A Brief Study of Security Aspects for Session Initiation Protocol Visualizer

Authors
Mithilesh Kumar Dubey¹, Dr. Vinod Gupta², Navin Kumar³

¹Assistant Professor, Department of Computer Science & IT, Jagan Nath University, Jaipur India
E-mail:⁠₃ mithileshkumar.dubey@jagannathuniversity.org
²Associate Professor, Department of Information Technology, Rajasthan University, Jaipur India
³Registrar, Jagan Nath University, Jaipur, India
E-mail³: navin.kumar@jimsindia.org

Abstract-
SIP (Session Initiation Protocol) Visualizer is related to Telecom & Development project. This tool has been designed for visualizing SIP call flows. It shows the status of the current messages, and also of the complete scenario that is taking place. With Visualizer a user can see, how the messages are flowing from one user agent to another user agent. SIP Visualizer is totally based on the SIP Protocol. The Session Initiation Protocol is a new signaling protocol developed to setup, modify, and teardown multimedia sessions over the Internet. SIP Visualizer works where the user wants to know about his session and SIP messages to the corresponding session. In the security aspects of SIP Visualizer we have studied & analyzed security of Sip Vis and proposed a solution for end to end system security.

Keywords: SIP (session Initiation protocol), Sip Vis( SIP Visualizer).

1.0 INTRODUCTION
During recent years the telecommunication industry has made tremendous progress in their development of systems that offer more bandwidth to the end user. Today, the performance of the systems is high enough to offer multimedia sessions, which are very bandwidth demanding. A session is divided in two phases. The signaling phase, which controls the session, and the media Phase, which handles the transportation of the data stream. If the participants in the session should be able to understand each other, a set of rules is required. These rules are specified in a protocol. The most likely protocol to be used in an IP based multimedia session for the signaling phase is the Session Initiation Protocol (SIP), which is designed by the Internet Engineering Task Force (IETF). Several Protocols with similar functionality exist and the H.323 protocol is the second most used protocol.

During the signaling phase, several parameters are exchanged between the end users. Some of these parameters may be sensitive to the users and should be kept secret, e.g. the location of the user and the user’s name. It is also important that each user identifies him to the other users and that unauthorized users are incapable of modifying,
inserting or removing messages sent during the signaling phase. Different security mechanisms as encryption.

1.1 PURPOSE:
- Identify the security mechanisms that are implemented in SIP and what type of protection they provide.
- Identify possible security threats against SIP.
- Evaluate which security mechanisms may be added to SIP to increase the protection against possible security threats.

Present a test specification for security tests performed on different SIP

2.0 Cryptographic goals

The main goal of cryptography is to provide the following services:

1. Confidentiality
2. Authentication
3. Data integrity
4. Non-repudiation

- **Confidentiality** is a service used to keep the information secret to everyone that is unauthorized to access it. Encryption is one method to provide confidentiality.

- **Authentication** is a service used for identification of information or entities. The identification of the information is often called data origin authentication or message authentication and identification.

- **Message authentication** ensures the receiver that only an authorized party can have created the specific information. An encrypted checksum of the information is often attached to the information which proves that only an authorized entity can have created the information.

- **Entity authentication** enables an entity to verify the identity of another entity. A common way to accomplish entity authentication is to challenge the other entity by giving it some type of information that only an authorized entity is often called **entity authentication**.

- **Data integrity** is a service to detect unauthorized manipulation of information. Manipulation includes insertion, deletion, and substitution. Secure hash functions may be used to provide data integrity.

**Non-repudiation** is a service which prevents an entity from denying previous commitments or actions. Digital signatures is one method of providing Non repudiation.

2.1 Conventional Encryption

Conventional encryption also referred to as symmetric encryption or single key encryption is
the most used encryption technique today. Conventional encryption uses a secret key that only the sender and receiver share. The key and the plaintext are the parameters for the encryption algorithm that produce the cipher text. And the key and the ciphertext are the parameters for the decryption algorithm. There exist several classical encryption algorithms that are easy to cryptoanalyze i.e. a third party finds the secret key or the plaintext. One of these is the Caesar Cipher which is based on a substitution technique, i.e. each character in the plaintext is mapped to another character by using tables or some mathematical function. The algorithm assigns a number to every character and produces the ciphertext by adding the numerical key to every character. The result is always modulo the number of characters in the alphabet. The number of possible keys is equal to the number of characters in the alphabet and therefore easy to cryptoanalyze with brute-force. Fortunately there exist modern encryption techniques that are very difficult to cryptoanalyze due to their complex structure. The most famous and most used algorithms are different variants of the Data Encryption Standard (DES). DES and other modern encryption algorithms are based on the Feistel Cipher which is characteristic by its rounds. The first round takes the plaintext and a sub key as parameters and the output is passed to the next round. The result from the last round is the actual ciphertext. This means that each round can be seen as an independent cipher. The major differences between different modern symmetric encryption techniques are the structure of these independent ciphers, i.e. they use different key lengths and bit operations. They also differ in how many rounds they use.

2.2 Public key Cryptography

The discovery of public key cryptography has been a revolution in cryptography. Public key algorithms are based on mathematical functions rather than on different types of bit transformations. Another big difference is that public key cryptography is asymmetric, i.e. uses two separate keys instead of one. The keys are referred to as the public key and the private key. The private key is kept secret while the public key is distributed to different individuals that will communicate with the owner of the private key. Encryption/decryption is just one of three different categories that can be used with public key cryptography. These are:

- Encryption/decryption
- Digital signature
- Key exchange

2.2.1 Encryption/Decryption

There exist several public key encryption algorithms but the most known is the Rivest-Shamir-Adleman algorithm. Another algorithm is Elliptic Curves encryption/decryption which is more complicated but can offer equal security with smaller keys than RSA. Bellow is the mathematical description of the RSA algorithm:
One way cryptoanalyze the algorithm is to factor $n$ into its two prime factors. That can easily be done with small $n$ but for large $n$ the degree of success will fall dramatically.

### 2.2.2 Digital signature

To sign a plaintext the sender encrypts it with its own private key and the receiver decrypts the cipher text with the sender’s public key. If the result from the decryption is readable, the receiver can be sure that it originates from the sender because the sender it’s the only one that knows its private key. This way of making digital signatures is not effective because the whole message is encrypted which requires a lot of computational resources. A better solution is to map the message to a smaller, fixed sized, value and encrypts it with the sender’s private key. The function that maps the plaintext to a fixed sized value is called a strong one-way hash function.

### 3.0 Security Mechanisms in SIP

This covers the security mechanisms that are standard in the current version of SIP. Because SIP still is under development, some security mechanisms that are discussed in this may be excluded in later versions. There may also be new mechanisms added as standard in later versions. Some of these candidates are described.

#### 3.1 Authentication

Authentication ensures that a message has been created by the claimed source and that the claimed source has sent it. Authentication includes protection against modification, delay, replay and reordering.

SIP provides a stateless challenged-based mechanism for authentication. The authentication mechanism is meant to be used only in one direction. But there is an option to make mutual authentication, i.e. authentication in both directions. There is also support for integrity protection of requests and responses.

IETF SIP working group has not developed a new scheme for authentication, and uses almost the same authentication scheme as is used for HTTP. One difference is the definition of the protection domain, which in the HTTP case is defined by the...
realm and canonical root URL. The canonical root URL does not exist in SIP, i.e. there are no files to get, put or delete like in HTTP. Therefore is the protection domain defined by the realm, user info, host and port? part of the Request-URI,

- **HTTP Authentication** Two different authentication schemes are standard in HTTP, namely Basic and Digest authentication. The first one is very primitive and insecure because it sends the credentials for the client in plain text. The Digest authentication is much more secure because the authentication scheme uses checksums for credentials. Although it is not a perfect solution for secure authentication, it protects against most of the security flaws in the Basic authentication. Schemes use four different header fields to accomplish the authentication. Some of these are specific for proxies and the rest are for UA authentication. The fields are (case-sensitive)
  - WWW-Authenticate
  - Authorization
  - Proxy-Authenticate
  - Proxy-Authorization

### 3.2 Integrity

Message integrity assures that only authorized parties are able to modify the message, i.e. an unauthorized third party cannot modify the message without detection by the authorized receiver. In most cases the integrity protection is only applied to special parts of a message, i.e. parts that are not allowed to be modified. The problem with integrity protection in SIP is that the messages are allowed to be changed by network intermediaries. This means that the parts that are allowed to be changed cannot be included in the integrity protection.

The standard of SIP defines how to use Pretty Good Privacy to supply signatures of message parts that are not changed by network intermediaries. A signature is one of several ways to supply message integrity by using hash functions. Even if the standard document for SIP, Request For Comments (RFC) 2543, is a standard track with “Draft Standard” status it will probably be obsolete and replaced with the draft “draft-ietf-sip-rfc2543bis-0x”, where x is the version number. In current version, version 5, the use of PGP signatures has been excluded. Today there only exists a very limited integrity protection in SIP which is provided by the Digest authentication scheme, described in the previous section. Although it is wrong to say that SIP does not support other integrity protection, the protocol does not make any standard definition how to implement these. The section above stated that there is no integrity protection for the complete message in SIP. But there exist definitions on how to protect the integrity of the message bodies by using S/MIME. The message bodies consist of descriptions of the media transfer which may be interesting to protect against modification. Even if there is no integrity protections defined for the complete message in
SIP, it is always possible to use transport and network layer protocols that provide this feature. In the SIP draft from IETF there is a recommendation for SIP endpoints to support Transport Layer Security. IP Security is also a hot topic for providing integrity protection.

3.3 Confidentiality
Message confidentiality assures that only authorized parties are able to read the content. In SIP, encryption is used to provide message confidentiality.

In RFC 2543 there exist two header fields, the Encryption and Response-Key that may be used for end-to-end encryption. There also exists a definition on how to use these header fields for PGP encryption. As in the case of message integrity this definition has been excluded in the coming draft. The header fields have also been excluded which indicates that the encryption will be out of the scope in the SIP protocol and probably be moved to lower layer protocols. The problem with end-to-end encryption in SIP is that network intermediaries have a need to view certain parts of the message to be able to accomplish their tasks. These parts may be sensitive to the users, which mean that most of the benefits of using encryption are lost. There is also a concern about the key exchange because end-to-end encryption algorithms are based on keys shared by different users. SIP does not define any mechanism for key-exchange as Lower layer protocols like TLS and IPSec do. The conclusion is that it is not likely to be any support for end-to-end encryption in the future standard for SIP. Security mechanisms in SIP although the complete message will not be encrypted, it is however possible to encrypt the message body end-to-end by using S/MIME,

3.4 Analysis
Modern cryptology schemes may provide protection against different security threats. But there are also other aspects to consider when designing an application e.g. performance, power consumption, user-friendliness etc. SIP will be implemented on many different platforms with some of them having long round-trip times and limited power supply, e.g. mobile phones. Complex schemes that provide strong protection will probably not be suitable in SIP. Constructing a new scheme based on the requirements and limitations is always possible but will require lot of time to develop. The history shows that new schemes always have serious security flaws when they first are released for public use. Even if the core of the new scheme is kept secret it does not prevent users from making reverse engineering to reveal the secrets. IETF have obviously thought about the requirements and limitations when they designed the security framework for SIP but there is still much more work left to be done. The framework contains only Basic and Digest authentication today, which is not sufficient to prohibit all security threats. The framework must be extended...
to prevent more security threats as the man-in-the-middle (MITM) attacks and eavesdropping.

3.4.1 Threats
Threats can be split into different areas, shown in Figure 2.

![Figure 2 Different Areas of threats](image)

The most serious threats are those made by insiders who have both the knowledge and capabilities to make serious harm to the target. The non-malicious persons are often unaware of the threats they cause, i.e. they do not have the intention to harm the target. A unintentional threat could be software bugs and loose security thinking but events like natural disaster also fits this category. Natural disasters are difficult to be protected against but a good recovery plan may decrease the damage to minimum. The most famous group of malicious outsiders that makes intentional threats is hackers and crackers who often use different types of self developed tools to harm the target. They often gain knowledge about weak points on the target before the actual attack occurs. The attack could be either active or passive. The passive attack is used to obtain information and the active attack is used to modify information.

4.0 SIP Captured Messages
The analyses of captured SIP Messages by Wireshark are shown here:

![Figure 3: Captured SIP Messages1](image)

![Figure 4: Captured SIP Messages2](image)
5.0 Flow Graph of Captured SIP Messages

The flow graphs of the captured SIP messages are defined as follows:

6.0 Conclusion

According to my opinion the security mechanisms provided by the SIP standard and those that are proposed to be used are sufficient to provide a secure Signaling session if they are used together in a well-specified way. The only restriction is that TLS and/or IPSec must be used in conjunction with SIP to achieve this. Both these protocols require the use of public key certificates or security associations. The idea of using public key certificates for distributing Public keys solve several problems. However, public key certificates are not suitable to be used by equipments that have limited storage resources and are used in environments with limited bandwidth, due to their size. Authentication in SIP. Even if it is more suitable to be used in the mobile telecommunication system than in the Internet systems, it may be a better solution than the Digest authentication. If someone finds a constructive way to use the produced symmetric keys for encryption and integrity protection of the
SIP messages, the IMS AKA should definitively replace Digest authentication as the default mechanism for entity authentication. This research paper is focused on the security mechanisms in SIP that have been developed by IETF. Most of the information about proposed security mechanisms has been obtained from drafts published by IETF. This may have influenced the information in this research and the results from the analysis in a way that does not give the full picture of how different security mechanisms may be used in future SIP applications, i.e. IETF tends to give the designers too many choices how to implement these security mechanisms. It does not matter if these security mechanisms are well done if no one implements them or makes an adequate implementation of recommended security mechanisms. Even if they are implemented adequately, the default option is not to use them in the application, i.e. the user is often responsible of turning them on. The tested SIP Captured messages & its analysis have been shown above.

7.0 References


