Volume 8 ▪ Issue 4 ▪ October 2014

INTERNATIONAL JOURNAL OF SECURITY (IJS)

ISSN : 1985-2320

Publication Frequency: 6 Issues / Year

CSC PUBLISHERS
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF SECURITY (IJS)

VOLUME 8, ISSUE 4, 2014

EDITED BY
DR. NABEEL TAHIR

ISSN (Online): 1985-2320

International Journal of Security (IJS) is published both in traditional paper form and in Internet. This journal is published at the website http://www.cscjournals.org, maintained by Computer Science Journals (CSC Journals), Malaysia.

IJS Journal is a part of CSC Publishers

Computer Science Journals

http://www.cscjournals.org

INTERNATIONAL JOURNAL OF SECURITY (IJS)

Book: Volume 8, Issue 4, October 2014
Publishing Date: 10-10-2014
ISSN (Online): 1985-2320

IJS Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers, 2014

EDITORIAL PREFACE

This is the *Fourth* Issue of Volume *Eight* of The International Journal of Security (IJS). The Journal is published bi-monthly, with papers being peer reviewed to high international standards. The International Journal of Security is not limited to a specific aspect of Security Science but it is devoted to the publication of high quality papers on all division of computer security in general. IJS intends to disseminate knowledge in the various disciplines of the computer security field from theoretical, practical and analytical research to physical implications and theoretical or quantitative discussion intended for academic and industrial progress. In order to position IJS as one of the good journal on Security Science, a group of highly valuable scholars are serving on the editorial board. The International Editorial Board ensures that significant developments in computer security from around the world are reflected in the Journal. Some important topics covers by journal are Access control and audit, Anonymity and pseudonym, Computer forensics, Denial of service, Network forensics etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with Volume 8, 2014, IJS appears in more focused issues. Besides normal publications, IJS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

The coverage of the journal includes all new theoretical and experimental findings in the fields of computer security which enhance the knowledge of scientist, industrials, researchers and all those persons who are coupled with computer security field. IJS objective is to publish articles that are not only technically proficient but also contains information and ideas of fresh interest for International readership. IJS aims to handle submissions courteously and promptly. IJS objectives are to promote and extend the use of all methods in the principal disciplines of computer security.

IJS editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the Journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJS. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJS provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members
International Journal of Security (IJS)

EDITORIAL BOARD

TABLE OF CONTENTS

Volume 8, Issue 4, October 2014

Pages

Novel construction of Secure RFID Authentication Protocol

Shafiqul Abidin *shafiqulabidin@yahoo.co.in*
Department of Information Technology
Northern India Engineering College
(GGSIP University)
Shastri Park, Delhi - 110053, India

Abstract

This article proposes an efficient and secure authentication protocol for secure and low-cost RFID systems in random oracles. Security is one of the prime concerns of RFID system. Proposed protocol relies on Elliptic Curve Discrete Logarithm Problem (ECDLP) to achieve security. The protocol achieves the most important security goals scalability, anonymity and anti-cloning for RFID system. A password based protocol has vulnerability on fixed password. This can be exploited by threats. In the proposed protocol, there is a provision to change the password of the Tags. Hence the vulnerability can be reduced in an acceptable level. Computation cost is very less as compare to the other protocols.

Keywords: Authentication, ECDLP, Counterfeiting, Multicast.

1. INTRODUCTION

RFID systems have many continuing and emerging applications like access controls, tool management, supply chains, airline baggage management, livestock or inventory tracking and so on. It can also be used to distinguish between counterfeits and authentic products. The important security and operational problems such as cloning problem, tracing problem and scalability can be solved by RFID system with cheaper RFID tags for commercial applications. Security can be CMOS technologies progressively efficient and the production costs decrease, which allows stronger security solutions on tags. More expensive tags with constraints power source, less memory, gate can be used for certain commercial applications such as access control systems and costly goods for security [1] [2].

2. SECURITY MODEL FOR RFID SYSTEM

This section describes a security model. The system consists of three components: a trusted server S, reader R, and tag T.

- Typically Tags do not have its own power. It operates on electromagnetic field. These are wireless Trans ponders.

- The fields are generated by the transceiver that is the Reader. There exits two kind of broadcast challenges by responding the tags. These are unicast and multi-cast. Under the range of reader, these are addressed to all tags. But unicast challenges are addressed to particular tags.

- Server: The system has a trusted Server communicates with the reader and also reader communicates with the server. We consider that all honest tags T follow the protocol's requirements and system specifications. The parameters fixed are applied to the honest readers R and the trusted server S. Both Tag T and reader R interact by sending and receiving of data as an authentication transcript. We assume that the communication

takes place through secure channel. Since two parties involve in this communication, we can consider it as two party protocols.

3. SECURITY PROPERTIES AND ADVERSARY

This section describes the security properties and the adversary model. The protocol can be modeled in terms of the following four games with players the PPT adversary A against the honest tags T and the readers R. We have followed the Chatmon et.al [3] protocol for this model.

- Gauth : Game for authentication
- Ganon : Game to achieve anonymity
- Gtrace : Game for tracing
- Gavail: Game for availability

The game runs by the following steps.

- Initialization: In this phase the adversary A interacts with the tags and the readers in arbitrary manner.

- The knowledge of A will be examined. AdvG(A) denotes the score of A in game G . The adversary A that has no negligible advantage A to win the game G. Formally we can say

$$Adv_G(A) = \epsilon(k) \leq k^{-\mu} \; \forall \; k > k_{\mu}, \mu > 0$$

3.1 Authentication

The process of authentications is to be performed in two ways. The reader is to be authenticated by the Tag and the tag is authenticated by the reader [4] [5]. Attackers can reveal the secret information by compromising and capturing only one tag [6]. After the reveled of the information, the tags which share the secret information are a threat that can be exploited by the attacker. Attackers may replicate the same to other tags. In the game for authentication Gauth, A must masquerade as some tag T to some reader R. During this masquerade step, A will be allowed to interact arbitrarily with all other tags and readers, except the one tag T that A is trying to masquerade. The advantage of the adversary advA on game Gauth is the probability that A succeeds in authenticating itself to R. An authenticated protocol is said to be secure under Gauth, if there does not exist PPT adversary that has no negligible advantage i.e

$$Adv_{Gauth}(A) = \epsilon(k) \leq k^{-\mu} \; \forall \; k > k_{\mu}, \mu > 0$$

3.2 Untraceability

In this game Gtrace, A traces various tags T. The attacker A is allowed to access to a challenge tag $\check{T}$ and pass the information whether $\check{T}$ is T or not, better than guessing. During the tracing, A is give to interact with all tags and readers, in particular, interacting with T. The advantage advA Gtrace of the adversary in this game is The protocol face untracebility if advA Gtrace is negligible i.e

$$adv^A G_{trace} = \epsilon(k) \leq k^{-\mu} \; \forall \; k > k \mu \, , \mu > 0$$

3.3 Unlinkability

This is a strong notion of anonymity. The advantage of the adversary is denoted by advAGanon. Here there will be two different interactions to the same tag in the linking. In the initial step of the game, the adversary has the knowledge about the tag T from the previous interaction. In Ganon both T and $\check{T}$ are challenge tags. Through interacting with T and $\check{T}$ as well as all other normal tags and readers, A must tell whether it is interacting with identical tags or not i.e whether T and $\check{T}$ have the same key or not.

3.4 Availability

In this game Gavail, the adversary A must thwart a tag T from being authenticated by a reader R in a challenge session ses, without interacting with this session ses. The advantage advAGanon of A in this game is the probability that R rejects T in the challenge session ses.

4. PROPOSED PROTOCOL

The proposed authentication protocol comprises five phases Registration, login, Verification and Mutual Authentication phases. The following phases are described bellow:

- **Registration Phase**
  1. The Tag T with identity IDi chooses a random password pwi and a random number t in Z*n. Computes pwj = H($pw_i \oplus t$).
  2. The tag T sends pw_j as registration request, after receiving the request, server S computes the tag authentication key as $K_{IDi} = q_s \cdot H_1(ID_i)$.
  3. Server S chooses the base point the P on the elliptic curve of order n and computes the public and private key pairs (q_s,Q_s), where $Q_s = q_s \cdot P$.
  4. S computes $\lambda_i = H(_{IDi} \oplus pw_j)$, $\mu_i = H(pw_j \| ID_i) \oplus K_{IDi}$.
  5. S stores the Tag's smart card <λ_i, μ_i>.

- **Login Phase**
  T sends the pairs <ID_i, pw_i> to obtain the S's message transcript and computes pw_j = H($pw_i \oplus t$), $\lambda'_i = H(ID_i \oplus pw_j)$ and check the equality $\lambda_i = \lambda'_i$. When the login phase has been accepted, the Tag T proceeds the following steps with the Reader R.
  1. T obtains its authenticated key K_{IDi} and selects a point $U_i = (x_i, y_i)$
  2. Computes $\theta_1 = H_2(T_1)$,$m_i = U_i + \theta_1 \cdot K_{IDi}$ and $\hat{U}_i = x_i \cdot P$ at time stamp T_i
  3. Sends the message transcript <T_1, ID_i, m_i, $\hat{U}_i$ > to S.

- **Verification Phase**
  After receiving the transcript message <T_1, ID_i, m_i, $\hat{U}_i$ > through the reader R, S performs the following steps to verify the tag:
  1 Computes $Q_{IDi} = H_1(IDi)$, $\theta_1 = H_2(T_1)$ and $U_i' = m_i - q_s\theta_1 Q_{IDi}$.
  2 S verifies whether $\hat{U}_i = x'_i \cdot P$. If holds then the tag is authenticated by the server.
  3 S sends the transcript message <T_2,m_s,m_k> through the reader R, S chooses a point U_s on the elliptic curve and computes $\theta_2 = H_2(T_2)$, $m_s = U_s + \theta_2 qs Q_{IDi}$ mod n. session key $SK = H_3(x_Q, x_i, x_s)$ and $m_k = (k + x_s) \cdot P$.

Finally S sends the message transcript <T_2,m_s,m_k> through the public channel in order to respond the request of R at time stamp T_2.

- **Mutual Authentication Phase**
  This phase performs the following steps:
  1. S sends the transcript <T_2,m_s,m_k> to the reader R, R sends a login request to S.

2. Computes $Q_{IDi} = H_1(ID_i)$, $\theta_2 = H_2(T_2)$, $U_s' = m_s - \theta_2 \cdot K_{IDi}$.
3. R computes $SK' = H_3(xQ \| x_i \| x'_s)$ and $m'_k = (k' + x'_s) \cdot P$.
4. Verify whether $m'_k = m_k$. If holds then S is authenticated by R.

5. PERFORMANCE ANALYSIS

We can evaluate the performance of the proposed protocol in term of its computation cost. Computation time for authentication can be evaluated in two phases, verification and mutual authentication [7] [8] [9]. Consider the following notation to compute computation time.

- T_H : time required to compute hash function.
- T_{add} : time required for addition of points on Elliptic curve.
- T_{PK} : time required to compute private key.
- T_{PU} : time required to compute public key.
- T_{mul} : time for point multiplication.
- Te : Elliptic curve polynomial computation time.

Total computation time is $T = 11T_H + 4T_{add} + 6T_{mul} + 2T_e$

In this research article, I have proposed an authentication protocol with provable security. It is resistant to insider attack, masquerade attack and provides mutual authentication. Security of the protocol relies on ECDLP. The protocol is also susceptible to forgery attacks. Since more expensive tags with constraints power source, less memory, gate can be used for certain commercial applications such as access control systems, the protocol is most suitable for implementation.

6. REFERENCES

[1] E.K. Ryu, and T. Takagi A hybrid approach for privacy-preserving RFID tags,Computer Standards & Interfaces, Vol. 31, 2009, pp. 812-815.

[2] 10. H.yeh, T.Ho Chen, Pin-Chuan Liu, Tai Hoo Kim and Hsin-Wen Wei A Secure Authenticated Protocol for Wireless Sensor Networks Using ECC, Sensor pp 4767-4779, 2011.

[3] C.Chatmon and T.Burmester Secure Anonymous RFID Authentication Protocols, available at www.cs.fsu.edu/ burmeste/TR-060112.pdf

[4] D. N. Duc, and K. Kim Defending RFID authentication protocols against DoS attacks, Computer Communications, 2010.

[5] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, V. Khandelwal Design and implementation of PUF-based unclonable RFID ICs for anti-counterfeiting and security applications, Proceedings of the IEEE International Conference on RFID, April 2008, pp. 58–64.

[6] Wenbo Mao Modern Cryptography - Theory And Practice, 2003, Prentice Hall, pp.196-203.

[7] D. Hankerson, A .Menezes and S.Vanstone. Guide to Elliptic Curve Cryptography, Springer Verlag, 2004

[8] "Certicom ECC Challenge and The Elliptic Curve Cryptosystem" available :http://www.certicom.com/index.php.

[9] Murat Fiskiran A and B Ruby Lee Workload characterization of elliptic curve cryptography and other network security algorithms for constrained environments.

Multi-part Dynamic Key Generation For Secure Data Encryption

Srivatsan Iyer *srivatsan.iyer.1990@gmail.com*
Software Engineer
Webshar LLC
Mulund, 400080, India

Tejas Arackal *tjeidolon@gmail.com*
Software Engineer
TCS TataCapital
Andheri Seepz, 400096, India

Abstract

Storage of user or application-generated user-specific private, confidential data on a third party storage provider comes with its own set of challenges. Although such data is usually encrypted while in transit, securely storing such data at rest presents unique security challenges. The first challenge is the generation of encryption keys to implement the desired threat containment. The second challenge is secure storage and management of these keys. This can be accomplished in several ways. A naive approach can be to trust the boundaries of a secure network and store the keys within these bounds in plain text. A more sophisticated method can be devised to calculate or infer the encryption key without explicitly storing it. This paper focuses on the latter approach. Additionally, the paper also describes the implementation of a system that in addition to exposing a set of REST APIs for secure CRUD operations also provides a means for sharing the data among specific users.

Keywords: Encryption, Dynamic Key Generation, Data At Rest Security, CRUD.

1. INTRODUCTION

Multiple international regulations[1], as well as expectations of users require that any system that stores private user-identifiable data take appropriate steps to ensure its privacy, security and integrity. Over and above these primary goals, are the requirements for the system to have very reliable and readily available storage[2]. Many applications, for reasons of business requirements, including ease of use, system robustness and data recovery choose to store data with third-party storage providers.

In typical cases such as above, the choice is between: a) Trust and allow the storage provider to encrypt the data before writing it out to the disk, or b) proactively encrypt the data prior to sending it over the wire. The prior option is very easy, and straightforward. If the storage provider does not encrypt data appropriately, the security of the data is at risk. The risk is multiplied when all the files are encrypted with the same key. The latter option, however, may be more secure especially since it gives the control of encryption to the application shepherding the data, or to the owner of the data itself.

This paper deals with the second option and tries to explore some of the many possibilities that come with it. As mentioned before, if the encryption is done at the premises, a mechanism is required to store the encryption key for the object being encrypted. If the key is lost, then the encrypted object might never get decrypted. It logically follows that management of the keys needs to be secure as well. In other words, the keys need to get the same treatment with respect to security as the original unencrypted objects. A very simple, unsophisticated approach would be to simply have an encryption key for the entire application, and all the data that it wants to store,

would be encrypted with this key. But this simplicity comes at the cost of security. If this key is compromised, then the entire data set is at risk.

This problem can be solved by assigning an encryption key per user, and storing it in the data store. This scheme is safer as compared to the previous one, because if a key is compromised only the files specific to that user are leaked; the remainder files are safe. Damages/leaks of this kind cannot be prevented fully. As the power of the hardware grows, it only becomes easier for attackers to orchestrate different kinds of attacks. This paper explores a very specific method to contain damages of these kinds.

This paper provides a brief overview of the architecture and framework of a system that can serve as a middleware between the application server and the storage layer. The benefit of such a system is that it can connect to existing data store to authenticate users and gives them access only to authorized resources.

2. LITERATURE SURVEY

The security of the storage in large scale applications has been a constant concern for a long time. Varied security models have been proposed considering the concerns of web business applications. Some common security factors such as encryption, access control, fault tolerance and high availability have been addressed in multi disparate view. While security models with trusted platform module implement a secure hardware location for encryption, authentication and attestation there are also some open source cloud computing applications that have their own implementation of security model.

The TCG trusted platform module (TPM)[3] implementation, using micro controller to store passwords, certificates & encryption keys, ensures security in terms of hardware-based cryptography, and hardware based approach to manage user authentication, network access and data protection. The confidentiality of the data is thus maintained by making it hard for the attacker to access information on computing device. The TPM is also considered a secure vault for storing keys, certificates and passwords. The module, by routinely inspecting the hardware status of the machines, is able to assert that hardware has not been tampered with. In one of the implementations of the specification, the authors of the paper maintain that storing the artifacts within the hardware is better than providing a software based security[4]. This approach will require changes to be implemented in the storage systems hardware in order to support TPM. As such there is a need for an approach that is much more portable and easily deployable than any TPM implementation.

OpenStack, an open source cloud computing software, uses an object storage system Swift[5], comprising of security model for encryption, authorization, access control and key management. The system provides different locations for the encrypted data and the encrypted keys associated with encryption. It maintains a master key for encrypting all other keys thus forming a two level encryption hierarchy. Additionally no implicit mapping is maintained between the data and the keys. The Openstack security model has its data encrypted and stored separately from the key that was used to encrypt it. For high-value data, OpenStack supports “dual-locking” in which every object is encrypted with a combination of “service key” and user-specific key[6]. Although this is secure, it can be improved by rotating keys among various files of the user so that if a key combination is somehow leaked only one file is affected.

OwnCloud, an open source project with similar core functionalities, is a “file-hosting” application that provides a web UI as well as APIs for desktop clients[7]. The system by default uses the server’s file system for storing incoming data, and can be configured to use different storage backend. Similarly, for user management it can be configured to work with many relational database servers. All the files being stored are encrypted with the password of the user. This has several implications. Firstly, since the application needs to encrypt and decrypt the data using clear text password, it should be able to retrieve the clear text password. This implies that the

passwords are not hashed. Secondly, since the user's login password and the data encryption key are identical, losing the password is equivalent to losing all the data. Thirdly, since all these passwords must be stored in the database, it becomes a high-risk component. If somehow the database gets compromised, data of all the users will be jeopardized.

As such there is a need for an approach that is much more portable & easily deployable than TPM implementation at the same time it should not store the direct key used for encryption either in encrypted or decrypted format within the system.

3. PROPOSED SYSTEM

To avoid the shortcomings of present security models, a model with additional improvements needs to implemented. The guidelines for this system are: a) using the same encryption key for multiple files increases the extent of damage if any key is compromised; b) for maximum security, system needs to use different keys for different files c) The key should be constructed by retrieving information from multiple sources. d) The system should let only authorized users access the data. The proposed design caters to all of the above requirements.

The solution that this paper proposes is named "Secure Data Storage Manager" (SDSM). SDSM is an application that operates from within an HTTP Web server placed in a secure network. It uses a User Data Store for storing various attributes of a user and a Metadata store (a NoSQL datastore) for storing metadata of the files stored in the storage layer. Both User Data Store and Metadata Store share the same secure network The two main functions of SDSM is to keep the information consistent between the metadata store and the storage layer, and to employ an appropriate encryption and decryption algorithm to deal with user data.

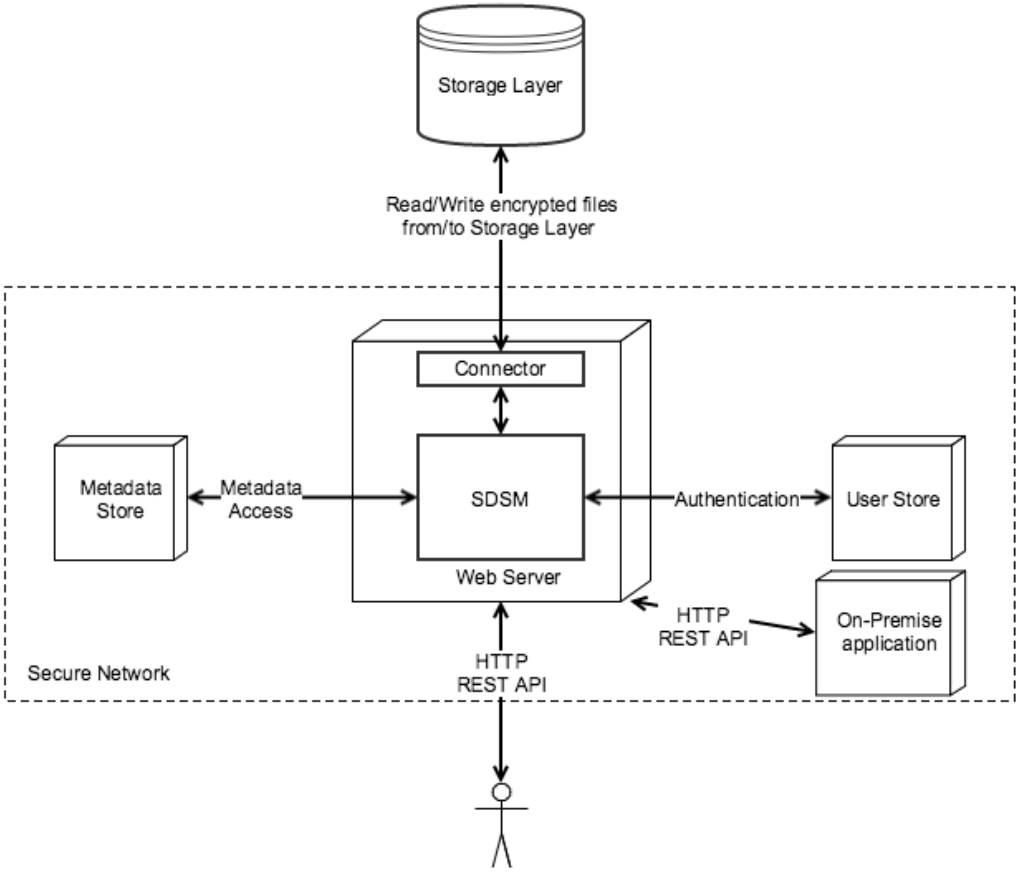

FIGURE 1: Proposed system architecture.

3.1 Metadata Store

The metadata store is essentially a key-value store, in which the keys are full file path on the storage layer. The value stored against each key is a complex structure that contains the following:

1. Timestamp of file creation and timestamp of last modification to the file.
2. Owner information
3. Hash of the file content
4. Access log list

Every file stored in the storage layer has a corresponding entry in the metadata store. The look-up key in this design is the full file path itself.

3.2 Encryption/Decryption

3.2.1 Preliminaries

Let's assume a mathematical function *'f'* to encrypt, and *'g'* to decrypt. Further assuming the cipher text to be represented by 'C' and original message to be represented by 'M', then the usual encryption/decryption process can be mathematically represented as:

$$C \equiv f_x(M),$$

$$M \equiv g_x(C),$$

$$M \equiv g_x(f_x(M)),$$

where, f_x and g_x are the encryption and decryption functions respectively, each initialised with the key 'x'.

Let's denote the metadata store by the letter *'S'*, the file path in consideration by letter 'P', the master key by letter 'K', function to retrieve the metadata structure against a file path by letter *'h'*. Note that metadata value *'V'* is encrypted with the master key. Now,

$$h(S, P) \rightarrow \{ V \text{ if } P \text{ exists, else null } \}.$$

Let there be a function 'j' that reads decrypted metadata structure to retrieve the last update timestamp *'T'* for the file. Assuming 'V' exists, mathematically,

$$j(g_K(V)) \rightarrow T.$$

The encrypted private key of the user who owns the file is represented by *'Q'*.

3.2.2 Encryption

Before encryption we update the metadata store for the access being made, specifically, there is an entry appended the access logs with mode as write. In other words, the function *j(..)*, returns the current timestamp.

To generate the encryption key $'R_1'$ for the file at P_1, we need to take the following steps:

$$h(S, P_1) \rightarrow V_1,$$

$$j(g_K(V_1)) \rightarrow T_1,$$

$$sha\text{-}256(\ string(T_1) + g_K(Q_1)) \rightarrow R,$$

where '+' operator stands for concatenation of strings.

The final ciphertext for the original message M_1 will be generated as:

$$f_{R1} (M_1) \rightarrow C_1.$$

The above encrypted payload will be uploaded to the storage layer

3.2.3 Decryption

To generate the symmetric decryption key *'S_1'* for the file at P_1, we need to take the following steps:

$$h(S, P_1) \rightarrow V_1$$

$$j(g_k(V_1)) \rightarrow T_1$$

$$sha\text{-}256(string(T_1) + g_K(Q_1)) \rightarrow R_1$$

The original message M_1 will be recreated from the ciphertext C_1 (read from the storage layer) as:

$$g_{R1}(C_1) \rightarrow M_1.$$

4. DESIGN

Secure Data Storage Manager System will consist of a web application server, a User Data Store (UDS), a Metadata Store (MS), a Temporary Credential Store (TCS) and a storage layer. The system expects only an interface to each of the sub systems. This allows the modules to be swapped out for a better alternative. Additionally, the application will benefit from not only flexibility, but also reliability because such systems are built purely for a singular purpose.

The SDSM will essentially be a set of REST API endpoints that clients can connect to. The user data, including the private keys of the users are securely stored within the UDS such as LDAP[8] for example. The credentials from the UDS are used for user authentication. Once authenticated, file metadata is retrieved from MS, for retrieving information related to the current request. The core of the SDSM is the set of procedures that operate upon the credentials and information retrieved from User Data store and metadata store respectively, to generate a symmetric key that will be used for encryption and decryption.

4.1 User Datastore Design

Every user account that is linked with our system will have a unique entry in the User Data Store (UDS). Each time a user tries to log into our system, authentication will be performed against UDS. Apart from general user information, every entry contains the hashed password, the secret key, and the user GUID. The password is used for authentication, while the secret key, which is generated when the user is onboarded, is used for encryption. It is assumed that this *secret key* is communicated to the end user via a different channel. The secret key and the hashed password are encrypted with the Master Encryption Key (MEK) of the system.

4.2 Temporary Credential Store Design

When a user authenticates with the system, the system will generate a temporary credential for use by clients in further requests. The schema for it is shown in the image below.

```
KEY = "0D513ACBB4DA4E60A7C37B5C1E6E5B87"
VALUE = "ZDhkMjFiM2VhZmYyNGYzNDk0NzJlNjQ5ZGRlZjkzYjYwYTg3MzBkOCAgLQo="
EXPIRE = 300 seconds
```

FIGURE 2: Temporary Credential Record Structure.

The key represents the user GUID and the value is a randomly generated string encoded in Base64 format when the user is successfully authenticated. The SDSM system can make use of the expiry feature typically provided by most NoSQL databases. The expiration of temporary credential implies that the requesting user will have to re-authenticate upon expiry of five minutes. This design of temporary credential reduces the use of passwords in requests.

4.3 Metadata Record Design

The preferred design to store the metadata entries is a simple key value store instead of a relation database. Every file stored in SDSM has a record in the Key-Value datastore. Multiple metadata attributes are associated with the file such as filename, path of file in the storage layer, creation time, owner information, file sharing information, access logs. The benefit of the key value store is that all the information that relates to a file is stored in a precise structure at one place. SDSM will seldom need to operate across multiple files. Also, the flexible schema allows the access logs as well as sharing information to be contained within the structure itself.

Like the user data store, all the values in the metadata store are encrypted with the MEK of the system. A typical decrypted record looks like below:

```
KEY = "/0D513ACBB4DA4E60A7C37B5C1E6E5B87/path/to/FileName.bin"
VALUE = {
            "timestamp_created" : "1407035466734",
            "timestamp_modified": "1407035497781",
            "hash": "50c29cb0b5cca6ddebd8b07b67407427c3ac0f9d",
            "owner" : "0D513ACBB4DA4E60A7C37B5C1E6E5B87",
            "shared_with": [{
                    "user": "9CEFC8F5447847D68469D8C202DE09FF",
                    "mode": "read,write"
                },{
                    "user": "3289098D55C3486E8A1CA25AF6A97AA3",
                    "mode": "read"
            }],
            "access_logs": [{
                    "user": "3289098D55C3486E8A1CA25AF6A97AA3",
                    "access_type": "create",
                    "timestamp": "1407035466734"
                },{
                    "user": "3289098D55C3486E8A1CA25AF6A97AA3",
                    "access_type": "read",
                    "timestamp": "1407035486734"
                },{
                    "user": "9CEFC8F5447847D68469D8C202DE09FF",
                    "access_type": "write",
                    "timestamp": "1407035497781"
            }]
        }
```

FIGURE 3: File Metadata Record Structure.

4.4 Interaction and Algorithm Design

The SDSM will support 3 categories of HTTPS requests -- a) Request to authenticate and generate a temporary credential, b) Request to perform CRUD operation on the files, c) Request to modify sharing and permission information.

The section below explains a set of algorithms to be followed for authentication and read/write operations. Other operations can be designed similar to the ones described below.

4.4.1 Generate Temporary Credential Request

The client will authenticate using an HTTPS POST request to the SDSM with the following parameters:

1. User GUID
2. Hashed Password

The server side will perform the following operation to authenticate the user and generate temporary credential for the user account.

1. Retrieve the GUID and hashed password from the request.
2. Retrieve values from LDAP. Decrypt the hashed password using MEK and proceed to authenticating the user
3. If request passes authentication, proceed with creation of temporary credential, else throw an error.
4. To generate the temporary credential SDSM will generate a secure random string and encode using Base64 to form temporary credential. This will be returned to the client.
5. SDSM will then create an entry into the Temporary Credential Store with Key as user GUID, temporary credential encrypted with MEK as value. This entry auto-expires after 300 seconds.

4.4.2 Create Secure Item Request

The client will send an HTTPS PUT request to the SDSM with the following parameters:

1. User GUID
2. Temporary credentials
3. File Content(FC)
4. File Path (with filename, relative to user's home directory)

The server side will perform the following operation in response to the request.

1. Retrieve the temporary credential from the requests, and validate it by looking up the user GUID in the Temporary Credential Store. Use MEK to decrypt the value in the Temporary Credential Store.
2. Retrieve the file content from the request.
3. Retrieve the secret key from the LDAP using the GUID. Decrypt it using MEK.
4. Concatenate the file content with the user's secret key and the timestamp provided within the request. Generate a SHA-256 hash.
5. Validate the hash for both the supplied and the server generated hash. If not valid throw an error.
6. CleanPath <- Sanitise-input-path(PathFromHTTPRequest)
7. FilePath <- "/" + <User GUID> + "/" + CleanPath
8. Ensure there is not entry against FilePath. Signal error otherwise.
9. Create a new record within the metadata store, with the following attributes, without committing to the store:
    a) Key <- FilePath
    b) Current user as the owner.
    c) Current timestamp for created and last modified
    d) SHA 256 Hash of the file content
    e) Shared with None
    f) Access Logs <- [{"user": "<current user>","access_type": "create","timestamp": "<time>"}]
10. Encrypt the incoming file
    a) Encryption key <- SHA-256 (<owner's secret key> + <last timestamp of last update/create from access logs>)
    b) Encrypt the incoming file with the above password.

11. Proceed to uploading the encrypted file to the Storage Layer
    a) File Name: Substring after the last slash.
    b) File Path: FilePath (from point 6)
12. Upon success, encrypt the new record using Master key, commit to metadata store and signal success. Else, rollback and signal error.

4.4.3 Read Secure Item Request

The client will send an HTTP GET request to the SDSM with the following parameters:

1. User GUID
2. Owner GUID
3. Temporary credentials
4. File Path (with filename, relative to owner-user's home directory)

In response to the request above, the server will perform the following actions:

1. Retrieve the temporary credential from the requests, and validate it by looking up the user GUID in the Temporary Credential Store. Use MEK to decrypt the value in the Temporary Credential Store.
2. CleanPath <- Sanitise-input-path(PathFromHTTPRequest)
3. FilePath <- "/" + <Owner GUID> + "/" + CleanPath
4. Check if FilePath exists in the metadata store. If not, error.
5. if User GUID != Owner GUID:
    a) Look into "shared_with" key. Read the array, and search for the element with "user" equal to the current user GUID. If none exist, signal item not found.
    b) If an item is found, check if "read" is a substring in "mode". If not, signal item not available for requested action.
6. Append to access_logs: {"user": "<guid>","access_type": "read","timestamp": "<time>"},
7. Fetch Owner's secret key from LDAP. Decrypt it using MEK.
8. Fetch the last update/create timestamp from the access_log
9. Key <- SHA-256(<owner's secret key> + <last timestamp of last update/create from access logs>)
10. From the storage layer, read the file at path = FilePath.
11. Decrypt the file using the Password in step 9.
12. Calculate the hash value of the decrypted file. Check if the hash within the metadata store is equal to the hash so generated. If not signal File externally modified error.
13. Send the decrypted file back to the user as the response to REST API request.

5. DISCUSSION

When storing the data on the third party storage device, confidential data should always be encrypted. As discussed before, encryption comes with the overhead of storing the encryption keys. A system can either be trusted to keep these keys safely, or the keys can be split securely between multiple systems. The SDSM relies on the fact that the chances of both systems getting simultaneously compromised is extremely thin. Even if one of the systems is attacked, the attacker will not be able to retrieve the key to decrypt the user data.

In the event of UDS getting compromised, the attacker will not be able to retrieve the password because they are hashed and encrypted with MEK. This also prevents the possibility of attacker sending the hashed password to obtain the temporary credentials. The private key is similarly encrypted. In the event of a breach in the MS, with every entry in the store encrypted, it is difficult for an attacker to retrieve the actual metadata value. The TCS, too, is encrypted similarly. This prevents the attacker from stealing the temporary credentials and making a request.

If the MEK is compromised it would culminate into a high risk situation. This can be prevented by using a highly secure mode of obtaining the MEK, which is out of the scope of the paper. The main benefit of the proposed system is that in the event of such an exposure, the MEK can be regenerated, and all encrypted values within dependent data stores -- TCS, MS and UDS can be re-encrypted. The data that stays on the storage layer can stay untouched. Finally, there is a possibility of a slightly different kind of attack wherein the encryption key for a file is somehow guessed by an attacker at the storage layer. In this case, the mechanism of the encryption key generation ensures that the key is distinct for every file. In other words, every other file will remain untouched.

Having seen the ability of the system to mitigate threats, it's worthwhile to compare it against the systems presented above. Trusted Computing Group's TPM needs a special hardware to be installed in the server where the data resides reducing the portability of the system. Moreover, if the encryption key is somehow compromised, the entire data on the disk can be decrypted. However, this is not the case in the proposed system as every file is encrypted with a different key.

When compared to OwnCloud's server side encryption mechanism, the encryption methodology provided in this paper is more reliable and resilient. The encryption in SDSM uses hashed passwords, providing an additional layer of security. The passwords in the OwnCloud's implementation provide for both authentication and encryption functionality. Thus the loss or modification of the login password has impact on encryption. Further, if the user store backend is a separate dedicated system like LDAP, then a change in the password without OwnCloud's knowledge will cause the data to be inaccessible until the password is reset to its original value. Moreover, change of password involves additional process in which all the objects stored in the storage layer will be re-encrypted with the new password. The separation of password for authentication and secret key for encryption in the proposed system ensures that the object still remains accessible even in the event of password modification or loss.

Interestingly, OpenStack offers dual locking. In this design, each object is encrypted with a combination of system's service key and user-specific key. This is more secure than a system that encrypts data using a fixed key. In this system, however, all files belonging to a specific user are still encrypted with the same key. SDSM takes this one step ahead and provides for different keys per file. In other words, encryption key of every file in the storage layer is unique.

6. FUTURE SCOPE

The system presented in the paper has a lot of scope for improvement. Some of them are described below.

The problem of concurrent updates is outside of the scope of this paper. The challenge in such concurrency control is that improper design can very easily lead to resource starvation. The system being *stateless* adds to the challenge of implementing it effectively. Since the concurrency-specific information will also be stored in the metadata store, there exists a possibility of stale concurrency specific information if it is being replicated or if the accesses to the store are not transactional and atomic. Designing a replication-aware system that implements efficient concurrency control would be a great improvement.

Currently, the update process overwrites the data at a particular location and leaves no way to retrieve the older version. A more favorable system would perform a *soft-deletion* instead of *hard-deletion*. In other words, data can be *versioned*. Fortunately, the non-relational structure of the metadata lends itself to storing version information. However, there are a few challenges involved with this enhancement — a) no two versions can have the same path on the file system. b) key of the metadata record no longer will be equivalent the actual path on the file system, c) with latest update timestamp being used for generating the decryption key, older versions can be decrypted

since they were encrypted at a different time. Fortunately, a system so designed need not focus on solving the problem of concurrent updates.

7. CONCLUSION

The challenges in securely storing users' confidential data into a datastore have given rise to an approach that would be vendor independent and theft secure. The SDSM system proposed in this paper is based on a set of guidelines for a very secure system, free of implementation dependencies. The elimination of single instance of encryption key by adopting a dynamic approach to determine encryption key, prevents the attacker from getting an access to the encryption key. The algorithm presented in the paper demonstrates the concept of dynamic generation of encryption key, as well as key rotation across files. This combination makes the system extremely secure.

8. REFERENCES

[1] E. McCallister, T. Grance, K. Scarfone. "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)." Internet: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf, Apr. 2010 [Sep 30, 2014].

[2] Taylor, N.E., Ives, Z.G. "Reliable storage and querying for collaborative data sharing systems." in Proc. International Conference on Data Engineering (ICDE), 2010, pp. 40-51.

[3] Trusted Computing Group. "TCG Specification Architecture Overview." Internet: http://www.trustedcomputinggroup.org/files/resource_files/AC652DE1-1D09-3519-ADA026A0C05CFAC2/TCG_1_4_Architecture_Overview.pdf, Aug. 2, 2007 [Aug. 10, 2014].

[4] A. Patel and M. Kumar. (2013, Apr.). "A Proposed Model for Data Security of Cloud Storage Using Trusted Platform Module." International Journal of Advanced Research in Computer Science and Software Engineering. [On-line]. 3(4), pp. 862-866. Available: http://www.ijarcsse.com/docs/papers/Volume_3/4_April2013/V3I4-0430.pdf [Aug. 10, 2014].

[5] OpenStack. "Object Encryption: Extending Swift." Internet: https://wiki.openstack.org/wiki/ObjectEncryption, Jul. 8, 2013 [Aug. 10, 2014].

[6] OpenStack. "KeyManager" Internet: https://wiki.openstack.org/wiki/KeyManager, Apr. 23, 2013 [Sep. 28, 2014].

[7] OwnCloud. "ownCloud Administrators Manual" Internet: http://doc.owncloud.org/server/6.0/admin_manual/configuration/configuration_encryption.html Sep 9, 2014 [Sep . 28, 2014].

[8] T. Howes. (1995, Jul.). "The Lightweight Directory Access Protocol: X.500 Lite." CITI Technical Report. [On-line]. 95(8), pp. 1-9. Available: http://www.openldap.org/pub/umich/ldap.pdf [Aug. 10, 2014].

INSTRUCTIONS TO CONTRIBUTORS

Information Security is an important aspect of protecting the information society from a wide variety of threats. The International Journal of Security (IJS) presents publications and research that builds on computer security and cryptography and also reaches out to other branches of the information sciences. Our aim is to provide research and development results of lasting significance in the theory, design, implementation, analysis, and application of secure computer systems.

IJS provides a platform to computer security experts, practitioners, executives, information security managers, academics, security consultants and graduate students to publish original, innovative and time-critical articles and other information describing research and good practices of important technical work in information security, whether theoretical, applicable, or related to implementation. It is also a platform for the sharing of ideas about the meaning and implications of security and privacy, particularly those with important consequences for the technical community. We welcome contributions towards the precise understanding of security policies through modeling, as well as the design and analysis of mechanisms for enforcing them, and the architectural principles of software and hardware system implementing them.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJS.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with Volume 9, 2015, IJS will appear with more focused issues. Besides normal publications, IJS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

We are open to contributions, proposals for any topic as well as for editors and reviewers. We understand that it is through the effort of volunteers that CSC Journals continues to grow and flourish.

IJS LIST OF TOPICS

The realm of International Journal of Security (IJS) extends, but not limited, to the following:

- Anonymity
- Attacks, security mechanisms, and security service
- Authorisation
- Cellular/wireless/mobile/satellite networks securi
- Public key cryptography and key management
- Cryptography and cryptanalysis
- Data integrity issues
- Database security
- Denial of service attacks and countermeasures
- Design or analysis of security protocols
- Distributed and parallel systems security
- Anonymity and pseudonymity
- Code security, including mobile code security
- Biometrics
- Authentication
- Confidentiality, privacy, integrity, authenticatio
- Data confidentiality issues
- Data recovery
- Denial of service
- Dependability and reliability
- Distributed access control
- Electronic commerce

- Formal security analyses
- Information flow
- Intellectual property protection
- Key management
- Network and Internet security
- Network security performance evaluation
- Peer-to-peer security
- Privacy protection
- Revocation of malicious parties
- Secure location determination
- Secure routing protocols
- Security in ad hoc networks
- Security in communications
- Security in distributed systems
- Security in e-mail
- Security in integrated networks
- Security in internet and WWW
- Security in mobile IP
- Security in peer-to-peer networks
- Security in sensor networks
- Security in wired and wireless integrated networks
- Security in wireless communications
- Security in wireless LANs (IEEE 802.11 WLAN, WiFi,
- Security in wireless PANs (Bluetooth and IEEE 802.
- Security specification techniques
- Tradeoff analysis between performance and security
- Viruses worms and other malicious code
- Fraudulent usage
- Information hiding and watermarking
- Intrusion detection
- Multicast security
- Network forensics
- Non-repudiation
- Prevention of traffic analysis
- Computer forensics
- Risk assessment and management
- Secure PHY/MAC/routing protocols
- Security group communications
- Security in cellular networks (2G, 2.5G, 3G, B3G,
- Security in content-delivery networks
- Security in domain name service
- Security in high-speed networks
- Security in integrated wireless networks
- Security in IP networks
- Security in optical systems and networks
- Security in satellite networks
- Security in VoIP
- Security in Wired Networks
- Security in wireless internet
- Security in wireless MANs (IEEE 802.16 and WiMAX)
- Security policies
- Security standards
- Trust establishment
- WLAN and Bluetooth security

CALL FOR PAPERS

Volume: 9 - **Issue:** 1

i. Submission Deadline : November 30, 2014 **ii. Author Notification:** December 31, 2014

iii. Issue Publication: January 2015

CONTACT INFORMATION

Computer Science Journals Sdn BhD

B-5-8 Plaza Mont Kiara, Mont Kiara

50480, Kuala Lumpur, MALAYSIA

Phone: 006 03 6204 5627

Fax: 006 03 6204 5628

Email: cscpress@cscjournals.org

CSC PUBLISHERS © 2014
COMPUTER SCIENCE JOURNALS SDN BHD
B-5-8 PLAZA MONT KIARA
MONT KIARA
50480, KUALA LUMPUR
MALAYSIA

PHONE: 006 03 6204 5627

FAX: 006 03 6204 5628
EMAIL: cscpress@cscjournals.org