Improving Enterprise Access Security Using RFID

Dr. zakaria Saleh, Yarmouk University Irbid, Jordan zzaatreh@yu.edu.jo,

Dr Izzat Alsmadi, Yarmouk University Irbid, Jordan ialsmadi@yu.edu.jo,

Ahmed Mashhour Yarmouk University Irbid, Jordan mashhour@yu.edu.jo

Abstract*—Personal Computers now a day are widely used as workstations on many organizations networks. Hence, the securities of the workstations become an integral part of the overall security of the network. Consequently, any good access control solution should be designed in such a manner that key information cannot be retrieved without proper authentication. RFID can be used an alternative for providing extended user authentication. This study believes that the most secure methods include storing the access information on another secure device such as a smart card, or an RFID tag. Standard operations require that workstation to be configured in a way that involves interactive user authentication is instead of an automatic login where the password is stored on the workstation. Using an RFID system will insure that this requirement is kept intact. Many security systems fail not because of technical reasons, but because of the people who could protect a system were not following the basic security standards like locking the workstation before moving away. The proposed RFID system will enforce locking the workstation as soon as the user moves away from that computer unit.

Keywords: RFID, Workstation Security, Authentication, Access Managers

I. INTRODUCTION

All computer systems contain vulnerabilities, and one of the most significant vulnerabilities is the user (intentionally or accidently). The best way to protect a workstation and the confidentiality of data it holds, is when access control is implemented, the access control should be hardware based so that the control is maintained as soon as possible in the during system startup and access. In addition, when a user wants to leave the workstation unattended for a period of time without powering off, sound security practice requires that no unauthorized access is allowed to the system in the user's absence. This paper will concentrate on user authentication and prevention of (or protection against) access to work station by unauthorized user, and ensuring that users are the persons they claim to be with the ability to protect information and system resources. System resources include CPUs, disks, and programs, in addition to information on the work station. Classically, access control logon sequences have required a user name and password combination to verify the identity of a user. This research will introduce biometric devices capable of reliably identifying users through an RFID system.

II. SIGNIFICANCE OF THE STUDY

All computer systems contain vulnerabilities, and one of the most significant vulnerabilities is the user [6]. Anytime a workstation is running and not locked, the workstation can be vulnerable and convenient to be used by an unauthorized person in the work place. Thus, user authentication is a required component of all workstations, not only at startup or log on, but while the system is being used as well to protect information assets from deliberate or unintentional unauthorized acquisition, disclosure, manipulation, modification, damage, loss, or use. Many security systems fail not so much for technical reasons, often the people who could protect a system were not the ones who suffered the costs of failure 7. User authentication is the backbone of any access control solution. Therefore, it is important that any good workstation security measure should provide a very high integrity user authentication solution. The proposed security enhancement of using RFID as an authentication means with continuance monitoring of the RFID tag, used to run the workstation, will insure a secure system that is impossible for unauthorized persons to break into. The RFID tag has adequate secure storage to store access control profiles. The major disadvantage of a using RFID is the necessity for supplying a An RFID reading device on each workstation. However, with the current price for RFID readers, this may be justified.

III. WORKSTATION SECURITY OVERVIEW

Security is the process of preventing unauthorized use of a computer or a workstation. The traditional foundation of

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

workstation security is based on implementing safeguards to ensure that users access only the resources and services that they are entitled to access. In addition, measures are taken so that qualified users are not denied access to services that they are expecting to receive. Absolute prevention is theoretical, and If a computer is compromised, the entire contents of the system are exposed to the attacker[6].

For any workstation, authentication can be done by one of three ways 4: Something the user knows (e.g., a password); something the user has (e.g., a token or card); something the user is (e.g., fingerprint, voice, eye scan). Each approach has advantages, and limitations. This paper is more concern with the limitation part:

1. "Something the user knows" can be forgotten, guessed by others, or inappropriately shared,
2. "Something the user has" can be misplaced or stolen, and
3. "Something the user is" can be difficult to distinguish reliably.

Therefore, combining two or more methods enhances the confidence level (e.g. a bank ATM machine requires both a card and a password). However, while an access control system must be effective, it should also be user friendly [1].

Currently, Windows and workstation authentication uses or depends on the first type of authentication techniques. Mixing this with RFID authentication (i.e. something the user has), will improve security and reduce the possible of wrongly indentifying a user.

When a user logs on to a computer running Microsoft Windows for example, the user needs to supply a user name and password. This becomes the default security context for connecting to other computers on networks and over the Internet. Thus, passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the entire corporate network. Passwords are still the most pervasive tool used to secure access to networks and databases. As the number of passwords per employee increases, the likelihood of them being forgotten rises [2]. For maximum security each member required to protect their password. Access can further protected by following good password practices (e.g. creating passwords that are a mix of letters, numbers, and other characters). Depending on the level of security needed, users can choose from standard to very high levels of password security.

A security breach in accessibility occurs when either access for a system is denied for an authorized user or access (an example of this category would be an authorized user of a system who is unable to access a system due to forgetting their password)[3] .To make passwords that are easy to remember, many people create passwords that contain their name or email address, or are a string of familiar digits, such as their phone number or birthday. The problem is, simple passwords like this are easy for intruders to guess, and could compromise the security of the network. Users accessing highly sensitive data on the network, need to employ "complex" passwords (e.g. passwords that do not contain parts of users name or birthday are complex), however, extensive password requirements can overload human memory capabilities as the number of passwords and their complexity level increases [3].

IV. Access or Account Managers

In Web application security deployments, and many other types of distributed systems, users accessing a protected application are authenticated via enterprise identity/access management products, such as Netegrity's SiteMinder, IBM's WebSEAL, and Oracle access manager. The authorization service, however, is delegated to the provider of the application itself, or to the application server. Generally, there are major goals or requirements for any access or account manager. Those are:

- Provide a single username and password.
- Accept alternative forms of authentication (such as RFID) beyond username/password
- Provide strong authentication mechanisms where needed
- Provide single sign on (SSO) where possible.
- Provide strong security that does not slow performance.

Most access managers provide an authentication API for integrating a variety of authentication methods and devices such as smart cards. Account manager information are usually updated to stay in synchronization with account in LDAP or active directory.

V. Authentication

Most current access managers are designed to deal with different types of authentication. This may include: Basic username/password, X.509 Certificates, Smart Cards, Two factor tokens, Form-based, and Custom authentications via Authentication APIs.

VI. LDAP

Lightweight directory access protocol (LDAP) is a directory service protocol that provides access to a directory over a network. It stores information in directory service (such as Microsoft Active Directory) and query it.

VII. Related Work

There are several applications related to using RFIDs in security and authentication [5], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], and [21]. This paper followed the trend of the majority of the papers that are discussing RFID where they present using RFID for a particular application. This may span from generic applications that can be applied in several domains such as users' authentication (e.g. students, employees, citizens, etc). In such applications, RFID authentication is used as an

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

alternative, more convenient authentication service for some other typical authentication tools such as biometrics, software authentication, etc. In general, authentication methods can be classified into 3 categories for users: something they are (e.g. biometrics, such as fingerprints, voice, etc), something they say, know or type such as passwords, and something they have such as the physical keys and the access or RFID cards. For better security, many entities are trying to combine methods from the different categories.

The second type of papers talking about RFID discusses security concerns and issues in the RFID network itself. Examples of such papers that discussed security and vulnerability issues in RFID networks are [5], [12], [14], [15], [18], and [21].

Ham et al studied merging RFID with PKI and DNS security extensions for establishing a secure network [8]. The DNS with security extensions can provide integrity and data authentication. Mao et al proposed an Interoperable Internet-Scale Security (IISS) framework for RFID networks on which multiple partners with different identity schemes can be authenticated [9]. The framework made authentications based on an aggregation of business context, enterprise information, and RFID tag information as a lightweight solution for the problem of relations trust authentication in RFID networks.

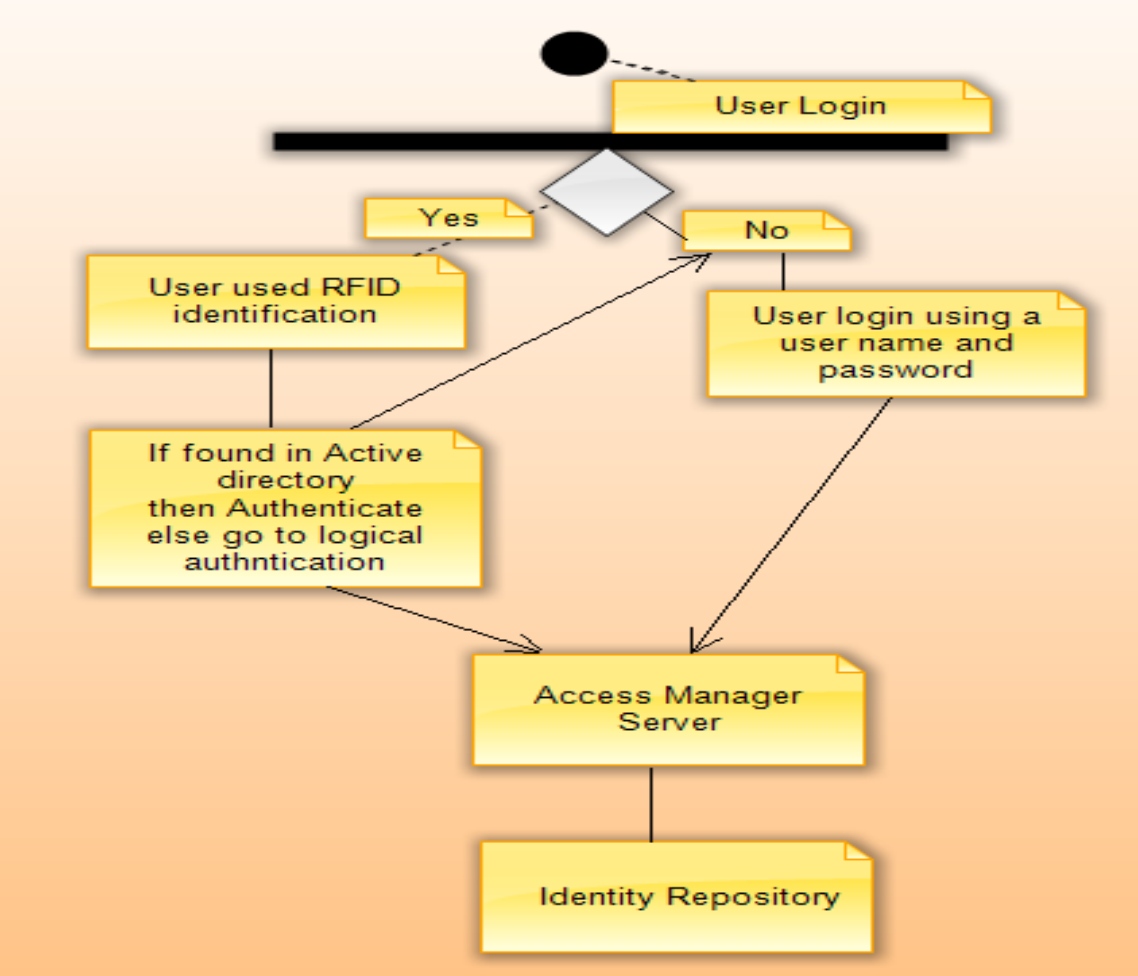

Figure1. Proposed modification on authentication systems to include RFID authentication.

Zhao et al proposed a hierarchical P2P based RFID code resolution network structure In order to alleviate or solve some performance and security problems of RFID code resolution [10]. RFID code resolution services and related security mechanism are implemented. Ku et al presents a complex event mining network which enables automatic and real-time routing, caching, filtering, aggregation and processing of RFID events and defines the fundamentals of RFID enabled supply chain event management [11]. Kim et al propose the modified hash based RFID security protocol to improve data privacy and authentication between a tag and a

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

reader [12]. The paper discussed some of the vulnerabilities that may occur in the RFID network.

Chang et al proposed a method similar to the one adopted in this research in combining RFID with cell phones for users' authentication [13]. They also studied security and vulnerability issues in RFID networks. To achieve message security, it is essential to keep anonymity to protect the privacy of the RFID credit card holders.

VIII. Design and approaches

Figure 1 shows a simplified diagram for the proposed modification on workstations authentication system. RFID cards can be connected to the workstation through wireless that enable users to be granted login once they are close enough (in a defined distance that depends on power and frequency). In order to simply system recognizing users and correlate users with RFIDs, RFID values can be generated using a seed value correlated with the user information. Proposed modification should guarantee Single Sign On (SSO) where user will be asked only once to verify their identity. Once system found a possible problem in authentication, it may ask for the second type of authentication. Users will be logged of whenever they leave the close distance range defined.

The proposed modification on authentication assuming that users' machines will be locked as soon as they leave them. Many users avoid locking screens as it is inconvenient for them to lock the screen and type passwords again and again over the day. As such, a solution is to have a program that automatically detect the user RFID whenever the user comes close to the machine. This can be very simple through implementing transceivers between the computers and the RFID. In most cases, however, we may need only one way communication where the RFID will transmit their ID to desktops.

The transmitted signal should be modulated or encrypted with the user information for two reasons: First, this is to guarantee that signals will not be intercepted in the middle and saved and possibly reused by intruders. On the other hand, this is a double identification matching technique where each RFID unique number will be attached to a particular user in which there is always a one to one relation between users' and their RFID.

IX. RFID range and frequency

Selecting the proper frequency for this RFID is significant. Recommended Frequency is 13.56 MHz. This frequency has several characteristics that may make it suitable. This include: low cost, ultra-thin, battery-less contactless read/write technology (approximate read range up to 1.5 meter), and offers increased and advanced security over 125 KHz proximity systems. The technology is capable of providing advanced security features like encryption algorithms, where each transponder has a unique tamper proof factory programmed ID code.

The RFID range selection is fundamental. If you're planning to use RFID you need to know what distance it will work over. For a computer workstation or server in a room, the typical distance that those equipments exist in may vary between 2 – 30 square meters. Besides frequency, there are several other parameters that regulate the RFID transmitting and receiving distance. Those other parameters include: RF transmit power, the receive sensitivity, the surroundings, how much water is present, the orientation of the tag, and the care that's gone into designing the products, planning and installing the system. Liquids such as water can absorb RF (especially at microwave frequencies) and metals can shield or reflect RF energy.

In terms of the power, the RFID component attached to the computer should not have a problem as it can be simply a USB extension which can take power through the USB port. For simplicity, the RFID part that will be attached to the employee card can be a simple active RFID tag can receive its power from a small battery or passive tags that can get their power from the RFID transmitter attached to the computer. Currently several companies such as Noxel (www.noxel.com/rfid-reader.html) and Gemia are developing RFID readers using Bluetooth technologies to combine those two technologies and eliminate the need to connect the RFID reader with the computer through a wire.

X. Experiment and Evaluation

In order to demonstrate the approach, we implemented the system and develop a program with RFID using USB connection. Such test can validate many features of the proposed system except those related to the required distance between the computer and the user for the program to detect the RFID and some other issues possibly related to security.

In the developed program, the program is started as a service and always in listening or receiving state, similar to those happened in socket programming such as chat or messaging services. As soon as users enter the RFID card in the reader, the RFID information are sent to the LDAP to verify the user identity using the information saved in the LDAP or the active directory about users that include user relevant RFID. This information should be encrypted and read only by system applications similar to passwords.

XI. University Campus, A case study

In order to assess the design and specification requirements for an RFID system, a small subset of Yarmouk University campus is selected. This represents the IT faculty which comprises of two major building with an approximate distance of 20-30 meters between those two building. An RFID simulator (Turck Inc.). Number of users based on computer workstations and servers is approximated to be 100 computer and server. This excludes computers in the labs as those computers are usually public and should not include private logins. Besides the number of RFID elements, the major

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

attributes selected in the simulation are distance, speed (of message transmission) and data quantity. Those 3 elements are adjustable in the simulator as they impact each other and the overall simulation process.

Read/Write distance is set at the range of: 0-40. While data quantity is not expected to be a major issue in the access verification scenario where the amount of data to transfer is minimal (i.e. that is required for authentication). This is different from other scenarios such as warehouse or store management where it is expected to have a large amount of data transmission among RFID system components. Nonetheless, speed is important and the speed of response by the simulators is set to the minimum to ensure that the logging system will not be a bottleneck and affect the overall working environment.

XII. Conclusion and Future Work

In this paper, we proposed using RFID to improve enterprise access security through combining typical software or logical security with RFID. This combination is expected to improve the overall security infrastructure of distributed systems while at this same do not impact the system performance or causing extra overhead elements.

RFID security access control system can be added to the existed infrastructure without the need for significant extra software or hardware elements. An elementary simulation is implemented to demonstrate the proposal and evaluate the major elements that can impact selecting the RFID security such as data quantity, speed and distance. Results showed that such security infrastructure can be applicable for local area distributed system as such University campuses, schools, warehouses, and small to medium size enterprises.

Reference

[1] Graham, I (1996). “PC Workstation Security” A paper presented by 1996 Information Security Summit on 29-31 May, 1996 at the Tattersal's Club, Sydney.

[2] Bjorn, V. (2006)"Solving the Weakest Link in Financial Institutions Network Security: Passwords". A Digital Persona, Inc. White Paper, September 2006.

[3] Carstens, D. & McCauley-Bell, P.(2004). "Evaluation of the Human Impact of Password Authentication Practices on Information Security". Informing Science Journal, Vol 7, 2004.

[4] Kolodgy, C. (2001). “Biometrics: You Are Your Own Key”. InfoWorld (January 29, 2001) Issue.

[5] Park, N., Choi, D., Kim, S., and Won, D. (2008). Enforcing Security in Mobile RFID Networks Multilateral Approaches and Solutions, IEEE.

[6] PNNL (20100. “2010 Guide for Home Computer Security”. Pacific Northwest National Laboratory. Retrieved for the WWW on April 6, 2010 from www.pnl.gov/media/homeguide_public.pdf.

[7] ANDERSON, R., & SCHNEIER, B. (2005). "Economics of Information Security". IEEE COMPUTER SOCIETY, vol. 3 no. 1.

[8] A Study on Establishment of Secure RFID, Network Using DNS Security Extension, YoungHwan Ham *, NaeSoo Kim * ,CheolSig Pyo*, JinWook Chung, 2005 Asia-Pacific Conference on Communications, Perth, Western Australia, 3 - 5 October 2005.

[9] An Interoperable Internet Scale Solution for RFID Network Security, Tingting Mao, John R. Williams, Abel Sanchez, 2009 IEEE.

[10] Research on hierarchical P2P based RFID code resolution network and its security, Wen Zhao, Xueyang Liu, Xinpeng Li, Dianxing Liu, Shikun Zhang, 2009 International Conference on Frontier of Computer Science and Technology.

[11] Novel Complex Event Mining Network for RFID-Enable Supply Chain Information Security, Tao Ku1, 2 YunLong Zhu1 KunYuan Hu1, 2008 International Conference on Computational Intelligence and Security.

[12] Analysis of the RFID Security Protocol for Secure Smart Home Network, Hyun-Seok Kim, Jung-Hyun Oh, and Jin-Young Choi, 2006 International Conference on Hybrid Information Technology (ICHIT'06)

[13] An Improved Certificate Mechanism for Transactions Using Radio Frequency Identification Enabled Mobile Phone, Allen Y. Chang, Dwen-Ren Tsai , Chang-Lung Tsai , Yong-Jiang Lin , 2009 IEEE

[14] Intrusion Detection in RFID Systems, Geethapriya Thamilarasu and Ramalingam Sridhar, 2008 IEEE

[15] Trust and Security in RFID-Based Product Authentication Systems, Mikko O. Lehtonen, Member, IEEE, Florian Michahelles, and Elgar Fleisch, IEEE SYSTEMS JOURNAL, VOL. 1, NO. 2, DECEMBER 2007.

[16] A Layered Approach to Design of Light-Weight Middleware Systems for Mobile RFID Security, (SMRM : Secure Mobile RFID Middleware System), Namje Park, Jooyoung Lee, Howon Kim, Kyoil Chung, and Sungwon Sohn,

[17] Engineering Management-Focused Radio Frequency Identification (RFID) Model Solutions, —PAUL G. RANKY, IEEE ENGINEERING MANAGEMENT REVIEW, VOL. 35, NO. 2, SECOND QUARTER 2007.

[18] The RFID Middleware System Supporting Context-Aware Access Control Service, Jieun Song and Howon Kim, Feb..20-22, 2006 ICA0T2006.

[19] NOVEL RFID-BASED SHIPPING CONTAINERS LOCATION AND IDENTIFICATION SOLUTION IN MULTIMODAL TRANSPORT, Zhengwu Yuan, Dongli Huang, CCECE/CCGEI May 5-7 2008 Niagara Falls. Canada.

[20] RFID for airport security and efficiency, Thomas Mccoy, R Bullock and P Brennan, IEE.

[21] Secure and Efficient Recommendation Service of RFID System using Authenticated Key Management, Jinsu Kim1, Changwoo Song, Taeyong Kim, Keewook Rim, Junghyun Lee, 2009, IEEE.

Authors Profile

Zakaria Saleh: Dr. Zakaria Saleh is an associate professor in the Faculty of IT and Computer Sciences, at Yramouk University. His work experience ranged for simply providing technical support and nonconformance resolutions for a “Compaq Computers” PC configuration center, to working on the design and development of electronic control systems in the Automotive Industry, where he has contributed to the introduction of M2M (Machine to Machine) Communication Systems.
Prior to joining Yarmouk’s Faculty Team, he was working as a Project Engineer, at Case Corporation, an International Designer and Manufacturer of Agricultural and Construction Equipment, located in the USA. He was a member of the engineering team where he has contributed to the design and

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

development of several microcontrollers, and was the lead engineer to work on the design and development of web based Fleet Management System.

Izzat Alsmadi: Dr Izzat Mahmoud Alsmadi is an assistant professor in the department of computer information systems at Yarmouk University in Jordan. He obtained his Ph.D degree in software engineering from NDSU (USA), his second master in software engineering from NDSU (USA) and his first master degree in CIS from University of Phoenix (USA). He has a B.sc degree in telecommunication engineering from Mutah university in Jordan. Before joining Yarmouk University he worked for several years in several computer science and information technology companies and institutions in Jordan, USA and UAE.
His research interests include: software engineering, software testing, software metrics and formal methods.

Ahmad Mashhour: Dr. Ahmad Mashhour earned his PhD degree from the University of London (LSE) 1989 in Information Systems. He is currently a faculty member at Yarmouk University, Jordan. He worked as a visiting professor at University of Qatar, and then at the University of Bahrain. His current research interest includes information systems modeling and analysis, information systems security, e-Business, and e-learning.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500