

Model-based Vulnerability Analysis of IMS Network

Dong Wang

College of Computer

Beijing University of Posts and Telecommunications, Beijing, China

Email: wangdong19852003@163.com

Chen Liu

College of Computer

Beijing University of Posts and Telecommunications, Beijing, China

Email: lchen@bupt.edu.cn

Abstract—IP Multimedia Subsystem (IMS) as the core of Next Generation Network (NGN), its security is vital important. However, IMS is a network with open-architecture based on IP, which brings a lot of security issues. There has already some research results about IMS security, but systematic and model-based research results are lacked. Based on TVRA method, this paper establishes a comprehensive vulnerability analysis model of IMS network, and makes a systematic analysis about the security objectives, assets, weaknesses, threats and other attributes of IMS network by using this model. The research results of this paper can provide the basis for the security assessment of IMS network.

Index Terms—IMS, security, TVRA, vulnerability, model

I. INTRODUCTION

Recent years, IP technology is continuing to change the concept and architecture of telecommunication network, IP has already become the key motive force of structural evolution of telecommunication network. Telecommunication network is moving towards full-IP, merging and opening. The Next Generation Network (NGN) will be based on IP technology as the core. The IP Multimedia Subsystem (IMS)[1], which developed by 3GPP, is a common architecture to provide multimedia service based on IP network, for its separation of control and bearer, centralized management of user profile, independence of access technology and open API, etc., has been accepted by 3GPP2, ETSI, ITU-T, becomes the core control layer of NGN[2].

NGN is a neural pivot of the information communication, must guarantee a reliable public telecommunication service. But for a long time, telecommunication network's security relies on a closed networking environment, such as PSTN, industry lacks the security analysis and protection technology of it. IMS as a goal of evolutionary and converged network, its open

architecture and IP-based characteristics bring NGN serious security problems, which is different from traditional telecommunication network. Attacks, viruses and other threats are brought into IMS, which are only happened on Internet in the past.

There is already a lot of research results on the vulnerability of Internet, however, due to the layered architecture and network elements which are different from Internet, centralized management of user profiles, high reliability requirement and so on, enable the vulnerability analysis methods used for Internet cannot be directly applied to IMS network. Existing research results of IMS vulnerability are mainly about protocol security, there is lack of systematic, model-based research results.

This paper builds a comprehensive vulnerability analysis model of IMS based on TVRA method [3], on the basis of this analysis model, identifies the source of vulnerability, makes a systematic analysis about the vulnerability in IMS, wishes to give a reference value for the safe deployment of IMS network and can also provide basic information for IMS network's security assessment.

II. IP MULTIMEDIA SUBSYSTEM (IMS)

IMS was started as a technology for 3G mobile network in 3GPP Release 5, but it is now being developed as a unified service architecture that allows fixed/mobile convergence, and as the core of the NGN. IMS mainly utilizes IP protocols such as Session Initial Protocol (SIP) [4] for session establishment and Diameter [5] for AAA (Authorization, Authentication and Accounting), in addition, other protocols are also used such as Session Description Protocol (SDP) [6] for media negotiation and Real-time Transport Protocol (RTP) [7] for media transmission. And IMS has a lot of entities and also defines many open and standard reference points for the communication between different equipments. The architecture of IMS is shown in Figure 1 [1].

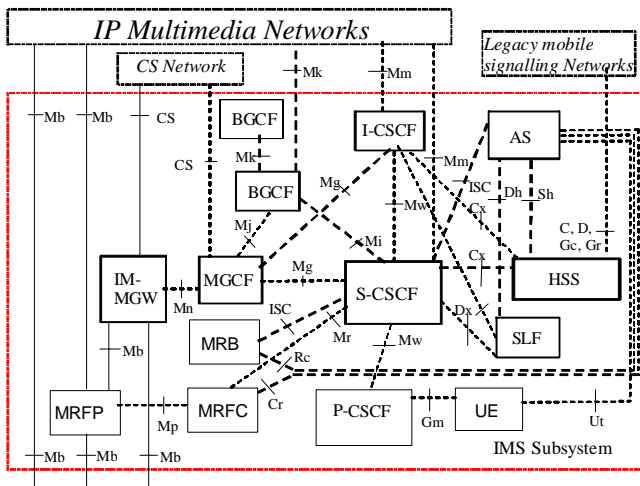


Figure 1. Architecture of the IP Multimedia Subsystem

A. Network Elements

IMS consists of CSCF (Call Session Control Function), MGCF (Media Gateway Control Function), MGW (Media Gateway), HSS (Home Subscriber Server) and other network elements. CSCF is divided into P-CSCF (Proxy-CSCF), I-CSCF (Interrogating CSCF) and S-CSCF (Serving CSCF), they are all SIP servers essentially.

1) *P-CSCF*: P-CSCF is the entry point for UEs to the IMS domain and services. This P-CSCF is discovered by DHCP or PDP and is responsible for maintaining security associations with the UE. The P-CSCF also enforces local policies, forwards incoming SIP signalings to UEs and forwards outgoing SIP signalings to the Interrogating-CSCF (I-CSCF).

2) *I-CSCF*: I-CSCF provides the entrance to the home domain, and assigns S-CSCF for a special user by contacting the HSS, it also responsible for topology hiding.

3) *S-CSCF*: S-CSCF provides services for subscriber users, it maintains a session state as needed by the network operator for support of the services. Even in the roaming state, services are also provided by home S-CSCF.

4) *HSS*: Similar with HLR in 2G, HSS is a database containing user profiles, HSS exchanges information with the S-CSCF and I-CSCF using the Diameter protocol.

5) *MGCF*: MGCF provides the protocol conversion between ISUP and SIP when the intercommunication of CS and IMS.

B. Session Establishment

The session establishment procedure of IMS has been defined by 3GPP specification [8]. Figure2 shows a session establishment procedure with media, UE A in domain A and UE B in domain B, UE A sends a SIP INVITE request to P-CSCF, P-CSCF forwards this request to UE A's S-CSCF, S-CSCF A will query DNS or ENUM according to UE B's SIP URI or SIP Tel to

determine the I-CSCF of IMS domain B, then the INVITE request will be forwarded to I-CSCF B, and the INVITE request will be handled in IMS B. When UE B receives ACK, the session is established. Then UE A can communicate with UE B.

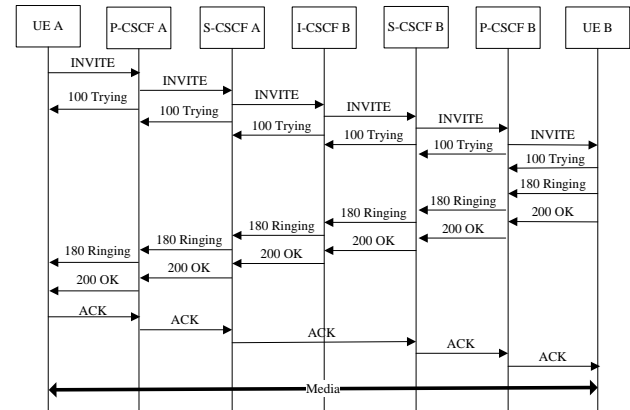


Figure 2. Session establishment procedure of IMS

In Figure2, this session is established in the scenario of once media negotiation, there are also other signaling required for the IMS in order for QoS reservation, involving PRACK and UPDATE in the scenario of twice media negotiation [8].

Further, it should be noted that the signaling path and the media path are different.

III. TVRA METHOD

Threat Vulnerability and Risk Analysis (TVRA) is a method defined by ETSI TISPAN used for an analysis of the threats, risks and vulnerabilities of a telecommunication system, and adopts UML to build a model for system analysis [2].

In TVRA, lots of attributes are defined. Followings will give a simple description for some main attributes.

A. Security Objective

It is means that a system should meet the specific security goal, and clear security objectives of the system must be defined, during the process of system operation, security objectives cannot be changed. Identify the security objectives is the basis of vulnerability analysis for a system.

B. Asset

Anything that has value to the organization can be regarded as asset. In TVRA, three kinds of assets are defined, physical assets (equipment), human assets and logical assets (the information stored in and handled by the physical assets).

C. Weakness

A system may have some weakness, which can be exploited by attacker.

D. Unwanted Incident

Incident such as loss of confidentiality, integrity and/or availability.

E. Threat

Potential cause of an incident that may result in harm to a system or organization.

F. Threat Family

One kind of threats undermines a security objective of a system.

G. Vulnerability

Weakness of an asset or group of assets that can be exploited by one or more threats.

Summarily, TVRA can be described as: Assets may have weaknesses that may be attacked by threats. A threat is enacted by a threat agent, and may lead to an unwanted incident breaking certain pre-defined security objectives. Vulnerability is modeled as the combination of a weakness that can be exploited by one or more threats [2].

IV. COMPREHENSIVE VULNERABILITY ANALYSIS MODEL OF IMS NETWORK

Based on TVRA, this paper extends it and put forward a comprehensive vulnerability analysis model of IMS. In IMS, there are lots of entities and reference points, threats may happen at these entities or reference points, so we add a new attribute of *location* in our model, and also refine the relationship between attributes in TVRA. This model is described in UML as Figure3 shows.

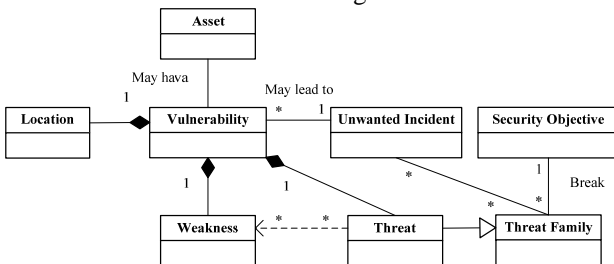


Figure 3. Comprehensive vulnerability analysis model

Step1: Identification of security objective in IMS

Step2: Identification of all assets in IMS

Assets include physical and logical assets.

Step3: Identification of weakness in IMS

Weakness is the original source of vulnerability, from the perspective of security mechanisms, network architecture, used protocol and provided services, deeply analyze the weaknesses of IMS.

Step4: Identification of threat family and threat in IMS

Threats break a certain security objective and with similar means, and also cause the similar unwanted incident are classified as a family, and a threat family can only break a certain security objective, threat family and security objective is many-to-one relationship; threat(such as attack) exploits the weakness, a threat can exploits several weaknesses, threat and weakness is many-to-many relationship.

Step5: Identification of location in IMS

Identify the location according to the entities and reference points in IMS.

Step6: Identification of unwanted incident in IMS

When the weakness exploited by threat, it will cause some damage to the asset, determine the unwanted incident by the damage, unwanted incident and vulnerability is many-to-one relationship.

Step7: Identification of vulnerability in IMS

Based on above steps, combine with asset, weakness, threat, location and unwanted incident according to their relationships. Vulnerability can be described as a vector, that is:

V<Assert, Weakness, Threat, Location, Unwanted Incident, Security Objective>

V. VULNERABILITY ANALYSIS OF IMS NETWORK

A. Security Objective

Multimedia services over IMS require security mechanisms to protect the transmitted information against modification, eavesdropping, damage, imitation [9], and could control the transmitted flow as well as charging. IMS network should meet the following security objectives.

1) *Confidentiality*: It is a feature that in IMS network, the user profile datas, signalings, medias, network topology and other informations will not be leaked or spied to non-authorized users or entities. That is certain informations can only be visible to authorized users or entities which locate at the same security domain.

2) *Integrity*: It is a feature that in IMS network, relevant informations such as signalling and media should remain unchanged without authorization. That is during the periods of transmission, these informations will not be altered, deleted, forged and replayed, etc.

3) *Availability*: It is a feature that in IMS network, informations and services can be visited or used by authorized users and entities. That is hardware and software resources should run efficiently to offer effective services for authorized users or entities. When disaster happens, IMS services should be able to recover quickly and completely.

4) *Accountability*: It is a feature that IMS network should have the ability of charging the services used by users timely and correctly. That is users can not evade or reduce the billing which they should pay.

5) *Authentication*: It is a feature that IMS network should provide a two-way authentication mechanism with high security level. That is IMS network can prevent illegal users from obtaining permissions owned by legal users, enable illegal users can not get IMS services, users can also authenticate IMS network, and network entities also have the ability of mutual authentication. IMS should have the ability of checking the authenticity of participant's identity during the progress of session interaction.

6) *Controllability*: It is a feature that IMS network should have the capability of monitoring and controlling the information's content and transmission. That is IMS can monitor and control informations on the network efficiently.

B. Asset

In IMS network, network element equipments, UEs and data links are divided into physical assets, logical assets have to be deployed in physical assets, such as a SIP message. Parts of assets in IMS are shown in Table I.

TABLE I. ASSETS IN IMS

Logical Asset	Physical Asset
UE IP address	UE, CSCF
UE SIP port number	UE, CSCF
IMPI	UE, CSCF, HSS
IMPU	UE, CSCF, HSS
Digest authentication password	UE, HSS
AKA authentication parameters	UE, HSS
UE Profile	HSS
Network element IP address	CSCF, HSS, AS
Network element service port	CSCF, HSS, AS
Network element domain name	CSCF, HSS, AS
Network topology structure	CSCF, HSS, AS
SIP message	UE, CSCF, Data Link
SDP message	UE, CSCF, Data Link
Diameter message	CSCF, HSS, Data Link
SIP session	UE, CSCF, Data Link
RTP session	UE, AS, Data Link
DNS message	CSCF, DNS, Data Link
ENUM message	CSCF, ENUM, Data Link
TCP protocol stack	UE, CSCF, AS
UDP protocol stack	UE, CSCF, AS
SIP protocol stack	UE, CSCF, AS
Diameter protocol stack	CSCF, HSS
RTP protocol stack	UE, AS
IPSec protocol stack	UE, CSCF

C. Weakness

Weaknesses are the unsafe factors, which are introduced in the period of design, development, deployment and configuration of IMS, weakness is the original source of vulnerability. From the perspective of security mechanisms, network architecture, actual networking, used protocol and provided services, this paper will give an analysis in detail.

1) *Security Mechanisms*: Specifications of 3GPP using two security mechanisms: IPSec and TLS [10]. However, in the actual networking, there has some problems when using IPSec and TLS.

a) *IPSec and NAT*: The original design of IMS assumed that IPv6 would be widely used by the time IMS was scheduled to be deployed. Unfortunately, IPv6 has yet to be largely used on the Internet, and IMS must adopt both IPV6 and IPv4. Because of the abundant address resources of IPv6, every UE can get an independent IP address, IPSec can work normally between UE and P-CSCF. However, IPv4 doesn't have sufficient IP addresses, cannot assign an independent IP to every UE, in order to solve the shortage of IPV4 addresses, NAT[11] is widely used in IPv4 network. In NAT scenario, it requires modification of the packet

header, that is the private IP address and port behind NAT firewall are converted to the public IP address and port, modifying the packet header content violates IPSec's check of integrity and origin authentication. Despite there is a way of IPSec across NAT under UDP, has partly solved the compatibility of IPSec and NAT. But the essential characteristics of IPSec and NAT have determined the two can't be totally compatible. The current lack of IPv6 deployment makes many encryption schemes that rely on end-to-end integrity difficult [12].

b) *TLS and TCP*: TLS is another security protocol to protect communication; authentication for the corresponding network elements during the handshaking procedure can be mutual and is performed by exchanging their certificates, TLS has many of the advantages of IPSec and the successful introduction of the protocol in the wired Internet has proved its usability and effectiveness. However, TLS only applies to TCP, cannot be combined with UDP[13]. Keeping too many TCP connections between UE and P-CSCF or other network elements is a heavy burden and potential security hazard for IMS.

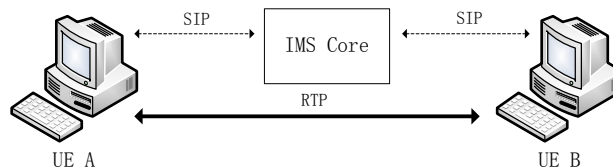


Figure 4. Session establishment procedure of IMS

The problems in the application of IPSec and TLS, might make the networking of IMS not requires data integrity and confidentiality compulsively. IMS network may have weaknesses of 1) signaling without integrity protection, 2) signaling without confidentiality protection, 3) media without integrity protection, and 4) media without confidentiality protection.

In the case of fixed-line access, media streams may connect directly between two UEs, IMS may 5) lack of effective control of media streams, it is also a weakness.

IMS is an open architecture based on IP, which makes IMS network inherit the vulnerability that brought by IP. This weakness is described as 6) network elements have public IP address.

IMS network relies on DNS and ENUM, IMS network also inherit the vulnerability brought by DNS and ENUM, this weakness is described as 7) dependence on DNS and ENUM.

In authentication and controllability level, AKA can be regarded as a good authentication method, however, due to UE, lots of UEs don't support ISIM, AKA is not widely used. HTTP Digest is the most popular authentication method for soft clients in IMS, but due to the HTTP Digest is a password-based authentication method [14], its authentication and certification is insufficient strength. In addition, IMS may have a poor authentication to subsequent SIP messages after registration and may also have a poor controllability of other IP-based messages. This weakness is 8) authentication and controllability mechanism is imperfect.

DoS (Denial of Service) is a simple but effective attack way in IP network. It can cause a greater destruction to the network with a smaller cost, and especially DDoS (Distributed Denial of Service) can cause a serious incident. Development of detection and defending tools is unlikely to every prove 100% effective, there are a lot of difficulties to defend DDoS [2]. IMS network will have the weakness of 9) unable to effectively prevent DDoS.

With the UE is becoming more and more intelligence, in TCP/IP environment, a UE can easily attack another UE, viruses and Trojan horses have already threaten intelligence UE, and compared to the traditional POTS UE, intelligence UE are mostly depend on electric power, 10) UE intelligence is also a weakness.

IMS using SIP as the control signaling, and many IMS services are also realized by SIP. SIP specification [4] does not contain any specific security mechanisms, and the utilization of other well-known Internet security mechanisms is suggested. And as the usage time of SIP protocol is short, there will inevitably some defects in the design and realization progress. A lot of published literatures have pointed out that the SIP protocol has a lot of security issues. Therefore IMS has the weakness of 11) using SIP protocol.

RTP protocol is used for media transmission in IMS; RTP protocol uses synchronization source (SSRC) identifiers as addresses of the peers. SSRCs are unique within the session. There are also some security problems in RTP [15]. For example, as any participant can easily send commands using the SSRC of another participant, it is possible to disturb other participants on the same session. So IMS has the weakness of 12) using RTP protocol.

D. Threat family and threat

As the weaknesses analyzed above, some threats will exploit them to damage IMS. We divide threats into 12 families, each family breaks one security objective, and one or more threats are also illustrated for each family.

1) *Network Spy*: Network spy break *Confidentiality*. Without the protection of confidentiality, it is easy for illegal users to capture signalling or media traffics, throughout network spy, some confidential informations will be visible to attackers, and these informations may help attackets to damage IMS network.

a) *Traffic sniffer*: In the absence of IPSec and TLS, it is easy to use sniffer tools, such as Wireshark to capture SIP messages and RTP media streams, by monitoring network traffic, some e-commerce transaction informations may be guessed, traffic sniffer includes signaling sniffer, media sniffer and traffic analysis, etc. Traffic sniffer use the weaknesses of *signaling without confidentiality protection* and *media without confidentiality protection*.

b) *Scan*: Using scanning tools to scan IMS network, may get some useful inforamtions for attackers, such as the version of operating system which CSCF used, and even the topology structure of IMS network, etc. Scan use the weaknesses of *signaling without confidentiality*

protection, media without confidentiality protection and authentication and controllability mechanism is imperfect.

2) *Session Hijacking Attacks*: Session hijacking attacks break *Integrity*. In a normal session progress, an attacker as a third party to participate in the session, the attacker can insert malicious packets to this session, and can monitor it, and even can be a substitute for a party to take over this session[9].

a) *SIP message tampering*: When SIP messages transport on the network without confidentiality and integrity protection, once intercepted by sniffer tools, it is easy to tamper SIP messages.

b) *SIP Bye attack*: If an attacker obtains the necessary parameters such as Call-ID of a session, then construct a forged SIP BYE request to CSCF, the session will tear down as Figure5 shows.

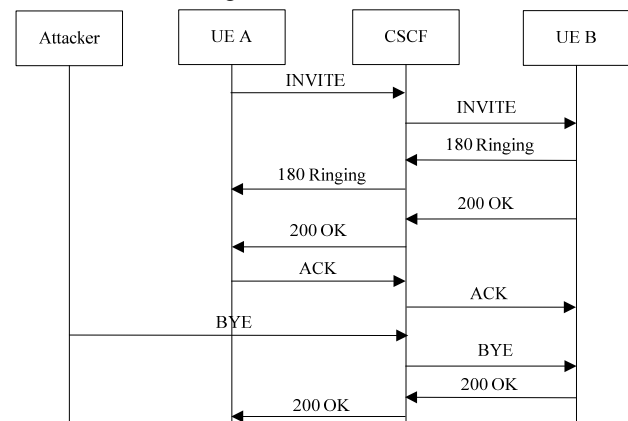


Figure 5. SIP Bye attack possibilities

c) *SIP Cancel attack*: Similarly with Bye attack, cancel attack used to break an establishing session, Bye attack used to break an established session.

d) *SIP Re-Invite attack*: Once a session has been established, an attacker can send a forged SIP Re-Invite request to modify the parameters of the session (e.g., address or port modification).

e) *SIP Update attack*: Similarly with Re-Invite attack, Update attack is utilized to modify the parameters of an establishing session.

In addition, RTP insert attack, RTP replay attack and RTP teardown [15] may threat media's security.

Threats of this family use the weaknesses of *signaling without integrity protection* or *media without integrity protection* and *using SIP protocol* or *using RTP protocol*.

3) *Flooding Attacks*: Flooding attacks break *Availability*. These attacks means attackers launch a large number of requests (such as TCP connection) to the network system in a short time, increase the network's traffic and load to achieve the purpose of DoS. TCP SYN floods, UDP floods, Smurf attack floods are the common flood attacks on the Internet, as the IMS network is also based on IP, these flood attacks in transport layer may also occur in IMS. Flood attacks in control layer will be discussed below.

Diameter message send to HSS is generated according to the SIP message, the Diameter message may also contains the malicious SQL, the SQL may be implemented in the HSS database, and manages to change Alice's first_name to Bob.

```
WWW-Authenticate: Digest realm="telestar.com";
Update subscriber set first_name=Bob
where username='Alice',
nonce="qD2yEcfg3RR09BP2zKHbxayQemj7DwAAIfGkN3vjD
Rw=", algorithm=AKAv1-MD5
.....
```

Figure 9. SQL injection in SIP possibilities

There are similar attacks such as SIP JavaScript injection, SIP Perl injection, RTP JavaScript injection, RTP Perl injection.

Embedded malicious program attacks are use the weaknesses of *using SIP protocol, using RTP protocol and authentication and controllability mechanism is imperfect.*

6) *P-CSCF Discovery Attacks:* P-CSCF discovery attacks break *Availability*. P-CSCF is the entry point for UEs to the IMS core, DHCP DNS is a common P-CSCF discovery method, when domain format of P-CSCF list is returned to UE, UE need to implement a DNS query to find the P-CSCF's IP address. Attackers may break the process of P-CSCF discovery through attacking DNS or other means.

a) *DNS cache attack:* In order to improve the efficiency of DNS queries, DNS cache is used[17], but once DNS cache is poisoned[18] by attacker, in the progress of P-CSCF discovery, a wrong P-CSCF domain name or IP will be returned to UE, and UE may cannot register in the IMS network correctly. More serious, if users register to the attacker's server, users' relevant information will leak to the attacker, however, users may not aware of it, if AKA authentication mechanism is not used. ENUM server may also face this attack.

This attack method uses the weaknesses of *network elements have public IP address and dependence on DNS and ENUM.*

b) *SIP 301/302 message attack:* If a disguised P-CSCF sends SIP 301/302 message[3] to UE, it will enable UE thinks that the current P-CSCF will close service permanently or temporarily. Then the subsequent SIP messages will be redirected to the wrong address.

This attack method uses the weaknesses of *authentication and controllability mechanism is imperfect and using SIP protocol.*

c) *UE configuration tampering:* As UE is becoming more intelligent, some Trojan viruses can modify UE's connection configuration, enables UE cannot correctly connect to the IMS network, but connect to the wrong address instead.

This attack method uses the weakness of *UE intelligence.*

7) *Service Abuse Attacks:* Service abuse attacks break *Availability*. IMS provides a lot of services, and gives

users a lot of convenience. However, these services with inherent potential security risks, if these risks exploited by illegal users, unwanted incidents will be happened.

a) *Refer attack:* Refer method provides a mechanism enables a referrer provides another referee's arbitrary URI. Therefore, the referee as an intermediate provides information to the refer object. The refer object can use this information to decide whether to accept the request from the referee. This mechanism can enable the referee as an eavesdropper, a man-in-the-middle attack can be launched. This threat uses the weakness of *using SIP protocol.*

Additionally, SIP allows third-party registration is also a potential security issue.

8) *Toll Fraud:* Toll Fraud break *Accountability*. In a fixed-line access environment, after a session between UE A and B was established, media streams may directly connect between two UEs, which is shown in Figure10.

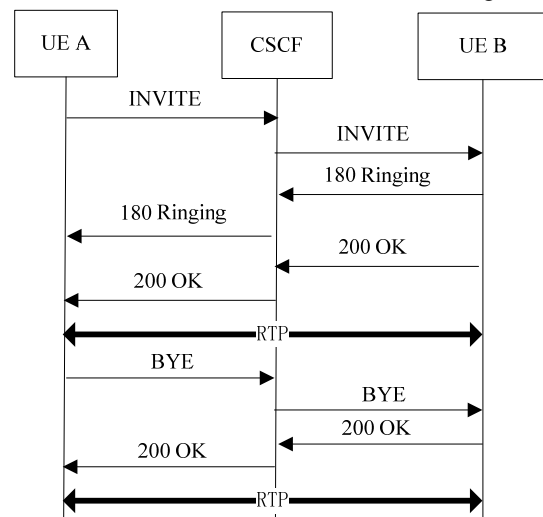


Figure 10. Media theft possibilities

In the common scenario, when UE sends or receives the SIP Bye request, it will release media streams actively. But if UE A and B are all tailor-made equipments, when one UE sends Bye request to CSCF, and CSCF will think that the session is end, and stop accounting. Actually, two UEs don't release the media streams, UE A and B can continue this session, to achieve the purpose of stealing media resources. This threat calls media theft, and use the weakness of *lack of effective control of media streams.*

9) *Server Impersonation Attacks:* Server impersonation attacks break *Authentication*. Attacker could impersonate their own equipments as IMS network elements thought some special means.

a) *P-CSCF in the middle attack:* Without the two-way AKA authentication, based on P-CSCF discovery attacks, UE wrongly believe attacker's equipment is P-CSCF, and UE sends SIP Register message to attacker, attacker modifies the *Via* and *Contact* fields of the Register message to the attacker's own address. When the attacker receives SIP 401 Challenge message, he sends it to UE, when UE sends the second Register message, attacker modifies the *Via* and *Contact* fields again,

then sends it to IMS core, finally attacker will register in IMS using attacker's own IP address combine with UE's IMPU. For IMS core, attacker is a UE, and for UE attacker is a P-CSCF.

If this attack is succeed, UEs will regard the attacker as a P-CSCF, and they will be monitored by the attacker, shown as Figure 11.

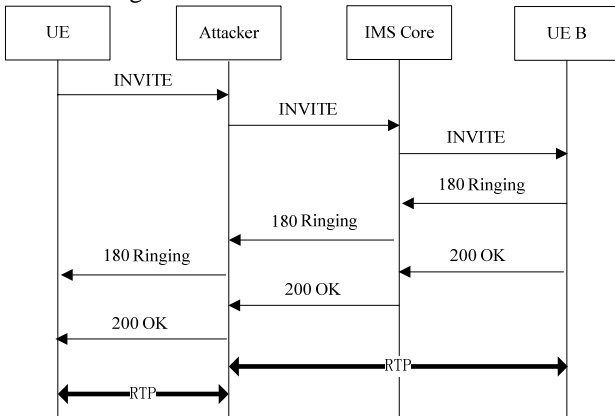


Figure 11. P-CSCF in the middle possibilities

The attacker plays a roll of SIP B2BUA, all messages send from or to UE A can be modified by attacker if necessary, the attacker can monitor the signaling and media traffics of UEs.

b) *Impersonation P-CSCF attack*: In roaming scenario, the UE needs to contact a roaming P-CSCF, then the roaming P-CSCF finds the home I-CSCF by DNS query, attackers may impersonate their own equipment as a roaming P-CSCF, attackers can tamper SIP messages send by UEs, attacker can hijack UE's contact address into any address, and can even do damages to the home I-CSCF.

This threat family uses the weaknesses of *authentication and controllability mechanism is imperfect and using SIP protocol*.

10) *Permission Acquisition Attacks*: Permission acquisition attacks break *Authentication*. Attackers can get some permissions by cracking password or by other methods.

a) *Authentication attack*: Restricted to terminals, most of the current IMS UE select HTTP Digest authentication, it is a username and password-based authentication method, the security level is not high, the specification of HTTP Digest lists several potential attacks, such as replay attack, chosen plaintext attack, batch brute force attack and son on[14].

b) *Illegal invasion*: Using hacking technology to invade IMS entities, and obtain entities' corresponding permissions, then steal informations or do some damages to the IMS network.

Attacks of this family use the weaknesses of *authentication and controllability mechanism is imperfect*.

11) *Spoofing Attacks*: Spoofing attacks break *Authentication*. Through IP spoofing, SIP URI spoofing and other means, the other side will mistakenly believe that the attacker is a trusted.

a) *Short message spoofing*: Shown in Figure12, the IP address of UE A is IP_A, UE A's register port is Port_A, IMPU is sip: userA@telestar.com, if there is no IPSec protection, an attacker can easily sends a forged SIP MESSAGE to IMS, and the forged SIP MESSAGE's original IP address is IP_A, using Port_A as the source port number, and IMPU is userA@telestar.com, when UE B receives this short message, he may believe that this message comes from UE A. The attacker could cheat UE B through this manner.

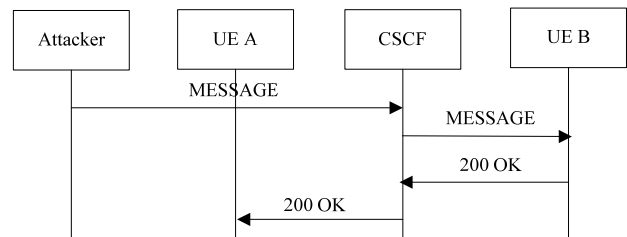


Figure 12. Short message spoofing possibilities

Attacks of this family use the weaknesses of *authentication and controllability mechanism is imperfect and using SIP protocol*.

12) *Unsolicited Communciation Attacks*: Unsolicited communciation attacks break *Controllability*. SPAM over internet telephony (SPIT)[19], because SPIT has the feature of highly real-time, it is difficult for IMS to filter real-time audio and video. Attackers spread advertisements, reactionary remarks, etc., will cause great harm. Similarly, there is also SPAM over Instant Message.

Attacks of this family use the weakness of *authentication and controllability mechanism is imperfect*.

E. Location

Location information is determined by IMS network elements and reference points in Figure1.

F. Unwanted Incident

According to the above analysis, unwanted incident will be divided as TableII. Unwanted incident and threat family is many-to-many relationship.

TABLE II. UNWANTED INCIDENT

Unwanted Incident	Threat Family Num
Loss of privacy	1
Damage of session	2
Single-user deny of service	5,6
Multi-user deny of service	3,4,5,6
Abuse of system	7,10
Acquisition of permission	10
Impersonation of a user	11
Impersonation of a server	9
Theft of services	8
Harassment of users	12

G. Vulnerability

Above has been completed the analysis of security objective, asset, weakness, threat and unwanted incident. Limited to pages, only some of the vulnerability of register and session are described in TableIII. Other vulnerabilities can be deduced in this model.

TABLE III. SOME VULNERABILITY OF IMS

ID	Asset	Weakness	Threat	Location	Unwanted Incident	Security Objective
1	SIP Session (Call-ID header)	Signaling without confidentiality protection/ Using SIP protocol	SIP sniffer	Gm	Loss of privacy	Confidentiality
2	Network topology structure	Authentication and controllability mechanism is imperfect	Scan	Gm/Mw	Loss of privacy	Confidentiality
3	SIP Session	Signaling without confidentiality protection/ Using SIP protocol	SIP Bye attack	Gm	Damage of session	Integrity
4	RTP Session	Media without integrity protection/ Using RTP protocol	RTP insert attack	UE-UE	Damage of session	Integrity
5	SIP Message (Register)	UE intelligence	UE configuration tampering	UE	Signal-user deny of service	Availability
6	SIP Message (Register)	Dependence on DNS and ENUM	DNS cache attack	Gm	Multi-user deny of service	Availability
7	SIP protocol stack	Network elements have public IP address/ Unable to effectively prevent DDoS	SIP Register flooding	Gm/CSCF	Multi-user deny of service	Availability
8	User profile	Authentication and controllability mechanism is imperfect/ Using SIP protocol	SIP SQL injection	HSS	Multi-user deny of service	Availability
9	RTP Session	Lack of effective control of media streams	Media theft	UE-UE	Theft of services	Accountability
10	SIP Message (Register)	Authentication and controllability mechanism is imperfect/ Using SIP protocol.	P-CSCF in the middle attack	Gm	Impersonation of a server	Authentication
11	SIP Session	Authentication and controllability mechanism is imperfect/ Using SIP protocol.	Short Message spoofing	Gm	Impersonation of a user	Authentication
12	RTP Session	Authentication and controllability mechanism is imperfect	SPIT	UE-UE	Harassment of users	Controllability

VI. CONCLUSION

This paper presents a vulnerability analysis model of IMS network, and based on this model, we give a systematic analysis for the vulnerability of IMS, have analyzed the weaknesses and faced threats of IMS emphatically, and can also provide the basis for security assessment of IMS network.

As the original source of vulnerability is weakness, the working of how to reduce the vulnerability of IMS should focus on how to reduce the weakness, which needs further study.

REFERENCES

- [1] 3GPP TS 23.228 V8.5.0 (2008-06)-IP Multimedia Subsystem (IMS); Stage 3 (Release 8).
- [2] ETSI TS 102 165-1 V4.2.1 (2006-12)-Method and Performa for Threat, Risk, Vulnerability Analysis.
- [3] ETSI ES 282 001 V2.0.0 (2008-03)- NGN Functional Architecture.
- [4] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initial Protocol," RFC 3261, June 2002.
- [5] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "DiameterBase Protocol," RFC3588, September 2003.
- [6] M. Handley and V. Jacobson, "SDP: Session Description Protocol," RFC 2327, Apr. 1998.
- [7] H. Schulzrinne et al., "RTP: A Transport Protocol for Real-time Applications," RFC 3550, July.2003.
- [8] 3GPP TS 24.229 V8.5.0 (2008-06)-IP Multimedia Subsystem (IMS); Stage 3 (Release 8).
- [9] Dimitris geneiatakis, Tasos dagiuklas, "Suvery of security vulnerability in session initiation protocol," 3rd IEEE Communications Surveys & Tutorials, Quarter. 2006.
- [10] 3GPP TS 33.203 V7.9.0 (2008-04)-Access security for IP-based services;(Release 7).
- [11] P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Consideration," RFC 2663, August.1999.
- [12] 3GPP TS 33.978 V7.0.0 (2007-07)-Security aspects of early IP multimedia subsystem (IMS);(Release 7).
- [13] T. Dierks, C. Allen, "The TLS Protocol Version 1.0," RFC 2246, January.1999.
- [14] J. Franks, P. Hallam-Baker, J. Hostetler et al., "HTTP Authentication: Basic and Digest Access Authentication," RFC 2617, June 1999.
- [15] Ville Hallivuori, "Real-time Transport Protocol (RTP) security," Seminar on Network Security Tik 1101501,2000
- [16] Dimitris Geneiatakis, Georgios Kambourakis, et al., "SIP Message Tampering: THE SQL Code INJECTION Attack," Proc. 13th Int'l. Conf. Software, Telecomm and Computer Networks (SoftCOM 2005) IEEE, Split, Croatia, September. 2005.
- [17] Mockapertis P, "Domain names-implementation and specification," RFC 1035, November. 1987.
- [18] D. Atkins, R. Austein, "Threat Analysis of the Domain Name System (DNS)," RFC3833, August. 2004.
- [19] D. Shim and C. Shim, "Voice Spam Control with Gray Scaling," 1th Workshop on Securing Voice over IP, December.2004.