Research Challenges in Securing VoIP

Dr. Xinyuan Wang
Assistant Professor
George Mason University

What Today's Talk is All About?

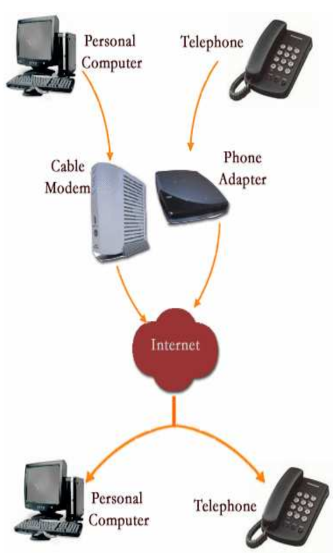
- Voice over IP (VoIP) basics
  - Signaling, voice stream, billing
- Security threats to VoIP
  - What are they?
  - How real are they?
  - Current VoIP security mechanisms
- Why securing VoIP is so challenging?
  - Open architecture, it's Internet
  - No prior established trust between caller & callee
  - Key management challenges
- Objectives of this tutorial
  - Bring the attention of the research community to the problems of VoIP security
  - Discuss the research challenges and open problems in securing VoIP
  - Seek your insight on securing VoIP

Outline

- Introduction
  - Motivation
- VoIP basics
  - Signaling, voice stream, billing
  - Security mechanisms
- Threats to VoIP security
  - Registration hijacking
  - DoS
- Exploits of VoIP security
  - Billing attack
  - Nuisance call
- Mitigations to VoIP exploits
  - IDS, corss-protocol correlation
- Research challenges and open problems
  - NAT traversal, key management

Proliferation of VoIP

- People are moving from POTS to VoIP service
  - VoIP is cheaper, more convenient and flexible, and it provides more features
- The number of residential VoIP subscribers worldwide is expected to grow from
  - current 38 million
  - to 267 million by 2012
- Types of VoIP
  - Managed
    - Vonage, AT&T, Verizon etc.
  - Unmanaged
    - Computer to computer VoIP (e.g., Skype)



Expectations on VoIP

- Confidentiality Security – No.1 concern
- E-911
- Lawful surveillance
- QoS

Security Requirements on VoIP

- Authenticity
  - When A dials B's number, the call will reach B.
  - The incoming call is really from who it claims to be – caller ID is authentic
- Confidentiality, privacy and anonymity
  - No one other than the caller(s) and callee(s) should
    - have access to the conversation content
    - Even know that Alice and Bob have talked over VoIP
- Integrity
  - The call signaling and content have not been tempered with
- Temper resistant billing
  - Service provider – no service stealing, toll fraud
  - Subscriber – no overcharge
- Availability
  - be resilient to denial-of-service (DoS) attack

Key Functional Components of VoIP

- VoIP signaling
  - Responsible for establishing, managing, tearing down VoIP sessions
  - H.323 – 1996 ITU
  - MGCP – 1999 IETF RFC
  - **SIP (Session Initiation Protocol)** – 1999, 2002 IETF RFC
    - The dominant VoIP signaling protocol
- VoIP voice stream
  - RTP (Real-time Transport Protocol)
  - SRTP (Secure RTP)
- VoIP billing
  - Indispensable for VoIP service providers (e.g., Vonage, AT&T, Vonage)

SIP Overview

- SIP is an IETF standard
  - RFC 2543 of 1999 (obsolete)
  - RFC 3261 of 2002
- SIP is
  - "an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants" (RFC 3261)
  - Text based, very similar to HTTP
- SIP sessions include
  - Internet telephone call
  - Multimedia conferences
  - Instant messaging
  - etc.

SIP Functionalities

- Learn, determine the location, availability of remote communicating party
  - Registration
  - Call routing
  - Call redirection
- Establish, a session between end points
  - Call setup, transfer, termination
- Negotiate the media capability
  - Use SDP (Session Description Protocol) to specify the media parameters (e.g., IP address, port number, codec)

SIP Components

- User Agents – owned/used by subscribers
  - User agent client (UAC) – who initiates a call
  - User agent server (UAS) – who receives a call
- SIP Servers – maintained by service providers
  - Proxy server
    - relays the signaling messages (and potential voice streams) between the caller and callee
  - Location server
    - Keeps where a subscriber's UA is currently at (the IP address)
  - Registrar server
    - Accept registration from subscribers about their current locations
    - Keeps track subscribers' whereabouts at Location server
  - Redirect server
    - Provides information about next hop to a subscriber

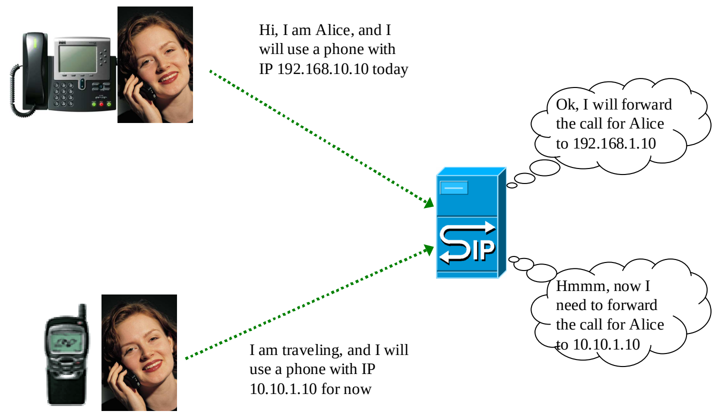
SIP Messages

- Two types
  - Request – identified by a method name
  - Response – identified by a number similar to HTTP
- SIP request messages
  - REGISTER – tell where the UAC is currently at
  - INVITE – initiate a call to someone
  - BYE – terminate an established call
  - ACK – acknowledge the receipt of some message
  - CANCEL – quit from an ongoing call setup
  - OPTION – to query the capability of a server

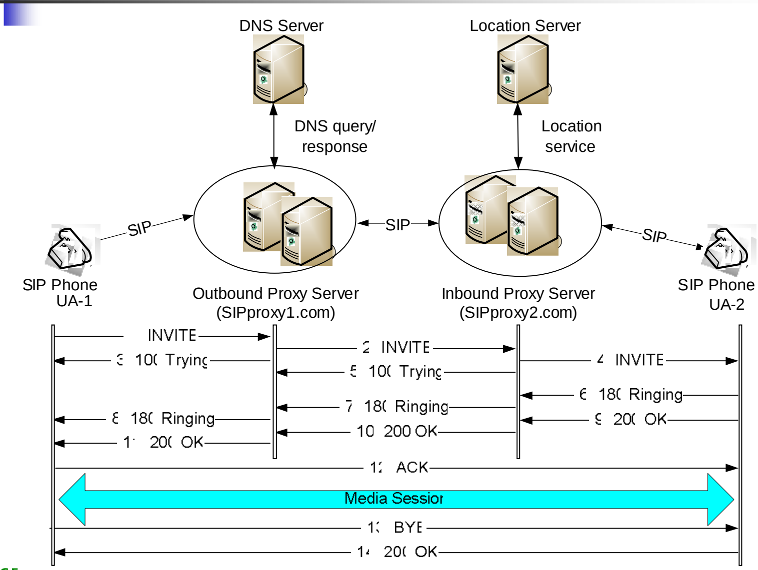
SIP Messages (cont'd)

- SIP response messages
  - 1xx Provisional – 100 Trying, 180 Ringing
  - 2xx Successful – 200 Ok
  - 3xx Redirection – 301 Moved Permanently, 302 Moved Temporarily
  - 4xx Failure – 404 Not Found, 410 Gone, 403 Forbidden
  - 5xx Server Failure – 503 Service Unavailable
  - 6xx Global Failure – 600 Busy Everywhere

SIP Registration



SIP Message Flow of Normal Call Setup & Tear Down



VoIP Security

- VoIP signaling security
  - Protect the authenticity, integrity of the signaling message
- VoIP voice stream security
  - Protect the authenticity, integrity and confidentiality of the voice content (including any keys pressed)
- VoIP billing security
  - Prevent service theft, toll fraud, undercharge, overcharge

SIP Security Mechanisms

- SIP does NOT define its own security mechanism, it reuses existing security mechanisms for HTTP, SMTP whenever possible
- Two building blocks of SIP security mechanisms
  - Authentication
    - HTTP digest authentication
  - Encryption
    - IPsec, TLS, S/MIME
- SIP authentication and encryption can NOT be applied to the whole SIP messages from end-to-end
  - Intermediate SIP proxies need to modify and insert SIP message fields
    - Add via field
    - Change request URI due to call-redirection
- SIP security is hop-by-hop

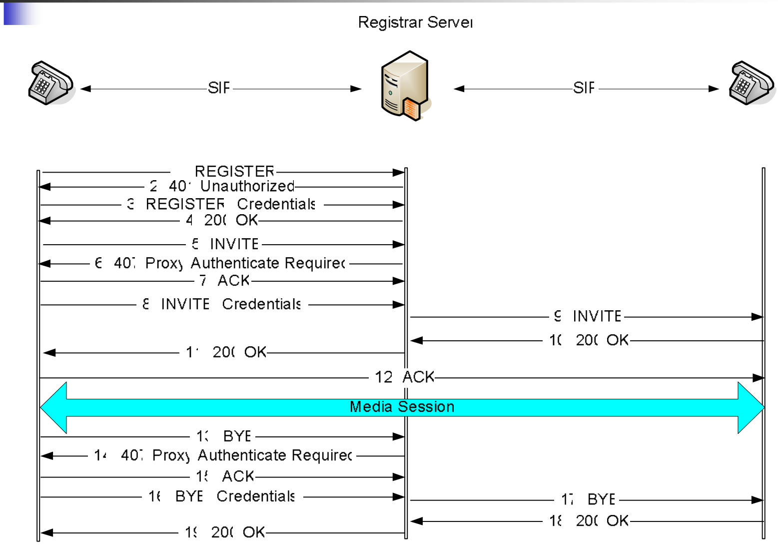
HTTP Digest Authentication

- Provides
  - one-way authentication
    - Identify UAC to a UAS or SIP Proxy
    - Does NOT identify UAS or SIP proxy!
  - anti-replay protection
- Assumes the two parities involved share a secret password
  - Usually hard-coded in the UAC (SIP phone adaptor)
- Uses challenge/response
  - Response = F(nonce, username, password, realm, SIP-method, request-URI)
- Must be supported by all SIP compliant UA and SIP servers

SIP Security Mechanisms (cont'd)

- TLS
  - Can provide authentication, integrity, confidentiality
  - But authenticate the server only
  - Applied hop-by-hop
  - All SIP compliant servers MUST support TLS
  - UAs are strongly recommended to support TLS
    - Each UA (SIP) has its own certificate?
- IPsec
  - Can provide authentication, integrity, confidentiality
  - No SIP component is required to support IPsec
  - Can be applied hop-by-hop
  - Key management issues
    - Setting up security association with every UA is too expensive
- S/MIME
  - Can provide some degree of end-to-end authentication, integrity or confidentiality for most SIP header fields
    - Excluding Request-URI, Via, Record-Route, Route, Max-Forwards, and Proxy-Authorization
  - Require PKI to be effective
  - No SIP component is required to support S/MIME

Message Flow of SIP Authentication



Unauthenticated INVITE Message

```
Session Initiation Protocol
  Request line: INVITE sip:******3255@d.voncp.com:10000 SIP/2.0
  Method: INVITE
  Message Header
   Via: SIP/2.0/UDP 192.168.0.108:10000;branch=z9hG4bK-85c98d52
   From: ***-***-3953 <sip:1******3953@d.voncp.com:10000>;
     tag=6297ece2276a6406o0
   To: <sip:******3255@d.voncp.com:10000>
   Remote-Party-ID: ***-***-3953 <sip:1******3953@d.voncp.com:10000>;
    screen=yes; party=calling
   Call-ID: a6b81312-da84f396@192.168.0.108
   CSeq: 101 INVITE
   Max-Forwards: 70
   Contact: ***-***-3953 <sip:1******3953@192.168.0.108:10000>
   Expires: 240
   User-Agent: 0013101DCFBB Linksys/RT31P2-3.1.6(LI)
   Content-Length: 308
   Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER
   Supported: x-sipura
   Content-Type: application/sdp
Session Description Protocol
  Session Description Protocol Version (v): 0
  Owner/Creator, Session Id (o): - 2305 2305 IN IP4 192.168.0.108
    . . .
  Connection Information (c): IN IP4 192.168.0.108
    . . .
  Media Description, name and address (m): audio 10076 RTP/AVP 2 0 8
   18 100 101
```

407 Authentication Required Message

```
Session Initiation Protocol
  Status line: SIP/2.0 407 Proxy Authentication Required
  Status-Code: 407
  Message Header
   Via: SIP/2.0/UDP 192.168.0.108:10000;branch=z9hG4bK-85c98d52
   From: ***-***-3953 <sip:1******3953@d.voncp.com:10000>;
    tag=6297ece2276a6406o0; natted=xx.xxx.102.135
   To: <sip:******3255@d.voncp.com:10000>
   Call-ID: a6b81312-da84f396@192.168.0.108
   CSeq: 101 INVITE
   Proxy-Authenticate: Digest realm="69.59.227.87",
    domain="sip:69.59.227.87", nonce="2036652154", algorithm=MD5
   Max-Forwards: 15
   Content-Length: 0
```


Authenticated INVITE Message

```
Session Initiation Protocol
  Request line: INVITE sip:******3255@d.voncp.com:10000 SIP/2.0
  Method: INVITE
  Message Header
   Via: SIP/2.0/UDP 192.168.0.108:10000;branch=z9hG4bK-511400f2
   From: ***-***-3953
    <sip:1******3953@d.voncp.com:10000>;tag=6297ece2276a6406o0
   To: <sip:******3255@d.voncp.com:10000>
   Remote-Party-ID: ***-***-3953
    <sip:1******3953@d.voncp.com:10000>;screen=yes;party=calling
   Call-ID: a6b81312-da84f396@192.168.0.108
   CSeq: 102 INVITE
   Max-Forwards: 70
   Proxy-Authorization: Digest username="1******3953",
    realm="69.59.227.87", nonce="2036652154",
    uri="sip:******3255@d.voncp.com:10000", algorithm=MD5,
    response="690680e4e138b38c1ba95271cc691b47"
   Contact: ***-***-3953 <sip:1******3953@192.168.0.108:10000>
   Expires: 240
   User-Agent: 0013101DCFBB Linksys/RT31P2-3.1.6(LI)
   Content-Length: 308
   Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER
   Supported: x-sipura
   Content-Type: application/sdp
Session Description Protocol
  Session Description Protocol Version (v): 0
  Owner/Creator, Session Id (o): - 2305 2305 IN IP4 192.168.0.108
    . . .
  Session Name (s): -
  Connection Information (c): IN IP4 192.168.0.108
    . . .
  Media Description, name and address (m): audio 10076 RTP/AVP 2 0 8
   18 100 101
```

Secure RTP

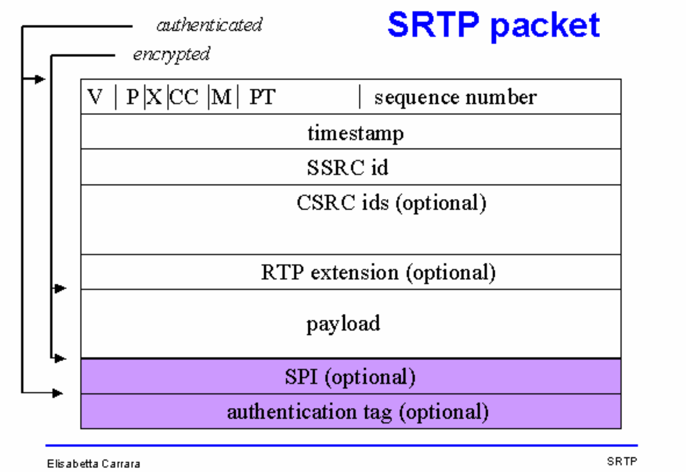


Image from IETF proceedings

Threats to VoIP Security

- Service stealing
  - Steal minutes from VoIP service provider
  - Call at other subscriber's expense
- Service disruption against
  - the VoIP infrastructure
  - individual subscriber
  - terminate established calls
  - prevent certain calls from being established
- Call hijacking
  - Registration spoofing
  - Unauthorized call redirection
  - Taking over established VoIP call via re-INVITE
- Interception and modification
  - Conversation alteration – mix, change the RTP voice stream

Threats to VoIP Security (cont'd)

- Eavesdropping
  - Wiretap and traffic analysis
- VoIP fraud
  - Voice phishing (aka vishing)
- Annoyance
  - SPIT (Spam over Internet Telephony)
  - Nuisance call
- Attack against others
  - Divert VoIP traffic to flood someone
- VoIP based botnet
  - What if attacker compromises the softphone running in the laptop or handheld?

VoIP Service Stealing Case

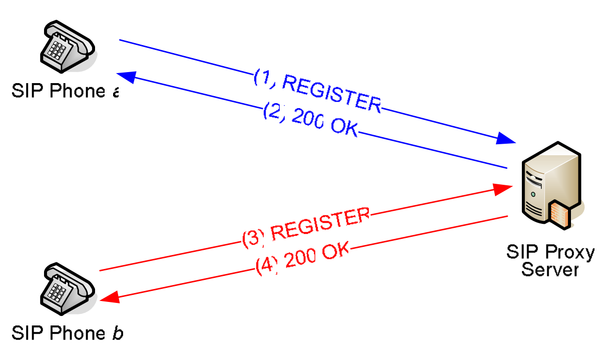
- In June 2006, FBI arrested Pena and Moore for VoIP fraud
  - They
    - broke into networks of 15 VoIP service providers and
    - routed calls through them
    - sold the stolen (up to 10million) minutes at rate as low as 0.4 cents a minute to telecommunications providers
  - One victim VoIP service provider handled 500,000 calls in 3 weeks
  - http://vonmag.com/editorial/web-exclusives/voip-fraud-hack

SIP Phone Registration Spoofing

- Before a SIP UA (i.e. phone) can be used to make or receive a call, it must register itself so that SIP proxy server knows it's current IP address.
- What if some attacker send spoofed REGISTER message to the registrar to trick the registrar into believing that the victim SIP phone is at an IP address chosen by the attacker
  - All the calls to the victim will reach attacker's phone!
- What about SIP digest authentication?
  - The SIP registrar does require authentication for registration
- Assuming the attacker does not know the secret password shared between the victim SIP phone and the registrar, can attacker still spoof registration
- Yes!

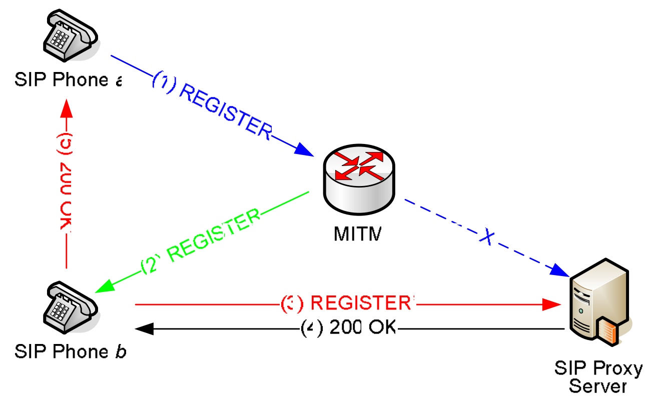
SIP Phone Registration Spoofing

- The SIP digest does NOT cover the IP address of the SIP phone!
- The registrar actually uses the source IP address of the packet containing the REGISTRER message
- The attacker could simply replay the legitimate REGISTER message from different IP address



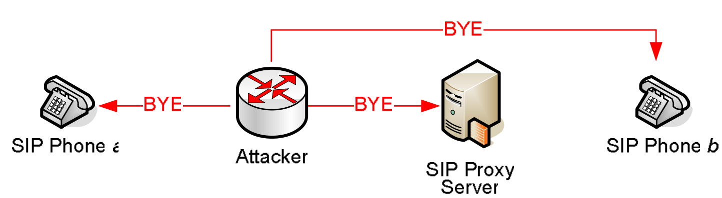
SIP Phone Registration Hijacking

- With a MITM, attacker could completely hijack calls to the victim



Fake BYE to Terminate Established SIP Call

- Attacker could terminate any established SIP call by sending fake BYE message to the SIP phone(s) and/or SIP proxy
- SIP proxy requires digest authentication, so it could detect fake BYE and ignore it.
- Existing SIP phones however will honor any BYE message with correct Call-ID.



VoIP CallerID Spoofing

- CallerID of SIP call is NOT trustworthy, and it is easy to spoof
  - Just modify the From field of INVITE message
- There are companies that offer callerID spoofing service to the public
  - http://www.telespoof.com/
  - http://www.spoofcard.com/
  - http://www.spoofcom.net/
  - https://www.itellas.com/
  - http://www.spooftel.com/
- More information can be found at http://www.calleridspoofing.info/

Billing of Managed VoIP

- Billing is fundamental to VoIP service providers (e.g. Vonage, AT&T)
  - Certain VoIP calls are charged on a per minute basis
    - International call
    - 900 call
  - Service providers rely on accounting and billing for charging their customers for the service they provided
  - × Loss any revenues from any billable services they provide
  - ? Overcharge to customers
- Billing has direct impact on each individual VoIP subscriber
  - ✓ Charges for the VoIP services they have chosen and used
  - × Charges on the calls they have NOT made
  - × Overcharged on the calls they have made

Requirements of VoIP Billing

- Billing needs to be reliable
  - Resilient to billing fraud
  - Provides consistent view on what the service provider has provided and what the subscriber has received
- Billing needs to be trustworthy
  - It will determine
    - how much money the service provider will make
    - how much money the subscriber will pay
  - Inaccurate or corrupted bill will create disputes between the service provider and its customers

Billing and Signaling of VoIP

- Existing VoIP billing is based on VoIP signaling
  - Signaling determines
    - the caller and callee of the call
    - when the call starts and ends
    - where the call will be routed
- Any vulnerability in VoIP signaling could be a potential vulnerability of VoIP signaling
- VoIP signaling protocols
  - SIP – the dominant VoIP signaling protocol
  - MGCP
  - H323
- We will focus on billing of SIP-based VoIP

VoIP Billing Vulnerabilities

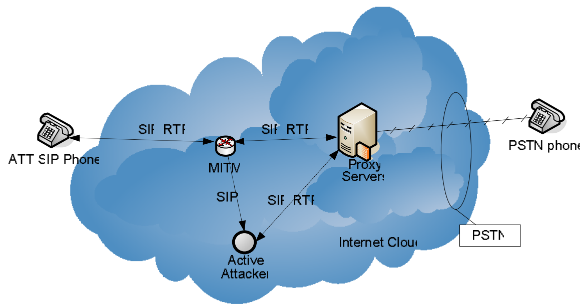
- Any vulnerability in VoIP signaling could be a potential vulnerability of VoIP signaling
  - Manipulation of SIP messages
  - Fake SIP messages
- The use public Internet for signaling and billing opens many doors for attacks
  - MITM at any router or gateway along the VoIP signaling path
- How vulnerable are those deployed commercial SIP-based VoIP services?
  - Vonage
  - AT&T
  - Verizon
  - Broadvoice

What We Have Done?

- Examined the billing vulnerabilities of SIP-based VoIP
- Identified a number of billing attacks on subscribers of deployed VoIP services
  - InviteReplay
  - FakeBusy
  - ByeDelay
  - ByeDrop
- Experimented with 2 leading VoIP services in US
  - Vonage – no. 1 in market chare 53.9%
  - AT&T callvantage – no.2 in market share 5.5%

INVITE Replay Billing Attack

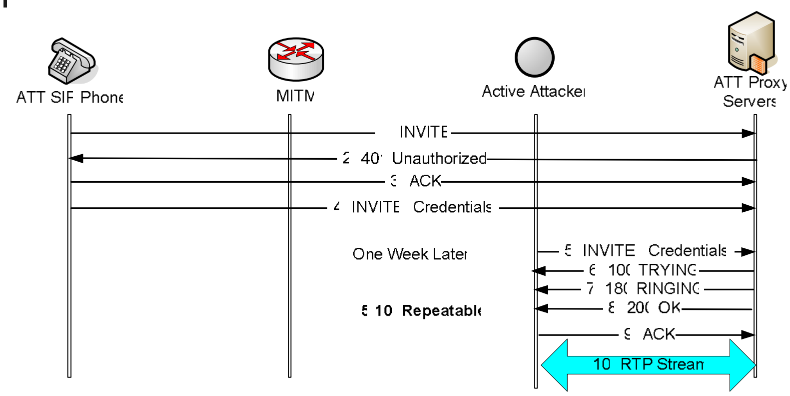
- Caller's SIP phone initiates a call by sending an INVITE message to its SIP server
  - SIP servers tracks the INVITE messages for billing and accounting
  - If one can replay some captured INVITE message, he can make calls at other's expense.



INVITE Replay Billing Attack on AT&T VoIP Subscribers

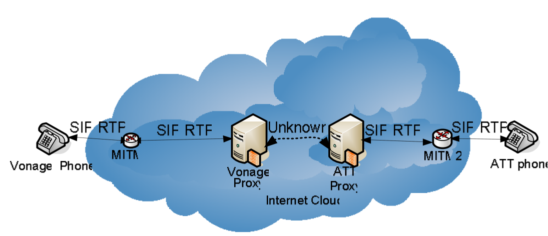
- SIP authentication does protect the INVITE message from the SIP phone to SIP server
  - Has built-in anti-replay protection
  - Hash (nonce, username, password, realm, SIP-method, request-URI)
  - Correct implementation of existing SIP authentication should prevent INVITE replay
    - Vonage
- Surprisingly, AT&T's callvantage appears vulnerable to INVITE replay
  - We could repeatedly replay the captured, legitimate INVITE (with modification on the SDP part) from our SIP phone one week after the original call
  - All replayed calls have been terminated by the AT&T SIP server after about 3 minutes.

INVITE Replay Billing Attack on AT&T VoIP Subscribers – SIP Message Flow

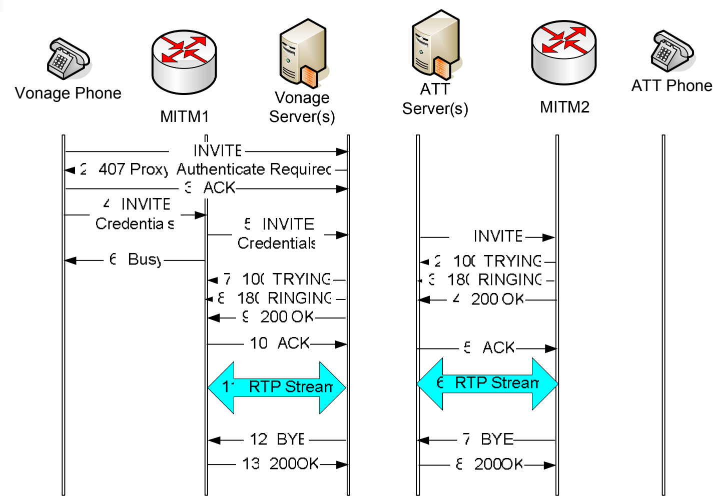


FakeBusy Billing Attack

- BUSY message is not protected by SIP authentication
  - The MITM between a SIP phone and SIP server could
    - hijack the VoIP calls of targeted SIP phone
    - Establish the calls with bogus content
    - When both the caller side and callee side have MITM, the MITMs could control the hijacked call duration while keeping the caller and callee unaware of the call
  - This could lead to overcharge on calls the VoIP subscriber has made



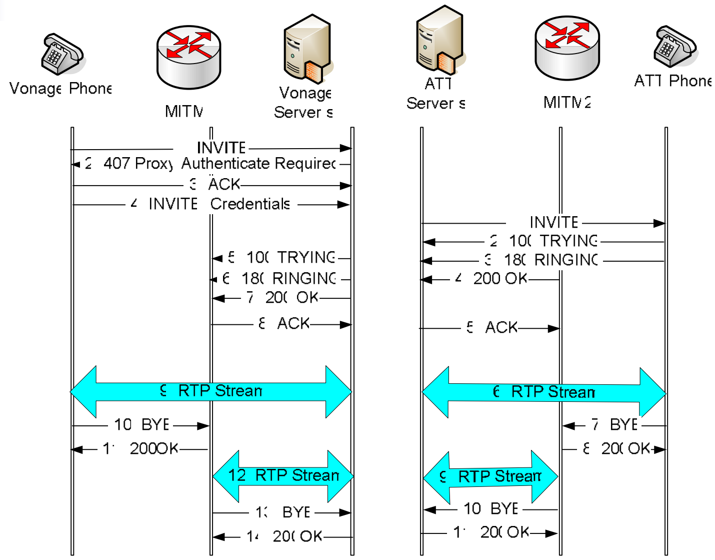
FakeBusy Billing Attack – SIP Message Flow



ByeDelay and ByeDrop Billing Attack

- Established SIP calls are terminated by BYE message
- What if the MITM can delay or simply drop the BYE message of established SIP call?
  - The SIP server will think the call is still alive, and count on the time.
  - This would transparently prolong the duration of established calls
  - This could also lead to overcharge on calls the VoIP subscriber has made
- Such a delay or drop of the BYE message does not involve any modification of the BYE message
  - SIP authentication won't help at all!

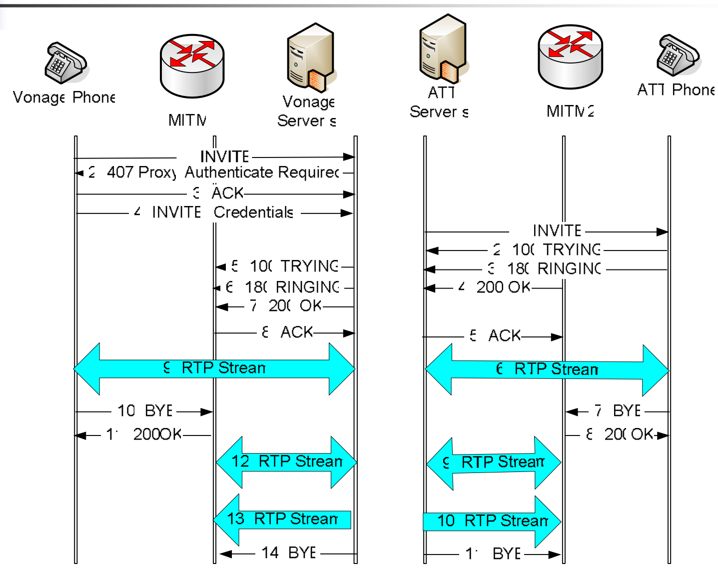
ByeDelay Billing Attack – SIP Message Flow



CCS 2007 Tutorial

43

ByeDrop Billing Attack – SIP Message Flow



CCS 2007 Tutorial

44

Potential Mitigations Against VoIP Billing Attacks

- INVITE replay
  - Just need to implement the SIP authentication correctly
- FakeBusy
  - Simply correlating the SIP and RTP messages won't help
  - Full integrity protection of SIP, RTP could defeat FakeBusy
- ByeDelay, ByeDrop
  - Hard to defend even with full SIP, RTP integrity protection
    - No modification of any SIP or RTP
    - Delay and drop could happen naturally
  - Some heuristics might help

Mitigations against Flooding Type of DoS

- Measure the difference between the numbers of attempted connections and completed handshakes by Reynolds and Goshal (NDSS 2003)
- Hellinger distance based anomaly detection by Sengar et al (IWQoS 2006)
- SIP-aware firewall by Columbia & Verizon
  - RTP pinhole filtering
  - Return routability check based on null-authentication
    - Could filter out those SIP message with spoofed source
  - State machine sequencing
    - Filter out-of-state SIP messages
  - Maintain dialogue state (source, contact)
    - Only accept BYE with legitimate address

VoIP Intrusion Detection

- SCIDIVE by Wu et al. (DSN 2004)
  - Sending fake BYE message to only one endpoint will leave an orphan RTP stream from the other endpoint.
  - Stateful, cross protocol correlation could detect this.
  - What if attacker sends bogus BYE to both endpoints?
    - No orphan RTP stream
    - This could indeed happen naturally if both sides hang up at about the same time!
- Interactive protocol state machine based detection by Sengar et al (DSN 2006)
  - Could detect those attacks that do not follow the SIP state machine
  - What if some attacks do follow the SIP state machine?
    - CallerID spoofing
    - Registration hijacking

Challenges in Securing VoIP

- Open architecture
- Real-time constraints
- Multiple protocols
- Key management issues
- E-911

Challenge #1: Open Architecture

- VoIP network is as open as the Internet
  - The endpoints (SIP phone) of VoIP could be anywhere, and they can freely change their location
- It's likely that we will interact with some endpoint that has NO prior established trust at all
  - We have to allow an unknown person calls us from an unknown SIP phone at an previously unknown IP address
  - We need to be able to call an unknown person at an previously unknown IP address
- How do we authenticate a caller/callee we don't know at all?
- How do we secure VoIP in such a case?
- Trust is NOT transitive!

Challenge #2: Real-Time Constraints

- Unlike other Internet applications such as Web, VoIP has stringent real-time constraints
  - End-to-end delay should be no more than 150ms
  - Each packet of voice stream should be delivered at constant rate (e.g., once every 20ms or 30ms)
    - The processing of each RTP packet should never be more than 20ms
  - The call setup time should not be too long
    - Callers expect to hear ring tone or voice within seconds after dialing
- All these put an upper bound on the total time that all the security mechanisms in all the SIP proxies, RTP servers and SIP phones can use

Challenge #3: Multiple Protocols

- VoIP involves a number of different protocols
  - Signaling
    - SIP
    - MGCP
    - H.323
  - Voice stream
    - RTP
    - SRTP
  - Security
    - HTTP digest – incorporated in SIP
    - TLS
    - IPsec
    - Key management
- In security, the whole systems is as strong as its weakest point!

Challenge #4: Key Management

- How could we establish session key with someone we don't know at all?
- Can we expect every SIP phone to have its own private/public keys?
  - How do we authenticate the public key of someone we don't know?
  - Can we expect PKI infrastructure for SIP phones?
- Scalability issue for the SIP servers
  - A SIP server may need to serve tens (or even hundreds) of thousands of subscribers
  - Dynamically establishing and managing keys with many concurrent callers/callees may overwhelm the SIP server

Challenge #5: E-911

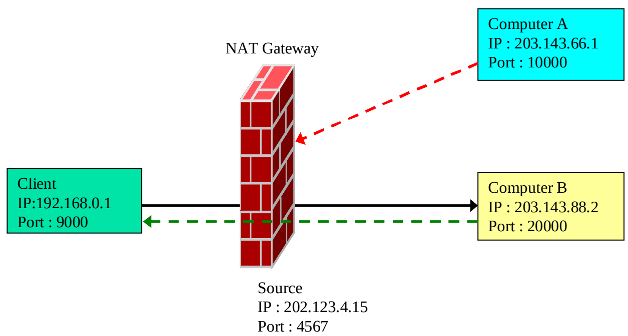
- How to provide authenticated caller ID?
  - It's easy to spoof caller ID
- How to determine the real origin of the call?
  - VoIP phones are highly mobile, they can be used from anywhere on the Internet
- How to route a VoIP 911 call to the appropriate PSAP (Public Safety Answering Point)?
- How to keep VoIP 911 connection with PSAP?
  - PSTN 911 call can only be terminated by PSAP
  - VoIP 911 call can be terminated by the caller through power cycle the SIP phone

Challenges #6 Firewall Traversal

- Firewall problem with VoIP
  - Firewall needs to block traffic based on
    - Source
    - Destination
    - Traffic type
  - VoIP needs to allow unsolicited incoming calls from unknown and untrusted sources
  - Conflicting requirements
- SIP-aware firewall
  - Allow SIP signaling message and corresponding RTP comes in
- Any exploits of SIP or RTP could compromise the security of SIP-aware firewall
- How to support such VoIP calls without compromising the firewall filtering policy?

Challenges #7 NAT Traversal

- NAT (Network Address Translation)
  - Dynamically maps internal, private IP & port with external, public IP & port
  - Allows multiple hosts in a private network to share one public IP address
  - Most residential IP phones are behind NAT



Challenges #7 NAT Traversal (cont'd)

- NAT problem with VoIP
  - NAT blocks unsolicited incoming traffic – it does not know how to translate that into private IP & port
  - VoIP needs to support unsolicited incoming calls from previously unknown and untrusted sources
  - SIP phones behind NAT will use its private IP for REGISTER, INVITE and 200OK
  - SIP phones behind NAT will dynamically choose the port number for receiving the incoming RTP stream and specify it in SDP part of INVITE or 200 OK messages

Challenges #7 NAT Traversal (cont'd)

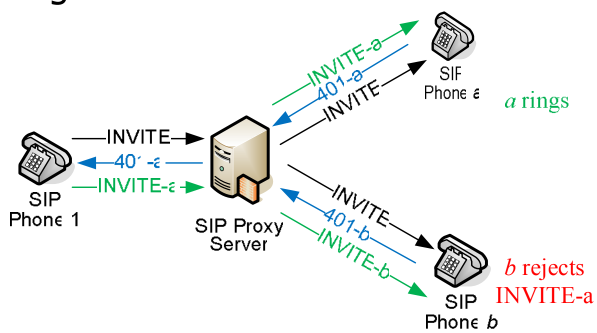
- Existing NAT traversal solutions
  - UPnP (Universal Plug and Play)
    - Queries the NAT device
    - Does not work with cascading NAT
  - STUN (Simple Traversal of UDP through NAT)
    - Uses TURN server on the public Internet
    - Works with Full Cone, Restricted Cone, and Port Restricted Cone NAT
    - Does NOT work with Symmetric (bidirectional) NAT
    - Does not support TCP
      - SIP RFC 3261 mandates TCP support
    - Susceptible to port scan
  - TURN (Traversal Using Relay NAT)
    - Relies on a TURN server in the middle of the signaling and media path
    - Works with Symmetric (bidirectional) NAT
    - May open door for MITM attack
  - ICE (Interactive Connectivity Establishment)
    - Make use of STUN and TURN

Challenges #7 NAT Traversal (cont'd)

- Security implications of NAT in VoIP
  - Makes it hard to enforce the integrity from end-to-end
  - Makes it hard to validate/authenticate the IP address of SIP phone
  - Opens door for
    - Registration hijacking
    - Call hijacking
    - MITM attack

Challenges #8 Challenge/Response with SIP Forking

- Challenge/Response would prevent replay attack, but it is difficult to work with SIP forking



Challenges #9 SPIT (Spam on Internet Telephony)

- VoIP spam could be more disturbing than email spam
  - People are used to respond to a phone call immediately
  - What if some spammer keeps ringing your phone all day long?
    - Could make your phone virtually unusable
- VoIP spam is harder to block than email spam
  - Caller ID is not trustworthy
  - Voice content based filtering is difficult

Challenges #9 SPIT (Spam on Internet Telephony) cont'd

- Turing test against SPIT
  - Before accepts a call, the callee's SIP phone (or proxy) asks the caller some question that is easy for human to answer but difficult for machine.
- However, such a voice Turing test scheme could be abused to launch DoS attack – similar to Smurf attack
  - Attacker send INVITE to lots of VoIP subscribers with spoofed IP address of the victim
  - The proxies of those VoIP subscribers will send RTP streams to the victims
  - The victim could be overwhelmed by those RTP streams

Challenges #10 Voice Phishing (aka Vishing)

- Attackers started using VoIP in phishing
  - Voice phishing attack on PayPal http://www.eweek.com/article2/0,1759,1985966,00.asp
  - Voice phishing attack on Santa Barbara Bank & Trust http://www.websense.com/securitylabs/alerts/alert.php?AlertID=534
- This essentially exploits people's trust in land line telephone.
- How to make VoIP as trustworthy as land line telephone?

References

- Voice Over Packet Security Forum http://www.vopsecurity.org/
- VoIP Security Alliance http://www.voipsa.org/
- SIPVicious - Tools for auditing SIP devices
- Jay Schulman. Phishing with Asterisk. http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Schulman.pdf
- David Endler and Mark Collier. Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions.
- http://www.hackingvoip.com/
- Jonathan Rosenberg. SIP Security. Dynamicsoft.
- Saverio Niccolini. SPIT Prevention: State of the Art and Research challenges. NEC Europe.
- Securing SIP: Scalable Mechanisms for Protecting SIP-Based VoIP Systems. www.nanog.org/mtg-0610/presenter-pdfs/schulzrinne.pdf

Summary

- VoIP is complicated, and it involves multiple protocols
- It is very challenging to secure VoIP while keeping it publicly accessible from unknown and untrusted sources
- We want bring the attention of research community to the problems of securing VoIP
- By no means, this tutorial is complete. I hope it will motivate more researchers to look into the security problems of VoIP

Thanks

Questions for me?

Xinyuan Wang
Department of Information & Software Engineering
Department of Computer Science
George Mason University
(703_ 993-9461
xwangc@gmu.edu