MULTI-DOMAIN RFID ACCESS CONTROL USING ASYMMETRIC KEY BASED TAG-READER MUTUAL AUTHENTICATION

Mingyan Li*, Radha Poovendran, Rainer Falk***, Andreas Koepf***, Michael Braun***, Krishna Sampigethaya*, Richard Robinson*, Scott Lintelman*, Hermann Seuschek*****
***Boeing Phantom Works, **University of Washington, *** Siemens Corporate Technology**
Keywords: *RFID Security, Access control, Tag cloning, Multi-Domain RFID systems*

Abstract

Multi-domain RFID applications, such as asset tracking across domains, shift the paradigm in business model and enable next-generation business processes for aviation industry. The increasing number of RFID applications also merits the consolidation of RFID tags so they can serve multiple purposes. However, the adoption of such multi-domain RFID applications depends on their ability to enforce access control to the tags that will be accessed by different stakeholders across multiple domains.

In this paper, we address multi-domain RFID access control. We evaluate existing solutions in the literature and identify their limitations. We propose using asymmetric key based tag-reader mutual authentication to grant only the authorized read/write access to tags. Challenges in deploying such an asymmetric-key based approach are identified, and solutions to one salient challenge, certificate management in resource-constrained RFID, are presented. Finally, we present a server-based access control scheme for multi-domain RFID systems and perform security analysis..

1 Introduction

The ubiquitous tracking capability and the low cost property of Radio Frequency Identification (RFID) tags have produced a wealth of applications in the aviation industry, such as airport security and supply chain [1]. With the emergence of network-capable or "eEnabled" commercial airplanes, a great opportunity has arisen for a wide range of RFID applications for eEnabled airplanes. For example, airplane maintenance is facilitated by connecting on-board RFID tags attached to airplane parts with data processing centers on the ground, and airline logistics is expedited by the communication between on-board RFID infrastructure and ground systems.

In [2], we envisioned an airplane mutli-purpose RFID system in which future on-board RFID tags and readers of eEnabled airplanes will be connected to different ground systems across multiple administrative domains, for multiple purposes such as logistics, maintenance, and access control. For example, the RFID tags attached to airplane parts will be accessed by airlines as airplane owner for logistics, may be contacted by third-party service providers for maintenance, and should allow the access from airplane manufacturer for part ordering. Another appealing cross-domain RFID application we foresee is the end-to-end part distribution, from supplier, manufacturer, to airlines. With part status recorded in the same tags, the tags will be read or written by different entities across domains during the distribution. Distribution status, in conjunction with workflow, enabled informed decisions and trigger events/actions timely, hence improve efficiency and accuracy of part distribution process.

The adoption of a multi-domain RFID system depends on its ability to enforce read/write access control to RFID tag data, as different stakeholders across domains have different ownership and read/write rights to RFID data. For example, in the part distribution application, the supplier can embed part price into RFID tags to facilitate the receiving process

at the manufacturer. However, such sensitive information should be restricted to only the finance department at the manufacturer. The part maintenance history contained in on-board RFID tags is the airline's proprietary information and the access should be protected against random or intentional access from illegal RFID readers, such as those of business competitors. Not only the reading of RFID tags need be controlled, but the writing to RFID tags has to be limited to authorized entities only. One example is that only certified personnel can inspect the part received and mark "inspection complete" to tags.

In this paper, we focus on the problem of access control in multi-domain RFID systems, i.e., how to ensure only authorized entities to read or write the correct portion of tag data. Our contributions are threefold. (i) We identify a vulnerability of prior works on RFID access control solution, i.e., the solutions are subject to tag cloning attack. We propose using tag-reader authentication to mitigate the loophole in the schemes. (ii) We propose a new server-based protocol for tag-reader mutual authentication that is suitable for resource-constrained RFID tags. (iii) We design a security protocol for controlling read/write RFID tags in the cross-domain scenarios and we perform security analysis of the proposed protocol.

The rest of paper is organized as follows. In Section 2, we state the problem and describe system and adversary models. In Section 3, we review two existing solutions related to RFID access control and point out their inadequacy as solutions to the multi-domain RFID tag access control. In Section 4, we first identify the tag-reader mutual authentication as a fundamental building block for multi-domain access control, and list the challenges in public key based authentication. We review two certificate management solutions suitable for resource-constrained RFID tags, and propose on-line and off-line server-based solutions. In Section 5, we present an access control protocol for multi-domain RFID applications, and perform security analysis on the proposed protocol. We conclude the paper with future research in Section 6.

2 Problem Statement and Assumptions

We envision that the multi-domain RFID applications will be widely invested in the future, due to the need to track tagged assets across domains and the need to consolidate the increasing number of various RFID applications. To enable the multi-domain RFID applications, we address the issue of access control in this paper, i.e., *correct portion of RFID tag data is read (write, respectively) only by authorized entities that are granted reading (write, respectively) right.*

2.1 System Model

As shown in Figure 1, a multi-domain RFID system considered in this paper consists of RFID tags, RFID readers (also called RFID interrogators) and backend servers located at different domains. Middleware as the software for interpreting the radio waves into logic terms which can be integrated into the portable RFID reader or separate from reader but resides with a PC, is not explicitly shown in the picture. Tags contain information that will be accessed by readers and backend servers from multiple domains. Each domain has different read/write access right to different portions of the data.

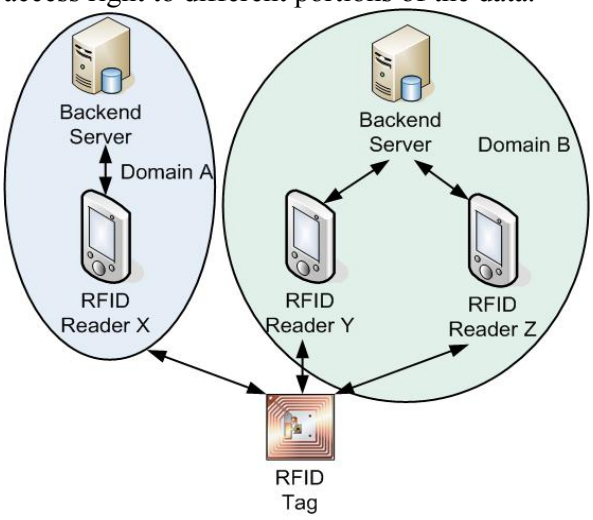

Fig.1 Multi-Domain RFID System

Network assumptions: We do not assume that the connections from tags to interrogators and from interrogators to backend server are online all the time; the network connection can be intermittent. For example, network

connection can be limited when RFID assisted maintenance is performed at a remote airport.

Trust assumptions: We assume that backend servers are trusted entities. Back-end servers are in charge of addition and deletion of tags, and readers (which we collectively call "nodes") in their domains by announcing revocation and providing new nodes with proper credentials.

2.2 Adversary Model

In this paper, we consider the adversary capable of launching passive attacks (e.g. eavesdropping) as well as active attacks (e.g. spoofing and node impersonation attacks), on the links between tags, readers and servers. We do not consider insider attackers, i.e., we assume that trusted entities will perform the authorized operation correctly. Accidental operational errors are not regarded as attacks: they will be addressed using standard fault tolerance and/or error remedy procedure, which are out of the scope of the paper. However, we do not address the malware attacks [4] that contaminate middleware and jamming attacks in this paper.

We assume that sufficient physical security checks are in place to prevent unauthorized cabin access to onboard systems, so to on-board RFID tags. Therefore, we do not consider node capture attack. The physical access control provides the first line of safeguards against the threats imposed by the adversary. In addition, we assume that the adversary is unable to obtain the private or secret keys of tags and readers.

The objective of the adversary is to disrupt the asset tracking and management by manipulating the RFID data and/or spy on the business sensitive information stored at RFID tags. For example, the adversary may try to retrieve the proprietary information of other domains for lubricant purpose. As an additional attack, the adversary can impersonate a bogus RFID tag by spoofing the tag identity (ID) to cause unnecessary operational cost and to induce false asset maintenance history, leading to a reduced reliability and confidence in the multi-domain RFID system.

In the subsequent sections, we investigate the technological challenges and solutions to protect the multi-domain RFID systems after reviewing the state of the art on RFID access control

3 Insufficiencies of Prior Solutions to Tag Clone Attack

Security and Privacy of RFID systems attract extensive research interest and efforts. Both [3] and [4] present excellent survey on the state-of-the-art solutions to RFID security and privacy. A more up-to-date bibliography on security and privacy in RFID systems is available online [5]. In [6], Ari Jules pointed out the lack of literature on key management for RFID systems, with most of research papers devoting to tag-level privacy-preserving authentication protocols.

In [7], a prototype of an end-to-end system solution for RFID security, called Authentication Processing Framework, was reported. In [8], the infrastructure for multi-context/domain RFID applications was proposed. One novel idea of [8] is that both location and time are taken into account when authenticating and authorizing the RFID readers. However, we identified that both solutions are subject to tag clone attacks. We now provide more details of protocols presented in [7] and [8], and illustrate how the solutions are insufficient to control the access to RFID tags whose data are updated from time to time.

3.1 Authentication Processing Framework [7]

Authentication Processing Framework (APF) consists of tags, readers and APF database. APF was proposed to preserve the confidentiality of RFID data and restrict the access only to authorized RFID readers [7]. There are three phases in the secure retrieval of RFID data: (i) registration phase, (ii) interaction between a tag and a reader (iii) interaction between the reader and the APF database. In phase one, tags and readers register their unique identities with APF database, the tags will also leave their decryption keys with APF database. Data stored in tags are encrypted to control the access. In phase two, a tag sends its ID in clear and offers the encrypted data to a requesting reader upon receiving a command from the reader. In phase

three, the reader will authenticate to the APF database, the APF will verify the access matrix and decide whether to issue the decryption key to the reader.

In this framework, authentication of readers is performed at the APF servers. The validation of tag ID is based the 'uniqueness' of RFID tags. However, Siemens-Boeing team has implemented an attack module (see Fig 2), capable of tag cloning by eavesdropping the tag ID, recording and replaying it. The attack module only costs 10-20 US dollars and the circuit can be built using materials from electronic hardware store such as RadioShack.

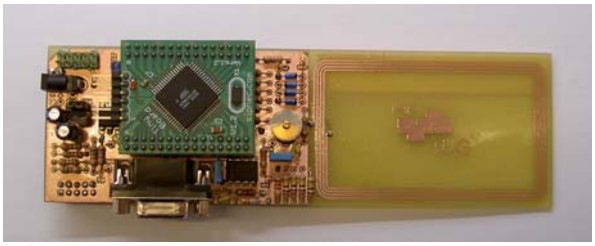

Fig. 2. The Tag Cloning Attacker

A forged tag may not be able to obtain the encryption key of the legitimate tag it impersonates, i.e., it cannot deceive an authorized reader into believing bogus information. However, it can cause an undesired delay in the data retrieval, unnecessarily consume the reader's computation time and power, and waste the APF database server time in communicating with the reader and verifying the access matrix.

3.2 Multi-Context RFID Infrastructure [8]

Secure access to multi-context RFID tags is addressed in [8], which is similar to access control in multi-domain RFID applications investigated in this paper. However, difference exists; their proposed protocol is limited to the applications where backend servers have a precise copy of tag data, while our cross-domain RFID access covers the applications where RFID tags are dynamically changed.

In [8], a backend server is assumed to have legitimate RFID tag IDs, reader IDs, and access policy. The protocol for the authorized interrogator to retrieve data from a cross-domain RFID tag is comprised of three phases. In phase one, reader acquires a ticket from the server to access the tag after authenticating itself to the server; In phase two, the reader submits the ticket to tag and also responds the tag's challenge (i.e., a nonce) by encrypting the nonce with reader's private key; the tag will encrypt the ticket, the encrypted nonce from the reader, and tag ID using the server's public key, and transmit to the reader the resulting cipher-text, called credential. In phase three, the reader presents the server with the credential and the server will selectively disclose the tag data to the reader based on its access right.

The multi-context RFID infrastructure implicitly assumes that the backend server keeps an exact copy of RFID tag data. The infrastructure applies to static data scenarios, such as RFID passport. However, it is inadequate for the scenarios where RFID data dynamically updated. In the example of tracking part during the cross-domain distribution, the current status of tagged part, such as received or inspected, is written to the tag to trig next action item in the work flow. Unless the backend server always synchronizes with RFID tags, which requires network connectivity and incurs communication overhead, the server does not retain an up-to-date copy of RFID data in general. In case that frequent data synchronization between the tags and the backend server is impossible, a more feasible solution is for the readers to bring back a copy of encrypted tag data for the server to decypt or to obtain an access token, such as decryption key in [7], that allows the reader to access the tag. Similar to the analysis of the APF, the lack of tag to reader cryptographic authentication leaves the system open to the injection of false tag data by forged RFID tags.

4 Cryptographic Tag-Reader Mutual Authentication for Access Control

We propose using public key cryptographically-derived digital signatures for mutual authentication between tags and interrogators, so that access control in multi-domain RFID applications can be enforced upon the authentication. Compared to leveraging encryption to control the access to tag such as APF [7], tag-reader mutual authentication based

approach provides two advantages: (i) it enables fine-granularity access control (ii) it reduces either key management overhead or the required computation and/or storage at tags. If data is encrypted using a symmetric key shared among all the recipients, any membership change of the set of the recipient set will incur rekey overhead at the key holders. If tag data is encrypted using public key of each intended recipients, the tag needs to prepare multiple copies of same data for recipients across domains.

Many prior works built the tag-reader authentication on the symmetric key cryptography, due to the consideration of limited computation power in RFID tags [7,9]. Symmetric key based authentication (i.e. the claimer and the verifier share a key) is vulnerable to the compromise of either party in the authentication. For example, in case of the compromise of a reader, all the tags that share a pair-wise key with the untrustworthy reader need to be updated with the new keys securely, hence incurring prohibitive overhead for key renewal.

In contrast, there is no secret key shared between the claimer and the verifier when using digital signatures. In public key cryptography (also called asymmetric key cryptography), a pair of keys including public key which is publicly available and private key which is kept as secret, are assigned to each entity. To authenticate to the verifier, the claimer signs a challenge message from verifier using its private key, and appends a digital certificate that confirms the link between the claimer and its public key. The verifier uses the certificate to verify the validity of the signer's public key and validates the integrity and authenticity of the message using the signer's public key. If an entity is no longer trustworthy, its certificate is revoked and the revocation is announced publicly by the certificate authority (CA).

4.1 Feasibility of Tag-Reader Mutual Authentication

The stronger security strength of public key based authentication, when compared to symmetric key based authentication, is achieved at the expense of computational complexity. Therefore, public key based cryptography used to be regarded as impractical for resource-constrained wireless sensors and RFID tags. However, it is reported in [10] in 2005 that Elliptic Curve Cryptography (ECC) signature verification takes 1.61s with 160-bit keys on ATmega128 8MHz, which confirms the viability of ECC based digital signature. In [11], four main state-of-the-art ultra-lower power public key cryptography algorithms are compared and implemented. NtruEncrypt and NtruSign were reported to have the least average power consumption and "the smallest implementation of Ntruencrypt with a single arithmetic unit takes up a chip area of less than 3000 gates consuming less than 20 μW".

In a recent collaborative effort between Siemens and Boeing, we have implemented ISO 14443-A passive RFID tags capable of ECC based mutual authentication with RFID readers [12]. The signature verification takes 70ms and the total cost of each RFID tag is around a few US dollars. The protocol for mutual authentication between the tags and the reader is a standard challenge-response protocol initiated by the reader.

With the advance in electronics technology, the manufacturing cost and computation cost (in terms of power expenditure) for tags of same performance are expected to drop further, and the public key based cryptography will be more widely acceptable and feasible for low-end devices such as RFID and sensors.

4.2 Challenges

Although it is computational feasible for a passive tag to mutually authenticate with an interrogator, realization of public key based tag-reader mutual authentication for access control presents challenges in multi-domain RFID applications.

4.2.1 Trust Establishment across Domains

The fundamental challenge for any cross-domain applications is the trust establishment across domain boundaries [13]. For example, how to enable an entity in domain A to verify a digital signature from domain B, i.e., how to check the status of the associated certificate?

The two domains either have established prior trust agreement so that domain A retains a copy of trusted certificates from domain B or they can leverage the trusted third party, for example a commonly trusted CA, to establish trust. The diversity of business relationships between different domains and the variety of policies and even technical readiness levels at each domain complicate the trust establishment.

4.3.2 Certificate Management

The challenge with public key based applications is the management of certificates that are used to bind the entity with its public key. Certificates have their lifetime and need to be updated when expired. Upon addition and/or revocation of certificates due to, for example, business dynamics in terms of role or authority change of public key owners, the status of certificates and new certificates need to be broadcast in a timely manner so verifiers have the updated knowledge of the trusted certificates.

4.3.3 Online Access to Backend Server

As online access to the backend server may not always be feasible, it impacts the capability of RFID tags and readers to verify the up-to-date certificate status and to obtain the latest access policy. In case of the intermittent network access to backend server, we propose that tags and readers should download the latest access control list/matrix and validate the status of certificates whenever there is a connection to backend server.

4.3.4 Resource Constraints in RFID Tags

RFID tags have limited transmission range, constrained storage and computation power. As RFID tags cannot be assumed to be constantly connected to the network one approach to obtaining the certificate for public key based applications is to store the trusted certificates locally. However, the storage limitation restricts the number of trusted certificates that can be stored in tags locally. For access control to different portion of data, it is desired that RFID tags have hardware built-in compartments that are used for different data owners and reviewers, which imposes a technical challenge on low-cost RFID tags.

4.3 Certificate Management for Resource-Constrained RFID Tags

The certificate management is widely known as a challenging issue for public key based applications, the resource constraints in RFID tags and intermittent access to backend server further add more complexity to the problem. In [12, 13], we have compared several conventional approaches for certificate management, including whitelist approach, certificate revocation list (CRL), online certificate status protocol, short-live certificates. In [12], we identified two suitable certificate management solutions for RFID tags, i.e., whitelist with bloom filter [14] and hash chain based certificate revocation [15].

In the following, we will present a new server-based approach that does not require RFID tags to hold readers' credentials, hence eliminating excessive storage requirements at tags. We also compare the newly proposed server-based approach with bloom-filter and hash-chain based approaches. For the purpose of completion, the next sections include a short description of the bloom filter and hash chain based approaches.

4.3.1 Whitelist with Bloom Filter [14]

In the whitelist approach, a list of trusted certificates are reloaded into tags via an out-of-band, integrity and authenticity protected mechanism. Due to limited storage resources, a tag or a sensor may contain only a limited number of certificates. To increase the number of certificates held in a tag, a Bloom filter was used to efficiently represent the current valid public keys [14]. Instead of storing a complete copy for each certificate, a Bloom filter provides a space-efficient probabilistic data structure to represent an element and to test if an element is in a set with a small probability of false positive.

In Bloom filter based public key validation, all the current valid public keys are mapped to a bit array of m bits by applying independent hash functions and setting the bits at the position indicated by hash results to 1. The m-bit Bloom filter is preloaded to each participating nodes in the RFID tags. When a signed message arrives, the verifier will first check if the public key is

contained in the list of valid public keys represented by the preloaded Bloom Filter. Upon the update of the status of a public key, a new Bloom filter is recomputed by the CA and only a compact representation of the changed bits is broadcast. The Bloom filter based approach improves the storage efficiency at the expense of its possibility of false positive, and false positive increases with the number of readers in the system.

4.3.2 Hash Chain based Certificate Revocation [15]

In the hash chain based certificate validation [15], a hash value is computed for every validity period, such as every day, week, or month. For illustration, we assume weekly validation is provided. For a certificate that is expected to be valid for a year after issued, a hash chain (X0, X1, …, X51) is computed where Xn = H(Xn-1) = Hn(X0) and H denotes the hash function, and the hash chain anchor X51 is loaded to tags or sensors. On the third week, if a reader needs to authenticate itself to a tag, it attaches its certificate with its digital signature and also provides the validation token, X48, obtained from the CA. To check if the certificate is valid, the tag applies the hash function H to the token X48 three times, H(H(H(X48))), and compares the result with the hash chain anchor X51. If equal, it demonstrates the validity of the certificate. Otherwise, the tag will discard the message and discontinue further communication with the reader.

Compared to CRL approach, the hash chain based certificate validation significantly reduces the communication overhead for certificate validation, from the size of CRL to the size of hash (for example, 160-bit), and only requires loose time synchronization between the verifier and the CA.

4.3.3 Server-based Authentication

In the server-based authentication approach, the mutual authentication between tag and reader is realized through the server. First, the RFID reader authenticates itself to the server. After successful authentication and validation of the reader's access right, the server will issue a session key to the reader. Then, the tag mutually authenticates with the server: the reader facilitates the process by forwarding the challenges-response exchange between the tag and the server. Please note that the reader has no incentive to disrupt this communication if the reader wants to read/write the tag. Finally, following upon the successful mutual authentication between the tag and the server, the server will issue the same session key to the tag to enable the secure communication between the tag and the reader.

The server-based approach removes the necessity of storing readers' certificates and verifying the status of readers' certificates at tags. A tag only needs to store the certificate(s) of authentication server(s). The drawback of this approach is the online tag-server requirement, which can be a challenge in practice. Therefore, we propose the following modified version of the server-based approach, called offline server-based approach, to loose the online requirement by leveraging time synchronization between the tag and the server.

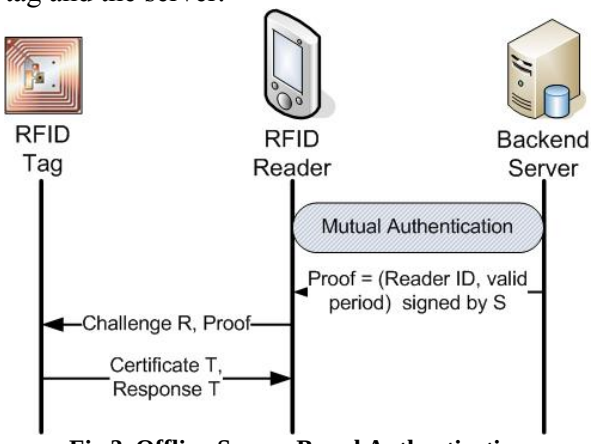

Fig 3. Offline Server-Based Authentication
(T and R stands for tag and reader, respectively)

As illustrated in Fig. 3, the reader and the server conduct mutual authentication first. In the responding to the challenges from the server, the reader will also send a request for a *proof* of the valid status of its certificate. The server will issue such a proof that is a signed copy of reader ID, and the validation period. The reader initiates the authentication with the tag by providing the proof to the tag as well as sending a challenge to the tag. Based on current time/date, the tag verifies the server signed message to confirm the validity of the reader. If successful, then the tag will respond to the readers' challenge to authenticate itself to the

reader. The offline server based approach requires tags to be able to acquire current time/date.

4.3.4 Comparisons

Table 1 compares all the approaches that address the complexity of certificate management at resource-constrained RFID tags.

Table 1. Comparison of Certificate Management Approaches suitable for RFID systems.
(mod. stands for moderate, comm. for communications)

Tag requirement	Whitelist with Bloom Filter	Hash Chain based	Server based online	Server based offline
Comm. overhead	Low	Mod.	Mod.	Mod.
Storage Requirement	Mod.	Low	Low	Low
Computation for certificate validity check	Mod.	Low ~ Mod.	Mod.	Mod.
Online Connectivity required	No	No	Yes	No
Loose Synchronization required	No	Yes	No	Yes

As presented in Table 1, the whitelist approach with bloom filter is the most communication efficient approach, and its drawback is the potential false positive in certificate status check. The hash chain based solution has the advantage of low storage at tags, however, it requires loose synchronization with the server in terms of date (or time). As the date/time of certificate status check determines the number of hashing computations to be performed, the computation cost at tags runs from low to moderate, depending on when to check the certificate status. Certificate management at tags is significantly simplified when using either online or offline server based approach, as the tags only need to verify or trust the certificates of the server. The proof used in the offline version of sever-based approach is similar to the token used in hash-based solution. However, these two approaches differ in that hash based approach requires the hash anchor to be pre-loaded at tags while no such a requirement exists for the offline server-based approach. It follows that the server-based approach accommodates the dynamics of readers more easily. Another advantage of the offline server-based authentication is that it can be easily adapted to the protocol for multi-domain access control, as demonstrated in next section. However, we will show the loose synchronization requirement is substituted by the concept of progressing, logic time.

5. Multi-Domain Access Control Protocol and Security Analysis

In this section, we define a multi-domain access control protocol and analyze its resilience to identified attacks.

5.1 Protocol Description

Our multi-domain access control protocol for RFID systems is built on the offline server based authentication. We assume that the cross-domain access control policy is established during the initialization phase, and every backend server holds a copy of the access control policy.

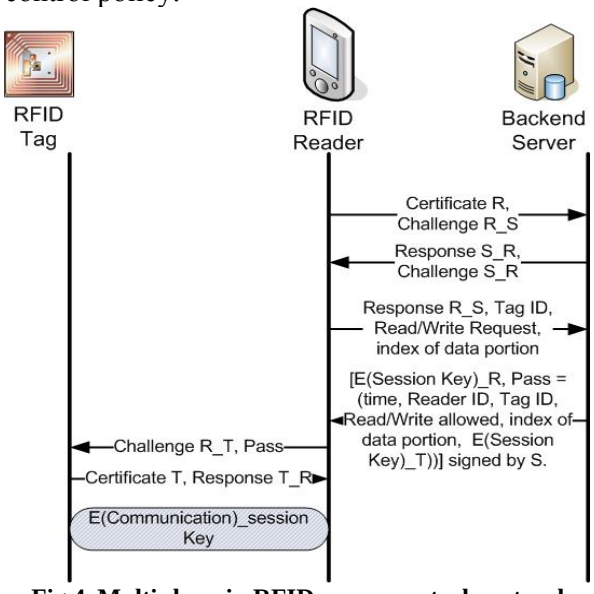

Fig 4. Multi-domain RFID access control protocol
(E(X)_y denotes encryption of X using key Y; we use T, R, S to denote tag, reader, and server; Challenge/response X_Y is a challenge/response from X to Y)

As illustrated in Fig. 4, after mutual authentication with the backend server, the reader sends an access request to the server with the intended tag ID, read or write access,

possibly with the intended portion of the tag data. The server will confirm the access right of the requesting reader against the stored access policy and issue a *pass* permitting access. Such a pass consists of time, the reader ID, the tag ID, read and/or write allowed, index of the portion of tag data, and encrypted session key using tag public key, and the digital signature of above information by the server. The server will also transmit to the reader the same session key encrypted using the reader's public key.

During tag-reader interaction, the reader sends a challenge and presents the pass to the tag. The tag validates the reader's access right by checking the server signed pass, verifies the time is newer than the time of the last received pass to ensure the freshness of the pass. If successful, the tag decrypts the session key contained in the pass and replies to the reader with a response to authenticate itself. Following the successful mutual authentication between the tag and the reader, they can start a protected communication using the session key issued by the server. In case the reader requests the write access to the tag, the content to be loaded to the tag is signed by the reader's private key for integrity protection.

When there is an addition or a revocation of readers and tags, or a change in their access rights, the access matrix/list needs to be renewed. In the access control protocol, the access policy resides with backend servers. Compared to distributed access policy management, e.g., at readers, the centralized management and enforcement of access policy in the proposed protocol make it easier to update the access policy, hence adapting to network and business dynamics more efficiently.

5.2 Capabilities Required at Tags

Using the proposed protocol, a tag needs to preload its own certificate and the certificates of the servers in each domain. In each tag query, the tag performs three public key computations, for validation of a pass, for decryption of a session key, for digital signing a reader's challenge. The following tag-reader messages are encrypted by symmetric session key. The tag is not required to have the knowledge of current time but to tell the time difference of the current pass from the previous one.

It is possible that reader X acquires a pass before reader Y but is refused the access to a tag, as reader Y used its pass to inquire tag prior to reader X. In this situation reader A can re-request a new pass from the server.

5.3 Security Analysis

The access control protocol we propose for multi-domain RFID applications is secure against the following attacks: eavesdropping, tag cloning, reader impersonation, and manipulation of tag data.

Eavesdropping: The communication between a tag and a reader regarding tag data is protected by a session key issued by the backend server. As the session is encrypted by the reader's or the tag's public key so only the reader and the tag can decrypt the session messages. Therefore, the eavesdropping of the wireless link between the reader and the server will not allow the adversary to peek tag data.

Tag Cloning: As a reader authenticates the tag by checking the tag's certificate, by verifying the signed response from the tag before downloading or inserting the data, tag cloning will be detected and the communication with a fake tag will be discarded.

Reader impersonation: There are three different types of reader impersonation attacks: bogus reader impersonation of a legitimate reader, impersonation of a reader with privileged access, and revoked reader pretending it is authorized by replaying a previously issued pass. The spoofing of legitimate reader by a fake one is defeated by the server's authentication of the reader before releasing a pass. Impersonation of a privileged reader is defended by the server's authentication of the reader and by deciding the reader's access rights according to the established access policy. The replay of a used pass in order to gain unauthorized access after the revocation of a reader will not succeed, as the time in a pass changes at each reader's request.

Manipulation of Tag Data: As the tag data will carry a digital signature from data

generator, manipulation of tag data by an adversary will be detected. Please note we do not consider insider attacks in this paper.

6 Conclusions and Future Research

With the advancement of RFID technology, the asymmetric key based mutual tag-reader authentication is feasible at resource-constrained tags. Mutual authentication enables fine-granularity access control, which is preferred especially in multi-domain RFID applications. However, with a vast number of potential readers, tags and their dynamics, the certificate management is a daunting challenge. In this paper, we first review and present efficient certificate management solutions suitable for RFID tags. Built on the server-based authentication, we present the mutual access control protocol for RFID systems, and the security analysis confirms the resilience of the proposed protocol against identified attacks.

In the future, we would like to formally analyze the security of the proposed protocol, using machine assisted model checker. Formalism of access control policy is of our research interest, as well as the investigation of distributed access control enforcement.

References

[1] S. Garfinkel, B. Rosenberg (Eds.), RFID Applications, Security, and Privacy, Addison-Wesley, 2005.

[2] R. Falk, F. Kohlmayer, A. Koepf, M. Li, High-assured Avionics Multi-Domain Processing System, *In Proceedings of IEEE RFID conference*, Las Vegas, NV, April 2008.

[3] A. Jules, RFID Security and Privacy, A research survey, *IEEE Journal on Selected Areas in Communications*, February 2006.

[4] M.R. Riebak, B. Crispo, A.S. Tanenbaum, Is your Cat Infected with a Computer Virus, *IEEE PerCom*, March 2006.

[5] A. Jules, Four Aspirations for RFID Security Research, *ACM Conference on Wireless Network Security*, 2008, http://sconce.ics.uci.edu/wisec08-rfid-panel/RFID-Juels.pdf

[6] G. Avoine, Bibliography on Security and Privacy in RFID systems, Version December 2007 http://lasecwww.epfl.ch/~gavoine/download/bib/bibliography-rfid.pdf

[7] J. Ayoade, O. Takizawa, K. Nakao, A Prototype System of the RFID Authentication. *In Proceedings of 3rd Intl. Workshop in Wireless Security Technologies*, London, U.K., April 2005.

[8] S. V. Kaya, E. Savas, A. Levi, O. Ercertin. Public key cryptography based privacy preserving multi-context RFID infrastructure, *Ad Hoc Networks*, online available, February, 2008.

[9] B. Alomair, L. Lazos, R. Poovendran, Passive attacks on a class of authentication protocols for RFID, *Int'l Conference on Information Security and Cryptology*, 2007.

[10] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, Energy analysis of public-key cryptography on small wireless devices, *IEEE PerCom*, March 2005.

[11] G. Gaubatz, J. P. Kaps, E. Ozturk, B. Sunar, Sate of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks, *Proceedings of 3rd Int'l IEEE PerCom workshop*, 2005 .

[12] M. Li, C. Fung, K. Sampigethaya, R. Robinson, R. Poovendran, R. Falk, A. Koepf, Public-key based authentication for secure integration of RFID and sensor data, *In Proceedings of 1st ACM workshop on heterogonous sensor and actor networks*, Hong Kong, China, May, 2008.

[13] R. Robinson, M. Li, S. Lintelman, K. Sampigethaya, R. Poovendran, D. von Oheimb, and J.-U. Bußer, Impact of public key enabled application on the operation and maintenance of commercial airplanes, *In Proceedings of AIAA ATIO Conference*, Belfast, Northern Ireland, September 18-20, 2007.

[14] K. Ren, W. Lou and Y. Zhang, Multi-user broadcast authentication in wireless sensor networks, *In Proceedings of IEEE SECON*,, San Diego, CA, June 18-21, 2007.

[15] S. Micali, NOVOMODO- Scalable Certificate validation and simplified PKI management, *In Proceedings of the 1st Annual PKI Research Workshop*, 2002.

Copyright Statement