International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-3, February 2014

Data Reliance Surveillance

Tushar Bedke, Dhanashree Kutre

Abstract*— Network Security and Data protection is a very important approach in which the users should be encouraged to turn on the module in order to practically make use of trusted computing against well known data security problems. The best way to deal with such problems is to use this technology that has been found to provide very real benefits in terms of assuring trust between systems and effectively protecting, through hardware based encryption, critical information .Moreover the results should necessary satisfy the requirements of the users in respect of access rights, privacy and interoperability. This paper outlines a client-server system utilizing a Data Reliance Surveillance Module (DRS)-enabled computer to hinder forensic examination. We have explored in detail the entire process from the encryption to the reverse process decryption on different file formats mainly image, audio and text files. We describe and implement an approach on data protection and network security by utilizing trusted computing technology. The system allows for data confidentiality, plausible deniability, and hiding of traces that incriminating data was present on the client.

I. INTRODUCTION

Electronic records such as word processing files, image and audio files increasingly provide essential and important evidence in solving criminal cases. As a result, electronic evidence processing had been established to ensure that evidences seized from electronic sources adhere to the standards of evidence that are admissible in courts of law. In order to obtain these records, law enforcement agents resort to forensic examination of seized electronic sources. While thus far forensics have proven useful in extracting incriminating data, it is possible to develop a system that hinders this effort. The outlines the concept of trusted computing, which essentially ensures that a system will consistently behave in specific, prearranged ways verifiable by a remote machine using a combination of hardware and software support. Basically is a secure crypto-processor that can generate and store secured information such as keys and passwords. It typically access the motherboard number of a computer(Client), and use this as a key for encryption. The client's state can always be established by proper authentication, and the data cannot be tampered by fake attestation by using some out of bound device (Memory Card or Pen Drive). At the Server side, the data is decrypted, only by using particular client's motherboard number. The above operation (Encryption and Decryption) is performed using Rijndael Algorithm.

Manuscript published on 28 February 2014.
* Correspondence Author (s)
Tushar Bedke, Electronics and Communication Department, Visvesvaraya Technological University/ Maratha Mandal Engineering College/ Organization-Maratha Mandal Engineering College, Belgaum, India.
Dhanashree Kutre, Electronics and Communication Department, Visvesvaraya Technological University/ Maratha Mandal Engineering College/ Organization-Maratha Mandal Engineering College, Belgaum, India.

The Design of secure distributed systems, when considering exchange of information between systems, must identify the endpoints of communication.
The composition and makeup of the endpoint is as important to the overall security of the system as is the communications protocol. The design endpoints are minimally comprised of symmetric key (i.e., the motherboard number), key storage and processing that protects protocol data items. Classic message exchange based on symmetric cryptography suggests that messages intended for one and only one individual system in loss of security. Thus aids in improving security by providing both key management and configuration management features (e.g. Protected Storage, Message exchange, Binding, Signing and Reporting).

II. MOTIVATION AND CHALLENGES

Network security is generally taken as providing protection at the boundaries of an organization by keeping out intruders. Network security starts from authenticating the user, commonly with a username and a password. Since this requires just one thing besides the user name, i.e., the password. The networks are comprised of "nodes", which are "client" terminals (individual user PCs), and one or more "servers" and/or "host" computers. They are linked by communication systems, some of which might be private, such as within a company, and others which might be open to public access. The obvious example of a network system that is open to public access is the Internet, but many private networks also utilize publicly-accessible communications. Today, most companies host computers can be accessed by their employees whether in their offices over a private communications network, or from their homes or hotel rooms while on the road through normal telephone lines. Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

III. SYSTEM OBJECTIVES

As security is necessarily the primary goal of most computer applications, there are various strategies and techniques used to design security systems. The following are the anti-forensics objectives of the system:
Confidentiality: The system must protect the confidentiality of incriminating data, and only reveal it when the system is in a trusted state.
Information / Action hiding: The system should provide no concrete evidence that any incriminating data has been manipulated.
Plausible deniability: The system should provide capabilities to plausibly deny existence of incriminating data.

A. *Confidentiality*

Security experts argue that it is impossible to prove the identity of a computer user with absolute certainty. It is only possible to apply one or more tests which, if passed, have been previously declared to be sufficient to proceed. The problem is to determine which tests are sufficient, and many such are inadequate. Any given test can be spoofed one way or another, with varying degrees of difficulty. Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. Breaches of confidentiality take many forms. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information. Thus, Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds. If your authentication request is approved, you become authorized to access the accounts of that account holder, but no others. Authorization, on the other hand, involves verifying that an authenticated subject has permission to perform certain operations or access specific resources. Authentication, therefore, must precede authorization. Confidentiality have been achieved by using a OOB device. The OOB device acts as an authentication of a user for the particular client machine. OOB device authenticates the user by the correct password and allows to read and write the data.

B. *Information/Action hiding*

Cryptography is the study of means of converting information from its normal comprehensible form into incomprehensible format, rendering it unreadable without secret knowledge. Thus, Cryptography is used to hide information and ensure secrecy in important communications, for those used by spies and also for other uses such as phone, fax and e-mail communication, bank transactions, bank account security, pins and passwords. It is also used for electronic signatures which are used to prove who sent a message. Information hiding means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of data. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer. Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information. Information hiding is achieved by using Encryption techniques such as Rijndael algorithm and maintaining security of system is achieved by proper authentication (using a OOB device).

C. *Plausible Deniability*

Plausible deniability refers to lack of evidence proving an allegation. If your opponent lacks incontrovertible proof (evidence) of their allegation, you can "plausibly deny" the allegation even though it may be true. However, the public might well disbelieve the denial, particularly if there is strong circumstantial evidence, or if the action is believed to be so unlikely that the only possible explanation is that the denial is false. In computer networks, deniability often refers to a situation where a person can deny transmitting a file, even when it is proven to come from his computer. Normally, this is done by setting the computer to relay certain types of broadcasts automatically, in such a way that the original transmitter of a file is indistinguishable from those who are merely relaying it. In this way, the person who first transmitted the file can claim that his computer had merely relayed it from elsewhere, and this claim cannot be dis-proven without a complete decrypted log of all network connections to and from that person's computer. Plausibility Deniability is achieved by proper Socket Programming of the Client and Server.

IV. IMPLEMENTATION DETAILS

A. *Architecture Overview of DRSM*

A Data Reliance Surveillance (), is a secure crypto-processor that can generate, store and share secure information between the two entities (Client and Server). The complete system consists of a Client, Server, and Out-of-Bound (OOB) device, as shown in Fig 1. The client is where all data manipulation takes place, while the server is used to store data after manipulation. The core of the system is a -enabled client. To be in a trusted state, the OOB device must be detected by the client and builds a chain of trust of every individual code executed on the system. The Out-Of-Bound device serves as authentication function for the particular user and Client Machine. As a consequence, the client's state can be established at any time by using OOB device and detection of mother board number. The server on the other hand authenticate and attest the client based on the stored motherboard number of the client. The server terminates immediately the transaction if authentication fails (e.g., incorrect mother board number of client). The above operation of sharing the information between two entities (Client and Server) is performed by using a Local Area Network (LAN).

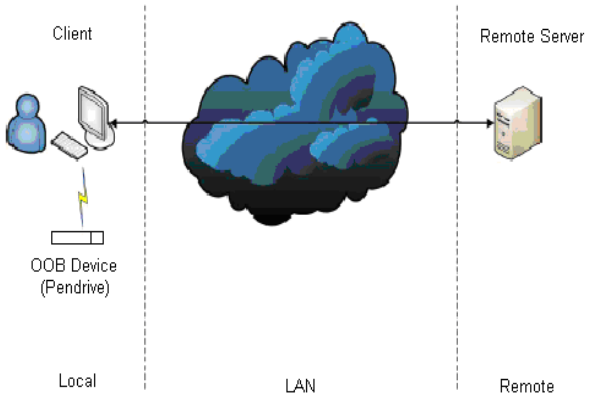

Fig 1: Architecture of Data Reliance Security Module

B. *Flow Process*

The flow process of working starts from authentication and attestation till the end of data transmission and reception. With reference to Fig 2 the exact idea can be drawn on how the flow takes place from Client and Server side.

A complete client-server transaction is divided into 2 sections, namely

- Authentication and Attestation
- Data transfer

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Attestation and authentication ensures the correct client is communicating with the server (authentication) and that the client configuration is in a known trusted state (attestation).

C. Authentication and Attestation

Authentication means maintaining the integrity of the individual systems. The way in which someone may be authenticated can be based on The Knowledge factor – Something the user knows such as password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question). However, authentication is the process of verifying a claim made by a subject that it should be allowed to act on behalf of a given principal (person, computer, process, etc.).

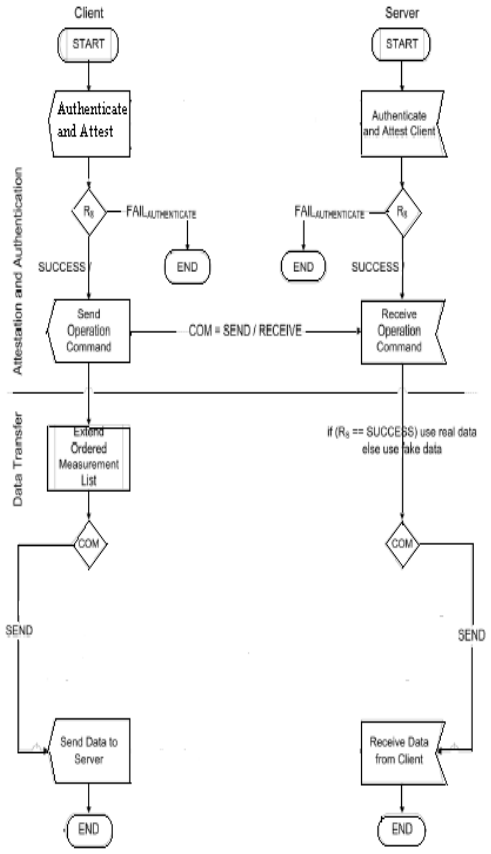

Fig 2: Flow Diagram of Data Reliance Security Module.

One familiar use of authentication is access control. A computer system that is supposed to be used only by those authorized, must attempt to detect and exclude the unauthorized. Access to it is therefore usually controlled by insisting on an authentication procedure to establish with some degree of confidence the identity of the user, granting privileges established for that identity. Attestation, on the other hand, involves verifying that an authenticated subject has permission to perform certain operations or access specific resources.

In this paper, we have achieved authentication by using a Out-Of-Bound device (Pen drive). The user must insert pen drive in client machine. Inside the Pen drive, the user must enter the correct password in the notepad file. Whenever the user wants to access the module for encryption of data, the login section checks whether the password entered in Pen drive matches with that password, stored in its database. If it matches then authentication for the particular user is successful to get the motherboard number of the client. This motherboard number acts as key for attestation of data. This key is used for encryption of data using the Rijndael algorithm The accessed motherboard number of Client is stored in Server which grants access of data after decryption from particular client machine.

D. Data Transfer

After Successful authentication the next step is Data Transfer between the Client and Server. The Encrypted data from Client is transmitted to the Server on a Local Area Network (LAN) using a LAN cable. Since main goal is to achieve high level Network Security, a proper network is to be constructed between the intended Client-Server pair. This can be achieved by Socket Programming. Data Transfer should be protective and integrity between the Client and Server is achieved on a Local Area Network.

V. SECURITY ANALYSIS

A. Encryption

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (referred to as cipher text). Encryption is used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems. Encrypting data in transit also helps to secure it as it is often difficult to physically secure all access to networks. Thus, Encryption, by itself, can protect the confidentiality of messages.

In this paper, Encryption of Data is achieved by using Rijndael algorithm. In Rijndael Algorithm, we have taken the mother board number of Client as a key for Encrypting the data. The same key (i.e., the client's motherboard number) is stored in Server's database which is used for Decryption on Server Side. By implementing Rijndael, we have successfully encrypted different forms of data such as text files, image files and audio files.

B. Decryption

Decryption is the opposite of Encryption. It is the process of converting a Cipher text to the Plain text. Decryption helps us to regain the original form of message by using an algorithm (called cipher). Decryption is an very important process and performed using the correct key shared between the two entities. As the data has to be successfully recovered to its original form, confidentiality has to be achieved between the two entities.

In this paper, Decryption of Data is achieved by performing reverse steps as that used in Encryption using the Rijndael Algorithm. While performing decryption, we should take care that key stored in database of Server matches with that key sent by the Client.

VI. ANTI – FORENSIC

Criminal law deals with offenses against the state - the prosecution of a person accused of breaking a law. Such offenses may of course include crimes against a person. A government body, or the representative of a government body accuses the person of having committed the offense, and the resources of the state are brought to bear against the accused. Guilty outcomes can result in fines, probation, incarceration, or even death.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

When a crime is reported the certain evidence of proof such as photograph images, audio recording of the victim, written statement of acceptance of crime has to be gathered to produce in the court of law. The evidence of proof of crime is termed as Forensic data and used by the Police authorities to produce in court of law. After taking these all steps, some physical violation of evidence may carry while transferring the proofs (evidence) to the court of law. Someone might stole the hard copies of evidence gathered or misguide with the evidence or even purposely create accidents to destroy the evidence of reported crime while carrying the data. So the Forensic data gathered by the police may be in danger and should be protectively and safely carried till the final destination.

To achieve this, we have designed a system known as Data Reliance Surveillance where the Police authorities acts as a Client and the Court authorities acts as a Server. The Crime evidence such as photograph images, written statements of criminals, audio recording of criminal of accepting crime can be made and established on a computer system (Client). Then these all data gathered can be encrypted and transmitted over the network to the intended recipient. Hence the physical crime of evidence violation is eliminated, the system is termed as Anti-Forensic System. Thus the main functions of Anti-Forensic Systems are:

- Virtual conflict management-Prevent disallowed actions
- Physical world differs- Punishment deters crimes.
- Framework must be agreed upon Commutativity of operations and
- Establishing chain of custody.

VII. BENEFITS OF DRS

The following are the huge benefits of using DRS module in different kinds of applications in the day to day world. For a instance, we have taken a Anti-Forensic system.

Multi-factor authentication: The DRS becomes one factor in allowing or denying access, so it can be combined with biometrics and digital certificates for stronger authentication.

Strong login authentication: Even when used for single-factor authentication the DRS can be stronger than traditional password solutions.

Machine binding: Ensure all data saved to external media is encrypted by a key managed by the DRS.

Digital signatures: A trusted audit trail can be created using the DRS to produce tamper-resistant digital signatures for documents, for proof and auditable chain of trust.

Password vaults: People should use stronger passwords, so the DRS provides a convenient store for such information. Even if your computer is stolen, passwords are securely locked away, and in addition, the DRS provides an easy way to backup this information and restore it to a replacement machine.

Network access control: DRS-equipped computer attest the DRS's identity and the health of the host system before granting access to network resource, and even quarantining the computer in real time if it gets infected.

Endpoint integrity: Trusted client/server security: The clients can now ensure the servers are trusted, forging a true two-way trusted relationship.

VIII. IMPLEMENTATION OF RIJNDAEL ALGORITHM

Rijndael was developed by Belgian cryptographers Joan Daemen of Proton World International and Vincent Rijmen of Kathlieke Universities Leuven. Rijndael is an iterated block cipher as implemented in Fig 3. Therefore, the encryption or decryption of a block of data is accomplished by the iteration (a round) of a specific transformation (a round function).It's a block cipher which works iteratively with a

- Block size: 128 bit (but also 192 or 256 bit)
- Key length: 128, 192, or 256 bit
- Number of rounds: 9, 11 or 13
- Key scheduling: 44, 52 or 60 sub keys having length = 32 bi

The following are the steps involved in Rijndael Algorithm

- Processes data as 4groups of 4bytes –128-bit block
- Input block copied into State array, modified at each stage of encryption or decryption and copied to the output matrix after the final round.
- Has 9/11/13 rounds (depending on which variant is used) in which State undergoes:
- byte substitution (one S-box used on every byte)
- shift rows: a simple permutation
- mix columns: substitution using arithmetic in GF(28)
- add round key (XOR State with the round key)Initial XOR of the plaintext with a round key

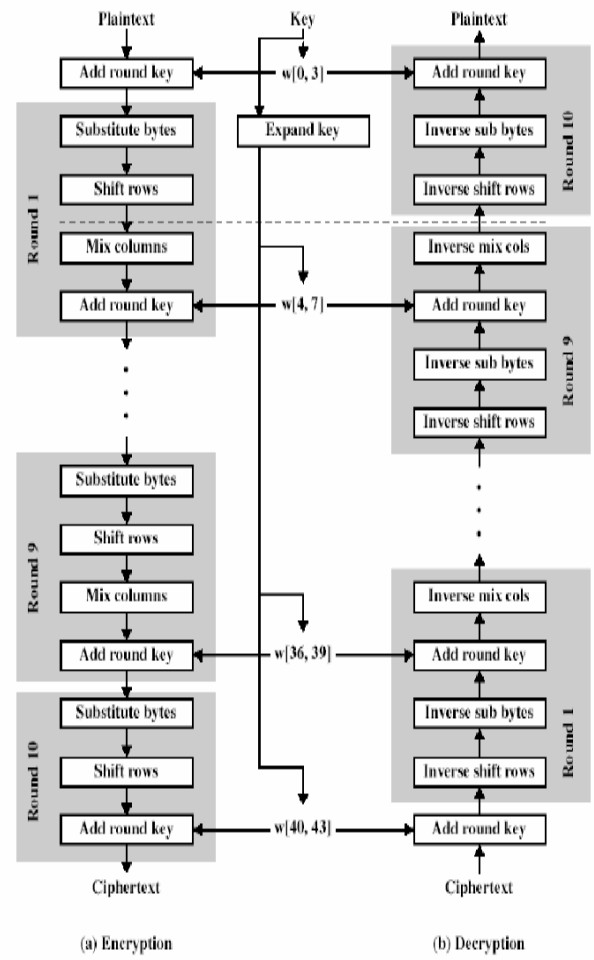

Fig 3. : Flow Diagram of Rijndael Algorithm

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

REFERENCES

[[1] National Aeronautics and Space Administration, "One Policy Approach Regarding Digital Evidence Acquisition and Analysis," *National Aeronautics and Space Administration*, August, 2007.
[2] J. Morris, "Maintaining System Integrity During Forensics," *Security Focus*, August 1, 2003.
[3] Trusted Computing Group, "TCG Specification Architecture Overview Revision 1.4," *Trusted Computing Group*, August 2, 2007.
[4] Trusted Computing Group, "Trusted Platform Module () Summary", *Trusted Computing Group*, May 5, 2008.
[5] P.C. Leong, "Some impacts of trusted computing on digital forensic," in Cyber Crime Investigation Workshop 2006, Singapore, November, 2006.
[6] Trusted Computing Group, "TCG Glossary of Technical Terms", *Trusted Computing Group*.
[7] R. Sailer, X. Zhang, T. Jaeger and L. van Doorn, "Design and Implementation of a TCG-based Integrity Measurement Architecture, "in 13th Usenix Security Symposium, San Diego, California, August,2004.
[8] B. Parno, "The Trusted Platform Module () and Sealed Storage,"*RSA*, June 21, 2007.
[9] R. Sailer, "Integrity Measurement Architecture (IMA)," *IBM Research*.
[10] J.A. Halderman et al, "Lest We Remember: Cold Boot Attacks on Encryption Keys" in 17th USENIX Security Symposium (Sec '08), San Jose, California, July 2008.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)