statistical classifier was used to observe the similarity between an observed fingerprint and the enrolled fingerprint. Since the wireless environment has noise and interference, a decision filter was applied to decide the final output based on multiple observations. A similar approach was used in [13] for intrusion detection in wireless networks.

Fingerprinting of sensor networks was performed in [14], which also used the transient portion of the signal. They extracted five attributes from the amplitude of the transient and used the mean and covariance matrix to represent a fingerprint. They used a Kalman filter to calculate the probability of a signal match to the stored fingerprint.

The steady-state portion of the signal was used to uniquely identify and track 10 Mbps wired Ethernet cards in [15]. An optimal detector, the matched filter, was used to create signal profiles of the Ethernet cards. They devised variations on the matched filter method depending upon on the device signals to improve results. They used a collection of signals taken over a period of time to developed adaptive methods that accurately track fluctuations in signal due to device aging, voltage variations, and temperature changes.

An integrated circuit (IC) identification circuit was proposed in [16] to provide dependable identification of IC chips. The proposed applications include tracking work in progress, counterfeiting, and transaction validation. The circuit uses the manufacturing differences that manifest themselves as apparently random but static voltage thresholds.

In [17], they proposed to use the initialization state of SRAM's in RFID tags to create a physical fingerprint. They used experimental data from virtual tags to show that a SRAM can be used to uniquely identify tags. A simple Hamming distance based matching was used to observe the identifying qualities.

In this work, we propose to use the physical attributes of the device to create an electronic fingerprint and then modify the fingerprint when performing ownership transfer. First, we create an electronic fingerprint of a tag by measuring its physical attributes. Then, instead of changing

stored secrets, we transfer ownership by permanently changing the physical attributes of the tag to a new but unpredictable value. We argue that incorporating an electronic fingerprint into ownership transfer could either enhance or replace existing proposed ownership transfer methods.

## 2. Ownership Transfer Experiment

The minimum power required to activate a RFID tag at a given distance measured at multiple frequencies is used to identify a tag much like a fingerprint is used to uniquely identify an individual [20]. This fingerprint is shown to be unique for each same-model tag that came from the same roll [20]. We perform an experiment to modify the fingerprint for ownership transfer in which eight tags are thermal cycled. After thermal cycling, the fingerprints of the tags are measured and analyzed to check whether it has changed permanently.

### 2.1 Minimum power response as an electronic fingerprint

Minimum power response is the minimum power required to activate and make a tag respond at multiple frequencies. The minimum power required for a tag to respond at a particular frequency was measured using the Avery Dennison M4E test cube [18] at the University of Arkansas RFID Research Center [19]. The RFID Research Center is not a clean lab but is a dirty lab used to model a production warehouse. In other words, electromagnetic interference is not controlled. However, the test cube was calibrated with a calibration tag. The test cube calibrated itself by referencing the current measurement with the preconfigured value.

The test cube consists of a computer, a RFID reader, an antenna, and an adjustable mount for tags. The software provides various options including calibrating the test cube with a calibration tag, writing or reading RFID tag data and performing frequency analysis. The frequency analysis feature was used to configure the reader to measure the minimum response power of a tag at a given frequency. The minimum power response was measured using a bottom-up algorithm. The bottom-up algorithm repeatedly sent signals from the reader to the tag starting from -20 dBm incrementing it by 0.01 dBm every time until a response from the tag was detected.

The minimum power response at eleven frequencies was measured for eight RFID tags [20]. Four of the eight tags were Avery Dennison AD-220 and were taken off one roll of tags. Therefore, it is likely that they were manufactured at approximately the same time. The other four tags were Avery Dennison AD-612 and they were also taken from one roll. The AD-220 tags are inexpensive and entry level RFID tags from Avery Dennison while the AD-612 tags are relatively expensive and higher quality RFID tags. The AD-220 tags were labeled from Tag A to Tag D and the AD-612 tags were labeled from Tag E to Tag H.

The minimum power response was measured at frequencies ranging from 902 MHz to 927 MHz in increments of 2.4 MHz. The test cube used dBm as the unit for the power. The values were converted to milliwatts for all calculations. During each experiment, the minimum power response measurement was repeated five times for each tag. The test cube measured the minimum power response from 902 MHz to 927 MHz and then started again from 902 MHz for each repetition. Response curves of the minimum power were created using curving fitting and representative curves for each of the tags. The response curves for the AD-612 tags are shown in Fig. 1. From the figures it can be clearly seen that minimum response power of each tag is unique and can be used as a fingerprint to identify each tag. In [20], analysis of variance was applied and the curves were found to be significantly different than each other.

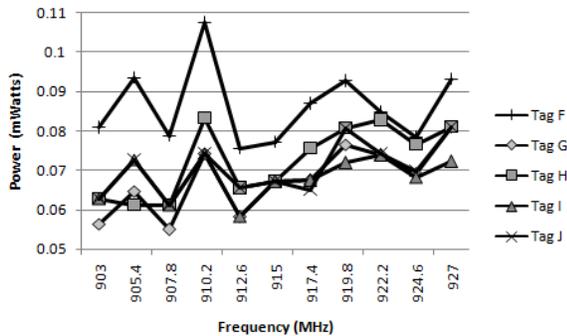


Fig. 1. Minimum power responses of five AD-612 tags

## 2.2 Thermal cycling to change fingerprint

Given that each tag has a unique minimum power response, a proof-of-concept experiment to change the minimum power response of tags for ownership transfer was performed. The tags were thermal cycled, a process of repeatedly heating and cooling the tag to determine if the minimum power response of a tag could be changed. The goal was to develop a method of transferring ownership [3-6].

Both AD-220 and AD-612 tags were thermal cycled for 10, 20, 30, and 60 seconds by heating them up from room temperature to 250°F and then letting them cool to room temperature. To ensure thermal-induced failure free, 250°F was chosen as the highest temperature in each thermal cycle and was chosen to be slightly above the typical maximum temperature for commercial semiconductors, which is 100°C (212°F), to slightly stress the components in the tag. After cooling, the frequency responses were measured again.

Fig. 2 shows the minimum power response of one of the AD-612 tags (tag F) before and after thermal cycling. The two groups of curves are well-separated and appropriate instruments can detect this difference easily.

Analysis of variance was applied to the tags and the analysis of variance of one tag is shown in Table I. The F

ratio is  $2.17 \times 10^4$  for the effect of tags on the minimum power response. Since  $F_{0.01, 1, 48} = 7.19$ , which is less than the F ratio, we conclude that the main effect of tags is significant. That is, the tag before and after thermal cycling has a significantly different minimum power response. The F ratio is  $6.26 \times 10^1$  for the effect of frequency on the minimum power response. Since  $F_{0.01, 5, 48} = 3.43$ , we conclude that the main effect of frequency is significant. That is, the frequency has a significant effect on the minimum power response. Furthermore, the F ratio is  $5.00 \times 10^1$  for the interaction between each tag and frequency on the minimum power response. Since  $F_{0.01, 5, 48} = 3.43$ , we conclude that there is significant interaction between each and tag and frequency. We conclude the minimum power response before and after thermal cycling are significantly different. *The results show that thermal cycling changed the minimum power response the tags permanently.*

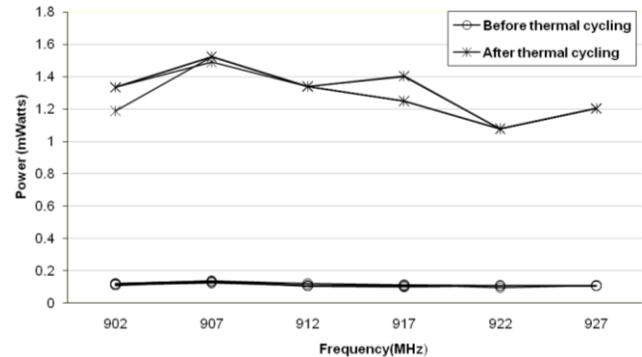


Fig. 2. Minimum power response of one tag (tag F) before and after thermal cycling

Table I. ANOVA table for tag K before and after thermal cycling

Source of Variation	Sum of Squares	D.O.F	Mean Square	F <sub>0</sub>	P-Value
Tag	$2.09 \times 10^1$	1	$2.09 \times 10^1$	$2.17 \times 10^4$	$2 \times 10^{-65}$
Frequency	$3.02 \times 10^{-1}$	5	$6.03 \times 10^{-2}$	$6.26 \times 10^1$	$7 \times 10^{-20}$
Interaction	$2.41 \times 10^{-1}$	5	$4.82 \times 10^{-2}$	$5.00 \times 10^1$	$7 \times 10^{-18}$
Error	$4.63 \times 10^{-2}$	48	$9.64 \times 10^{-4}$		
Total	$2.15 \times 10^1$	59			

## 3. Future Work

Exposing the tag to extreme temperatures is probably not the best way to transfer ownership. Therefore, a more reliable method to change the value of the physical attributes is required. The method should not be a function of normal environmental conditions and should not possibly damage the tag. However, the proof-of-concept experiment does prove that at least one method can be used to permanently alter the electronic fingerprint.

## 4. Conclusion

Ownership transfer will be necessary for pervasive computing devices such as RFID and wearable computing devices as they become more common. Changing the physical attributes to new and unpredictable values could replace or enhance previously proposed methods of changing stored secrets on the device. The addition of physical attributes to the authentication process could significantly strengthen the security and acceptance of these devices.

## 5. Acknowledgment

This material is based upon work supported by the National Science Foundation CISE/CNS and the Cyber Trust area under Grant No. CNS-0716578.

The authors wish to thank Bill Hardgrave, Justin Patton, and David Cromhout from the University of Arkansas RFID Research Center and George Dyche from Avery Dennison.

## 6. References

- [1] A. Juels, "RFID security and privacy: a research survey," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 24, no. 2, pp. 381-394, Feb. 2006.
- [2] N. Chaudhry, D. R. Thompson, and C. Thompson, *RFID Technical Tutorial and Threat Modeling*, ver. 1.0, tech. report, Dept. of Computer Science and Computer Engineering, University of Arkansas, Fayetteville, Arkansas, Dec. 8, 2005. Available: <http://comp.uark.edu/~drt/rfid>
- [3] D. Molnar, A. Soppera, and D. Wagner, "A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags," in *Selected Areas in Cryptography -- SAC 2005; Lecture Notes in Computer Science*, 2005, pp. 276-290.
- [4] K. Osaka, T. Takagi, K. Yamazaki and O. Takahashi, "An efficient and secure RFID security method with ownership transfer," in *Int'l Conf. Computational Intelligence and Security*, 2006, pp. 1090-1095.
- [5] C. H. Lim and T. Kwon, "Strong and robust RFID authentication enabling perfect ownership transfer," in *Conference on Information and Communications Security -- ICICS'06; Lecture Notes in Computer Science*, 2006.
- [6] K. H. S. S. Koralalage, S. M. Reza, J. Miura, Y. Goto, and J. Cheng, "POP method: An approach to enhance the security and privacy of RFID systems used in product lifecycle with an anonymous ownership transferring mechanism," in *Proc. ACM Symposium on Applied Computing (SAC)*, 2007, pp. 270-275.
- [7] G. Avoine and P. Oechslin, "A scalable and provable secure hash based RFID protocol," in *Proc. IEEE Int'l Workshop Pervasive Computing and Communication Security (PerSec)*, 2005, pp. 110-114.
- [8] M. Ohkubo, K. Suzuki, and S. Kinoshita, "A cryptographic approach to privacy-friendly tag," *RFID Privacy Workshop*, Nov. 2003.
- [9] R. Jones, *Most Secret war*, Hamilton, 1978.
- [10] M. J. Riezenman, "Cellular security: better, but foes still lurk," *IEEE Spectrum*, vol. 37, pp. 39-42, 2000.
- [11] T. Kohno, A. Broido and K. C. Claffy, "Remote physical device fingerprinting," *IEEE trans. Dependable and Secure Computing*, vol. 2, pp. 93-108, 2005.
- [12] J. H. M. Barbeau and E. Kranakis, "Detecting rogue devices in Bluetooth networks using radio frequency fingerprinting," in *Proc. IASTED Int'l Conf. Communications and Computer Networks*, Lima, Peru, Oct. 2006.
- [13] J. Hall, M. Barbeau and E. Kranakis, "Enhancing intrusion detection in wireless networks using radio frequency fingerprinting," in *Proc. Communications, Internet and Information Technology (CIIT)*, St. Thomas, US Virgin Islands, November 22-24, 2004.
- [14] K. B. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *Proc. Int'l Conf. Security and Privacy in Communication Networks (Securecomm)*, Nice, France, Sep. 17-20, 2007.
- [15] R. Gerdes, T. E. Daniels, M. Mina and S. Russell, "Device identification via analog signal fingerprinting: A matched filter approach," in *Proc. 13<sup>th</sup> Annual Network and Distributed System Security Symposium*, San Diego, California, Feb 2006.
- [16] K. Lofstrom, W. R. Daasch, and D. Taylor, "IC identification circuit using device mismatch," in *Proc. IEEE Int'l Conf. Solid-State Circuits*, 2000.
- [17] D. E. Holcomb, W. P. Burleson and K. Fu, "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags," in *Proc. Conf. RFID Security*, 2007.
- [18] Avery Dennison RFID. Available: <http://www.rfid.averydennison.com>
- [19] RFID Research Center, University of Arkansas. Available: <http://itri.uark.edu/rfid/>
- [20] S. Chinnappa Gounder Periaswamy, D. R. Thompson, and J. Di, "Fingerprinting RFID tags," in review.