Paper On Storage Privacy Via Black-Box And Sanitizable Signature

First A. Ruchika P Dungarani Student,Department of CE G.M.F.E, Second B. Rakesh Shah Asst. Professor, Department of CE G.M.F.E Himmatnagar(rakesh.shah@growmore.ac.in) , Third C. Ketan Patel Asst. Professor, Department of CE G.M.F.E Himmatnagar (ketan.patel@growmore.ac.in)

Abstract - Storage privacy is basic need for security because today's generation is become digital .Every person use internet for money transaction and other important document transformation. In this paper we use redactable signature and sanitizable signature for security. Sanitizable signature is used to modify the sensitive information of document by sanitizer and this was not known by the original signer.[21] We use black-box for tighten security. We are going to apply this concept in black-box for better security. Sanitizable signature allow third party to do modification in signature.

Index Terms - Storage privacy, Black-box, Sanitizable signature, Eclipse, CDT.

`

I. INTRODUCTION

Storage privacy is basic need for security because today's generation is become digital .Every person use internet for money transaction and other important document transformation. Sanitizable signature is used to modify the sensitive information of document by sanitizer and this was not known by the original signer. Lot of information is shared through internet using different means now a day. From that information some information are sensitive and we cannot compromise with its security. Different techniques and algorithms we use to secure our data. Sanitizable signature is important techniques which help to decide that information provider and provided information both are genuine. Black-box is very important concept for provide better security to storage. We also use sanitizable signature and redactable signature for storage privacy. Redactable signature allow anyone to remove blocks from Document, without invalidating the signature. When we don't want to share particular portion of document we just dark out that portion the same thing was done by using redactable signature. Sanitizable signature is used to modify the sensitive information of document by sanitizer and this was not known by the original signer.

In this paper for storage privacy we are going to use combine algorithm of redactable signature and sanitizable signature.

In this algorithm we have to follow seven different steps like key generation, signature, sanitization, redactation, judge and verify. We have to use seven different algorithms for creating this algorithm. We are applying this algorithm in black-box for tighten security.

II. STORAGE PRIVACY

"Authorized users and trusted networks can only use the available resources unauthorized person cannot use the resources" is the basic concept of storage privacy. We have to protect information against online threats such as Viruses, Worms, Trojans, and other malicious code. Effectiveness of storage security methodology can determine from two criteria[10]

1) Implementing system cost should be a small fraction of value of protected data.[14]
2) It should cost a potential hacker more, in term of money and/or time, to compromise the system than the protected data is worth[14]

fig:2.1 Storage Privacy

III. BLACK-BOX

In black-box We get output of given input without knowing its internal working. Implementation of code in black-box is "opaque".[8] Ex:- human brain

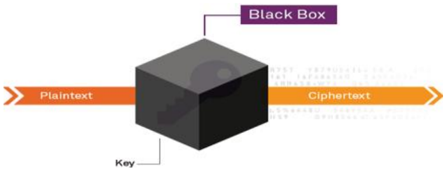


Fig:2.2 BLACK-BOX

IV. SANITIZABLE SIGNATURE

Data sanitization is the process of change or modifies the data. In cryptosystem we use this concept for security purpose. We use sanitizable signature which allow a person to modify the original portion of the data without knowing to the original signer.[7] Who made these changes are known as sanitizer. The sanitizer can produce a valid signature if it modify the designated portion no other parts of message.[7] sanitizer have authority to modify the portion of signature.

Following problem can solve using sanitizable signature: We want a properly signed document by any authorized signer, without harming the original data behind, we need some portion of that signed document hidden or masked to protect some important information. Sanitizing process can be done without original signer to sign again.[7] This concept is very useful in case signer is not available at a moment.[2]

A. Properties of sanitizable signature

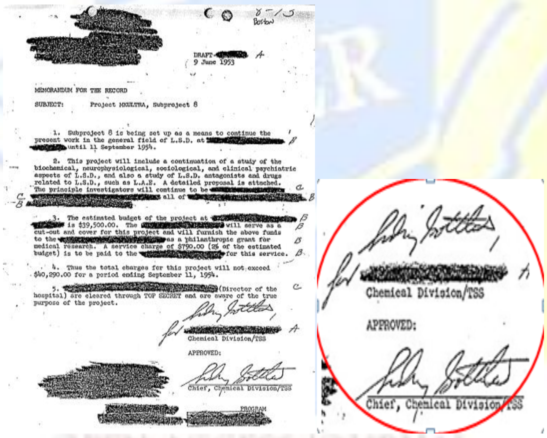
- Unforgeability:- Says that no one except for the honest signer and sanitizer can create valid signature[3]
- Immutability:- sanitizer cannot change message parts which have not marked as modifiable by signer.[3]
- Privacy:- Secure sanitized message parts from outsider to recover that.
- Transparency:- Clear the indistinguishaibility of signature created by sanitizer or signer.[3]

Signing:- The Sign algorithm takes
m = (m[1]; : : : ;m[`])(message) ,the signer's secret key sksig, the sanitizer's public key pksan, as well as a description adm of the admissibly modifiable blocks, where adm contains the number of blocks in m, as well the indices of the modifiable blocks. It outputs the message m and a signature[7]
Sign(m; sksig; pksan; adm)

Sanitizing:- Algorithm Sanit takes a message

B. Algorithm for sanitizable signature

- Accountability:- By this the signer can prove that a particular signature is his not by the sanitizer.



[redacted] Boston

DRAFT [redacted] A
9 June 1953

MEMORANDUM FOR THE RECORD

SUBJECT: Project MKULTRA, Subproject 8

1. Subproject 8 is being set up as a means to continue the present work in the general field of L.S.D. at [redacted] until 11 September 1954. B

2. This project will include a continuation of a study of the biochemical, neurophysiological, sociological, and clinical psychiatric aspects of L.S.D., and also a study of L.S.D. antagonists and drugs related to L.S.D., such as L.A.E. A detailed proposal is attached. The principle investigators will continue to be [redacted] all of [redacted] a C B B

3. The estimated budget of the project at [redacted] is $39,500.00. The [redacted] will serve as a cut-out and cover for this project and will furnish the above funds to the [redacted] as a philanthropic grant for medical research. A service charge of $790.00 (2% of the estimated budget) is to be paid to the [redacted] for this service. B B B B

4. Thus the total charges for this project will not exceed $40,290.00 for a period ending September 11, 1954.

5. [redacted] (Director of the hospital) are cleared through TOP SECRET and are aware of the true purpose of the project. C

Sidney Gottlieb
for [redacted] A
Chemical Division/TSS

APPROVED:

[redacted]

Sidney Gottlieb
Chief, Chemical Division/TSS

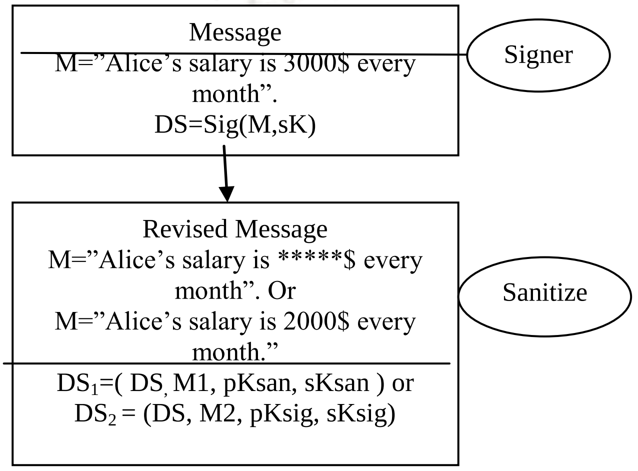
[redacted] PROGRAM [redacted]

Sidney Gottlieb
for [redacted] A
Chemical Division/TSS

APPROVED:

Sidney Gottlieb
Chief, Chemical Division/TSS

- Easy to install
- Easy to use
- A new release every year



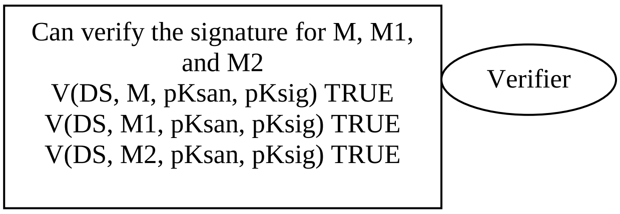
Message
M=”Alice’s salary is 3000$ every month”.
DS=Sig(M,sK)

Signer

Revised Message
M=”Alice’s salary is *****$ every month”. Or
M=”Alice’s salary is 2000$ every month.”

DS_1=(DS, M1, pKsan, sKsan) or
DS_2 = (DS, M2, pKsig, sKsig)

Sanitize


Can verify the signature for M, M1, and M2
V(DS, M, pKsan, pKsig) TRUE
V(DS, M1, pKsan, pKsig) TRUE
V(DS, M2, pKsan, pKsig) TRUE
Verifier

The functions of genetic operators are as follows:-

Key Generation:- There are two key generation algorithms are used, two pair of keys are generated one for signer and second for sanitizer.[7]

D. CDT(C/C++ Developing Tooling):

The CDT Project provides a fully functional C and C++ Integrated. Development Environment based on the Eclipse platform[27].

m = (m[1]; : : : ;m[`]), m[i] , the public key pksig of the signer and the secret key sksan of the sanitizer. It
modifies the message m according to the modification instruction mod, which contains pairs (i;m[i]0) for those blocks that shall be modified. Sanit calculates a new signature _0 for the modified message m0 mod(m). Then Sanit outputs m0 [7]
Sanit(m;mod; _; pksig; sksan)

Verification:- The Verify algorithm outputs a decision verifying the validity of a signature
for a message m = (m[1]; : : : ;m[`]),m[i] with respect to the public keys.[7]

E. Introduction To Eclipse:

- Eclipse is a universal platform for integrating development tools. Multi-language software development environment comprising an

  integrated development environment and an extensible plug-in system.[23] Eclipse was Started by IBM (Canada) in late 1990s.[27] A small Java program with loader functionality. Eclipse Can be infinitely extensible by 3rd parties products are created in the form of plug-in which are then loaded by Eclipse[27]

F. Goal:

- Development tools platform
- Common platform for all IBM development products[23]
- Integrated experiences for the customers Formed and created Eclipse Foundation (non profit org.) in 2003-2004[27]

➢ Latest Version:

- Neon 22 June 2016 4.6

➢ Next Version:

- Oxygen June 2017 4.7

G. Layer of eclipse:

- PDE: Plug-in Development Environment
- JDT: Java Development Tool

Platform: Eclipse Platform
JVM: Java Virtual Machine

➢ Features:

Check: http://wiki.eclipse.org/CDT/User/NewIn82
Signatures and a Black-Box Construction of Strongly Private Schemes” David Derler and Daniel Slamanig[27]

Editor: C/C++ syntax highlighting
Code completion (Camel Case Completion)
Hover help Automatic indentation[23]
Parser: Parses source files in project to extract C/C++ elements Information used to search, outline and code completion[27]
Search
API and extension points to allow extensibility
C++ Development:
Class creation wizards

ECLIPSE
We are using eclipse platform to implement proposed algorithm.

C. Purpose for Using Eclipse:

- Open source and FREE!
- One IDE for almost all languages!
- Supported on most operating system
- OS independent GUI

➢ Latest Version:

- Neon 28 Sept 2016 9.1.0

➢ Next Version:

- Neon Dec 2016 9.2.0

VI. CONCLUSION

We get better privacy using Black-Box in Sanitizable signature. We believe that our algorithms can be further tuned in order to achieve an even larger performance increase. Sanitizable signatures permit a designated party to remove or replace designated parts of a document. Any unauthorized person cannot access the data without permission. Create the black box from where they can access the system of company.

VI. FUTUREWORK

Future work will be implementation of proposed
algorithm using Eclipse. Once it will be implemented, testing will be done and result will be compared with current results for conclusion.

REFERENCES

[1] “Blackbox: Distributed Peer-to-Peer File Storage and Backup” Payut Pantawongdecha,Isabella Tromba,Chelsea Voss,Gary Wang May 14, 2014

[2] “Rethinking Privacy for Extended Sanitizable
Xu, Anjia Yang, Jianying Zhou, and Duncan S. Wong [3] “A General Framework for Redactable Signatures and New Constructions” David Derler1z, Henrich C. P,ohls2;z;x, Kai Samelin3k, Daniel Slamanig1z

[4] “Efficient and Perfectly Unlinkable Sanitizable Signatures without Group Signatures” Christina Brzuska, Henrich ohls, Kai Samelin

[5] “Active Learning of Nondeterministic Finite State Machines” Warawoot Pacharoen, Toshiaki Aoki, Pattarasinee Bhattarakosol,and Athasit Surarerks

[6] “An Analysis of Black-Box Web Application Security Scanners against Stored SQL Injection” Nidal Khoury, Pavol Zavarsky, Dale Lindskog, Ron Ruhl

[7] “Sanitizable Signatures”Giuseppe Ateniese, Daniel H. Chou, Breno de Medeiros,and Gene Tsudik

[8] “Black Box Backup System”Iyad Aldasouqi & Arafat Awajan International Daniel Slamanig International Conference, CANS 2016, Milan, Italy, November 14-16, 2016. Proceedings, Sara Foresti and Giuseppe Persiano Eds., Springer Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (3) : 2011 368

[9] “A General Framework for Redactable Signatures and New Constructions”David Derler z, Henrich ohls, Kai Samelin, Daniel Slamanig

[10] “ Research Design: Qualitative, Quantitative and Mixed Methods Approaches” ,J. W. Cresswell, 2nd. Ed. California: Sage Publications, Inc. 2002.

[11]“Secure Privacy Preserving Public Auditing for Cloud storage” International Journal of Innovative Research in Science, Engineering
Springer-Verlag 1998.

[12] “Using Invariant Detection Mechanism in Black Box Inference” Muzammil Shahbaz and Roland Groz

[13] “Cyber security, Innovation And The Internet Economy”The Department Of Commerce Internet Policy Task Force

[14] “Lightweight Delegatable Proofs of Storage” Jia
Fortran” Carla Guillen, Leibniz Supercomputing Centre 19th March 2015.

[15] “Information security and privacy in healthcare:current state of research” Ajit Appari and M. Eric Johnson *Int. J. Internet and Enterprise Management, Vol. 6, No. 4, 2010*

[16]“The Structure of a Programming Language Revolution”Richard P. Gabriel

IBM,2010

[17]“Design and Compilation of an Object-Oriented Microprogramming Language for Wireless Sensor Networks” Felix Jonathan Oppermann, Kay R omer, Luca Mottolayz, Gian Pietro Picco, Andrea Gaglione 978-1-4799-3784-4/14/$31.00

©2014 IEEE

[18]“Signer-Anonymous Designated-Verifier Redactable Signatures for Cloud-Based Data Sharing”David Derler, Stephan Krenn

[19] “A Cipher Design with Automatic Key Generation using the Combination of Substitution and Transposition Techniques and Basic Arithmetic and Logic Operations” Govind Prasad Arya,Aayushi Nautiyal, Ashish Pant, Shiv Singh & Tishi Handa The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 1, No. 1, March-April 2013

[20] “Recommendation for Cryptographic Key Generation” Allen Roginsky, Elaine

Barker NIST Special Publication 800-133 December 2012

[21] “Digital Steganography: A Symmetric Key Algorithm” Joshua C. Clark and Technology Sathiskumar R1, Dr.Jeberson Retnaraj

[22] “On the Determinization of Weighted Finite Automata” Adam L. Buchsbaum, Raffaele Giancarlo, and Jeffery R. Westbrook To appear in Proc. 25th ICALP, Aalborg, Denmark, 1998.[23] “Eclipse: C/C++ Programming and Fortran” Carla Guillen, Leibniz Supercomputing Centre 19th March 2015

[24] “BlackBox”,2014,Wikipedia,15July2016, <https://en.wikipedia.org/wiki/Black_box >

[25]“Angluin’sLearningAlgorithmforDFA’s”,2012,sun.ac.za,viewed,2Aug2016<http://www.cs.sun.ac.za/rw711/2012term2/lectures12/112.pdf>

[26]“8 Best Cloud Storage Providers For Corporate Privacy”, May 5, 2014, Hongkiat

,viewed20 Aug 2016 http://www.hongkiat.com /blog/8-best-cloud-storage-providers-for-corporate - data-privacy/

[27]“Eclipse”,2016,eclipse,viewed 9 October 2016 < https://eclipse.org/>[28]“Cryptography”, Wikipedia, viewed 22 July 2016 https://en.wikipedia.org/ wiki/ Key_(cryptography)

[29] Computer Security – ESORICS 2005: 10th European Symposium on Research in Computer Security,Milan,Italy,September 12-14, 2005, Proceeding

[30] “Redactable vs. Sanitizable Signatures” Kai Samelin, Henrich C., P ohls, Joachim Posegga, Hermann de Meer , Nov 2012