A Framework for RFID Systems' Security for Human Identification Based on Three-Tier Categorization Model

Mu'awya Naser, Mohammad Al Majaly, Muhammad Rafie, Rahmat Budiarto
Computer Science school
Univrsiti Sains Malaysia (USM)
Penang- Malaysia
aldlieen@yahoo.com ,moh.majali@gmail, {rafie,rhmat }@cs.usm.my

Abstract— **Recent researches in the Radio Frequency IDentification (RFID) attempt to raise solutions for general applications within the field, these solutions often are hindered by the fact that different RFID deployments do not meet in their specifications and need. In order for these solutions to be valid and more useful; it has to be classified based on certain design requirements, and exploitation area. Our research contributes to those solutions in a novel model for a three-tiered categorization of the RFID systems in an attempt to undertake security and privacy risks into a better understanding within a specific domain for a more optimized addressing of the problems encountered.**

Keywords-component; RFID securtiy, MAC mutual authontecation protocol.

I. INTRODUCTION

The Radio Frequency Identification systems produce methodologies to data portability through embedding these data in small devices (Tags) that can be mobile and held within other objects. These data may have human identification data to grant access authentication to several transactions or entry passes through secured checkpoints in different locations, the security and privacy issues of this data are intimidated by various threats.

This paper proposes a framework for choosing among different available solutions based on categorizing the intended use of the systems and the (Tag-Reader-backend database) protocols involved in hardware configurations. On the other hand, the paper limits the framework for human identification purposes and the security issues related to mutual authentication schemata.

II. RELATED WORK

There is a huge need to configure systems that holds human data in their applications in order to personalize the use of these applications, and/or to create stand alone data for analysis and tracking purposes [6]. Human identification tags may seize this data but, however, the privacy issues and security threats hamper the wide applications of such tags; who is capable of reading and obtaining this data? When and where to read it? And how this data is being transferred between the RFID infrastructure main components i.e. Tags, Readers, and Back-end databases?

Many security schemata can be used in identification, some are efficient, some are effective, and some are both [8]. In the case of mutual authentications it balances between security capabilities, cost, and easiness of appliance. Mutual Authentication Code (MAC) protocols may vary against various threats; these protocols can cover a wide range of threats based on the desired security level by projecting what threats are valid for the application. Some of the threats mentioned in previous researches for MAC include but not limited to Eavesdropping, Relay attacks, unauthorized tag reading, Tag cloning, People tracking, Replay attacks, Tag content changes, Physical tag destruction, Blocking and jamming. [6]

This paper categorizes the RFID based on number of tags it reads each time and how many readers are involved. Moreover, based on that; the system features will be described, and the security concerns will be distinguished, the categorization of the RFID system will be in three categories.

III. PROPOSED FRAMEWORK

For those who interest in RFID they should put the next categorization in their consideration, because so far, many approaches and protocols have been conducted but most of them could not fit all RFID categories. Also, previous work does not categorize RFID applications according to these components.

New applications need to assess the protocols which will be used in securing the attacks faced by data within the tags, or between the tags and readers during the transfer of data. The following categorization allows further evaluation for choosing appropriate methods and protocols to correspond the data between components:

1. many tag- one reader
2. one tag- one reader
3. many tag- many reader

Many-Tags-One-Reader (MTOR) represents the status where the reader has to handle many tags at the same time. The protocols that will be used should be simple enough to carry on reading a relatively big number of tags at the same time to avoid facing a jamming threat. An example for MTOR is an organization access control where all employees are entering the location in varying flow numbers through one reader.

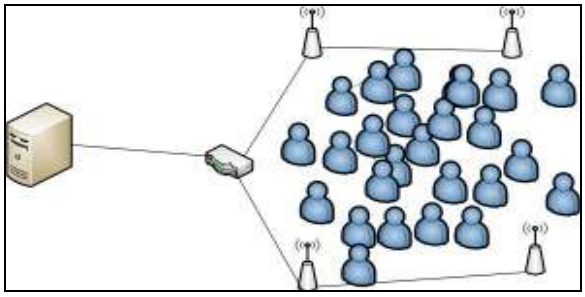

Figure 1. MTOR Architecture

One Tag One Reader (OTOR) is considered a special case of many tags one reader where the tags pass through the reading zone one by one e.g. e-passport access control in the airport where the passenger exhibits his/her e-passport (which carries a tag) to the reader's point and maybe his/her biometric identification data in order to allow him/her to pass the checkpoints. This category will be –mainly- in very limited location. Furthermore, OTOR is regarded as the simplest category because the security protocol designer does not have to go through very low-weight protocol in order to authenticate the assumed tag(s). In addition, OTOR do not have DNS or jamming threats.

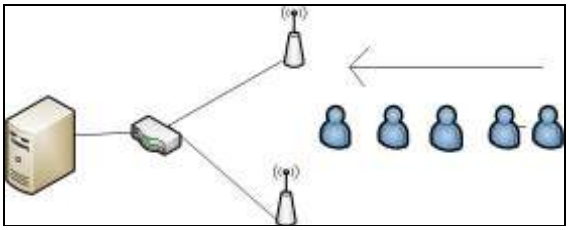

Figure 2. OTOR Architecture

Moreover, the MTOR reading zone probably is going to be larger than OTOR category where the reader is able to use more than one antenna in order to increase the coverage area, in addition to the number of tags that will be read. Obviously, threat and security risks will rapidly increase due to the increment of the tag number.

Many tag many readers (MTMR) is when the reading zone area is extendable and contains many readers handling a huge number of tags at the same time, like crowed monitoring applications, which drives to create extremely simple protocols which could handle this big number of tags, added to that, we have more security risks and threats to undertake in consideration. Some of these considerations under this category are the time and space coordinates for a certain tag; as in each tag is read by a certain reader – covering a certain space- at a specific time. When the tag depart this space (zone) or for an example the reader becomes out of service, the rest of the readers should be able to handle the situation (read the tag by a different reader) or the system will be compromised.

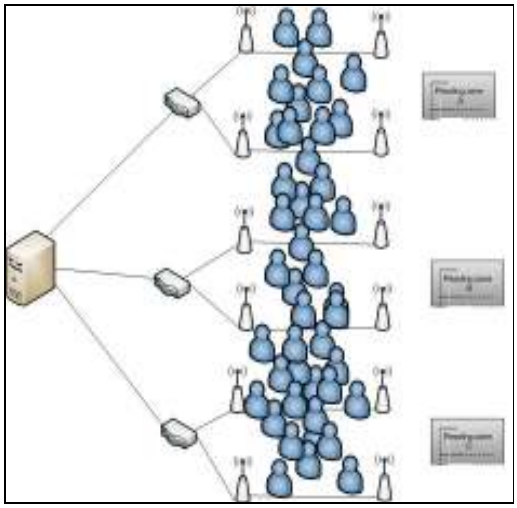

Figure 3. MTMR Architecture

MTMR in MAC protocols could not carry the tags secret keys in the reader's since the number of tags are too many to be handle in that method, in addition, once the key is updated, it is not easy to update it by all readers' memory because of network jamming ,dissection or missing data among other problems. Furthermore, this paper recommends shifting all processes to the backend database in order to make sure all keys are updated completely. In this case, the reader will become a third party device serving just as a modulator to transfer the data between the tag and the backend database.

IV. FEATURES OF THE CATEGORIZATION

The three-tier categorization of the tag-reader combinations differ on its handling to the features involved in the overall architecture; the purpose here is to decrease the complexity of these systems in the implementation perspective. The efficiency of each category bases on the requirements of these features and could aid in the design and development in the time and cost manner needed. Experts are not required for each and every simple application of these categories; this would allow organizations to choose developers based on their needed rather than desired outcome. Figure 4 illustrates the level of concern regarding the features in the categorization:

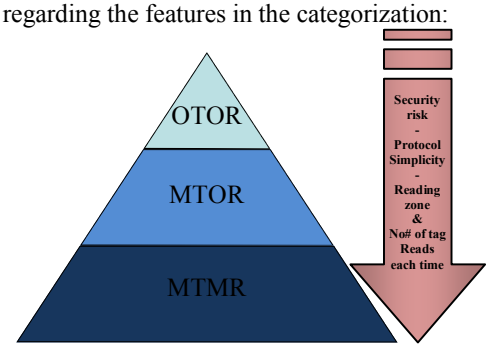

Figure 4. three-tier pyramid model characteristics

Following is a description of the features of the three categories dividing those features into ranges of consideration, the features are compared for the categorization in table 1:

a) Protocol simplicity: the more tags involved, the more we need a complex algorithm to increase the simplicity of handling those tags, increased simplicity refers to a high algorithm complexity to raise the efficiency of process.

b) Jamming threats: the possible parts of the system were the jamming could occur, the jamming threat itself will be explained later on the security threats section.

c) Reading area: each reader has a limited area that it can perform its processes within; the coverage of areas larger than the boundaries of single readers should be covered by other readers, the relation between the increment of area and the increment of readers are mutual.

d) Processing location: the processing of the tag reading and the key replacement, encryption, and termination –if any- can occur at the tag reader itself, however, when the tags increase over a certain level the processing has to be moved to a more reliable processor capable of handling all processing efficiently and on time-restrained manner.

e) Number of tags: each reader has the capability to process a relatively limited number of tags at the same time, the more tags to read, the more reader's process efficiency needed. Within the three-tier category, the number of tags rules the category chosen.

f) Risk level: the more complex the architecture of the RFID system gets, the higher security and privacy issues will be concerned, the overall risk level determines the portion of interest the security issues has to be addressed within the overall system design. The next section will discuss the security and privacy issues faced by RFID systems and compare the three categories against those threats.

TABLE I. RFID SYSTEMS' FEATURES

Features	Category		
	MTOR	***OTOR***	***MTMR***
Protocol Simplicity	simple	Medium	Very simple
Jamming threat	Reader jamming	No jamming	Reader & back end DB
Reading area	Wide area	very limited	Huge area
Processing location	Reader	Reader	Back en DB
Number of tag read	10s to few 100s Based on reader capability	One by one	Unlimited based on reader number
Risk level	High	Limited	Very high

V. THE MODEL APPLIANCE AGAINST COMMON PROTOCOLS:

Several proposed protocols for exchanging data between tags and readers are being presented as valid to use; these protocols are assumed to be applicable within similar systems –RFID systems in general-. Nevertheless, when investigating those protocols against the proposed categorization; the results were found doubtful, some of the unjustified setbacks in these protocols are clarified when opposed to the three-tier model.

Generally we could consider the OTOR a special case of MTOR, thus Efficient Mutual Authentication Protocol (EMAP)[3], Lightweight Mutual Authentication Protocol (LMAP)[1], and Minimalist Mutual Authentication Protocol (M2AP)[2] proposed protocols generally work in exchanging messages between tags and readers. In order to Authenticate each other by using index-pseudonyms (IDSs) and secret key (K) which are updated continuously while the tag stays in the reader's reading zone. In addition, those mutual authentication protocols holds all IDSs and keys in the reader; which means, any update in one reader should be updated by all other readers (synchronized) which is not efficient in the MTMR category but still considered so in OTOR and MTOR categories.[4]

The reason that those light mutual authentication protocols could not fit MTMR category is because the reader authenticate the tags 50 to 100 times per second based on the used protocol, this means the IDSs and the key will updated 50 to 100 times per second on all readers[1][2][3], which causes a jamming in the network where we suppose all reader in the system are doing the same function, some of these reader will not be updated in case it was separated from the other readers due to the system jam or network failure or latency; thereafter, in next stage when the tag shifts to the non-updated reader's zone, it will not be authenticated.

Our framework recommends -in the MTMR category- to shift all protocol processes to the backend database where the reader becomes a third party used for passing the data without changing it. In this way, all processes are moved to the backend database in order for the IDSs and the key exchanging and updating occurs at the same centralized location, and consequently all synchronization and network jamming problem will be solved.

VI. SECURITY AND PRIVACY:

The kinds of threats which might be used to attack RFID systems are vast and could not be addressed individually, in order to cover those threats; nine clusters of risks were established within the RFID research community –with respect to MAC- to characterize the problems in order to face them with the most optimal solutions: Eavesdropping; Relay attacks; Unauthorized tag reading; Tag cloning; People tracking; Replay attacks; Tag content changes; Physical tag destruction; and Blocking and jamming. The following table compares the risk level for the three categories in order to better understand the security requirements for different systems.

TABLE II. RFID SECURITY THREATS

Security threats	Category		
	MTOR	***OTOR***	***MTMR***
Blocking and jamming	high	low	high
Eavesdropping	Very high	Medium	Very high
Relay attacks	high	high	high
unauthorized tag reading	high	high	high
Tag cloning	high	high	high
People tracking	high	high	high
Replay attacks	high	high	high
Tag content changes	high	high	high
Physical tag destruction	high	low	high

A basic distinction of the categories in regards to the above mentioned threats serves tobetter tackle and monitor these threats and designalgorithms and solutions against them.

a) Blocking and jamming: basically once the number of tag increases, the possibility for jamming and blocking will increase. Inserting a number of fake tags in the reading zone becomes easier; it increases the probability for denial of service (DNS) to arise. Based on that, we analyze the threat to be low in OTOR limited-area and become more probable in MTOR and MTMR because of the number of tags read each time is variable.

b) Eavesdropping: is the process of intercepting data transmitted between two system's components. It is not an easy process in case the reader reads one tag each time but still is considered a risk especially when the attacker attach eavesdropping device with legitimate reader, but in the other two cases the eavesdropping is highly possible due to the many components involved and this could ease such a threat.

c) Tag cloning: creating a duplicate of a legitimate tag and making the system read it. The possibility is the same at all three categories at the same level because it is not based on the number of tags and readers involved in the application.

d) Unauthorized tag reading: collecting the data through reading the tags by an unauthorized external reader –a duplicate from the systems' readers or at least follows the same reading protocol-, the risk depends on external elements of the system which effects and can be solved equally between the three categories like, for an example, using an authenticating procedure.

e) Relay attacks: here the attacker establishes a false connection between an authenticated tag and an authenticated reader using a medium of unauthenticated tag and reader; the connection uses the authentication data on both of the original devices where they assume that the transferred data is from the authenticated source and establishes a valid connection allowing the data to be leaked to the unauthenticated devices.

f) People tracking: tracking mobile objects (carriers) which are holding a tag using different methods, to collect data about the carrier itself. i.e. human carrier.

g) Replay attack: is capturing the authenticating data sent between the tag and the reader allowing the interrupting device to use this authentication data to attack the system where it will be considered a clone for the tag and addresses the system in such identity.

h) Tag content change: altering the data – authentication data- on the tag to a false identity state where the reader will recognize the tag as unauthenticated tag and denies access.

i) Physical tag destruction: the physical destruction of the tag does not allow the tag carrier to pass through the reader; however, in certain cases especially where the tag is used for minor purposes such as item count. In OTOR schema the reader reads the tags one by one, so there is a little possibility to release any object that dose not carry identification tag, nevertheless, it would be known that the carrier holds a destructed tag, but in other schemata; it may happen easily without knowing because the number of tags is not preset as in crowded places e.g. train station or an stadium.

In relay attacks, unauthorized tag reading, Tag cloning, People tracking, Replay attacks, and tag content changes: those threats do not make any difference in all categories because all of them are based on data changing –through interception of data in the space while being transmitted between the system components- which is not related with our framework aspects; therefore, the categorization of RFID systems deals with these threats as general security concerns in data security and not as RFID architectural problems.

VII. DISCUSSION ON THE FRAMEWORK

The categorization in this paper distinct from other researches on RFID in the basis of categorization, some related researches included the security concept of authentication, and others on the implementation domains for the system.

(Yawer and vidyasagar,2008) classified RFID mutual authentication in three categories based on basic elements, such as authentication-type and challenge-value. Moreover, implicit authentication, origin authentication and destination authentication were the categories they came up with. And these categories differed based on the message generation whether by private key, public key or neither[5].these factors, quite a few categorization models emerged to describe those combinations, yet, none so far have tackled the physical implementation of the real-life systems which at the end

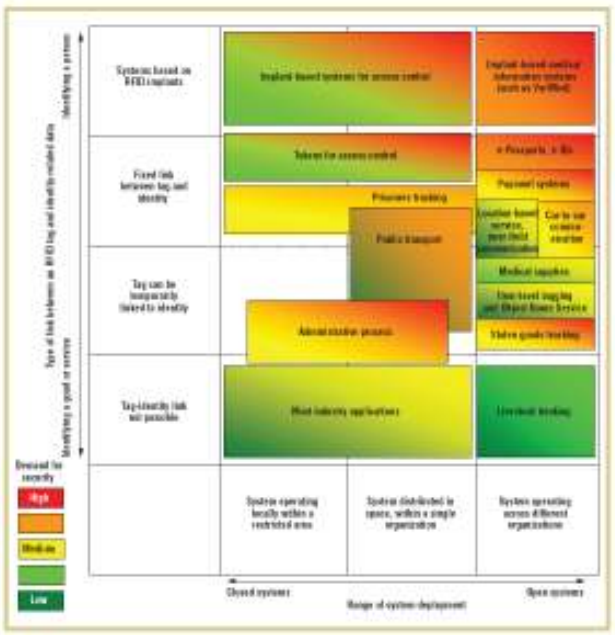

Figure 5. Privacy and Security risk assessment taxonomy

(Rotter, 2008) also assessed security threats and privacy issues from an implementation view; however, the implementation viewpoint (figure 5) was more related to identification and space rather than environment and hardware. Their proposed model assessed the risk level based on specific criterion of identity-related data link with the tags, and ranged the implementation space into clusters from closed to open systems' spaces where the application environment falls poorly within these ranges due to poor estimations of the physical environment and technical needs[6].

The proposed three-tier categorization of the RFID system is designed for human identification purposes based on the mutual authentication code, the assumption made within the system classifies the implementation based on the actual environment's structure, and consequently the hardware requirements in need to fulfill security and privacy measures for such a system. The business analysis for the system will identify the technical requirements that will classify the category under which the system will be applied, therefore, will propose the security measures and concerns that need to be taken into consideration for the deployment.

VIII. CONCLUSION

The RFID systems vary in their applications based on several factors, these factors are to be considered infinite –in a way- but the issue here is the combination of these factors, quite a few categorization models emerged to describe those combinations, yet, none so far have tackled the physical implementation of the real-life systems which at the end are the most satisfying for needs and threats accompanied.

Disjoining the objectives and needs for the system from the risks and threats facing these implementations does not prove effectiveness nor efficiency of RFID intended purposes; where it adds more security concerns than the systems were designed to handle.

The proposed three-tier categorization model reflects the faces of security threats in view of implementation and functionality of RFID and the advances applicable in useful appliances through the already used systems, platforms, and hardware.

Investigation against known threats are opposed to the model to provide an insightful glance to the prioritization of solutions for threats intimidating the data within these system, the focus was on human identification data stored within tags carried by humans.

REFERENCES

[1] Peris-Lopez, Pedro and Hernandez-Castro, Julio Cesar and Estevez-Tapiador, Juan and Ribagorda, Arturo,"LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags" Printed handout of Workshop on RFID Security -- RFIDSec 06, July 2006.

[2] Peris-Lopez, Pedro and Hernandez-Castro, Julio Cesar and Estevez-Tapiador, Juan and Ribagorda, Arturo,"M2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags", Lecture Notes in Computer Science, 912--923, Springer-Verlag,Sep-2006.

[3] Peris-Lopez, Pedro and Hernandez-Castro, Julio Cesar and Estevez-Tapiador, Juan M. and Ribagorda, Arturo, "EMAP: An Efficient Mutual Authentication Protocol for Low-cost RFID Tags", OTM Federated Conferences and Workshop: IS Workshop -- IS'06, 2006, 4277 Lecture Notes in Computer Science, P-352—361.

[4] Li, Tieyan and Wang, Guilin "Security Analysis of Two Ultra-Lightweight {RFID} Authentication" Protocols IFIP SEC 2007.

[5] Yawer Yousuf, Vidyasagar PotdarA "Survey of RFID Authentication Protocols", 22nd International Conference on Advanced Information Networking and Applications, IEEE computer society 2005.

[6] Paweł Rotter," A Framework for Assessing RFID System Security and Privacy Risks", IEEE CS PERVASIVE computing, pg 1536-1268, 2008

[7] PAWEŁ ROTTER, BARBARA DASKALA, AND RAMÓN COMPAÑÓ," RFID Implants: Opportunities and Challenges for Identifying People" IEEE TECHNOLOGY AND SOCIETY MAGAZINE, pg 1932-4529, summer 2008.

[8] Jeonil Kang and DaeHun Nyang ," RFID Authentication Protocol with Strong Resistance Against Traceability and Denial of Service Attacks", White paper in Springer-Verlag Berlin Heidelberg .2005