Volume 4, No. 9, September 2013
Journal of Global Research in Computer Science
RESEARCH PAPER
Available Online at www.jgrcs.info
ISSN-2229-371X

PRIVACY AND SECURITY ISSUES IN CLOUD COMPUTING

Ankit Sharma*
M. Tech., Dept. of C.S.E.
Lovely Professional University
Jalandhar, India
erankitsharma1991@gmail.com

Shashank Gupta
M. Tech., Dept. of C.S.E.
Lovely Professional University
Jalandhar, India
coolshashank22@rediffmail.com

Deep Mann
Asst. Prof., Dept. of C.S.E.
Lovely Professional University
Jalandhar, India
er.deepmann@gmail.com

***Abstract*—**Cloud computing is one of the most widely used and acceptable technique. Because of this it came into attention of various groups of people, so the security and maintenance of cloud is major issue. In this paper we have point out some of the major issues effecting the security and reliability of the cloud.

***Index Terms*—**MFCSA, Microsoft Card Space, Privacy, Identity Management, Security.

INTRODUCTION

Service providers are using infrastructure which are provided by their respective cloud providers which have different aspects of security and privacy. Like using different cryptographic techniques for the security purpose to encrypt the data and maintain the confidentiality of the data, but there are various attacks developed which are starting resolving these algorithms very fast like Method of Formal Coding Side Channel Attack (MFCSA) [3] resolves XOR function which is major threat for algorithms using XOR function for computation purpose which is now a day almost all the cryptographic algorithms.

There is a need for a solution for above problem either in form of modification in previous algorithm or to develop a new algorithm which does not use the XOR function for computation purpose.

The data of the user are very sensitive in nature, so to provide privacy to them service providers provide username and password to authenticate the user and only use of the username/password security token for authentication leaves consumer vulnerable to phishing attack. The solution of the problem would be the use of a proper Identity Management (IDM) [20]. But there are various problems in existing IDM's which leads to the breach in privacy of the consumer like one of the most acceptable IDM is Microsoft CardSpace [7] which also have several limitation (Section III) which are needed to be removed.

SECURITY ISSUE IN CLOUD

To maintain the confidentiality of the data of cloud various cryptographic techniques are used to ensure security of the data but recent attacks make this work much difficult, one of the major attack need to be resolved today is MFCSA which is used to resolve almost every cryptographic algorithms.

A. Description of the Method of Formal Coding-Side Channel Attack (MFCSA)

MFCSA is also said as extended version of Algebraic Side Channel Attack (ASCA) [4, 5]. Algebraic Side Channel has three Steps:

1) Offline phase 1: algebraic description of the cryptosystem.
2) Online measurement phase to obtain leaked information.
3) Offline phase 2: equation system solving by SAT method.

MFCSA also have above three steps but step 1 and 2 of MFCSA is different from that of ASCA.

In step 1) of ASCA, the algebraic description of a block cipher is done which consists of two parts:

a) The equation system is following the idea of the algebraic side channel attack [13].
b) The equation system is generated from the leaked Hamming weight.

In MFCSA, first the direct explicit representation of the outputs is given in terms of plain text and master key with the help of symbolic computation software like Mathematica [16]. Then the Hamming weight (mod 2) of the outputs is explicitly represented by the bits of plaintext and master key.

In step 3) of ASCA, SAT solving technique [14] is used to find solution of equation system while in MFCSA, Gröbner basis based [15] methods are used to find solution of equation system.

PRIVACY ISSUE IN CLOUD

Privacy is an important and very crucial factor for cloud as a network there are many users which results a lot of sensitive data present in cloud so maintain the privacy of the data is very important. Cloud uses IDM to maintain the privacy of data one of the most famous IDM is Microsoft CardSpace which is able to help consumers to manage their various digital identities and various username/password which are associated with each service provider, centrally.

A. Description of Microsoft CardSpace

Microsoft CardSpace is an Identity-metasystem which manages multiple digital identities of a user [7]. It is claims based access platform/ architecture, which is developed for windows XP. It uses a plug-in for Internet explorer 7 browser [8] to provide services in cloud.

The CardSpace is designed to comply with the seven Laws of identities given by Kim Cameron of Microsoft [9].

In CardSpace digital identities are transmitted on the network containing some kind of security token. A security token consists of various set of claims (Figure 1). These security tokens provide information in order to prove that claimer and user is same person.

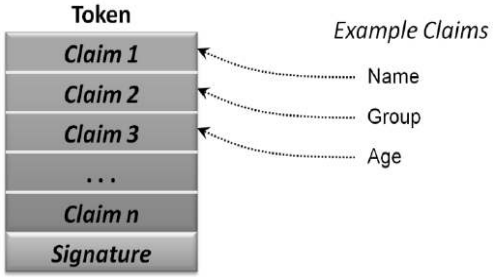

FIGURE 1. A token contains claims about a user along with a digital signature that can be used to verify its issue [8]

Windows CardSpace model involve three parties:

- *Identity provider (Idp):* It issues digital identities (as trusted third-party) like, a credit card provider might issue digital identities (security tokens) enabling payment.
- *Relying Parties (RP)*: It requires identities to provide a service to a user like, a web site.
- *Subjects (service requestor):* They are individuals and other entities about whom the claims are made.

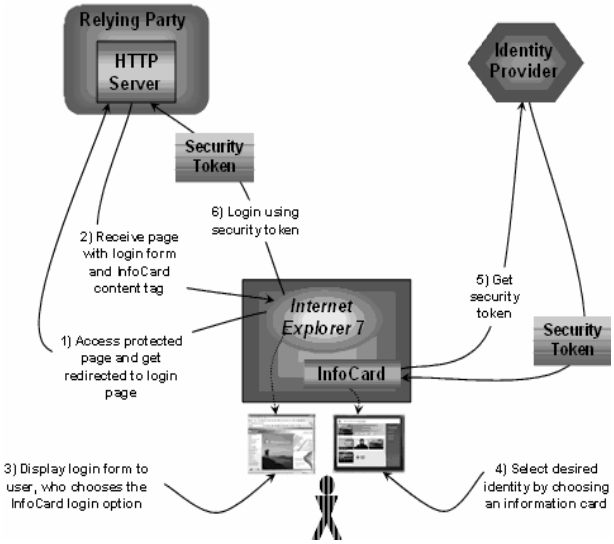

FIGURE 2. CardSpace Model of Identity Management [7]

B. Limitations of CardSpace Model

We only discuss the two major limitations of CardSpace [10]:

1. Trust worthiness of Relying Parties (RP)

As user is prompted for the selecting RP using a particular InfoCard, the user has to select the RP. As user, generally does not pay attention on the value of right selection or unaware about the judgment factors this leads to a major challenge or limitation for the IDM.

2. Single Layer of Authentication

As CardSpace authentication relies on the IdP so as in real scenario number of RP is more than IdP so within a session the authentication process will lead to a single layered architecture which is also a limitation for the IDM.

CONCLUSION

In this paper we have mentioned a security related problem and a privacy related problem in cloud. These problems have to be solved to maintain the privacy and security in cloud.

For the security issue the MFCSA is resolved by simply modifying the previous algorithms to find a new operation in against of the XOR operation or the alternative way is to develop new algorithms without use of XOR operation providing the security in equivalence to previous ones or even more.

For the privacy issue the Microsoft CardSpace is very useful IDM but the limitation are decreasing its reliability in order to remove these limitations we can develop new token mechanism which are multi layered in nature use the involvement of the third party the certification process will have to be improved so that the authentication process would become more reliable.

REFERENCES

[1] Bogdanov, A., Kizhvatov, I., Pyshkin, A.: Algebraic Methods in Side-Channel Collision Attcks and Practical Collision Detection. In: Chowdhury, D.R., Rijmen, V., Das, A. (Eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 251-265. Springer, Heidelberg

[2] Dinur, I., Shamir, A.: Side Channel Cube Attacks on Block Ciphers. Cryptology ePrint Archive, Report 2009/127 (2009), http://eprint.iacr.org/2009/127

[3] Changyong Peng, Chuangying Zhu, Yuefei Zhu, Fei Kang ;" Improved side channel attack on the block cipher NOEKEON".

[4] Mathieu Renauld and Frano¸is-Xavier Standaert. Algebraic Side-Channel Attacks. In Feng Bao, Moti Yung, Dongdai Lin, and Jiwu Jing, editors, Inscrypt, volume 6151 of Lecture Notes in Computer Science, pages 393-410. Springer, 2009.

[5] Mathieu Renauld, Frano¸is-Xavier Standaert, and Nicolas Veyrat-Charvillon. Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA. In Christophe Clavier and Kris Gaj, editors,

CHES, volume 5747 of Lecture Notes in Computer Science, pages 97-111. Springer, 2009.

[6] Yang, L., Wang, M., Qiao, S.: Side Channel Cube Attack on PRESENT. In: Garay, J.A., Miyaji, A., Otsuka, A. (Eds.) CANS 2009. LNCS, vol. 5888, pp. 379-391. Springer, Heidelberg (2009)

[7] Introducing Windows CardSpace, http://msdn.microsoft.com

[8] CLAIMS-BASED IDENTITY FOR WINDOWS http://download.microsoft.com

[9] K. Cameron, M.B. Jones. Design Rationale behind the Identity Metasystem Architecture, http://research.microsoft.com

[10] W. A. Alrodhan, C. J. Mitchell, Improving the Security of CardSpace, EURASIP Journal on Information Security Vol. 2009

[11] B. Laurie. Selective Disclosure, http://research.google.com/pubs/author9639.html/ , 2007

[12] Zero knowledge example Fiat-Shamir proof of identity http://pages.swcp.com/~mccurley/talks/msri2/node24.html

[13] SAML Tokens and Claims -msdn http://msdn.microsoft.com/en-us/library/ms733083.aspx

[14] (2008) .S. F. Hubner, HCI work in PRIME, https://www.prime-project.eu/,

[15] (2011) Understanding WS-Federation http://msdn.microsoft.com

[16] E Biham, A Biryukov, \An Improvement of Davies' Attack on DES", in *Journal of Cryptology* v 10 no 3 (Summer 97) pp 195{205

