International Journal of Advanced Research in Engineering and Applied Sciences

ISSN: 2278-6252
Impact Factor: 7.358

A SECURE AND RELIABLE AUTHENTICATION MECHANISM FOR USERS OF MICROSOFT CARDSPACE FRAMEWORK

Surbhi Singh, Research Scholar, Department of Computer Science & Engineering, Deenbandhu Chhotu Ram University of Science & Technology, Sonipat

Abstract: *The development of web applications on Cloud computing platform has given rise to various concerns about the private data of the consumers of cloud. The traditional form of security tokens like username/password used to access cloud services are prone to phishing attacks and hence do not provide complete security.*

CardSpace (formerly known as InfoCard) is a Digital Identity Management system that has recently been adopted by Microsoft. In this paper identification of two security flaws in CardSpace that may lead to a serious privacy violation have been detected. The first flaw is the reliance on Internet user judgements of the trustworthiness of service providers, and the second is the reliance of the system on a single layer of authentication. A multi-level solution is designed to address both flaws using biometric authentication techniques. Solution is compatible with the currently deployed CardSpace identity metasystem, and should enhance the privacy of the system with minor changes to the current CardSpace framework.

Keywords: *Authentication, Microsoft Cardspace, biometric, token*

1. INTRODUCTION

Along with the growing reliance on Internet web applications in our daily life, comes the problem of managing the necessary digital identities and preserving their privacy. In an open large-scale domain such as the Internet, preserving user privacy is not a straightforward task. Identity theft, which occurs when an impostor uses a legitimate user's identifying information without his/her consent, is becoming one of the biggest concerns for organizations offering services on the Internet. Many solutions have been proposed in the last few years to address the threat of identity theft, and to tackle identity oriented attacks such as phishing and pharming. Most of those solutions are based on the concept of Identity Federation (different identities that belong to the same user in a particular trust domain are "federated"), and Single Sign-On (where a user performs an authentication process only once in a single working session).

In 1999, Microsoft adopted .NET Passport, an identity federation and ticket-based single sign-on system. Although .NET Passport was supported by a number of well-known service providers, such as eBay and Visa, it was not widely used for single sign-on. The single sign-on features have since been dropped, and Passport now functions simply as a means of logging into Microsoft sites. In 2005, Microsoft published two papers that discuss the "failure" of .NET Passport.

Recently, Microsoft has proposed a new identity management framework named CardSpace. CardSpace has some similarities to other identity federation systems; however it is not a single sign-on system. CardSpace is designed to reduce the reliance on passwords for Internet user authentication by service providers, and to improve the privacy of personal information.

In this paper, identification of significant security and privacy issues in the CardSpace scheme is done. The main focus is on two particular security problems, namely, its reliance on user judgements of the trustworthiness of service providers and its dependency on a single layer of user authentication to the Identity Provider.

2. MICROSOFT CARDSPACE

In line with the continuing increase in the number of online services requiring authentication, there has been a proportional rise in the number of digital identities needed for authentication purposes. This has contributed to the recent rapid growth in identity-oriented attacks, such as phishing, pharming, etc. In an attempt to mitigate such attacks, a number of identity management systems have been proposed.

Identity management deals with uniquely identifying individuals in a system, and with effectively controlling access to the system resources by managing the rights and privileges associated with digital identities. The most important service provided by an identity management system is authentication.

Most identity management architectures involve the following main roles:-

1. The identity provider (IdP), which issues an identity token to a user.
2. The service provider (SP), or the relying party (RP) in CardSpace terminology, which consumes the identity token issued by the IdP in order to identify the user, before granting him/her access.

3. The user, also known as the principal.
4. The user agent, i.e. software employed by a user to send requests to webservers and receive data from them, such as a web browser. Typically, the user agent processes protocol messages on behalf of the user, and prompts the user to make decisions, provide secrets, etc.

CardSpace is the name for a Microsoft WinFX set of software components that form an identity management system or an identity metasystem, since it is a system of systems. This identity metasystem is designed to comply with the Laws of Identity promulgated by Microsoft1. Digital identities in CardSpace are represented as claims made by one digital subject (e.g. an Internet user) about itself or another digital subject. A claim is an assertion that certain identifying information (e.g. given name, SSN, credit card number, etc.) belongs to a given digital subject . According to this definition, identifiers (e.g. username) and attributes (e.g. user gender) are both treated as claims within the identity metasystem.

2.1 The CardSpace Framework

The CardSpace framework is based on the identification process we experience in the real world using physical identification cards. Within the CardSpace framework, an identity provider issues a user with a virtual card called *InfoCard*, which is an XML file containing (relatively) nonsensitive metainformation about the user. Subsequently, a user can use one of its InfoCards to help identify itself to any service provider who trusts the identity provider that issued the selected InfoCard. InfoCards can also be self-issued by the users themselves. Figure 1 provides a simplified sketch of the CardSpace framework. In the figure it is assumed that the user has already been issued an InfoCard by an identity provider (IdP).

1. In step 1, the CardSpace-enabled user agent or the *Service Requestor* (henceforth abbreviated to CEUA), which is essentially a CardSpace-enabled web browser, requests a service from the relying party (RP), that is, the service provider.
2. In step 2, the RP identifies itself using a public key certificate (e.g., a certificate used for SSL/TLS) and declares itself as a CardSpace-enabled RP using XHTML code or HTML object tags.
3. After recognizing that the RP is CardSpace-enabled, the CEUA retrieves the RP security policy in step 3. This policy contains a list of the claim types that must be

asserted about the Internet user (henceforth abbreviated to user) in order for this user to be granted the service, the IdPs that are trusted to make such assertions, and the types of security token that are acceptable to the RP. The security policy also specifies requirements that must be met by the retrieved security token (e.g., the type of proof key, or the maximum token age). It is important to emphasize here that CardSpace identity metasystem itself does not restrict the type of security tokens; that is, all types of token can be used within the framework.

4. In step 4 the CEUA matches the RP's security policy with the InfoCards possessed by the user in order to find one that satisfies the RP's policy. If one or more suitable InfoCards are found, the user is prompted to select an InfoCard from amongst them. After the user has selected an InfoCard, the CEUA initiates a connection with the IdP that issued that InfoCard.
5. The user performs an authentication process with the IdP in step 5.
6. If the authentication process succeeds, step 6 takes place, in which the CEUA requests the IdP to provide a security token that holds an assertion of the truth of the claims listed within the selected InfoCard; the message that holds this request is called a *request security token* message. The IdP will then check whether its security policy permits it to generate the requested security token. If so, the IdP will reply by sending a security token within a message called a *request security token response* message.
7. Finally, the CEUA forwards the security token to the RP in step 7.
8. If the RP verifies it successfully, the service will be granted in step 8.

It is worth mentioning here that, after step 6, the contents of the security token can optionally be displayed to the user before proceeding to step 7. Moreover, the RP will get an assertion from the IdP that the security token received was issued to a particular user. This assertion is based on the use of a secret "proof-key," where a user asserts ownership of a security token by demonstrating knowledge of the proof key included in the token. This assertion helps to prevent token replay attacks, that is, where an attacker "steals" a token for another user.

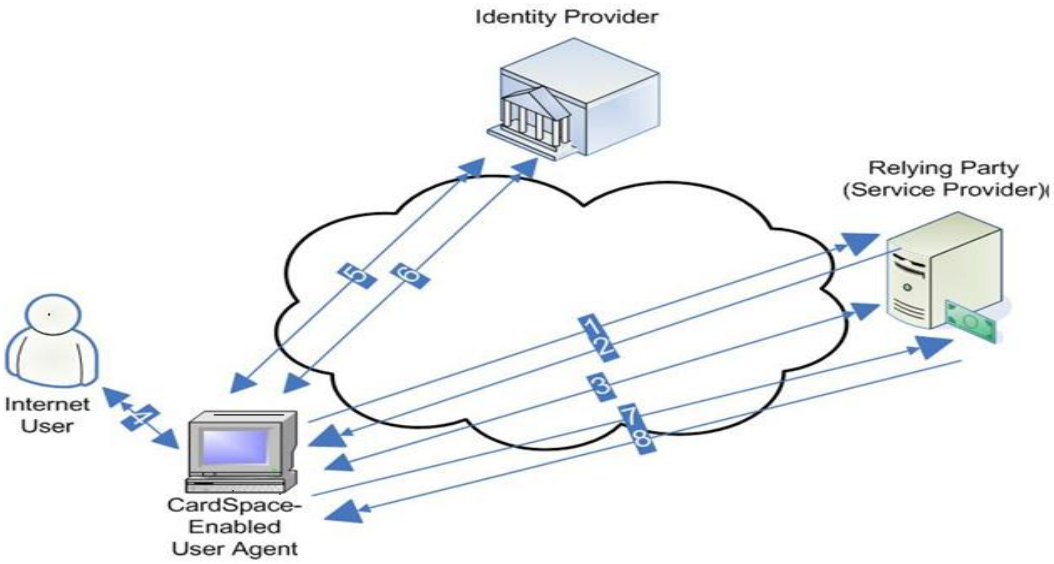

Fig 1 Cardspace Framework

It is worth mentioning here that, after step 6, the contents of the security token can optionally be displayed to the user before proceeding to step 7. Moreover, the RP will get an assertion from the IdP that the security token received was issued to a particular user. This assertion is based on the use of a secret "proof-key," where a user asserts ownership of a security token by demonstrating knowledge of the proof key included in the token. This assertion helps to prevent token replay attacks, that is, where an attacker "steals" a token for another user.

The message flows of the CardSpace framework are as follows:

(1) **CEUA** → **RP**: HTTPGETLoginHTML Page Request

(2) **RP** → **CEUA**: HTML Login Page + InfoCard Tags (XHTML or HTML object tags)

(3) **CEUA** ↔ **RP**: CEUA retrieves security policy via *WSSecurityPolicy*

(4) **CEUA** ↔ **User**: User picks an InfoCard

(5) **CEUA** ↔ **IdP**: User Authentication

(6) **CEUA** ↔ **IdP**: CEUA retrieves security token via *WSMetadataExchange* and *WS-Trust*

(7) **CEUA** → **RP**: CEUA presents the security token via *WS-Trust*

(8) **RP** → **CEUA**:Welcome, you are now logged in!

WS-MetadataExchange, WS-Trust, and WSSecurityPolicy messages are transported over SOAP. The messages in steps 3, 5, 6, and 7 must be carried over an SSL/TLS channel to preserve their confidentiality. It appears reasonable to assume that the most commonly

used security token type will be a SAML assertion, carried over SOAP. The integrity of the security token is preserved using an XMLSignature as part of theWS-Security protocol.

3. SECURITY LIMITATIONS

CardSpace framework suffers from serious drawbacks. One such limitation is its reliance on DNS names to identify the IdPs and the RPs. If the DNS server is controlled by an attacker, it can direct the identity metasystem parties to false websites. This problem is common to many current Internet identity management solutions and is very difficult to address. Probably the only long-term solution to this problem is to hope that the use of DNSSEC, or some other secure address resolution solution, will become widespread. Another limitation is that, in the default scenario for the CardSpace framework, the IdP is aware of the identities of the RPs to which the user attempts to log in. Accordingly, the IdP can learn about the behavior of users on the web.

3.1 . Judgements of RP Trustworthiness

The user judgement regarding the honesty of the RP is a security-critical task. The RP will obtain personal information belonging to the user in the form of “asserted claims” within a security token, as sent in step 7 of the message flow. Thus, if the RP is not trustworthy, it could gather information about users and potentially use this information in unauthorized ways. Accordingly, any misjudgment of the trustworthiness of an RP could result in a serious privacy violation. Hence, the task of judging the honesty of the RP is a very important one. In the CardSpace framework, when the user is prompted for its consent to be authenticated to an RP using a particular InfoCard, the user makes a judgment regarding the trustworthiness of the RP based on one of the following:

(1) a high-assurance public key certificate belonging to the RP,

(2) an “ordinary” public key certificate belonging to the RP (e.g., a certificate used for SSL/TLS), or

(3) no certificate at all.

Obviously, in the third situation the user has no evidence of the honesty of the RP.

Microsoft recommends the first option, that is, the use of a high assurance certificate (also referred to as a “higher-value,” “higher-assurance” or “extended validation” certificate). Such a certificate is an X.509 certificate that is only issued after a rigorous and well-defined registration process, unlike the CA-specific procedures used for issuing certificates

commonly employed as the basis for SSL/TLS security. A high assurance certificate might include a digitally signed bitmap of the RP's company logo in order to make it easier for the user to identify the certificate holder (The inclusion of such a logo is discussed in a number of documents circulated by Microsoft, although the latest version of the draft standard for extended validation certificates, as published by the CA/Browser Forum, does not mandate the inclusion of a logo. Whether or not such a requirement will be included in the standard at a later date remains unclear.)

3.2. Reliance on a Single Layer of Authentication

The security of the CardSpace identity metasystem relies on the authentication of the user by the IdP. In a case where a single IdP and multiple RPs are involved in a single working session, which we expect to be a typical scenario, the security of the identity metasystem within that working session will rely on a single layer of authentication, that is, the authentication of the user to the IdP. This user authentication can be achieved in a variety of ways (e.g., using an X.509 certificate, Kerberos v5 ticket, self-issued token or password); however, it seems likely that, in the majority of cases, a simple username/password authentication technique will be used. If a working session is hijacked (e.g., by compromising a self-issued token) or the password is cracked (e.g., via guessing, brute-force, key logging, or dictionary attacks), the security of the entire system will be compromised. It is fair to mention here that most of the deployed Internet identity management solutions, such as Liberty and OpenID, suffer from the same vulnerability.

4. LITERATURE SURVEY

1. **"Privacy in cloud computing through identity management"** paper basically focuses on the security issues in the Microsoft cardspace technique which is recently developed by the Microsoft in order to provide the privacy to the users data. In this paper already implemented tools are discussed such as OpenId and PRIME (privacy and identity management for Europe). But these also suffer from the problems like phishing and single layer authentication. So they discussed Microsoft cardspace technique with its loopholes such as single layer authentication and relying on third party for private data. The authors come up with new technique called "zero knowledge proofing" which do not allow disclosing private data to anybody and

"SAML" which offers broader authentication and is compatible with all existing products.[1]

2. In the paper **"Improving the security of cardspace"** whole card space technique is discussed in detail with its full architecture and its 2 major flaws are taken into consideration and a new methodology with 3 approaches is developed. Its analysis is also made in order to check its level of providing required security.[2]
3. **"Privacy Preserving Multi-Factor Authentication with Biometrics"** paper focuses on a two-phase authentication mechanism for federated identity management systems. The first phase consists of a two-factor biometric authentication based on zero knowledge proofs. The authors employ techniques from vector-space model to generate cryptographic biometric keys. These keys are kept secret, thus preserving the confidentiality of the biometric data, and at the same time exploit the advantages of a biometric authentication. The second authentication combines several authentication factors in conjunction with the biometric to provide a strong authentication. A key advantage of our approach is that any unanticipated combination of factors can be used. Such authentication system leverages the information of the user that are available from the federated identity management system. They provide a new application of vector-space model to generate efficiently cryptographic biometric keys. They preserve privacy and unconditional security of the biometric key by employing information theoretically secures ZKPK.[3]
4. **"Truststore: Making Amazon S3 Trustworthy with Services Composition"** have successfully proposed a secure virtual file system, called TrustStore to preserve the privacy, integrity and confidentiality of the data stored in the untrusted storage service. Firstly, they develop a service-oriented architecture for provisioning Trustworthy Storage Services (TSS) with untrusted storage service providers where the data is encrypted to cipher text on the client computer and then this cipher text is stored on the SSP. Further the key form is stored on KMSP which can reverse the whole process but does not have the cipher text to apply on. The prototype design, TrustStore preserves the confidentiality of the outsourced data and also encrypts the meta data and file structure. Efficient integrity check detects if any data is corrupted and performance wise outperforms the ordinary usage latency with Amazon S3.[4]

5. THE PROPOSED SECURED SOLUTION

After going through the various papers related to Microsoft card space technique, it has been observed that although it is a good technique to provide the security but then also it has two major loopholes in security that needed to be overcome. One is to reduce Judgements of RP Trustworthiness and the other is to remove single layer authentication. So there is a need to implement multi-level authentication architecture in it, to use some strong technique for providing authentication and prevent relying on third party for claims.

It will remove the dependability on the third party and the tokens generated for the users will be more secure as the authentication process will be made more complex to attack by attacker.

In this paper, we will take irises as the biometric characteristic that is used for authentication. We adopt the XOR operation as the function and we use a secret, randomly chosen string, as the secret information. The XOR operation is chosen because it will not affect the matching result, because the matching algorithm for irises uses a Hamming distance comparison between two biometric strings. That is, since the Hamming distance is, itself, a population count of a bitwise XOR, the affect of the extra XORs will be canceled out. The idea is shown in Fig. 2

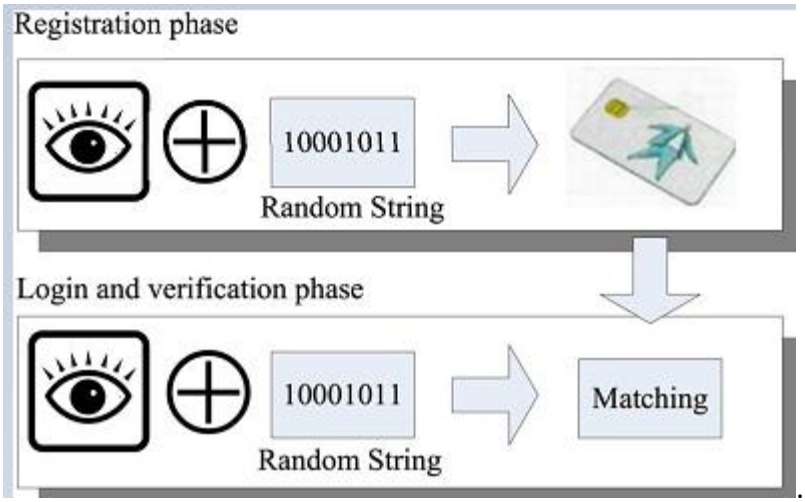

Fig 2 Iris matching

Users randomly select a string and combine it with their iris data via the exclusive-or operation.

The combined string is stored in the smart card in the registration phase. The smart card then combines the same randomly chosen string with the iris data input in the login phase.

Finally, the two strings created from the registration phase and from the login phase are sent to the server for matching. The proposed protocol therefore meets our needs: the server cannot learn the user's biometric data, but the correctness of the data can still be checked by the server.

6. CONCLUSION

We summarize the main contributions of the paper as follows.

1) Truly Three-Tier Authentication: The three true factors (smart cards, passwords, and biometrics) are of three different data types, where smart cards display *what you have*, passwords depicts *what you know*, and biometrics represent *what you are*, and they are all verified in the server.
2) Strong Privacy based on Biometrics: In our proposed scheme, the biometric template and biometric samples of every user are protected while the server performs the matching algorithm, so that the server cannot learn biometric data in authentication processes. Moreover, the server itself or any adversary who has corrupted the server cannot still obtain users' biometric data even if users' cards have been stolen or lost and the data in the cards are leaked.
3) Efficiency: The server does not need to maintain password or biometric databases, and the user does not perform time-consuming operations, such as exponentiation computations, in the smart card.
4) Provable Security: We formally analyze the proposed protocol to show the completeness and prove the soundness of the protocol theoretically with our security definition of three-factor authentication.

REFERENCES

[1] Bhargava Bharat, Noopur Singh, "Privacy in cloud computing through identity management".

[2] Waleed A. Alrodhan, Chris J.Mitchell, "Improving the Security of CardSpace", EURASIP Journal on Information Security, Volume 2009, Article ID 167216, 8 pages doi:10.1155/2009/167216.

[3] Anna Squicciarini, Elisa Bertino," Privacy Preserving Multi-Factor Authentication with Biometrics", DIM'06, November 3, 2006, Alexandria, Virginia, USA. Copyright 2006.

[4] Yao, J., Chen, S., & Nepal, S. (2010). Truststore: Making Amazon S3 Trustworthy with Services Composition. 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing.

[5] H. S. Kim, J. K. Lee, and K. Y.Yoo, "ID-based password authentication scheme using smart cards and fingerprints," ACM SIGOPS Operating Syst. Rev., vol. 37, no. 4, pp. 32–41, 2003.

[6] J. K. Lee, S. R. Ryu, and K. Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," Electron. Lett., vol. 38, no. 12, pp. 554–555, 2002.

[7] Y. Lee and T. Kwon, "An improved fingerprint-based remote user authentication scheme using smart cards," in Proc. ICCSA 2006, 2006, vol. 3981, pp. 915–922, Lecture Notes in Computer Science.

[8] C. H. Lin and Y. Y. Lai, "A flexible biometrics remote user authentication scheme," Comput. Standards Interfaces, vol. 27, no. 1, pp. 19–23, 2004.