INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

COM 17 – C 122 – E

September 2009

English only

Original: English

Question(s): 4/17

STUDY GROUP 17 – CONTRIBUTION 122

Source: Korea (Republic of)

Title: A Proposal of draft text for draft Recommendation X.sips

Summary

- A framework for countering cyber attacks in SIP-based services(X.sips) has been agreed as a new study item at the SG17 meeting(15-19 September 2008, Geneva)
- This contribution proposes draft text for the draft Recommendation X.sips.

Contact:	Kyoung Hee Ko KISA Korea	Tel: +82 2 405 5268 Fax: +82 2 405 5219 Email: khko@kisa.or.kr
Contact:	Hwan Kuk Kim KISA Korea	Tel: +82 2 405 5217 Fax: +82 2 405 5219 Email: rinyfeel@kisa.or.kr

The proposed text is as follows.

1 Scope

This draft Recommendation provides a framework for cyber attack detection and response in SIP-based services. This draft Recommendation covers as follows;

- Overview of cyber attacks in SIP-based services: cyber attacks like session hijacking, denial-of-service, service abuse, and service misuse are addressed. Eavesdropping and spam are out of scope.
- Detection and response capability for cyber attacks in SIP-based services
- Framework for cyber attacks detection and response in SIP-based services

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

<TBD>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 SIP [IETF RFC 3261]: Session Initiation Protocol is an application-layer control protocol that can establish, modify, and terminate multimedia sessions (conferences) such as Internet telephony calls.

3.1.2 SDP [IETF RFC 4566]: Session Description Protocol is a format for session description.

3.1.3 RTP[IETF RFC 1889]: Real-time Transport Protocol provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

<TBD>

4 Abbreviation

This Recommendation uses the following abbreviations and acronyms:

<TBD>

5 Conventions

None.

6 Overview of cyber attacks in SIP-based services

SIP-based services are IP multimedia communication services in which SIP is used for initiating, managing and terminating multimedia session. There are services such as VoIP(Voice over Internet Protocol), presence, instant messaging, video conferencing and unified communications in SIP-based services.

In order to providing SIP-based services, SIP user agent, SIP-based infrastructure and application servers are needed. SIP user agent can send registrations, invitations to sessions, and other requests. In SIP-based infrastructure, there are SIP proxy server, redirect server and registrar server. SIP proxy server receives SIP requests and forwards them on behalf of the requestor. SIP redirect server is a user agent server that generates 3xx responses to requests it receives, directing the client to contact an alternate set of URIs. SIP registrar is a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles. Application servers deal with application-specific messages and protocols.

Cyber attacks to SIP-based services are as follows.

Session hijacking: there are attacks such as invite session hijacking, registration hijacking, and so on. Sessions between legitimate users or sessions between legitimate user and SIP servers are targeted.

Denial of Service(DoS): there are attacks such as RTP flooding, SIP request method flooding, SIP response message flooding, malformed message attacks, and so on. DoS attacks target SIP user agent, SIP-based infrastructure and application servers. Especially, because SIP user agent has relatively limited computing resources, it is more vulnerable to DoS attack.

Service misuse and abuse: there are attacks such as forged registry message aiming at toll fraud, bypassing authentication using SQL injection, bypassing proxy servers, and so on.

Toll fraud attack can be divided into three groups. In the first group, attackers steal register information and forge this registry message for bypassing authentication. In the second group, attackers exploit vulnerability of SIP-based infrastructure. SQL injection and buffer overflow attack can be used. In the third group, attackers utilize misconfiguration of SIP-based infrastructure. Default password of SIP proxy server can be used. SIP trunk with no authentication is also used for bypassing.

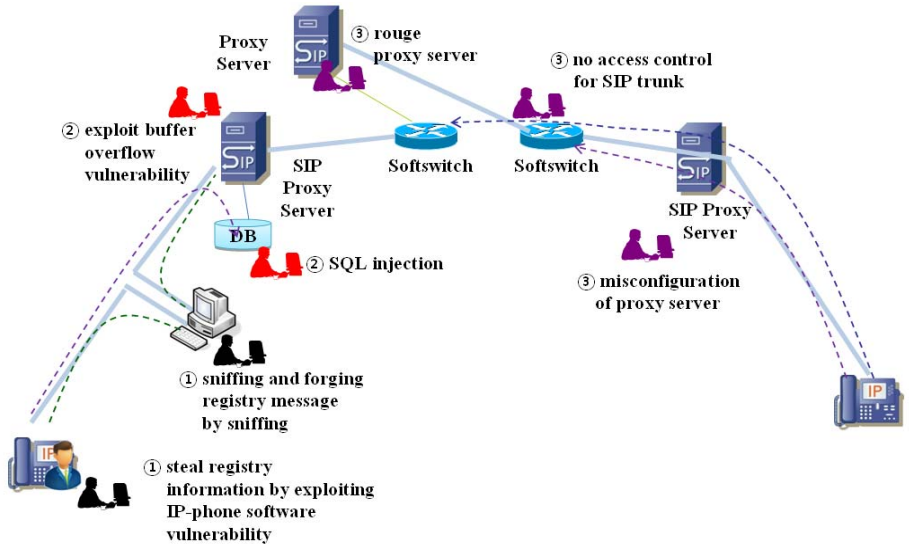


Figure 1 – Toll fraud attacks in SIP-based services

Besides the above mentioned attacks, SIP-based services have potential security threats which had happened in the data communication networks. SIP proxy servers or registrar servers can be compromised by traditional attacks such as brute force attack, security vulnerability exploitation of operating system, or malwares.

7 Detection and response capability for cyber attacks in SIP-based services

This clause clarifies capability for detecting and responding to cyber attacks in SIP-based services.

7.1 Detection capability for cyber attacks in SIP-based services

The followings are requirements for detecting cyber attacks in SIP-based services.

- It is required to capture packets at both signalling and media channels. Because signalling path and media path is separated physically or logically, points for traffic monitoring need to be separated.
- It is also required to monitor stream of packets at both signalling and media channels.
- It is required to inspect signalling messages and media packets. For inspecting signalling messages at application layer, deep packet inspection is needed. In deep packet inspection, SIP header fields, SDP message fields, and RTP headers fields are parsed according to protocol specifications. For example, malformed message attacks can be detected based on parsed information.
- SIP flow information can be helpful for traffic analysis. Collecting and aggregating SIP flow information also need to inspect signalling messages and media packets.
- It is required to collect and manage dialog-related information. A dialog is defined by the combination of From tag, To tag, and CALL-ID. For example, session hijacking can be detected based on this dialog-related information.
- It is required to manage dynamic media port. Media port for media stream is determined during establishing session. For example, if RTP packets target ports which are not allocated during session establishment, these packets can be detected as RTP flooding.
- It is required to measure QoS metrics such as delay, jitter and packet loss rate between legitimate users to check if QoS metrics may be affected by detection functionality.
- It is required to share detection information. Aggregated and integrated detection information can produce improved detection by security information and event correlation.
- It is needed to detect non-SIP-specific attacks. Otherwise traffic which doesn’t serve SIP-based services must be blocked according to organization’s security policy.
- As SIP-based applications become popular, more SIP methods are being suggested. Therefore it is needed to keep track of changes in SIP message format.

7.2 Response capability for cyber attacks in SIP-based services

The followings are requirements for responding to cyber attacks in SIP-based services.

- It is required to properly handle packets detected as an attack or anomaly. These packets can be simply dropped, or regenerated as an appropriate format.
- Abnormal stream of packets can be blocked, detoured, traffic shaping or rate-limited.

- Traffic shaping or rate-limited is applied to stream of packets which exceed predefined bandwidth capacity. In this case, response functionality needs to provide connection between legitimate users by managing white list of users.
- It is required to measure QoS metrics such as delay, jitter and packet loss rate between legitimate users to check if QoS metrics may be affected by response functionality.
- It is required to share response information. Aggregated and integrated response information can produce improved response by security information and event correlation.
- It is also required to share detection and response information across multiple domains. Shared black lists contains as follows: IP of SIP user agent, From URI, To URI, IP and port of rogue IP-PBX. Shared white lists contains as follows: IP of SIP user agent, IP and port of IP-PBX.

8 Framework for cyber attacks detection and response in SIP-based services

The following figure shows the proposed framework. The framework has functional blocks and interfaces between blocks.

Functional blocks are as follows:

- SPCTM : SIP-based Packet Capture and Traffic Monitoring
- SAAID : SIP-based Attack and Intrusion Detection
- SARTC : SIP-based Attack Response and Traffic Control
- SSMPC : SIP-based Security Management and Policy Control

Interfaces between functional blocks are as follows:

- Interface between SPCTM and SAAID
- Interface between SPCTM and SSMPC
- Interface between SAAID and SARTC
- Interface between SAAID and SSMPC
- Interface between SARTC and SSMPC
- Interface between SSMPC and SSMPC

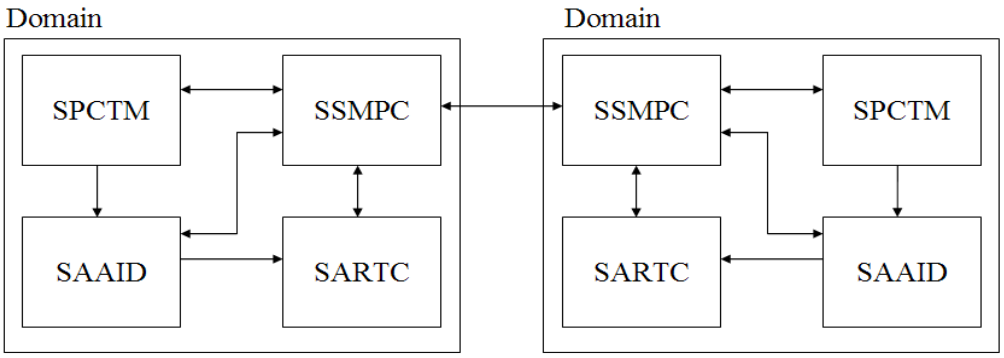


Figure 2 – Framework for cyber attack detection and response in SIP-based services

8.1 Function of blocks

SPCTM is responsible for packet capturing and traffic monitoring. SPCTM captures packets and check if captured packets serve SIP-based services. If captured packets serve SIP-based service, SPCTM parse packets according to protocol specification. SPCTM generates SIP flow information and measures QoS metrics. In order to measure QoS metrics, SPCTM utilize two methods. The first method is to send probe packets to SIP use agent. The second method is to analyze RTCP packets to measure end-to-end QoS metrics.

SAAID is responsible for detecting SIP-based attacks. In order to detect attacks, SAAID manage related information such as dialog, dialog start time, dialog end time, dialog duration, transaction, media port, and so on. SAAID use misuse and anomaly detection mechanism.

SARTC is responsible for responding to SIP-based attacks.

SSMPC is responsible for sharing detection and response information. SSMPC is also responsible for enforcing security policy to SPCTM, SAAID, and SARTC.

8.2 Function of interfaces between blocks

Interface between SPCTM and SAAID: information which is made by SPCTM such as parsing header and traffic statistics is sent to the SAAID.

Interface between SPCTM and SSMPC: information which is made by SPCTM such as parsing header and traffic statistics is sent to SAAID. Security policy such as rules for packet capturing is send to SPCTM from SSMPC.

Interface between SAAID and SARTC: detection information which is made by SAAID is sent to SARTC. SARTC responds to attacks based on this information.

Interface between SAAID and SSMPC: detection information which is made by SAAID is sent to SSMPC. Security policy such as updating attack signature is send to SAAID from SSMPC.

Interface between SARTC and SSMPC: response information which is made by SARTC is sent to SSMPC. Security policy such as blocking specific From URI is send to SARTC from SSMPC.

Interface between SSMPC and SSMPC: multiple domains share detection and response information through this interface. Based on business agreement, SSMPC sends information such as attacker IP and rouge IP-PBX IP to SSMPC in other domains.

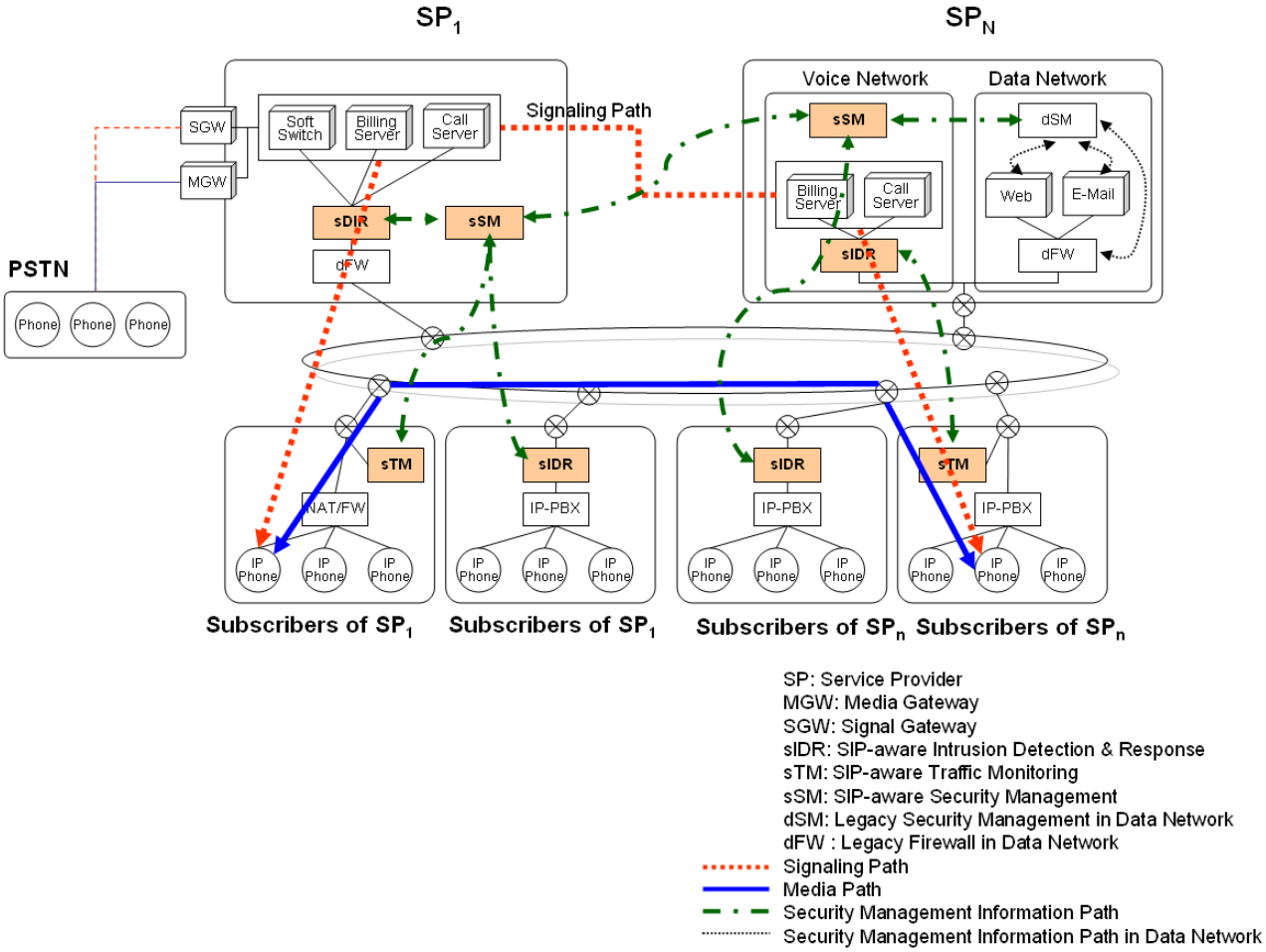
Appendix I

Use case of the framework for cyber attacks detection and response in SIP-based services

This appendix shows use case of the proposed framework. In SIP-based VoIP environment, there are IP telephony service providers (SP_1, ... , SP_n). Each SP has its subscribers. Each SP has separated voice network and data network.

There are three systems which implement functional blocks of the proposed framework.

- sIDR(SIP-aware Intrusion Detection and Response System) : sIDR implements SPCTM, SAAID, and SARTC. Secure SBC(Session Border Controller) or SIP-aware IPS(Intrusion Prevention System) is an example of sIDR.
- sTM(SIP-aware Traffic Monitoring System) : sTM implements SPCTM. sTM can be implemented as an independent system. sTM uses switch devices with mirrored ports or roving analysis port. Routers which can generate and export SIP flow information is an example of sTM.
- sSM(SIP-aware Security Management System) : sSM implements SSMPC.



sIDR is responsible for inspecting, detecting and responding to attacks in SIP-based services. sIDR is placed on both signaling and media channels. sIDR captures packets and inspects headers and payloads. sIDR can use attack signature to detect intrusions. sIDR can also model normal behavior of user agents or systems to detect anomaly. sIDR filters packets detected as an attack.

sTM is responsible for monitoring traffic. sTM is placed on both signaling and media channels. While it is monitoring stream of packets, sTM generates traffic statistics or traffic flow information using IPFIX. According to security policy, sTM drops, detours, or rate-limited attack packets.

sSM is responsible for collecting security information and events. sSM is also responsible for sharing information among multiple service providers.

In the interface between sIDR and sSM, sIDR sends attack information to sSM.

Attack information sent to sSM is as follows:

- sender and receiver information such as source IP address, source port number, destination IP address, destination port number, from uri, to uri
- detection information such as attack category, attack severity,
- response information such as drop, log, pass, rate-limited, detour

sSM sends detection and response policy to sIDR.

In the interface between sTM and sSM, sTM send aggregated traffic information to sSM.

sSM sends monitoring and response policy to sTM.

In the interface between sIDR and sTM, sTM send aggregated traffic information to sIDR. sIDR utilizes traffic statistics for improving detection accuracy.

_____