Communication and Network, 2010, 2, 69-72
doi:10.4236/cn.2010.21011 Published Online February 2010 (http://www.scirp.org/journal/cn)

Proposed Model for SIP Security Enhancement

Munir B. Sayyad[1], Abhik Chatterjee[2], S. L. Nalbalwar[3]
[1]*Technology Innovation Center Reliance Communication, Maharashtra, India*
[2]*Electronics Engineering of Lokmanya Tilak College of Engineering, Mumbai University Maharashtra, India*
[3]*Department of Electronics and Telecommunication, Dr. Babasaheb Ambedkar Technological University, Maharashtra, India*
E-mail: *powerabhik@yahoo.com.in, nalbalwar_sanjayan@yahoo.com*
Received October 24, 2009; *accepted November* 12, 2009

Abstract: This paper aims to examine the various methods of protecting and securing a SIP architecture and also propose a new model to enhance SIP security in certain selected, specific and confidential environments as this proposed method cannot be generalized. Several security measures and techniques have already been experimented with, proposed and implemented by several authors as SIP security is an issue of utmost importance in today's world. This paper however, aims to summarize some of the better known techniques and propose a unique method of its own. It also aims to mathematically represent SIP fitness values graphically as well via a simulation using the popular Fuzz Data Generation Algorithm. Thus this paper not only aims to contribute to the already vast field of SIP security in an effective manner but also aims to acknowledge and represent some of the fail proof methods and encryption techniques that have helped in making SIP a more secure and less wobbly network for all of us to function in.

Keywords: SIP, SoS, VoIP

1. Introduction

Session Initiation Protocol (SIP) is the Internet Engineering Task Force (IETF) standard for IP Telephony which is making huge inroads into the Voice-Over-IP (VoIP) market, previously domineered by implementations which stuck to the rather difficult H.323 ITU-T Internet Telephony standard [4]. The apparent reality is that Voice and Data services are being quickly shifted from the legacy network to the IPbased network.

The standardization of SIP helped to realize the call control function. SIP is the present as well the future of commercial communication systems. SIP is the present as well the future of commercial communication systems.

Many carriers and providers are extensively adopting it; therefore SIP security has become a topic of high importance and priority [5]. With VoIP, voice can now be transported on a traditional IP data network, making use of the vast resources of the Internet and thus drastically lowering the cost of operation.

However in the recent past, VoIP services have been plagued and hampered by numerous security threats and issues. With Internet being the primary carrier, VoIP networks are exposed to threats and dangers that an IP data network faces e.g., IP spoofing, denial of service (DoS) etc. [5].

SIP has become the effective standard for VoIP services. It is described as "an application layer control protocol that can establish, modify and terminate multimedia sessions (conferences) such as Internet telephony calls". It is an ASCII/text based request-response based protocol that works on a client server mode.

2. Security in Sip

SIP security is an issue of prime importance. Basically we can broadly classify the attacks on any type of system into two categories [2]:

- **Passive Attacks**: This threatens the confidentiality of the data/signal being transmitted.
- **Active Attacks**: This threatens the integrity or availability of the data/signal being transmitted.

The feasibility of a passive network primarily depends on the physical transmission media in use and its physical accessibility for any intruder. Fortunately enough, the use of switching technologies makes it harder and more difficult for an attacker to passively attack a signal segment. Now in an active attack, more often than not, the intruder manipulates the domain name system (DNS) to place himself between the sender and recipient of a message. In this situation, the intruder acts as a man-in-the-middle. A very common form of attack is to spoof signals/messages on another (or nonexistent) user's behalf.

These two types of attacks can most probably encompass all the different types of attacks and forced attempts within their broadly diversified branches. The following diagram will give a clearer picture of a SIP security

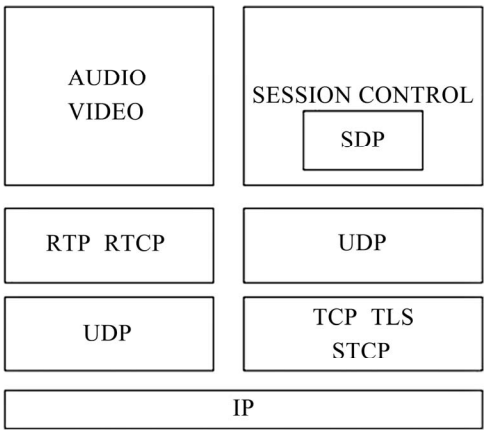

Figure 1. Protocol architecture

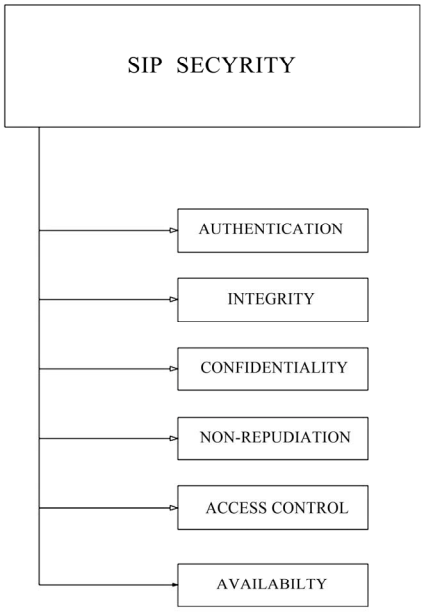

Figure 2. SIP security breakup

breakup.

Authentication and maintaining the integrity of data/ signaling is a matter of the highest priority. It is also important to monitor the access control and the availability of information because it will prevent malformation and spoofing of data.

We will now define a structure which will include all the important points mentioned above which are of primary importance. Authentication, integrity, confidentiality, non-repudiation, access control and availability form a framework upon which the others will be derived.

Authentication is the property by which the correct identity of an entity, such as a user or a terminal, or the originality of a message that has been transmitted, is established with a required assurance.

Authentication can basically be divided into two classes, which are peer entity authentication and data origin authentication. Peer entity authentication assures that the communicating parties are who they claim to be. Data origin authentication assures that a message has come from a legitimate and authenticated source. Authentication is typically needed to provide safety against masquerading as well as modification.

Integrity means the avoidance of unauthorized modification of information. Integrity is an important security service that proves that transmitted data has not been tampered with. Authenticating the communicating parties is not enough if the system cannot guarantee that a message has not been altered during transmission.

Confidentiality is the avoidance of the disclosure of information without the permission of its owner. Secrecy and privacy are terms synonymous to confidentiality. Confidentiality may be ensured with encipherment of the messages.

Non_Repudiation is the property by which one of the entities or parties in a communication cannot deny having participated in the whole or part of the communication. Non-repudiation prevents an entity from denying something that actually happened.

Access Control is the denial of unauthorized use of a resource. Access control is closely related to authentication, which gives the ability to limit and control access to network systems and applications.

Availability means the accessibility of systems and information by authorized users. It is closely related to authentication and access control. An authenticated entity must have access to a system and on the other hand unauthorized entity must not prevent the usability of the system (Denial of service attacks).

3. Some Security Protocols and Applications for Sip

1) **Encryption** is a mechanism to secure information so that only receiver can use it. In encryption, a cleartext message or plaintext is hidden by using cryptographic techniques, the resulting message is known as ciphertext. The receiver recovers the original plaintext by decrypting the ciphertext.

A key is a mathematical value that modern cryptographic algorithms make use of when encrypting or decrypting a message. Cryptographic techniques are not only used to provide confidentiality, but also other services, like authentication, integrity and non-repudiation may be provided. Cryptographic techniques are typically divided into two generic types: symmetric key and asymmetric key techniques.

a) **Symmetric Encryption** means that the key can be calculated from the decryption key and vice versa. In most cases both keys are the same one and the mechanism is called secret key or single key encryption. The security in symmetric key encryption rests in the key, which must be agreed before any communication. As long as the com-

munication needs to remain secret, the key must be secret, divulging the key means that anyone could encrypt and decrypt the messages.

The Data Encryption Standard (DES) is currently the most widely used symmetric encryption scheme. DES is a symmetric block cipher that processes 64-bit blocks of plaintext producing 64-bit blocks of cipher text The key length is 64 bits, but since every eighth bit (8, 16, . . . , 64) is a parity bit for error detection, the effective key length is 56 bits.

b) **Asymmetric Encryption** also called public-key encryption, the key used for encryption is different from the key used for decryption and the decryption key cannot be calculated from the encryption key. The encryption key may be published, so that anyone could use the encryption key to encrypt the message, but only the receiver with the corresponding decryption key can decrypt the message. So the encryption key is also called the public key and the decryption key is called private key.

The RSA algorithm is perhaps the most popular public-key algorithm. It was invented by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. RSA can be used for encryption / decryption, providing digital signatures and key exchange. decrypt the message.

The Diffie-Hellman algorithm was the first ever public-key algorithm, invented in 1976 by Whitfield Diffie and Martin Hellman. The algorithm can be used for key exchange but not for encryption/decryption, thus the algorithm is typically used for exchanging the secret keys.

2) **Message-Digest Algorithms** are compact "distillate" or "fingerprints" of your message or file checksum. A message-digest algorithm takes a variable length message as input and produces a fixed length digest as output. This fixed length output is called the message digest, a digest or a hash of the message. The digest, which is typically shorter than the original message, acts as a fingerprint of the inputted message. The message digest verifies your message and makes it possible to detect any changes made to the message by a forger.

4. Novel Proposed Method to Enhance Sip Security in Specific Confidential Sectors: TOUCH ME NOT

In some secure and confidential sectors such as the army (for e.g.) data and signaling leakage is highly volatile and potentially very dangerous. In such cases signal tapping is neither lawful nor desirable. Thus a new security architecture termed TOUCH ME NOT is being proposed inorder to avoid signal tapping. This proposed model is currently under test and development. Its source code has been written in Turbo C++. The testing activity has been carried out using freely available evaluation copies of several popular SIP soft phone clients. Since our testing activity is not complete, we have not informed the vendors about our produced results. Hence, in this paper we

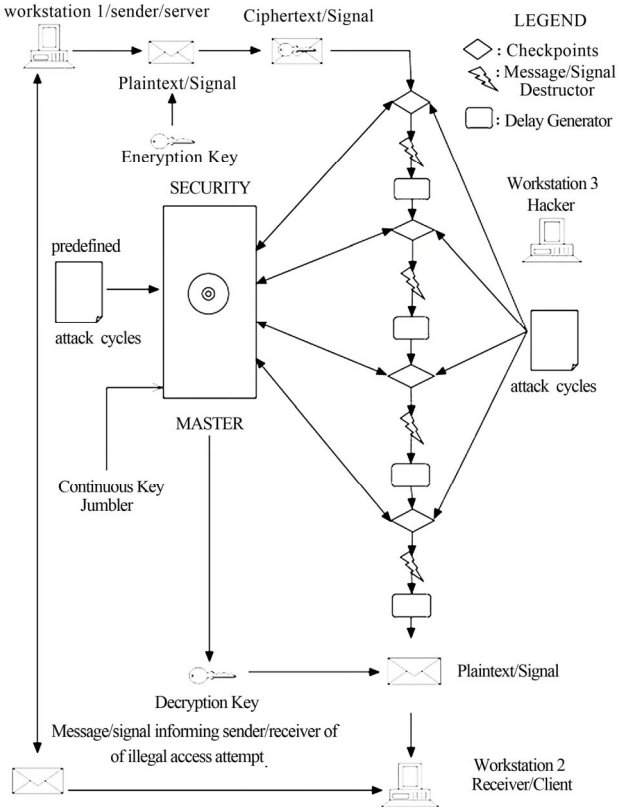

Figure 3. TOUCH ME NOT architecture

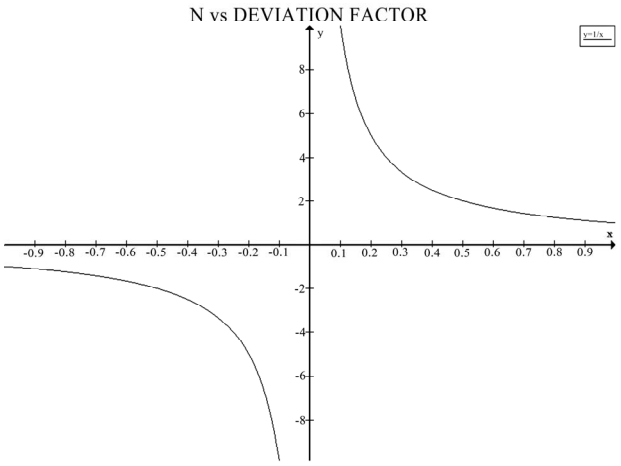

Figure 4. N vs deviation factor

are refraining from using client names.

In this process, there will be present a main security master which will be consisting of a continuous key jumbler whose task will be to randomly jumble and reassign key values in order to prevent key cracking by an intruder.

The security master will also be consisting of a list of predefined attack cycles and algorithms so that it can detect and recognize the most common and difficult types of attacks if any.

The entire signaling route from the sender to the sender to the receiver will be divided into several checkpoints. If the attacker attempts to access or tap the signal at any point, on or between the checkpoints, a pre programmed delay generator which may be an exe file will appear as a non removable pop up, displaying random gibberish values or a blank screen.

This will act a cover for the signal to self destruct, in other words the signal will be auto terminated at that point and a signal informing the sender and receiver of the interception or attempted attack on the sent signal will reach the sender as well as the receiver in due time. This will prevent the signal from being tapped with, examined or malformed. This method cannot however be generalized in all sectors as tapping is lawful in several government as well as private sectors.

5. Fuzz Data Generation

We are already aware of the Fuzz Data Generation Algorithm. Fuzz testing or fuzzing is a software testing technique used to find implementation defects using malformed or semi malformed input data [1]. We have to define a set of parameters that contribute to the overall fitness value of a given data. All these parameters need not always be used: a subset of them can be used depending on the input population and the application being fuzzed. They can be for e.g. Native size, Native type, Parent's Fitness etc. [1] The challenge will be to define more and more criterion to define a fitness value. The more the value of N, the better the fitness value. This can be verified from the graph given below as well as the set of relations provided [1].

Let N be the number of parameters chosen to contribute to the fitness value.

Calculate the deviation factor DF+1/N (We can also calculate a weighted DF, if some of the parameters need to be given more weight compared to the others).

Calculate the deviation contribution DC=A*DF, for each parameter, where A is the deviation percentage.

Calculate total deviation contribution TDC=SUM(DC) for all N.

Final Fitness Value F= Ceiling [TDC*10]

6. Conclusions

Thus we have analyzed some of the methods which make SIP a more secure network. The proposed TOUCH ME NOT architecture is an effective way to prevent illegal tapping in selected confidential setups. Fuzzing data generation along with the simulation can be used to determine fitness values. These steps will hopefully help in making SIP a stronger and a more secure network.

REFERENCES

[1] IEEE Paper: A SIP Security Testing Framework: Hemanth Srinivasan and Kamil Sarac.

[2] Applied Cryptography-Second Edition-Protocols, algorithms and Source code in C: Bruce Scheneier.

[3] SIP Tutorial: Daniel-Constantin Mierla.

[4] IEEE Paper: SIP Security Issues: The SIP Authentication Procedure and its Processing Load: Stefano Salsano, Luca Veltri, Donald Papalilo.

[5] IEEE Paper: Security Challenges for Peer-to-Peer SIP: Jan Seedorf.

