Replay-resilient Authentication for IoT

Ge Wang ^{†‡}, Chen Qian [‡], Haofan Cai [‡], Jinsong Han ^{*#}, Jizhong Zhao [†]

[†]Xi'an Jiaotong University, Xi'an, China.

[‡] University of California, Santa Cruz, CA, USA.

^{*}Institute of Cybersecurity Research, Zhejiang University, China.

[#]ZJU-Alibaba Joint Cyber Security and Privacy Research Laboratory, China.

ABSTRACT

We provide the first solution to an important question, “how a physical-layer RFID authentication method can defend against signal replay attacks”. It was believed that if the attacker has a device that can replay the exact same reply signal of a legitimate tag, any physical-layer authentication method will fail. This paper presents Hu-Fu, the first physical layer RFID authentication protocol that is resilient to the major attacks including tag counterfeiting, signal replay, signal compensation, and brute-force feature reply. Hu-Fu is built on two fundamental ideas, namely inductive coupling of two tags and signal randomization. Hu-Fu does not require any hardware or protocol modification on COTS passive tags and can be implemented with COTS devices. We implement a prototype of Hu-Fu and demonstrate that it is accurate and robust to device diversity and environmental changes.

CCS CONCEPTS

• Security and privacy → Mobile and wireless security;

KEYWORDS

Internet of things; RFID; Device authentication

ACM Reference Format:

Ge Wang, Chen Qian, Haofan Cai, Jinsong Han, Jizhong Zhao. 2018. Replay-resilient Authentication for IoT. In *10th Wireless of the Students, by the Students, and for the Students Workshop*

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

S3'18, November 2, 2018, New Delhi, India

© 2018 Association for Computing Machinery.

ACM ISBN 978-1-4503-5932-0/18/11...\$15.00

<https://doi.org/10.1145/3264877.3264878>

(S3'18), November 2, 2018, New Delhi, India. ACM, New York, NY, USA, 3 pages. <https://doi.org/10.1145/3264877.3264878>

1 INTRODUCTION

Battery-free wireless communication, in particular passive RFID, is a promising solution of the Internet of Things (IoT), due to its energy efficiency and low cost. In recent years, security issues of IoT devices have drawn increasing attentions. Among these issues, device authentication is one of the most important problems. IoT device authentication aims to validate whether a device is indeed the legitimate one which has been registered in the system. It is a crucial task in many applications such as the access control to an area or event, electronic payment, and tamper-evident packaging. However, the limited computing capability of battery-free devices restricts the execution of cryptographic algorithms such as hashing and encryption. In fact, commodity off-the-shelf (COTS) passive RFID tags do not support any cryptographic operation. Hence many classic security solutions are impossible to use on commodity passive tags.

To this end, many researchers investigate to utilize physical-layer information of RFID tags for identification/authentication tasks [1]. Physical-layer identification methods are based on the fact that different tags may include hardware differences due to manufactural imperfection. Hence a tag can be verified using certain physical features and a counterfeited tag is unlikely to have highly similar physical features with the legitimate one. However, it is known that physical-layer identification/authentication is vulnerable to several major attacks, and whether there exists a solution to defend against them was considered an “open question” [1].

We summarize four major attacks in RFID authentication: 1) *Tag counterfeiting*; the attacker uses an unauthorized tag to let it carry the same ID of a legitimate tag [4]. 2) *Signal replay*; the attacker eavesdrops the physical signals of a legitimate tag, captures them in a digital form, and then replays the exactly same signals towards the reader [1]. 3) *Signal compensation*; the attacker obtains a signal that can pass the

Figure 1: Utilize coupling state and signal randomization to defend against various attacks

authentication, called a valid signal. Then during the authentication process, it compensates the current signal to become the valid signal. 4) *Brute-force feature replay*; Assuming the attacker knows the feature extraction algorithm and owns sufficiently many tags, it extracts the feature of every tag until getting one tag that presents a feature close enough to the legitimate tag.

In this paper, we propose an authentication method called Hu-Fu¹, which is a **new direction of physical-layer authentication that is resilient the attacks listed above**. Hu-Fu is based on two ideas, namely *inductive coupling* and *signal randomization*. The inductive coupling phenomenon is that two tags that placed closely will inductive with each other and their signals will be different from the signals by putting one tag along. And signal randomization is that the reader transmits a random signal instead of the carrier waves to shadow the tags' responses. Both inductive coupling and signal randomization are essential components of Hu-Fu. They work together to block the access of attackers to valid signals and features from legitimate tags.

The major contributions of Hu-Fu are as follows: 1) Hu-Fu is the **first tag authentication solution** to defend against signal replay and compensation attacks that is compatible to the standard protocol. It provides a new direction of battery-free/low-power IoT device authentication. 2) Hu-Fu is robust to the device and environment diversity. It uses environment- and reader-independent features, hence it can accurately authenticate tags that are registered at different places.

2 OVERVIEW

Hu-Fu solves the following fundamental problem in an RFID system. Given a tag reply that reports a registered tag ID (EPC), the RFID system needs to decide whether the reply was from the authorized tag that has been registered with

this ID, called a *legitimate tag*, or from an attacker who does not hold the legitimate tag.

To cope with this problem, we propose Hu-Fu, whose basic idea is utilizing two mechanism, namely **inductive coupling** phenomenon and **signal randomization**. The *inductive coupling* is based on a phenomenon of two adjacent tags that the backscatter signal from either tag would be different from the signal by putting the tag alone[2]. The coupling signal of a tag also depends on the other tag. Hence we use a tag, called the Retained Tag (or Left Tag) T_L , along with the reader as the authenticator. When an authenticatee, called the Right Tag T_R , is putted close to T_L and an inductive coupling state is created. The system validates whether the features from the physical signals of T_R and T_L are consistent to the signals collected previously using the legitimate tag T_R . As shown in Fig. 1(a), if T_L and T_R are separate, they will reply non-coupling signals U_L and U_R . However if they are close enough, in Fig. 1(b) their signals will become C_L and C_R . The authentication features are extracted from C_L and C_R . The second idea, called *signal randomization* and introduced in a recent work [3], is to allow the reader sends an one-time random signal $s(t)$ that changes with time t . Then the backscatter signal C_R become $C_R \cdot s(t)$, which appears random to an eavesdropper who has no information of $s(t)$, shown in Fig. 1(c). The eavesdropper is even unable to tell whether a tag is transmitting or not. But the reader is able to remove $s(t)$ for decoding. Hu-Fu makes an attacker incapable to capture, replay, or compensate the signal or feature that can pass the authentication, because C_L and C_R are hidden. For example in Fig. 1(d), if an attacker records U_R by querying T_R using an unauthorized reader, even if it replays U_R , Hu-Fu will find the difference between $\langle C_L, C_R \rangle$ and $\langle U_L, U_R \rangle$ and reject the replay. As in Fig. 1(e), since the attacker does not know C_R , the signal from a counterfeit C'_c will highly likely to be different from C_R and it cannot get accepted.

Depending on the application requirements, Hu-Fu may be utilized in two situations, namely static scenarios and dynamic scenarios. In a **static scenario**, a legitimate tag is

¹Hu-Fu were authentication seals used by ancient Chinese emperors. The right piece was retained by the emperor and the left piece was issued to the army general. A messenger of imperial should show the right tally that matches exactly to the left piece to the general.

registered at the *check-in site* and its physical-layer feature is collected by the system. Later it is verified at the same place for authentication. Such scenario is useful for applications like access control, entrance guard, *etc.*. For example, a user who want to open the door authenticate his/her Right tag with the Left tag at the entrance. In a **dynamic scenario**, the *authentication site* where a tag is verified may be different from the check-in site. Such scenario is useful for applications such as a baggage claim system. For example, a user pick up his/her luggage by authenticating the Left tag attached on the luggage and the Right tag he/she holds.

3 SYSTEM DESIGN

To defend against different types of attacks, we propose to use two features in Hu-Fu, namely the *coupling feature* and *authentication feature*. We define the coupling feature as:

$$F_c = \frac{\int_{t_s}^{t_e} U_L dt}{\int_{t_s}^{t_e} C_L dt} = \frac{\int_{t_s}^{t_e} h(R, T_L) dt}{\int_{t_s}^{t_e} h(R, T_L, T_R) dt}, \quad (1)$$

where t_s and t_e are the start and end time of the tag's EPC segment. $h(R, T_L)$ and $h(R, T_L, T_R)$ are the hardware parameters, which are only related to the reader, Left tag and Right tag themselves. F_c can be used to detect signal replay attack.

We propose two metrics as the authentication feature. The first metric is defined as the specific value of energy spectrum of the Left and Right Tags:

$$F_e = \frac{\int_{t_s}^{t_e} C_L dt}{\int_{t_s}^{t_e} C_R dt} = \frac{h(T_L, T_R) \cdot \int_{t_s}^{t_e} x_L(t) dt}{\int_{t_s}^{t_e} x_R(t) dt}, \quad (2)$$

where $h(T_L, T_R)$ is hardware parameter, which is only depending on the hardware characteristic of the two tags. $x_L(t)$ and $x_R(t)$ are the code modulation of the Left and Right Tags, respectively. F_e is independent of the environment or reader.

The second authentication metric F_p is defined as:

$$F_p(T_i) = \left| \int_{t_s}^{t_e} e^{-j2\pi f_i t} C_i(t) dt \right|^2, \quad i = 'L' \text{ or } 'R', \quad (3)$$

where f_L and f_R represent the corresponding frequencies of the Left and Right Tags. Hu-Fu calculates and records both $F_p(T_L)$ and $F_p(T_R)$ from each EPC segment of the two tags.

Hu-Fu calculates the *Cross Correlation Coefficient* (CORR) of the two authentication vectors collected at the registration and authentication phases.

4 EXPERIMENTS AND EVALUATION

To demonstrate that the feature used in Hu-Fu is unique and can be used for authentication purpose, we conduct the following experiments. We use 101 ALN-9840 tags, pick one tag as the Left Tag, and use the other 100 tags as the Right Tag. We calculate the feature CORR of all pairs among the 100 Right tags, which are coupled with the same Left tag

Figure 2: CORR among 100 tags

under the same situation. As shown in Fig. 2, we find that 84% features have distinctly different features ($\text{CORR} < 0.5$). Only 0.55% of the CORR values show similar features of two Right Tags ($\text{CORR} > 0.74$, where 0.74 is the default value of threshold and can be set higher). We use other Right tags, which show similar results. Hence Hu-Fu can successfully detect counterfeited tags that carry the same ID but different physical features.

5 CONCLUSION AND FUTURE WORK

Hu-Fu is a physical layer authentication method for passive RFID tags. Hu-Fu is the first solution that is resilient to the a number of major attacks to tag authentication. We design Hu-Fu with two essential ideas, namely inductive coupling and signal randomization. In the complete version, we will build a prototype of Hu-Fu and conduct extensive experiments to show that Hu-Fu can achieve reliable accuracy.

6 ACKNOWLEDGMENT

This work was supported by National Basic Research Program of China under Grant No 2015CB351705, NSFC Grant No. 61572396, 61751211, 61772413, National Science and Technology Major Project of the Ministry of Science and Technology of China JZ- 20150910 and Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies. Chen Qian and Haofan Cai were partially supported by National Science Foundation Grants CNS-1717948 and CNS-1750704.

REFERENCES

- [1] B. Danev, D. Zanetti, and S. Capkun. 2012. On physical-layer identification of wireless devices. *Comput. Surveys* (2012).
- [2] Jinsong Han, Chen Qian, Xing Wang, Dan Ma, Jizhong Zhao, Wei Xi, Zhiping Jiang, and Zhi Wang. 2016. Twins: Device-free object tracking using passive tags. *IEEE/ACM Transactions on Networking* (2016).
- [3] Haitham Hassanieh, Jue Wang, Dina Katabi, and Tadayoshi Kohno. 2015. Securing RFIDs by randomizing the modulation and channel. In *Proceedings of USENIX NSDI*.
- [4] Ge Wang, Chen Qian, Haofan Cai, Jinsong Han, Han Ding, and Jizhong Zhao. 2017. Replay-resilient Physical-layer Authentication for Battery-free IoT Devices. In *Proceedings of ACM Workshop on HotWireless*.