UDC 004.773.5

THREAD AND DATA SECURITY ANALYSIS IN SIP NETWORK

Pasichnyk O.V.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: alexeypasichnik2.71828@gmail.com

АНАЛІЗ ЗАГРОЗ ТА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ SIP ТЕЛЕФОНІЇ

В роботі досліджуються особливості забезпечення безпеки даних мережі SIP, вектори атак на мережу SIP, такі як: перехоплення реєстрації, перехоплення сесії, підміна сервера, підробка змісту повідомлення, розрив сесії зв'язку, атака типу «Відмова в Обслуговуванні» та «примноження», боти та DDoS атаки; та засоби захисту від подібного роду загроз.

Hackers approach attacks in stages, beginning with probing of the network. Hackers first look for networks with easy access. Once a vulnerability is found, it is recorded for later use. Once a vulnerability has been identified and validated, it is used later for a larger attack. It is a combination of vulnerabilities that allows hackers to reach through many different networks, traverse through all of these networks unnoticed, and launch largescale DoS attacks on unsuspecting networks. [1]

Here are listed some common methods used when attacking a SIP-based network.

Registration hijacking. Since SIP uses clear text, if a hacker can capture these messages, that hacker is able to read subscribers' sensitive information such as their public and private identities. This information can then be used to gain access into the operator's network. [1]

Session Hijacking. For maintaining session authorization, the cookie is used. They are generated by a server when the server is first accessed. [2] If these cookies are intercepted and copied, they allow the interceptor full access to the session already in progress. This means the hacker will have access to all of your transactions and account information. [1] This problem can be critical when open Wi-Fi hotspot is used, a cookie can be intercepted through the process of eavesdropping.

To prevent the use of this vulnerability it is possible to check the time and date stamp of an incoming request or response. When a UAS receives a request, it should check the date and time with its own internal clock. If there is a difference in time stamp with internal clock (more than 30 minutes, for example), then it is very likely that the message was intercepted and has been relayed with a changed destination address. [3]

Impersonating a Server. In SIP networks DNS is used to identify the IP address for domains and their applications. [2] In case if DNS records are changed either both a subscriber and an operator could be redirected to hacker`s server, which in this case will impersonate itself as trusted leading to data leakage.

Tampering with Message Bodies. a hacker may capture an *INVITE* message from a subscriber and change the *FROM* header to reflect his own address. This would provide the hacker access to a network he is not authorized to use and would allow him to initiate sessions with other subscribers while pretending to be someone else [1].

Tearing Down Sessions. Hackers could intercept requests from various subscribers and send a *BYE* message as a response [2]. This would then terminate the session and cause it to be torn down. It is much easier to execute than regular DoS as it requires only one proxy to be hacked however it may cause same result – impossibility to make a call in whole network region.

Denial of Service. DoS attacks can take many different forms and can be launched using many different techniques. The most common is flooding the network with specific traffic types. For example, using a call generator, a hacker can send millions of *INVITE*s into the network attempting

to flood the network with call requests [1]. Another form of DoS attack involves application servers [2]. By launching a flood of requests to an application server, the network element is immediately flooded and congested, taking it out of service. This can also happen with the DNS through flooding with DNS queries. When the DNS is attacked, the entire network can be impacted, depending on where the server sits within the DNS hierarchy and whether or not redundancy has been implemented. [3]

Amplification SIP allows registering multiple identities within single user [2]. Utilizing this feature hacker can register a subscriber listing many different user identities for the same subscription. This then provides the registrar with a list of multiple destinations for a request. The hacker then launches requests toward the public identity, which the registrar and proxies then send to multiple destinations based on the registration made by the hacker [1]. Similar result can be accomplished through making registrar to run out of memory. It is done by registering many different identities. The way to prevent this could be different levels of authentication, preventing unauthorized subscribers from accessing the registrar.

Bots and DDoS Attacks. *Bots* are scripts that in different ways are carried to a subscriber's device then listening opened TCP/UDP sockets and distributing themselves through them. When one hacker successfully launches bots, they create their own little network of bots known as botnets which on demand generate traffic to a single network element resulting in Denial of Service (Distributed DoS)[3]. The main concern is that the botnet in its idle state is hard to track also the user equipment is infected rather than the provider equipment and safety measures are relied on the end user which tends to neglect them.

Good security solution should meet the following requirements:

1. Thread management efficiency
2. Transparency, security measures should not interfere with the end user.

Main aspects of secure SIP network are authentication, authorization, monitoring [3].

Authentication requires the use of passwords and the exchange of credentials. Each time the subscriber registers in the network, the registrar needs to carry out the procedure of initial registration [2].

Authorization requires high performance database containing basic information about the user, including the levels of access to different services. [3]

Monitoring include means that allow operator to have total visibility to every network transaction that takes place. This includes any downloads that the subscriber may have made.

Encryption should be performed, however not all headers are encrypted but only those that do not contain information about the destination and the source of the message because this would lead to the impossibility of the exchange of messages between routers without distribution of encryption keys [3].

Transport Layer Security (TLS) is a good means of providing encryption between networks, while SIP Secure (SIPS) [2] is designed for use within a trusted domain. TLS works at the TCP layer and is best when used between two networks where two network elements do not know each other [4]. To encode voice messages Secure Real-time Transport Protocol should be used [5].

TLS is to be used at proxies, redirect proxies, and registrars when interconnecting with other networks. They should also possess a site certificate for authentication. These proxies also must have the ability to validate certificates from other trusted sites, by storing the certificates from these sites [6].

Another approach to encryption is tunneling a SIP message within another SIP message. The original SIP message is encrypted and then encapsulated within another SIP message for routing. The routing information from the original SIP message is used to populate the routing headers in the outside message, but nothing else is given in the outside message. When the User Agent Server compares the encapsulated message with the outer message, it will identify whether or not there have been any other alterations to the original message [1].

Strict routing. With strict routing, the routing path is recorded as the subscriber registers in the network. The REGISTER message contains the RECORD-ROUTE headers, used to collect the

addresses of each of the proxies in the path. These addresses are saved in the order they were added, so that a route list can be established for the subscriber. The route list then becomes part of the subscriber's registration. Stateful proxies in the path then also store the route list for the subscriber so that they know how to route messages (both requests and responses) to the user identity. Even if a hacker attempted a session hijack, for example, the proxies would ignore the routing provided in the message, relying instead on the route list they recorded for the subscriber during the registration [1].

Intrusion detection. Effective monitoring can be accomplished through an intrusion detection system which can operate in real time (or near real time) or historical mode. A real-time system is needed for detecting attacks while they are in progress. However, these systems should also have some capacity of storage to allow for the investigation of network events at a later time. The IDS identifies the source of data (the network, application, or host). It performs analysis on the traffic based on rules (policy) and could also have the ability to establish its own policy through neural technology. Since IDS systems are passive, they are unable to actively exchange encryption keys and negotiate these keys with other network elements [7].

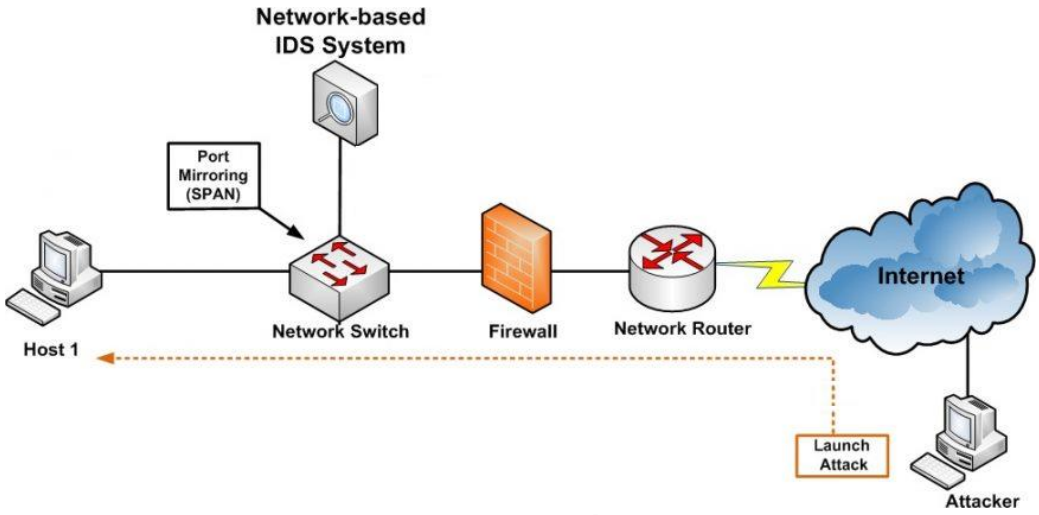

Fig 1. IDS System implementation

Considered attacks are aimed at the SIP signaling and its network equipment. The consequences of an attack could be leaking user's personal data to third parties, a compromising of user actions based on it personal identities and disabling network by overusing its elements with both authorized or unauthorized access. The consequence of such actions is operator money losses, during idle of service and losses of users. From the above it can be concluded that the implementation of network security is the first responsibility for an operator. However, it should be noted that no measures can completely protect the network so the main method to protect data is to create conditions under which the invasion into the network is not economically viable for an attacker.

References

1. McGraw-Hill Communication Series, "Session Initiation Protocol (SIP): Controlling Convergent Networks", 1st Edition, p.133-156
2. J. Arkko, V. Torvinen, G. Camarillo, A. Niemi, T. Haukka "Security Mechanism Agreement for the Session Initiation Protocol (SIP)" RFC 3329, January 2003
3. Porter, Thomas; Andy Zmolek; Jan Kanclirz; Antonio Rosela "Practical VoIP Security. Syngress" 2006.
4. Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1," RFC 4346, April 2006
5. D. McGrew, D. McGrew, M. Naslund, E. Carrara, K. Norrman "The Secure Real-time Transport Protocol" RFC 3711, March 2004
6. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol" RFC 3261, June 2002
7. Amoroso, Edward, "Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response," Intrusion.Net Books, Sparta, New Jersey, 1999.