Generic Security Services API authentication support for the Session Initiation Protocol

Lars Strand
Josef Noll
Wolfgang Leister

The Seventh Advanced International Conference on Telecommunications (AICT 2011)
20-25 March 2011
St. Maarten, The Netherlands Antilles
"It's appalling how much worse VoIP is compared to the PSTN. If these problems aren't fixed, VoIP is going nowhere."

--- Philip Zimmerman on VoIP security in “SIP Security”, Sisalem et. al. (2009)
With VoIP, Old Attacks Find New Targets

April 16, 2005
By David Noodle
Submit Feedback »
More by Author »

IT professionals can add VoIP to the growing list of security threats they need to monitor. Security firm WatchGuard Technologies detailed seven leading threats to Voice over IP services in a release this week. While they aren’t new per se, they stand to become higher profiles as the bad guys seek to exploit VoIP’s increased popularity.

*“Some of these are tested and true blue data hacks that have been around for a while, and now there’s a lucrative new field for hackers and criminals to go after on the VoIP side,” WatchGuard spokesman ChrisMcKie told InternetNews.com “The bad guys are going to go where the money is.”*

WatchGuard says recent reports predict as much as 75 percent of corporate phone lines will be using VoIP in the next two years. By the end of this year, the total number of VoIP subscribers worldwide (residential and commercial) is expected to reach nearly 100 million.

Heading WatchGuard’s list are Denial of Service (DoS) attacks, similar to those made to data networks. VoIP DoS attacks leverage the same tactic of running multiple packet streams, such as call requests and registrations, to the point where VoIP services fail.

These types of attack often target SIP (Session Initiation Protocol) extensions, according to WatchGuard, that ultimately exhaust VoIP server resources, which can cause systems to disconnects.

Another is Spam over Internet Telephony (SPIT). Like unwanted e-mail, SPIT can be generated in a similar way by botsnets that target millions of VoIP users from compromised systems. Like junk mail, SPIT messages can slow system performance, bog voicemail boxes and inhibit user productivity.

**Security Strategy**

Hackers to attack VoIP in two years

Video and all, Nortel says...

Tags: hackers, voip, nortel

By Dan Sallit
Published: 15 October 2005 15:25 EDT

Hackers will attack voice over IP (VoIP) telephone conversations with spam and malicious code within two years, equipment manufacturer Nortel has claimed.

Companies using VoIP and other multimedia services, such as videoconferencing, should plan to defend against unsolicited adverts appearing mid-conversation, the company said.

Hackers have breached the VoIP PBX telephone system of a small Perth business and made over 11,000 international calls in 46 hours, resulting in a bill in excess of $120,000, according to WA Police.

Detectives from the West Australian Police Technology Crime Investigations Unit said the business was only alerted to the security breach when they received an invoice from their service provider.

"Business operators should invest in appropriate security software to protect their communication systems," said Detective Sergeant Jamie McDonald.


For a continuous update on the SANS Top 20 vulnerabilities, subscribe to @Risk. If you need an in-depth, more cut-and-dried look, please see the following excerpts.

**Security Policy and I:**

- Excessive User Rights
- IC: Fiching/Sever Fiching
- H: Uncrypted Laptops

**Application Abuse:**

- A1: Instant Messaging
- A2: Peer-to-Peer Programs

**Network Devices:**

- N1: VoIP Servers and Phones

**Zero Day Attacks:**

- Z1: Zero Day Attacks

**Security Policy and I:**

- H: Uncrypted Laptops
- IC: Fiching/Sever Fiching

**Application Abuse:**

- A1: Instant Messaging
- A2: Peer-to-Peer Programs

**Network Devices:**

- N1: VoIP Servers and Phones

**Zero Day Attacks:**

- Z1: Zero Day Attacks
VoIP?

- Voice over IP (VoIP) protocols and technology is a merge of telecom and data communication

**What is VoIP?**
- Broad definition: Sending and receiving media (voice/video) over IP

**Why VoIP?**
- Added functionality and flexibility – which may be hard to provide over PSTN
- Reduced cost – uses Internet as carrier
- Less administration – no separate telephone and data network

Industry have high focus on VoIP today

But, VoIP is known to be insecure
- Inherits problems from traditional IP networks
- Multiple attack on SIP based VoIP exists
Session Initiation Protocol (SIP) is the *de facto* standard signaling protocol for VoIP

- Application layer (TCP, UDP, SCTP)
- Setting up, modifying and tearing down multimedia sessions
- Establishing and negotiating the *context* of a call
- No media transfer (voice/video)

RTP transfer the actual multimedia

SIP specified in RFC 3261 published by IETF 2002

- First iteration in 1999 (RFC2543)
- Additional functionality specified in over 120 different RFCs(!)
- Even more pending drafts...
- Known to be complex and sometimes vague – difficult for software engineers to implement
- Interoperability conference - “SIPit”
SIP specification – huge, complex and sometimes vague
Excerpts from an email posted on IEFT RAI mailing list:

I'm finally getting into SIP. I've got Speakeasy VoIP service, two sipphone accounts, a Cisco 7960 and a copy of x-ten on my Mac.

And I still can't make it work. Voice flows in one direction only. I'm not even behind a NAT or firewall -- both machines have global addresses, with no port translations or firewalls.

I've been working with Internet protocols for over 20 years. I've implemented and contributed to them. And if *I* can't figure out how to make this stuff work, how is the average grandmother expected to do so? SIP is unbelievably complex, with extraordinarily confusing terms. There must be half a dozen different "names" -- Display Name, User Name, Authorization User Name, etc -- and a dozen "proxies". Even the word "domain" is overloaded a half dozen different ways. This is ridiculous!

Sorry. I just had to get this off my chest. Regards,

SIP call flow

Alice

Local domain

SIP server

"Alice is at IP X"

INVITE sent to X

Bob

Call: sip:alice@companyA.com or +47 2212 3456

Internet

INVITE

DB
Three SIP authentication scenarios

scenario I

scenario II

scenario III
SIP authentication - today

1) **Digest Access Authentication (DAA) (RFC3261)**
   - Mandatory but weak
   - Widespread adoption - “everyone” use this
   - Used to authenticate locally within a domain/realm (during REGISTER or INVITE)

2) **S/MIME (RFC3261)**
   - Goal: Security service end to end
   - Uses certificates, needs PKI = “complex and expensive”
   - Not supported, not used.

3) **Other user identity handling methods**
   - P-Asserted identity (RFC3325) – in a trusted environment
   - Strong Identity (RFC4474) – using authentication service
   - Other academic approaches.
WANTED

Strong and flexible authentication method in SIP!
Problem and goal

- SIP is flexible

- Problem: Different usage scenarios have different security requirements
  - Handheld devices vs. high-end SIP servers

- Goal: Modification to the SIP standard should be minimum

- Goal 2: A strong and flexible authentication methods wanted

- Solution: Add support for GSS-API
GSS-API

- **Generic Security Services Application**
  - Program Interface = Interface for an application to access security services
- Mature and well-proven standard (RFC2743)
- NOT a communication protocol
  - Relies on the application (SIP) to pass data *tokens* between client and server
- Does NOT provide any security in itself
  - Relies on underlying security mechanisms
- GSS-API implementations (may) support different authentication methods
  - Digest
  - Kerberos
  - TLS
  - ...
- All methods are *transparent* to the application
GSS-API stack (with SIP)

- Kerberos
- Digest
- Other
- SPNEGO
- GSS-API
- SIP
- TCP/UDP/SCTP
- IP
SIP messages with embedded GSS-API tokens
SIP REGISTER message

1. REGISTER sip:CompanyA SIP/2.0
2. Via: SIP/2.0/UDP 192.168.1.102;branch=z9hG4bK32F3EC44EB23347BF0D4888
3. From: Alice <sip:alice@CompanyA>;tag=1234648905
4. To: Alice <sip:alice@CompanyA>
5. Contact: "Alice" <sip:alice@192.168.1.102:5060>
6. Call-ID: 2B6449C74C10D4F95006A6C034E79E8E@CompanyA
7. CSeq: 19481 REGISTER
8. User-Agent: PolycomSoundPointIP-SPIP_550-UA/3.1.2.0392
10. Max-Forwards: 70
11. Expires: 3600
12. Content-Length: 0

GSS-API token

1. REGISTER sip:CompanyA SIP/2.0
2. Via: SIP/2.0/UDP 192.168.1.102;branch=z9hG4bK32F3EC44EB23347BF0D4888
3. From: Alice <sip:alice@CompanyA>;tag=1234648905
4. To: Alice <sip:alice@CompanyA>
5. Contact: "Alice" <sip:alice@192.168.1.102:5060>
6. Call-ID: 2B6449C74C10D4F95006A6C034E79E8E@CompanyA
7. CSeq: 19481 REGISTER
8. User-Agent: PolycomSoundPointIP-SPIP_550-UA/3.1.2.0392
9. Authorization: GSSAPI ttype="context"
token="0401000B06092A864886F712010202DADC139402AA44350CDE32"
10. Max-Forwards: 70
11. Expires: 3600
12. Content-Length: 0
Conclusion

- Our solution require minimal changes to the SIP protocol standard
- Add support to a range of different authentication methods
- Flexible – different implementations can support different authentication methods
- New authentication methods can be added later WITHOUT change to the SIP standard

Future work
- Add an SIP extension to maintain backwards compatibility?
- Require some authentication methods to be supported as standard? Which?
- Vulnerable to a REGISTRATION attack?
- Look into different GSS-API auth methods
- Compare with SASL and SAML
Thank you!