RFID-based Authentication Middleware for Mobile Devices

Ewa Syta
Central Connecticut State University
sytaewa@ccsu.edu

Stan Kurkovsky
Central Connecticut State University
kurkovskysta@ccsu.edu

Bernardo Casano
Central Connecticut State University
bcasano@logtime.com

Abstract

Ever-growing popularity of mobile devices, such as smart phones and netbooks, coupled with anytime and anyplace availability of high-speed network access is changing the ways how we compute and communicate. Mobile devices play an increasingly important role in our lives and tend to become representations of our digital selves when we trust these devices with sensitive information. Consequently, the problem of securing mobile devices against unauthorized access has never been more important. We present an RFID-based Authentication Middleware (RFID-AM) that combines point of entry and continuous authentication with transparent on-demand encryption of user files. This paper details the architecture of RFID-AM, discusses its fully functional prototype, and presents experimental results demonstrating its performance in various conditions. This paper also surveys different methods and technologies that have been proposed and implemented on mobile devices.

1. Introduction

Recent years have witnessed a surge of popularity in mobile devices such as smart phones, and most recently, netbooks. – small and relatively cheap laptops geared towards network-centric applications [9]. Mobile devices provide access to a wide range of applications and services while offering a significant computational power and data storage space, as users often choose to keep their sensitive and valuable data on these devices that may include personal and financial information, social security numbers, credit card numbers, user names, passwords, etc. Unauthorized access to a device may cause serious adverse consequences; therefore, a need to secure a device against misuse has become a crucial issue. The first line of defense is restricting access based on the user's identity check, which can be accomplished by one or a combination of several user authentication methods. A wide range of different user authentication methods has been developed for mobile devices. However, users often perceive some of these technologies as complicated and cumbersome, which creates a significant barrier to user adoption. In fact, in many cases, there is an inverse relationship between the usability of a security-related technology and the degree of protection it provides [13,24].

This paper described an approach that uses token-based authentication to create a cost effective, easy to use and secure user authentication mechanism for a range of mobile devices including netbooks, laptops and smart phones. Token-based authentication relies on a small hardware device that a user carries with them. Identity of the user is verified if a possession of the token is confirmed. The framework described here, RFID-AM (Radio-Frequency Identification-based Authentication Middleware) uses an RFID tag as a token with an RFID sensor to perform user authentication over a short-range wireless link. RFID systems have been widely used in supply chain management (e.g., by Wal-Mart in the US and Tesco in the UK), ticketing applications (e.g., the Oyster card in London and the Suica card in Tokyo), and in passports or national identification cards of many countries. For the purpose of possession-based user authentication (Section 2), it is assumed that whenever an RFID tag is present within a certain range, a legitimate user is present as well and access to a device should be granted. However, our framework provides for composite user authentication that combines several independent techniques, e.g. possession-based and knowledge-based authentication. Such an approach provides the system with the flexibility to perform continuous authentication and secure the device by making it accessible only when the correct RFID tag can be read. This method provides a transparent, secure and non-intrusive method of user authentication.

This paper is organized as follows. Section 2 briefly surveys different authentication methods that have been proposed and implemented for mobile devices. Sections 3 and 4 describe RFID-AM architecture and related security/privacy issues, while Section 5 discusses its implementation, reliability and performance. Section 6 concludes the paper with a summary and an outline of future work.

IEEE computer society

978-0-7695-3869-3/10 $26.00

2. Authentication on Mobile Devices

User authentication is a process of validating the identity of a user to ensure that the user is who she or he claims to be. User authentication is the only way to secure a device; it can be performed based on three categories of factors. The first category (something you know) is based on a shared secret that has to be provided in order to prove an identity. It is the most widely used kind of authentication that includes numeric, alpha-numeric, and graphical passwords. The second category (something you have) can be viewed as a proof by possession. The user has to demonstrate a possession of a certain device e.g. hardware token, smart card, or even another device like a cellular phone. The last category of authentication methods (something you are) uses user's biometric features like fingerprint, voiceprint, or hand geometry.

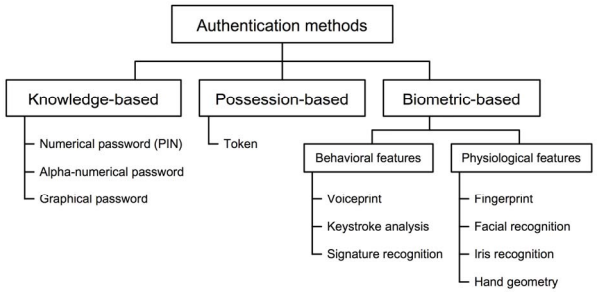

Figure 1. Classification of authentication methods

Usage patterns of mobile devices vary widely: some (such as smart phones) are used frequently for short periods of time, while others (such as laptops) may remain in active use for extended periods. User authentication must be performed every time when a user logs into a system, turns a device on, or when a device is used after a period of inactivity. For these reasons, user authentication cannot be burdensome because it may discourage users from using authentication. In a perfect situation user authentication should be quick, easy, and user-friendly, especially on a mobile device, such as a netbook, which may be used intermittently. Usability of authentication techniques is a very important factor, which may create a significant barrier to user adoption. In many cases, there is a certain tension between the degree of protection of a security-related technology and its usability [13,24].

User authentication is most often viewed as point-of-entry authentication performed whenever a device is turned on or used after a period of inactivity. However, after an authorized user has been authenticated, the device is vulnerable if the user leaves it unattended. Continuous authentication performed periodically could solve this problem by ensuring that the same user who has been successfully authenticated is still using the device. The solution implemented by RFID-AM and described in this paper, meets the requirements for both point-of-entry and continuous authentication.

The remainder of this section briefly surveys some authentication methods implemented for mobile devices that are applicable to RFID-AM.

2.1. Knowledge-based Authentication: Password-based Authentication

Password-based method is the most widely used approach to knowledge-based authentication. User's identity is checked based on a shared secret that has to be known in order to gain access to the device. Alpha-numeric passwords and numeric passwords (Personal Identification Number, PIN) are the most popular knowledge-based approaches. However, PINs and passwords proved themselves to be a weak solution that does not provide an adequate level of security. Short, memorable passwords are weak and guessable while long, random sets of characters are difficult to remember and increase user inconvenience. The main weakness of this approach is a significant reliance on the user. People tend to choose uncomplicated passwords that often contain easy to obtain information, such as name or age. Users often write them down and share them with others. Moreover, the default set passwords or PINs are rarely changed. For these reasons, such passwords are particularly vulnerable to dictionary attacks, as well as brute force attacks. For example, PINs are often 4 digits long, which results in only 10^4 possible combinations. Assuming a regular keyboard with 95 printable ASCII characters, it is possible to achieve 95^n possible combinations, where n is the length of the password. However, a strong password should be long and as random as possible which makes it difficult to remember and inconvenient to use. The problem of convenience becomes significantly more severe taking into account small keyboards available on many mobile devices, not to mention that some of the smart phones do not have full keyboards. As a result, mobile users often choose to deactivate existing authentication mechanisms because they perceived them as cumbersome and inconvenient [13,24].

2.2. Knowledge-based Authentication: Image-based Authentication

Image-based methods have been proposed as an alternative to password-based authentication on mobile devices. Authentication process relies on the ability of a legitimate user to recognize images to which they

have been exposed previously because humans are more capable of recalling previously seen image rather than previously seen text [27]. The user may be asked to select formerly chosen pictures, provide a correct sequence of pictures, click on formerly chosen points or regions of a picture, or recognize degraded images. Image-based authentication is often viewed as more user-oriented; users find it more enjoyable and may be more likely to use this model compared to other knowledge-based authentication techniques [14]. Image-based techniques can be classified into two categories: recognition-based and recall-based.

Recognition-based authentication methods require a user to choose a certain number of pre-selected pictures from a presented set. During an initial phase the user picks a number of pictures from the set of all available images (Image Space, IS) and creates a unique portfolio (Individual Image Space, IIS). IS can contain images provided by system or the user can add their own pictures to extend and personalize the IIS on their mobile device [35]. The process of authentication consists of one or several rounds during which a subset of IIS mixed with random pictures is displayed. The user needs to select all pictures that belong to IIS or declare that there are no such pictures. Recognition-based authentication has been implemented using a set of computer-generated images [10], large sets of different images showing similar or related objects [33], or human faces [8,11]. Nevertheless, people tend to choose faces of people from the same race, or gender what may facilitate an attack from a person that is familiar with the user [8,11].

Recall-based authentication techniques use images in a slightly different way; they require the user to repeat or reproduce a secret that the user created before. Recall-based authentication schemes have been implemented using techniques that allows users to draw unique passwords [20], require user to choose few points of the predetermined image and use them as a password [2] or clicking on different areas of an image [40].

A number of studies show that the users took fewer attempts to authenticate with image-based passwords than with alpha-numerical passwords. On the other hand, image-based techniques took more time during authentication phase. In addition, graphical password users had more difficulties learning the password than the users of alpha-numerical passwords.

2.3. Possession-based Authentication

Token-based authentication relies on a small hardware device that the user carries with them. The identity of a user is verified if a possession of the token is confirmed. The token can be in the form of a smart card or can be embedded in a USB fob, or a key chain. Unlike passwords, tokens are physical objects so they are vulnerable to loss, theft, or damage.

Four types of tokens can be distinguished. *Static* tokens are devices that only allow storing data (secret number, cryptographic keys, digital signature, or biometric data). *Synchronous dynamic* tokens allow the generation of a one-time password. *Asynchronous* tokens present the user with a challenge number that should be entered on the token keypad to generate a response to the challenge, which can be used as one-time password. *Challenge response* tokens use the challenge response protocol in order to perform authentication process; some smart cards fall under this category.

Many different token-based authentication schemes have been developed for mobile devices. Here we focus on transient authentication using wireless tokens and smart cards.

Transient authentication provides a model to resolve the tension between protection and usability discussed in Section 2. Transient authentication can be implemented using a small wearable token that performs authentication on a user's behalf over a short-range wireless link. The user is constantly authenticated to the device in a transparent way what resolves the problem with infrequent and persistent authentication brought by other methods [30]. The device secures itself whenever the token is not present. This approach helps minimize the possibility of unauthorized access to the device due to negligence or theft. In this context, the token is a small, portable, and often wearable device that can range from uncomplicated RFID cards to devices that can perform computations and store data.

Transient authentication schemes have been implemented for mobile devices using a wide variety of tokens, which include a small wireless device with modest computational resources [29], e.g. an IBM Linux wristwatch [28], Bluetooth-enabled mobile phones [1,18], and Smart Multimedia Cards (SMC) [19].

2.4. Biometric Authentication

Biometrics is an automated process of recognizing an individual based on measurable biological and behavioral characteristics. Human body possesses many characteristics that are unique and difficult, if not impossible, to copy or falsify. The term biometrics is associated with two different processes, verification and identification, that are often used interchangeably. Identification is a process of determining the user's identity, while verification is a process of confirming a claimed identity. Therefore, biometric verification is a

part of the authentication process. Biometric characteristics suitable for authentication must be unique for each person and must not change noticeably with time. In addition, the process of measuring traits should be fast, efficient, and uncomplicated. In addition to high accuracy and transparency, the main advantage of biometric authentication over other solutions is that the authentication factors cannot be lost, stolen, or forgotten, and are always with the user.

Biometric characteristics are most often categorized as biological and behavioral. Biological characteristics are primarily based on an individual's anatomy or physiology. Fingerprint [3], iris [7] and retina, face [17,32], hand [25], and ear geometry [26] are among biological traits most frequently used in biometric systems. Behavioral characteristics are learned and acquired over time and can be viewed as traits associated with an individual's behavior. Popular behavioral characteristics are voiceprint [36], keystroke dynamics [16], and signature dynamics [5].

Fingerprint has been the most widely used biological characteristic due to its uniqueness, consistency over time, and easiness of acquisition [3]. Despite their advantages, fingerprints are fairly easy to copy. The first fully functional cell phone with a fingerprint reader was presented by Siemens 1999 at CeBIT.

Voice recognition is a behavioral biometric verification method based on the voice features. Voice recognition method falls under two categories: text-dependent that uses the same text for enrollment and verification, or text-independent where there are no constraints on text. Voice-based verification seems to be well-suited for use in mobile devices. As mobile devices are most often communication tools, acquiring a biometric sample is effortless. Every mobile device is capable of capturing a voice sample. In addition, users have a very positive attitude toward this method since saying a sentence or repeating a few numbers is convenient, non-intrusive, and transparent. However, noise can have a very significant effect on the quality of voice-based recognition.

3. RFID-based Authentication Middleware

In the discussion below, the term "mobile device" refers to a handheld computing device providing a various range of functions and capable of running third-party software. Such devices include smart mobile phones, personal digital assistants, handheld PCs, as well as netbooks, which are not small enough to fit comfortably into a pocket but are likely to be kept at all times with users.

RFID-based authentication middleware (RFID-AM) described in this paper is designed to provide composite authentication, which combines two or more methods of user authentication, preferably using different factors, e.g. knowledge-based and possession-based [4]. With many knowledge-based authentication methods, the user bears the responsibility of choosing and using a strong password. However, with intermittent usage patterns exhibited by many users of mobile devices, authentication should be easy, unobtrusive and transparent. These factors necessitate the following requirements for an authentication framework suitable for mobile devices:

- Unobtrusive: users should find the authentication process simple and easy to use;
- Transparent: some or all steps of the authentication process may occur without an explicit interaction with the user;
- Cost-effective: no additional and/or expensive hardware should be required;
- Continuous: authentication should not stop after the initial login (point of entry); presence of an authenticated user should be ensured at all times.

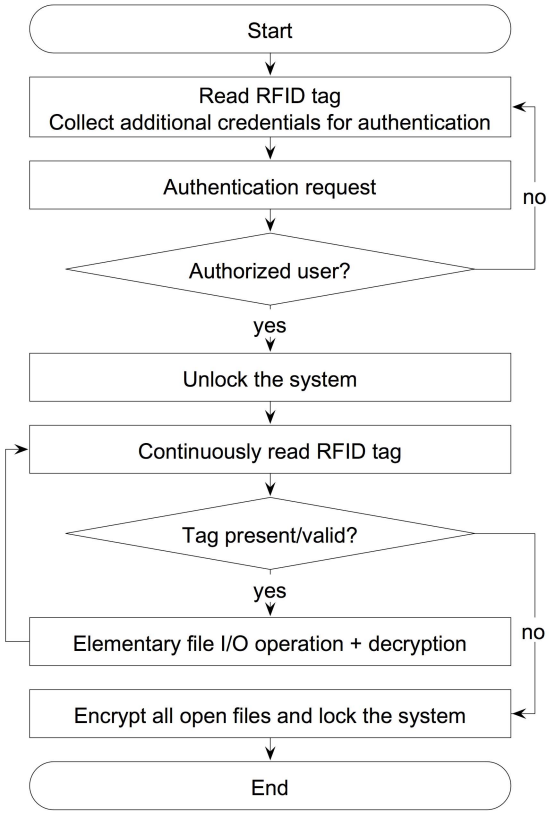

Figure 2. Continuous authentication process.

Following the point of entry authentication, continuous authentication verifies authentication

credentials of the user at predetermined intervals of time. At any moment when the user credentials are found to be no longer valid, the access rights will be revoked, as illustrated in Figure 2. Dependent on the authentication interval length, verification of the user credentials may also occur every time a file I/O operation is performed on an encrypted file system. Consequently, when the user logs off, walks away, or if the user's credentials cannot be verified for some other reason, all open files are encrypted and the system is locked.

Possession-based user authentication combined with an authentication method based on another factor could satisfy all of these requirements. Possession-based authentication could guarantee continuous user authentication in an unobtrusive and transparent fashion, while a knowledge- or biometric-based method could guarantee a strong point of entry verification of the user's credentials. In particular, RFID-based authentication could serve as a cost-effective possession-based method.

RFID is a non-contact sensor technology that uses radio waves to automatically identify people or objects. There are two devices used in an RFID system, an RFID transponder (tag) and an RFID transceiver (reader). Generally, RFID tags contain an antenna and a microchip with a small data storage and limited computational functionality. Passive RFID tags do not contain their own power source and rely on the electromagnetic field created by the reader to power its circuitry and modulate its radio-frequency signal. Active RFID tags typically use a battery or an external power source. Since passive tags do not contain a power source they have a shorter range, but are less expensive, more compact and never require any servicing. RFID reader receives the modulated electromagnetic waves and converts them into digital data, which is streamed to the device connected to the reader. The read range of a tag depends on many factors including the frequency of the RFID system, the power of the reader, environmental conditions, size of the antenna, and interference from other electrical devices.

Passive RFID transponders and transceivers with a range of up to three feet could be used in an authentication framework conforming to the requirements listed at the beginning of this section. Typically, an RFID card can be carried in a wallet, on a lanyard or on a keychain; the chosen operating range would ensure that the user would not need to place the transponder in a close proximity of the transceiver while using a secured device. Yet, operational range should be short enough to minimize interference from similar RFID systems employed by other users, and at the same time guarantee that whenever the authorized user leaves the device it enters a locked state. Adequate range, cost-effectiveness, and small form factor make Class 1 Gen 2 passive RFID tags an excellent choice for these purposes [6,15]. These tags typically store an Electronic Product Code (EPC), a unique number that identifies the manufacturer, serial number of the product and its type; the length of EPC can range from 64 to 256 bits. Dependent on the complexity of the transceiver, it may also contain two 32-bit passwords: the "access" password used to access the EPC, and the "kill" password used to permanently disable the tag.

RFID systems use low (~170 kHz), high (~13.56 MHz), or ultra-high (~868 and 928 MHz) frequency. In general, a higher frequency provides a faster transfer rate and broader read range, but is also more sensitive to environmental factors such as liquid and metal. RFID tags that used by RFID-AM work at a low frequency (125 kHz) that minimizes the chances of interference by the user's body and other objects [38].

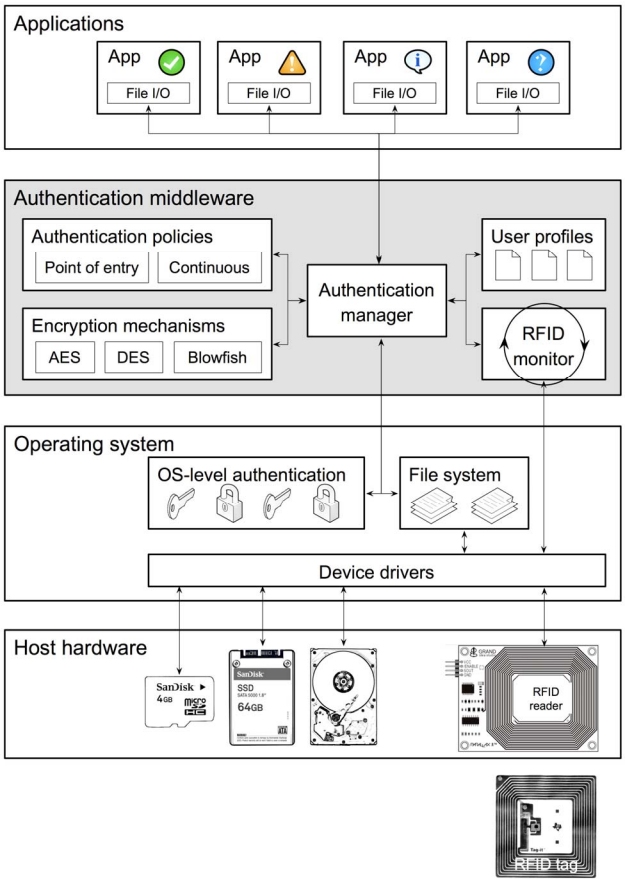

Figure 3. Architecture of RFID-AM.

As shown in Figure 3, RFID-AM is designed as middleware that serves as an intermediary between the host operating system and all software applications. RFID-AM is designed to take advantage of

authentication features provided by the host operating system to augment RFID-enabled possession-based authentication with knowledge- or biometrics-based authentication. For example, smart phone operating systems provide an authentication feature based on SIM card lock PIN, while many netbooks and laptops are equipped with fingerprint scanners. As a result, operating system can provide an efficient point of entry authentication, while RFID-AM implements transparent continuous authentication. With the assistance of RFID-AM layer, all user files can be kept encrypted until they are open by an authenticated user. Consequently, if an open file is closed, it is automatically encrypted. Whenever continuous authentication fails (i.e., the user walks away without logging off or turning off the device), all open files are closed and encrypted and the device is locked.

RFID-AM employs user profiles that determine authentication policies applicable to each user; they establish file ownership relationships, associate each profile with one or more RFID tags, and select a particular encryption mechanism employed by RFID-AM to secure user files. A user profile also determines whether the encryption key used to secure the user files is stored directly in the RFID tag's EPC data or whether the key is derived from EPC using a password-based key derivation function, as described below in this section. It is important to note, however, that a typical mobile device, a smart phone or a netbook, is normally used by only one person, which requires maintaining only a single user profile.

RFID-AM requires a one-time set up process to register tags that are in possession of legitimate users. Tags are associated with user profiles and are used to distinguish between them. Authentication policies determine a set of parameters applied to the process of verification of credential supplied by the users for point of entry or continuous verification, or both. Continuous authentication policies also specify the frequency of querying the presence of a valid RFID tag and actions to be taken if it is not present.

RFID monitor continuously queries the RFID reader with the frequency specified in the current user profile. RFID reader checks the presence of a tag and verifies its correctness using a secure tag/reader authentication protocol. An excellent survey of existing protocols developed in recent years can be found in [31]. RFID monitor may time out while acquiring valid RFID credentials due to one of three factors: if no RFID tag is present; due to failure of the authentication protocol due to interference; or due to authentication failure if an invalid RFID tag is present. If interference problems are detected, RFID monitor may query the reader several times in attempt to establish successful communication with the tag before finally timing out. An RFID monitor timeout event leads to authentication failure. Since it is impossible to predict when a device might fail, recovery procedures have to be in place. Our model deploys multi factor authentication; therefore, in case of a RFID reader failure (also due to a DoS attack), authentication can be performed using a password. Although RFID transceiver is shown as a part of the host hardware in Figure 3, an external RFID reader can typically be connected via a USB interface.

Authentication manager acts as the front-end interface for all file I/O operations performed by the user applications: it facilitates just-in-time user authentication whenever a file operation is requested. Although RFID monitor queries the presence of a valid tag periodically, if the time since last such operation exceeds a certain threshold, it will be performed again at the time of the file I/O request.

In RFID-AM, an RFID tag is used to verify a user's presence. EPC data stored on the RFID tag could contain the key used for encryption; alternatively, EPC data can be used to create and validate an encryption key. Password-based key derivation function (PBKDF) is a technique that utilizes an alpha-numerical password and other parameters as a salt value and an iteration count to create an encryption key. In case if the required encryption key length is greater than the size of EPC, RFID-AM takes advantage of PBKDF2, as specified in RFC 2898 [23] that applies a pseudorandom function to derive a key of any length. Unique EPC value stored in the RFID tag is used as a password to create an encryption key of the required length to be used with encryption algorithms.

RFID-AM secures files using encryption. There are two basic techniques for encrypting information: symmetric (secret key) encryption and asymmetric (public key) encryption. In symmetric algorithms, data encrypted with a particular key can only be decrypted using the same key. For this reason, the key has to be secured and exchanged between two parties, which can be seen as the main drawback. In contrast, asymmetric encryption uses a pair of keys (public and private) one for encryption, one for decryption, which solves the key management problem. However, asymmetric encryption is slower than symmetric and requires more processing power to both encrypt and decrypt data. Since the speed is an important factor and the key distribution is not an issue (the key is created and used within the RFID-AM because both encryption and decryption take place on the same mobile device), RFID-AM uses symmetric-key algorithms. Symmetric-key encryption algorithms (ciphers) can be further divided into stream ciphers and block ciphers. Stream ciphers encrypt the bits of information one at a time, typically by an exclusive-or operation with a pseudorandom key stream. They are fast and small but

vulnerable to a reused key attack if the key is used more than once. Block ciphers encrypt data by breaking it down into blocks and encrypting them separately. The same key can be used multiple times as long as it is not revealed. Given these characteristics, symmetric block algorithms were an obvious choice for RFID-AM, which supports DES (64b key), AES (128b key), and Blowfish (32-128b key).

The Data Encryption Standard (DES) was published in 1977 by the US National Bureau of Standards and subsequently became an ANSI standard. Over time, various vulnerabilities were discovered, mainly due to a relatively short key length. In 2002 DES was superseded by the Advanced Encryption Standard (AES) originally published as Rijndael. AES is an iterated cipher with a variable block length and a variable key length (128, 192, and 256 bits) that has been analyzed extensively and now is used worldwide. Blowfish was designed in 1993 by Bruce Schneier as a fast, license-free alternative to existing encryption algorithms. It takes a 64-bit data block and a variable-length key, from 32 bits to 448 bits. It has been analyzed considerably, and it is gaining acceptance as a strong encryption algorithm.

4. Privacy and Security Issues

RFID technology has been widely adopted by the industry due to its unique benefits. However, as RFID applications become widespread, privacy and security issues have arisen. Privacy concerns include but are not limited to covert tracking or surveillance of individuals and the ability to profile individuals by their belongings containing RFID tags. Because of the contactless nature of RFID technology, any reader operating at the same frequency can read passive tags. Most tags have no authentication mechanisms implemented; consequently, the tag's ID is available to non-intended recipients. Fundamental information security objectives, such as confidentiality, integrity, authentication, and anonymity are not achieved in RFID systems unless special security techniques are integrated into the system [34,37]. In addition to privacy issues, RFID technology is open to the following security threats: eavesdropping, denial of services attack, relay attack, and tag cloning. Eavesdropping is possible as the tag automatically responds to an inquiring reader. A malicious user can easily obtain the data saved on the tag and use it to track individuals or objects, to perform a relay attack (an adversary acts as a man-in-the middle between a tag and a reader) or even clone the tag. A denial of service attack is a well-known weakness of RFID-based solutions based on simple passive tags. The attack can be due to physical characteristics of the reader that could be blocked by water or metal, too many different tags in its range, or a failure of the device.

Most passive RFID tags can be read only at very short distances, a few feet at most. Tags used in RFID-AM have an even shorter range of a few inches. Given the nature of the tags, potential adversaries would be physically constrained since they must have physical proximity to the tag in order to read it. As mentioned above, the range is narrow enough to partially reduce eavesdropping and DoS problems. In addition, there are many solutions to address the issues of security in RFID environments. Some of them focus on blocking tags whenever they are not in use (RFID Blocking Wallets [12], Blocker tags [22], special commands like SLEEP to deactivate a tag) while others use specially designed cryptography techniques (also called "minimalist cryptography" [21]) and communications schemes that can be efficiently implemented for low-cost tags [39].

Potential security vulnerabilities could also include over-the-air modifications or deletion and SQL injection attacks. As long as software runs on the top of the device's operating system the unwanted modification or deletion may occur. The potential solution could add the middleware code directly to the RFID reader. An SQL injection attack can be prevented by filtering user input or using parameterized queries.

There are many challenges in implementing an RFID solution without compromising privacy and security. However, a variety of solutions are in place to preserve privacy and ensure security. RFID technology has a potential to become a major enabler of ubiquitous computing. A quick and uncomplicated authentication scheme such as RFID-AM is crucial to implementing a seamless and unobtrusive interaction in a computing environment with a significant number of different devices that users can access. In this context, the tracking problem may have a positive side. Being able to track users and the usage of their devices might be useful in a corporate environment to implement and enforce proper access and security policies.

5. Performance of RFID-AM

To test the viability of the proposed RFID-AM architecture, a fully functional prototype was implemented and subjected to a series of operational experiments. The objective of these experiments was to test the reliability of continuous authentication implemented using a Class 1 Gen 2 RFID system in conjunction with one of three data encryption mechanisms: AES, DES, and Blowfish.

A prototype of RFID-AM was installed on a low-end laptop. Continuous authentication was employed in conjunction with a simulated application cycle of opening and closing files of varying sizes (10kB, 500kB, 1MB, 5MB, and 10MB). RFID-AM handled these requests by transparently authenticating the user prior to opening of any file, at which time the file was decrypted using a key obtained via PBKDF2 from the RFID tag's EPC data. For the purposes of this experiment, RFID monitor forced verification of a valid RFID tag prior to opening of each file. This experiment was repeated using three different encryption algorithms under two operational conditions: when the device was idle and when there were a number of other computationally expensive tasks running at the same time. The time taken by the RFID monitor to query the reader was measured separately from the time taken to encrypt the file. As Figure 4 shows, processing and querying the RFID reader introduced a constant delay of 0.5-0.6 second, while encryption time grew linearly with the file size. Each of the graphs showing the RFID-AM performance reflects a standard measurement error, which shows a significantly higher variance in the timing of RFID interface, primarily due to varying CPU load and repeated RFID reader requests due to interference. As expected, AES and Blowfish encryption algorithms consistently provided the best performance with a total overhead of about 1.5 seconds incurred while performing continuous authentication and decryption of a 10MB file, or about 1 second for a 5MB file. A similar set of experiments was conducted to test RFID-AM performance while closing and encrypting user files, which does not necessitate verification of a valid RFID tag. Performance of RFID-AM encryption operation that occurs every time a file is closed was nearly identical to that presented in Figure 4 (less the time incurred by RFID monitor) and therefore is not presented here.

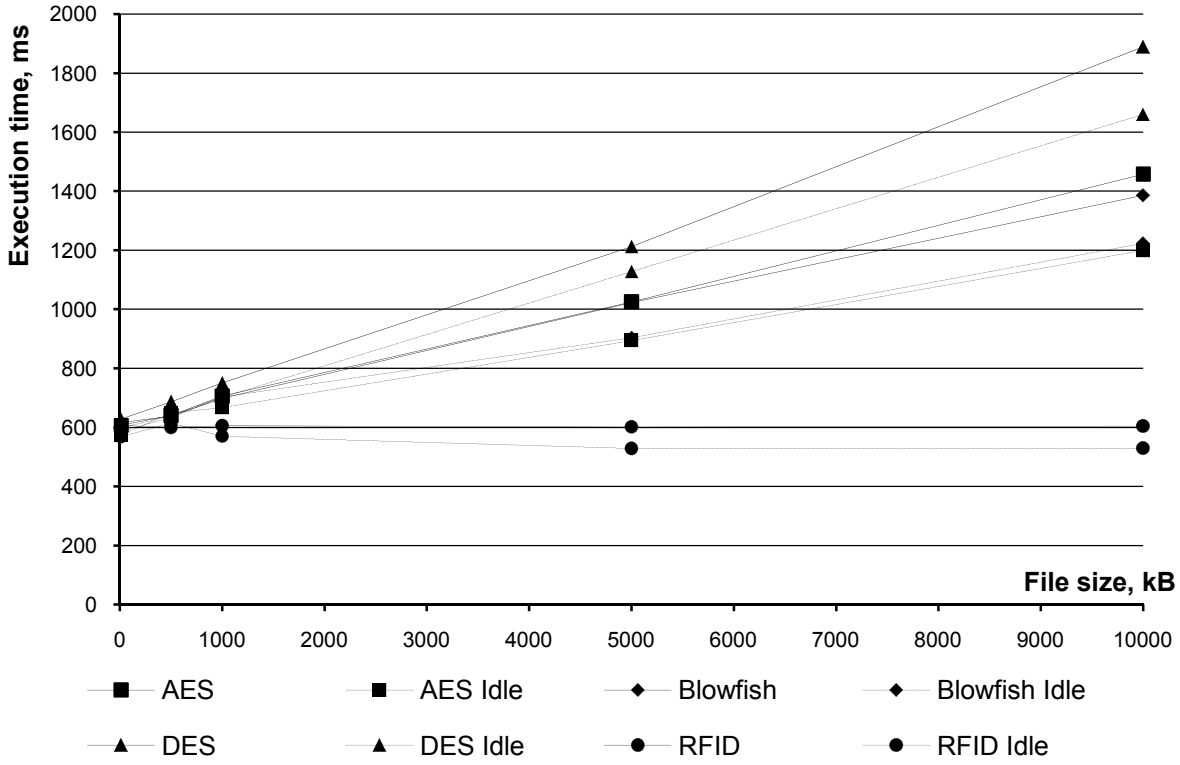

Figure 4. Performance of RFID-AM with three encryption algorithms under idle and busy conditions.

6. Summary and Discussion

Tremendous growth of popularity of mobile consumer devices, such as smart phones and netbooks, coupled with omnipresent high-speed network connectivity has changed the ways how we compute and communicate. These mobile devices play an increasingly important role in our lives and often are becoming a representation of our digital selves when we choose to trust these devices with sensitive

information. The issue of securing mobile devices against unauthorized access has never been more important.

This paper described RFID-based Authentication Middleware designed to combine point of entry authentication provided by the operating system with continuous authentication using a possession-based method, while also securing sensitive user data with encryption. Authenticity of the user is checked with a given frequency by verifying that a valid RFID transponder is present within certain proximity of the user and the secured device. RFID-AM triggers system lockdown and automatic encryption of all open files when either an invalid RFID tag is presented or when an authorized user walks away from the device.

A fully functional prototype of RFID-AM has been implemented to test the viability of the proposed approach. Experimental data presented here demonstrates stable system performance with acceptable timing. Although the prototype of RFID-AM has been deployed on a low-end laptop, it has not yet been tested on a smart phone. It is important to note that it is highly unlikely for users to keep very large files on a resource-constrained device, such as a mobile phone. As can be seen in Figure 4, for files smaller than 5 MB, the performance of the systems is primarily constrained by the speed of RFID sensor and not by the computational overhead.

There are a number of ways in which the use of RFID-AM could be extended, For example, it is possible that the user may have the right credentials for the point of entry, but not for the continuous authentication provided by RFID-AM. If the user does not possess the correct RFID tag, the system will not unlock regardless whether they are supplying the correct operating system authentication credentials. Furthermore, RFID-AM could be used not only to augment, but also to replace the authentication features of the host operating system.

In many corporate environments employees are asked to lock their computer when they walk away from their workplaces but there is no guarantee and no reasonable way to enforce that they would actually do so. RFID-AM deployed in such environments could offer such a guarantee and relieve the users from the burden of remembering to lock their workstations and offer an effective security solution to the enterprise. By keeping the user authentication features provided by the operating system, RFID-AM could offer a non-intrusive proactive method to secure computing devices when the user walks away, without downgrading security or eliminating existing user authentication protocols.

7. References

[1] Abdelhameed, R., Khatun, S., Borhanuddin, A., and Ramli, A. “Application of Mobile Phone in Laptop Security”. Journal of Applied Sciences. 2005, pp. 215-219.

[2] Blonder, G. "Graphical Passwords". US Patent 5559961, 1996.

[3] Chen, X., Tian, J., Su, Q., Yang, X., and Wang, E.Y. “A Secured Mobile Phone Based on Embedded Fingerprint Recognition Systems”. Lecture Notes in Computer Science, Springer, Apr. 2005, Vol. 3495, pp. 549-553.

[4] Clarke, N., and Furnell S. “A Composite User Authentication Architecture for Mobile Devices”, Journal of Information Warfare, 2006, vol. 5, no. 2, 11-29.

[5] Clarke, N. and Mekala, A. “The application of signature recognition to transparent handwriting verification for mobile devices”. Information Management & Computer Security, Emerald Publishing, 2007, Vol. 1, No. 3, pp. 214-225.

[6] Curty, J., Declercq, M., Dehollain, C. and Joehl, N. “Design and Optimization of Passive UHF RFID Systems”. Springer, 2006.

[7] Daugman, J. “High confidence visual recognition of persons by a test of statistical independence”. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1993, pp. 1148-1161.

[8] Davis, D., Monrose, F., and Reiter, M. “On User Choice in Graphical Password Schemes”. In Proc. 13th USENIX Security Symposium. California, 2008.

[9] Descy, D.E. “Netbooks: Small but Powerful Friends”. TechTrends, Springer, Mar. 2009, Vol. 53, No. 2, pp. 9-10.

[10] Dhamija, R., and Perrig, A. “Deja Vu: A User Study Using Images for Authentication”. 9th Usenix Security Symposium, Aug. 2000, Denver, Colorado pp. 45–58.,

[11] Dunphy, P., Nicholson, J., Olivier, P. “Securing Passfaces for Description”. In Proc. 4th Symposium on Usable Privacy and Security, 2008, Pittsburgh, PA, pp. 24-35.

[12] Dustin, K. “How To Make A RFID Blocking Wallet”. Cryptology ePrint Archive, Report 2005/049, January 2006.

[13] Furnell, S. M., Clarke, N. L,, Karatzouni, S. “Beyond the PIN: Enhancing user authentication for mobile devices”. 2008, 8, pp. 12-17.

[14] Hayashi, E., Christin, N., Dhamija, R., and Perrig, A. “Mental Trapdoors for User Authentication on Small Mobile Devices”. Tech. Rep. CMU-CyLab-07-011, Carnegie Mellon Univ., 2007.

[15] Henrici, D. “RFID Security and Privacy: Concepts, Protocols, and Architectures”. Springer, 2008.

[16] Hwang, S., Cho, S., Park, S., “Keystroke dynamics-based authentication for mobile devices”. Computers & Security, Vol. 28, No. 1-2, Feb.-Mar. 2009, pp. 85-93.

[17] Ijiri, Y., Sakuragi, M., and Shihong, L. "Security Management for Mobile Devices by Face Recognition". In Proc. 7th International Conference on Mobile Data Management, 2006, pp. 40-49.

[18] Jansen, W. "Authenticating Users on Handheld Devices". In Proc. Canadian Information Technology Security Symposium, May 2003.

[19] Jansen, W., Gavrila, S., and Seveillac, C. "Smart Cards for mobile devices". International Journal of Information and Computer Security, 2007, 400-413.

[20] Jermyn, I., Mayer, A., Monrose, F., Reiter, M., and Rubin, A. "The Design and Analysis of Graphical Passwords". In Proc 8th USENIX Security Symposium. 1999, Berkeley, CA.

[21] Juels, A. "Minimalist cryptography for low-cost RFID tags." In C. Blundo and S. Cimato, editors, The Fourth International Conference on Security in Communication Networks – SCN 2004, volume 3352 of Lecture Notes in Computer Science, pages 149–164. Springer-Verlag.

[22] Juels A., Rivest R., and Szydlo M., "The blocker tag: selective blocking of RFID tags for consumer privacy", Proceedings of the 10th ACM conference on Computer and communications security, October 27-30, 2003, Washington D.C., USA

[23] Kaliski, B. "Password-Based Cryptography Specification". RFC 2898. http://www.ietf.org/rfc/rfc2898.txt

[24] Karatzouni, S., Furnell, S., Clarke, N., and Botha, R. "Perceptions of User Authentication on Mobile Devices". In Proc. ISOneWorld Conference. Las Vegas, 2007.

[25] Kumar, A. and Zhang, D. "Personal recognition using hand shape and texture". IEEE Trans. Image Processing, Aug. 2006, Vol. 15, No. 8, pp. 2454-2461.

[26] Lammi, H.-K. "Ear Biometrics". Lappeenranta, Finland: Lappeenranta University of Technology, 2003.

[27] Melcher, D. "Persistence of visual memory for scenes". Nature, 412 (6845), Jul. 2001, p. 401.

[28] Narayanaswami, C., and Raghunath, M.T. "Application Design for a Smart Watch with a High Resolution Display," Proc. Fourth Int'l Symp. Wearable Computers, Oct. 2000, pp. 7-14.

[29] Nicholson, A., Corner, M., and Noble, M. "Mobile Device Security Using Transient Authentication". IEEE Transactions on Mobile Computing, 2006, pp. 1489-1502.

[30] Noble, B., and Corner, M. "The case for transient authentication". In Proc. 10th workshop on ACM SIGOPS European, 2002, pp. 24-29.

[31] Piramuthu, S. "Protocols for RFID tag/reader authentication". Decision Support Systems, Apr. 2007, Vol. 43, No. 3, pp. 897-914.

[32] Qian, T., & Veldhuis, R. "Biometric Authentication for a Mobile Personal Device". In Proc. 3rd Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, 2006, pp. 1-3).

[33] Sobrado, L., and Birget, J. "Graphical Passwords". The Rutgers Scholar, vol. 4, 2002.

[34] Syamsuddin, I., Dillon, T., Chang, E., and Han, S., "A Survey of RFID Authentication Protocols Based on Hash-Chain Method," iccit, vol. 2, pp.559-564, 2008 Third International Conference on Convergence and Hybrid Information Technology, 2008.

[35] Takada, T., and Koike, H. "Awase-E: Image-Based Authentication for Mobile Phones Using User's Favorite Images". Lecture Notes in Computer Science, vol. 2795, 2003. pp. 347-351.

[36] Vildjiounaite, E., Makela, S., Lindholm, M., Kyllonen, V., and Ailisto, H. "Increasing Security of Mobile Devices by Decreasing User Effort in Verification". In Proc. 2nd International Conference on Systems and Networks Communications. 2007.

[37] Wang, H., Sun, L., Yong, J., and Zhang, Y., "Privacy preserving on Radio Frequency Identification systems," cscwd, pp. 674-679, 2009 13th International Conference on Computer Supported Cooperative Work in Design, 2009.

[38] Want, R. "RFID explained: a primer on radio frequency identification technologies", Synthesis Lectures on Mobile and Pervasive Computing (Intel Research), Vol. 1, 1 USA, pp. 1-94. January, 2006.

[39] Weis S. A., Sarma S. E., Rivest R. L., and Engels D. W.. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Security in Pervasive Computing, volume 2802 of Lecture Notes in Computer Science, pages 201–212, 2004.

[40] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon, N. "Authentication using graphical passwords: Basic results". Human-Computer Interaction International, 2005, Las Vegas, NV.