A Security Framework in RFID

Pawankumar Tanavarappu

Department of MCA, YMT College of Management, Kharghar, Navi Mumbai, Maharashtra, India

ABSTRACT

Radio Frequency Identification (RFID) tags generally belong to a single domain system which is called has RFID single domain system. Till date, most of the researches in the RFID single domain system have been authentication protocol against a variety of attacks. This topic generally describes about the security and privacy mechanism in RFID multi-domain which is further divided into three sub-topics that is RFID forehand system security, RFID backhand system security and RFID inter-domain system security.

KEYWORDS: *RFID forehead System, backend System, Middleware system, tags*

How to cite this paper: Pawankumar Tanavarappu "A Security Framework in RFID" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-2, February 2020, pp.1026-1029, URL: www.ijtsrd.com/papers/ijtsrd30217.pdf

IJTSRD30217

INRODUCTION

One of the main obstacles to solve in Radio Frequency Identification(RFID) is security and privacy. Generally all RFID tags belong to a single domain security system. RFID security system is further divided into three sub-topic that is RFID forehand system security, RFID backhand system security and RFID inter-domain system security. RFID multi-domain system is particularly concerning the aspect of authorization and authentication. RFID cards are more secure choice then some card-based authentication.

Architecture:

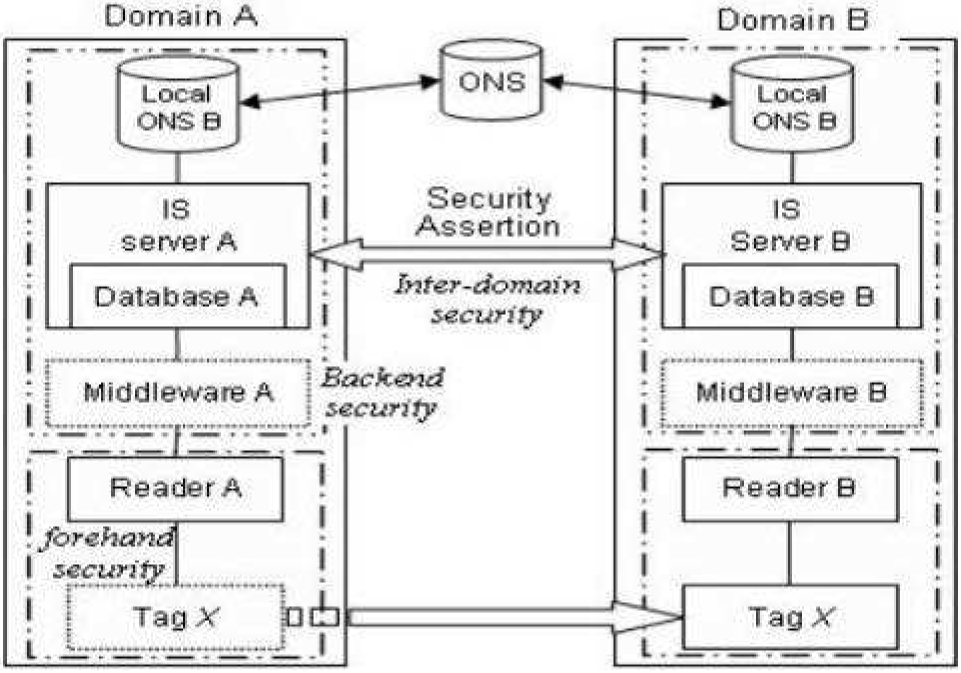

Figure: RFID Multi-domain System

RFID forehand system is commonly called has RFID system. It commonly consist of RFID reader, RFID tags and RFID database. Mainly security and privacy for RFID forehand system has not taken into account of security and privacy.

RFID backend system consist of RFID middleware, RFID Information Service and local object Name service. RFID backend system are of twofold that is entity security in backend system and communication security between entities. The entities in RFID backend system need to secure against threats.

RFID middleware system performs filtering, aggregation and counting the data. RFID middleware has to provide the security mechanism such as Denial of service tolerance or malicious request.

RFID tags are embedded into card which posses unique id number that is tagged inside the card. These id number are scanned

RFID Reader is a device capable of reading, storing and retrieving information stored inside the RFID tag. There are two type of RFID reader that is active and passive RFID reader, Active RFID reader can detect active reader from a long distance while passive RFID reader can detect a passive RFID tag a few centimetre away from a reader.

The above diagram describes has, suppose there are two different RFID domain under collaboration, the security policies are different to each other and don't share any common information. RFID tag X belongs to single domain A. The forehand security mechanism between tag X and reader can be applied according to the specification of tag X. The authentication protocols enable RFID reader to determine whether tag X is legitimate or not. Once the tag X is identified, the information of tag X and its related information can be stored in IS server in the format of PML through the RFID middleware. RFID middleware filters the malicious data from illegitimate RFID tag. ONS is used to retrieve the information od tag X. An existing security protocols such as SSL can be used to provide secure transaction between backend system entities. The tag X is attached on an object and moved to domain B.

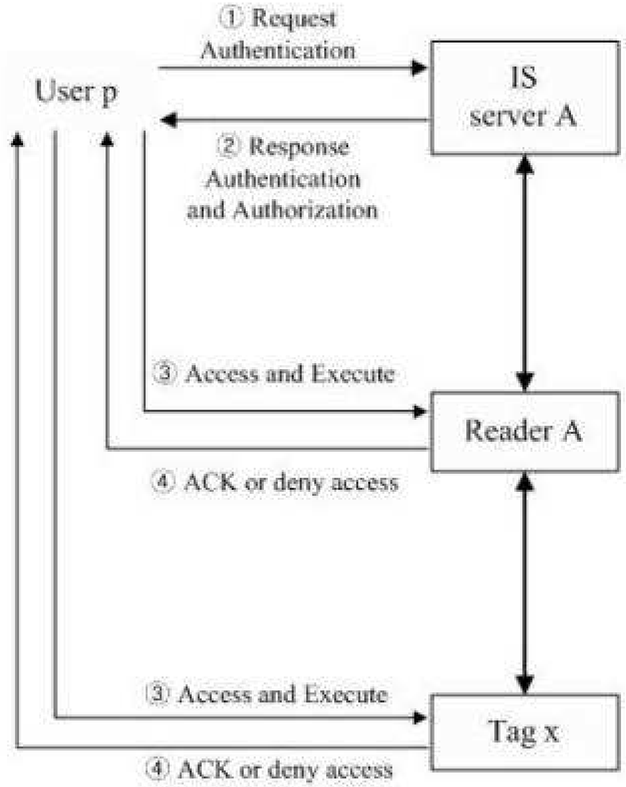

Figure: The authentication and authorization in single domain.

Suppose that there are user p and user q who belongs to domain A and domain B respectively, the user q requires authenticating her identification to domain A if she wants to get the permission to tag X. And the permission to be granted to user q will be determined on the security policy of domain A. This problem can be resolved as the authentication and authorization in the RFID inter-domain.

According to location of users service request, we classify the authentication and authorization into two case: One of the case that authenticate and authorize for users is performed in a single RFID domain if users service request is stemmed from internal in the single RFID domain. The other that authorize and authenticate for users is performed in the RFID inter-domain if users service request is out of responding RFID domain. The user p present a service administration in EPC global Network belongs to domain A. This paper proposes an authentication and authorization methodology in EPC global Network.

IS server A represent Information Service server A in EPC global Network. The reader and tag represent RFID reader and tag, respectively. The user p sends an authentication request to IS server. The IS server replies to user with authentication and authorization information of the user p. The access request is granted if the user q is authenticated by IS server, otherwise the access request is rejected. The user p may use service of reader and/or tag with respect to authentication granted by the IS server in domain A. The role of user and authentication information needs to be specified.

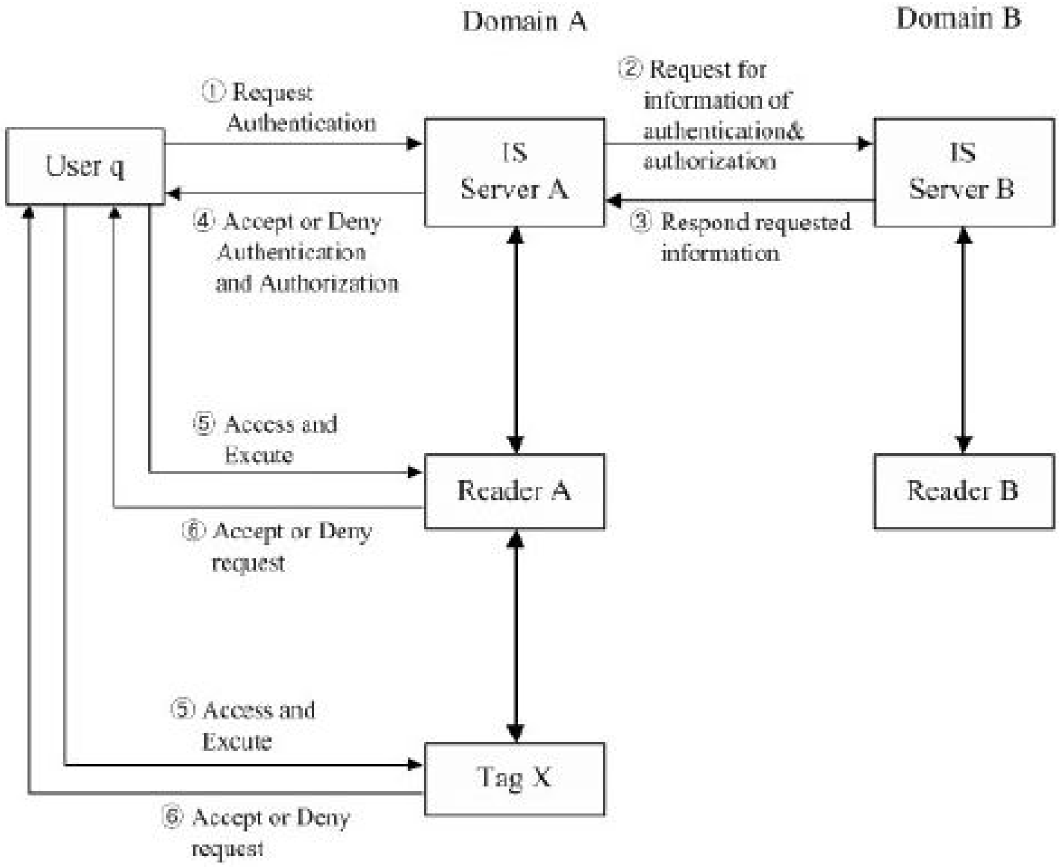

Figure: The authentication and authorization in inter-domain.

The flow of authentication and authorization in RFID inter-domain is depicted in the above figure. Suppose that domain A and domain B have the trusted security association beforehand. The user q is registered, authenticated and authorized in domain B. In this situation, user q sends a service request with users authentication information to domain A. The user q sends request for authentication to domain A. not the domain B. This implies that the authentication and authorization are delegated to domain A from domain B. This is one of the most important parts in authentication and authorization in RFID inter-domain. After user q sends the request to the domain A, the domain A sends it to the domain B. The IS server in domain B responds to domain A, with the requested information, including identification and attributes of the requested user q. The IS server in the domain A determines whether it accepts or denies the requested user q. If the user q is authenticated and authorized the user q is able to make use of service with respect to user's authorization. The user q may use reader or tag in the domain A.

Application of RFID network security:

The Radio Frequency Identification (RFID) Social Application Areas:

The areas of significant use are financial services for Information Technology and asset tracking and health care with more than 60% of the top medical device companies using passive UHF RFID in 2010.

Public Transit (bus rail, subway): In some country t-money card are used to pay the public transpsits.

Schools and Universities: RFID are used to track employees in company or students or staff are in or out the building via specially designed card.

Application of RFID used in Technical areas:

Electronic Vehicle Registration.

Payment by Mobile Phones.

Transportation Payment.

Security Attack On RFID System:

Man-in-the-middle or Sniffing: Man-in-the-middle happens during the transmission of a signal. The hacker listen the communication between RFID tag and reader and intercept and manipulate the information. The hacker diverts the information and sends the false data as it is a normal information in the RFID system.

Denial of service: This attack are usually physical attack like jamming the system with noise interference, blocking the radio signal and many more.

Cloning and Spoofing: This technic are done back to back. Cloning is duplicating the data of existing one, and Spoofing is then using the cloned data to gain the access to a secured area, so hacker has to know the data on the tag to clone it.

Conclusion:

This paper presents a security framework in RFID multi-domain system. The RFID forehand, backend and inter-domain security mechanism have been reviewed. An authentication and authorization in RFID inter-domain system have been evaluated with a case study.

References:

[1] https://ieeexplore.ieee.org/document/8204180

[2] https://tarjomefa.com/wp-content/uploads/2018/01/8544-English-TarjomeFa.pdf

[3] http://ijsrset.com/paper/3527.pdf

[4] D. M. Konidala, D. Kim, C. Y. Yeun and B. Lee, “Security Framework for RFID-based Applications in Smart Home Environment,” Journal of Information Processing Systems.

[5] Application Notes, “Introduction to RFID Technology” CAEN RFID The Art of Identification (2008).

[6] International Journal of Advance Research in Computer Science and Management Studies. Research Article/Case Study available: www.ijarcsms.com Development of a Student Attendance Management System Using RFID and Face Recognition.

[7] Secured Attendance Management System Using RFID Technology.www.irjet.net 08|Nov-2015.

[8] RFID based student monitoring and attendance tracking system. Author -Chatrati Sai Krishna, Naidu Sumanth, C Raghava Prasad Date:- 30 January 2014.

[9] Automation of Attendance system using RFID, Biometric, GSM Modern with .NET Framework. Author: Aamir Nizam Ansari, Arundhati Nevada, Sanchita Agarwal, Siddharth Patil, Balwant Date: 2011.