VoIP Security

2010. 4. 22.
KISA
Kim, JoongMan
seopo@kisa.or.kr
I. Background
II. VoIP Concept
III. VoIP Security Issues & Case
IV. Countermeasures
V. Other Issues
Provides multimedia communications over IP networks
Low-cost alternative to PSTN calling
By the end of 2009, total VoIP users were about 6.2 million
I-2. Background - Environment

- (Infra) PSTN → WiFi, Wibro, PLMN ...
- (Device) Various platform: VoIP Phone, WiFi Phone, Smart Phone ...
- (Service) Convergence Service: Phone banking, Video Call, FMC ...

**<Integrated infra>**

- WiFi
- Wibro
- BCN
- Internet
- PLMN

**<Various Service>**

- Voice
- Video
- Messenger
- Weather
- Stock
- Banking

**<Platform>**

- VoIP Phone
- Smart Phone
- WiFi Phone

**<Application>**

- fring
- GizmoVoIP
- buzz!
- NJMI
- Skype
I-3. Background - Trend

- Google VoIP Security Keyword Searching Trend
- VoIP Security Articles: Concentrated on from 2005 to 2007
- Threat Comparison: VoIP Security, Web hacking, DDoS

VoIP Security Keyword Searching

Google Trends

VoIP Security Articles

News Archives

Google T

Averages

Regions:
1. India
2. South Korea
3. Singapore
4. Malaysia
5. Australia
6. United States
7. Israel
8. Canada

Cities:
1. Bangalore, India
2. Seoul, South Korea
3. Ottawa, Canada
4. Mumbai, India
5. Dallas, TX, USA
6. Washington, DC, USA
7. San Francisco

Languages:
1. Korean
2. English
3. Dutch
4. German
5. Italian
6. Chinese
7. Portuguese
8. French

Threat Comparison
Voice Over IP (VoIP)

- Signaling protocols: SIP, H.323, SCCP, MGCP, or MegaCo signaling protocol
- Media protocols: RTP media protocol
II-2. VoIP Concept

SIP
- RFC 3261
- “The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants.”

SDP
- IETF RFC 2327
- “SDP is intended for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation.”
- SDP includes:
  - The type of media (video, audio, etc.)
  - The transport protocol (RTP/UDP/IP, H.320, etc.)
  - The format of the media (H.261 video, MPEG video, etc.)
  - Information to receive those media (addresses, ports, formats, etc)
  - Crypto keys
II-3. VoIP Concept

- INVITE: create a session
- BYE: terminates a session
- ACK: acknowledges a final response for an INVITE request
- CANCEL: cancels an INVITE request
- REGISTER: binds a public SIP URI to a Contact address
- OPTIONS: queries a server for capabilities
- SUBSCRIBE: installs a subscription for a resource
- NOTIFY: informs about changes in the state of the resource
- MESSAGE: delivers an Instant Message
- REFER: used for call transfer, call diversion, etc.
- PRACK: acknowledges a provisional response for an INVITE request
- UPDATE: changes the media description (e.g. SDP) in an existing session
- INFO: used to transport mid-session information
- PUBLISH: publication of presence information
II-4. VoIP Concept

- **RTP**
  - Real-time Transport Protocol
    - RFC 3550
    - Standardized packet format for delivering audio and video over IP
    - Frequently used in streaming media systems

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+===============================================
|V=2|P|X| CC | M | PT | sequence number |
+===============================================
  | timestamp |
+===============================================
  | synchronization source (SSRC) identifier |
+===============================================
  | contributing source (CSRC) identifiers |
| .... |
```

- **CODECs**
  - Audio Codec: G.711, G.723, G.729
  - Video Codec: H.263, MPEG4, H.264
**User Agents**
- Clients – Make requests
- Servers – Accept requests

**Server types**
- Proxy Server
- Registrar Server
- Location Server

**Gateways**
II-6. VoIP Concept – SIP Call Flow

Alice Calls Bob
Is Bob there?
No. I need Bob.
Thanks. Bye.

Bob

Steve answers Bob’s phone
Sorry, no, can I help you

Outbound Proxy
INVITE
180 Ringing
100 Trying
200 OK

Inbound Proxy
BYE
INVITE
100 Trying
200 OK
180 Ringing

RTP Voice

Alice

Bob
III-1. VoIP Security Issues & Case

- Containing most Internet Security Threats
- Eavesdropping, Hacking, DDoS → Service Quality Low, Toll Fraud, Privacy infringement

VoIP Service

- Eavesdropping
- INVITE floods, DDoS
- BYE, Cancel attack
- VoIP SPAM
- VoIP toll fraud (SQL Injection, Proxy bypass)
Eavesdropping

- Sniffing conversation between two VoIP phones
  - Wireshark/Cain can identify VoIP calls, and even comes with a Player to replay the conversation
III-3. VoIP Security Issues

Registration hijacking (Relay)
- Attacker can replay this request and substitute another IP address, thereby redirecting all calls to the attacker.

Before modifying:
- Session Initiation Protocol
  - Request-Line: REGISTER sip:168.188.129.161 SIP/2.0
  - Contact: sip:168.188.129.161;tag=3
  - From: "X-Lite"<sip:168.188.129.161@192.168.1.10>
  - Via: SIP/2.0/UDP 168.188.129.154;branch=z9hG4bK-8754z-32110f605e39fa77-1-8754z-:rport
  - Max-Forwards: 70
  - Content-Length: 0

After modifying:
- Session Initiation Protocol
  - Request-Line: REGISTER sip:168.188.129.161 SIP/2.0
  - Contact: sip:168.188.129.164;tag=11084;rrinstance=ef06bd70cedf9f57
  - From: "X-Lite"<sip:168.188.129.161@192.168.1.10>
  - Via: SIP/2.0/UDP 168.188.129.154;branch=z9hG4bK-8754z-32110f605e39fa77-1-8754z-:rport
  - Max-Forwards: 70
  - Content-Length: 0

Same Authentication:
- Authentication Scheme: Digest
  - Username: "6001"
  - Realm: "asterisk"
  - Nonce value: "042a0eb"
  - Authentication URI: "sip:168.188.129.161"
  - Digest Authentication Response: bb42f68fe405c2b6dbf0d3238d819e
  - Algorithm: MD5
SIP Flooding DOS attack

- Attacker sends a large amount of INVITE/REGISTER requests to the ‘victim’
III-5. VoIP Security Issues

- Intentional interruption of service
  - Dropping the call (terminating conversation) by sending spoofed BYE/CANCEL message
VoIP SPAM
- Voice SPAM refers to bulk, automatically generated, unsolicited phone calls

“Insurance, Advertisement ~~~”
**III-7. VoIP Security Issues**

- **SIP Toll Fraud**
  - Attacker gains access to a VoIP network (proxy or gateway) and makes unauthorized calls (usually long distance or international)
  - exploiting weak usernames and passwords, open proxy, and other application-level attacks

**SIP SQL injection attack**

```
REGISTER SIP: home1.de SIP/2.0
Authorization: Digest Username= "user_private@home1.de;delete table subscriber",
realm="home1.de", nonce="", uri="SIP: home1.de" resonce=
```

User DB table modification

Attacker
Softphone copy
- Reusing user’s setting information (username, password, domain, ...)

Data Copying

User A (6006)

User A (6006')

- RTP Insertion/Mixing
  - Injecting sound files into an RTP media stream (a voice conversation between two or more IP phones)

Mixing/interlacing the pre-recorded audio with the target audio stream has completed.

```
bt rtpmixsound_v3.0 # 음성트래픽 올레 삐어서 보내가~
bt rtpmixsound_v3.0 # ./rtpmixsound -a 172.16.1.153 -A 19276 -b 172.16.1.152 -B 17424 hello_sidny_mod.wav -f 1 -j 70
```
Extracting Touch Tones from Recorded Calls

- DTMF Decoder: Telebanking account numbers
VoIP Phishing

- Similar to email phishing, but with a phone number delivered through email or voice
- When the victim dials the number, the recording requests entry of personal information
There are Specialized Hacking Tools

- SIPScan - enumerate SIP interfaces
- TFTPBrute - TFTP directory attacking
- UDP and RTP Flooder - DoS tools
- hping2 – TCP session flooding
- Registration Hijacker - tool to take over H.323 session
- SIVUS - SIP authentication and registration auditor
- Vomit - RTP Playback
- VOIP HOPPER – IP Phone mimicking tool
- LDAPMiner - collect ldap directory information
- Dsniff - various utilitarian tools (macof and arpspoof)
- Wireshark (Ethereal) / tcpdump - packet capture and protocol analysis
- Cain&Abel – recording VoIP conversation, cracking password,...
Searching for attack tools

- www.securityfocus.com/bid
Citibank UK Call bombing attack (‘09.9)

- Send multiple SIP INVITE to open SIP gateways and PBXs → call noise
- But is this a DoS attack on Citibank? Why call the Citibank on a Sunday 5 a.m.?

※ Norwegian Honeynet Project 2009.09.20

---

**Citibank UK number was target for a “lawnmower” telephone attack today!**

September 20th, 2009 by sjur (2) Analysis

Citibank is or has been under a telephone calling attack latest 12 hours. Here I will explain the attack and how it was done.

Have you seen the movie “lawnmower man”, when in the phones rings in the who city? This was the aim for today’s attack on Citibank in UK. The attack was simple, but probably effective when it was done. Send SIP INVITE to open SIP gateways and PBXs with an IP that will actually use the traditional phonesystem (POTS) to call the target. Suddenly you need DoS protection on your traditional lines...

- 180 Ringing 0042075005000@67.170........
- 403 Not Found 011442075000@67.170......

Target

INVITE sip:00442075005000@67.170,104,216
INVITE sip:011442075005000@67.170,104,216
INVITE sip:0442075005000@67.170,104,216
INVITE sip:0000442075005000@67.170,104,216

And more...
III-15. Case 2

Germany IP Phone Forum ('08.9)
- Call Scan DoS attack for german users
- Generate random Call-ID and forging URI information

※ Heise.de 2008.09.23
NANOG (North American Network Operators Group) (’09.4)

- Exponential increase on VoIP traffic
  - 300GB (incoming), 400GB (outgoing) signaling traffic for 24 hours
  - Total RTP traffic for 24 hours is only in the region of 150 Kb -- so a vast unbalance

※ NANOG mail archive 2009.04.10
Skype wiretap (‘09.8)

- Recording Skype phone calls on Windows PCs
- Bypassing Skype's encryption—SRTP, AES

**New Trojan Snags Skype Calls on Windows PCs**

Trojan Peskyspy beats Skype encryption through Windows API attack. How serious is the threat?

August 28, 2009

By Alex Goldman

More stories by this author.

A new Trojan is recording Skype phone calls on Windows PCs, security research firm Symantec (NASDAQ: SYMC) reported today.
Skype SMS botnet(’09.11)

- Detected by Trend Micro as TROJ_VILSEL.EA
- Steals a user’s contact list, phone numbers, location, and other information

※ TrendLab Malware Blog, 2009.11.26
U.S. Government, $5.5 billion toll fraud ring for targeting enterprise PBXs ('09.6)
- Fraudsters controlled the hacked PBXs and, used them to make long-distance calls.

※ Computer World Security, 2009.10

(1) Open public long-distance calling centers in Italy and Spain
(2) Hack the companies' PBXs in U.S.
(3) Fraudsters controlled the hacked PBXs and, charging the company to make long-distance calls
I telecom, 110 million won toll fraud call through hacking PBX (’09.10)

- After attacker hacked PBX of I telecom, making a international call to Maldives and Somalia

VoIP 해킹 위협이 현실로…1억원 전화요금 고지 피해

비디오 캡션의 이념에 따라 사내 VoIP 교환기 해킹 당해, 해결책 부재로 피해액 KT 간 문쟁 소지도

[디지털데일리] 2009년 12월 01일(화) 오전 05:26

사내 VoIP 교환기 해킹 당해, 해결책 부재로 피해액 KT 간 문쟁 소지도

1일, 피해를 입은 복정통신사업자 발행 관계자 세시(휘) 해킹으로 1억 1000만원 이상의 막대한 대폭이 발생한

참여 경로

1. VOIP Gateway
2. Server
3. PSTN

발신자
IV-1. Countermeasures

- Segment networks into separate VLANs
  - Voice network
  - Data network
  - Monitoring and control network
IV-2. Countermeasures

**VoIP Security Threat**
- Eavesdropping
- Registration hijacking (Relay)
- SIP Flooding DoS Attack
- Intentional interruption of service
- VoIP SPAM
- SIP Toll Fraud
- RTP Insertion/Mixing

**Countermeasure**
- Encryption (TLS, SRTP, MIKEY)
- Authentication (HTTP Digest...)
- VoIP IPS/Firewall
IV-3. Countermeasures

VoIP Security Guideline

Diagram showing the use of SIP Proxy, HTTP Digest, TLS/IPSec/DTLS, Registrar, S/MIME, SRTP(MIKEY/SDES), and VoIP Phone in a VoIP security framework.
IV-4. Countermeasures

- Maintain VoIP application server updates
  - VoIP Phone, SIP Server
  - IP-PBX, Soft Switch
    - Install current Operating System patches
    - Install current application software patches
V. Other Issues - Legal

- **Lawful Intercept**
  - CALEA / Law Enforcement
  - the Protection of Communications Secrets Act (통신비밀보호법 개정 논의)
  - Key Recovery

- **E911**
  - Emergency Call(119)
  - User location(Privacy?)
MVoIP (Mobile VoIP)

- VoIP over Wi-Fi
  - KT FMC (Qook & Show)
- VoIP over 3G
  - AT&T, Verizon Wireless
VoIP Security References

- NIST - Security Considerations for Voice Over IP Systems, 2005
- Practical VoIP Security, Syngress Publishing © 2006
- Voice over IP Security Alliance (VOIPSA) www.voipsa.org
- KISA-VoIP 정보보호 가이드라인, 2007
Thank you.