

ShoreTel

Practical vendor integration with SIP -

Handling interoperability issues

Martin Ruddle
Product Management



Today's Agenda

- ShoreTel's philosophy on integration
- The issues
- ShoreTel approach on SIP extensions & trunks



ShoreTel's philosophy on integration

- Provide partners and customers with validated 'end to end' multi-vendor solutions in the SIP 'plug and pray' era
 - Making it all work together is as complex as solving a third order differential equation
 - Allow ShoreTel partners to work with 'known entities'
 - One visit to the customer's site



QuickStart™ and a
ShoreTel logo are
registered trademarks of
ShoreTel, Inc.

ShoreTel's philosophy on integration

- *Provide partners and customers with validated 'end to end' multi-vendor solutions in the SIP 'plug and pray' era*

ShoreTel Technology Partner Program - **Mission**

Enable ShoreTel Reseller Partners to deliver complete business solutions to end customers with confidence

- Products undergo mutual validation testing to check compatibility
- We have validated interworking with 8 SIP carriers
- There are 20 ITSPs in the pipeline
- **Ingate** and **Bandwidth.com** are **TPP certified partners**

CloudGen™ and a
ShoreTel trademark.
are needed to see this picture.

Provide a consistent 'traversal' solution

- **Maintain Product Certifications**
 - Dedicated Lab and Engineers
 - Re-certification for each of ShoreTel major releases within 90 days of the release
 - Re-certification of each major release of the partner's product within 90 days of the release
 - Application note produced detailing validated ShoreTel-partner configuration
- **With Ingate we solve SIP firewall and NAT traversal issues with a consistent solution**
 - The 'solution' is [secure](#)

ShoreTel Technology Partner Program

Mission

Enable ShoreTel Reseller Partners to deliver complete business solutions to end customers with confidence

		T P P A P P N O T E
		TPP-10021 Date: August 8, 2007
Product: ShoreTel® Ingate Bandwidth.com		
System version: ShoreTel 6.1 & 7		

ShoreTel, Ingate & Bandwidth.com for SIP Trunking

SIP Trunking allows the use of Session Initiation Protocol (SIP) communications from an Internet Telephony Service Provider (ITSP) instead of the typical analog, Basic Rate Interface (BRI), T1 or E1 trunk connections. Having the pure IP trunk to the Internet Telephone Service Provider allows for more control and options over the communication link. This application note provides the details on connecting the ShoreTel IP phone system through an Ingate box which is connected to both the LAN and WAN and acts as a gateway to the ITSP for SIP Trunking.

Table of Contents

Overview.....	2	Figure 9 – Administration Trunk Groups.....	14
---------------	---	---	----

QuickStart™ and a
ShoreTel logo are
used in this document.

Allow 'customization' of configuration settings

- Provide a mechanism for feature update
 - Don't want to wait for a 'release change' to allow a new configuration
- Allow 'customization' of configuration settings for 3rd party devices & trunks in our management interface
 - Understand things change
 - Be sure you can get back to a working configuration
- Make it as plug and play as possible
- Allow for customer additions
 - VARS or Customers may want to 'risk' trying something out themselves
 - Ensure we can get back to a supported configuration after customer modification

ShoreWare Director - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address <http://localhost/ShoreWareDirector/MainFrame.asp> Go Links >>

Google Go Bookmarks 0 blocked Check AutoLink AutoFill Send to Settings

Developer Mode

Build 13.6.7900.0
Logoff Administrator

- Users...
- Trunks...
- IP Phones...
- Switches
- Call Control...
 - Account Codes
 - Bridged Call Appearances
 - Hunt Groups
 - Paging Groups
 - Pickup Groups
 - Route Points
 - Supported Codecs
 - Codec Lists
 - SIP Profiles
 - Options
- Voice Mail...
- Auto-Attendant Menus
- Workgroups
- Schedules
- Personal Call Manager...
- System Directory
- Application Servers
- Conference Bridges
- IM Servers
- Sites
- System Parameters...
 - Dialing Plan
 - Digit Translation Tables

SIP Profile

Edit SIP Profile

[New](#) [Copy](#) [Save](#) [Delete](#) [Reset](#) [Help](#)

Edit this record [Refresh this page](#)

Name: ←

User Agent: ←

Priority: ←

☒ Enable

System Parameters: OptionsPing=1
SendEarlyMedia=0
MWI=none
lCodecAnswer=0
StripVideoCodec=0 ←

Custom Parameters:

`optionsping=0
sendearlymedia=1
mwi=none` ←

© 1998-2007 ShoreTel, Inc. All rights reserved.

Local intranet

Summary

- SIP trunks and end points can inter-work in the 'plug and pray' era
- There are many flavors of SIP out there be sure you only use those validated by the vendors as working together
- Ensure vendors have published information on support parameters



THANK YOU

Why Not Just Connect Directly?



[Site Map](#)

[company](#)

[products](#)

[solutions](#)

[partners](#)

[viper](#)

[support](#)

[contact](#)

[about viper](#)

[viper services](#)

[recent attacks](#)

[threat advisories](#)

[generic threats](#)

[specific threats](#)

[viper blog](#)

[CONTACT SALES](#)

[VIPER](#) > [Threat Advisories](#)

Service provider call feature servers may be vulnerable to call hijacking

Advisory Number: VIPER-2007-012-G
Release Date: 2007.03.19
Source: Sipera VIPER Lab
Systems Affected: SIP Service Provider Servers
Category: Interception and Modification
Severity: High

Overview

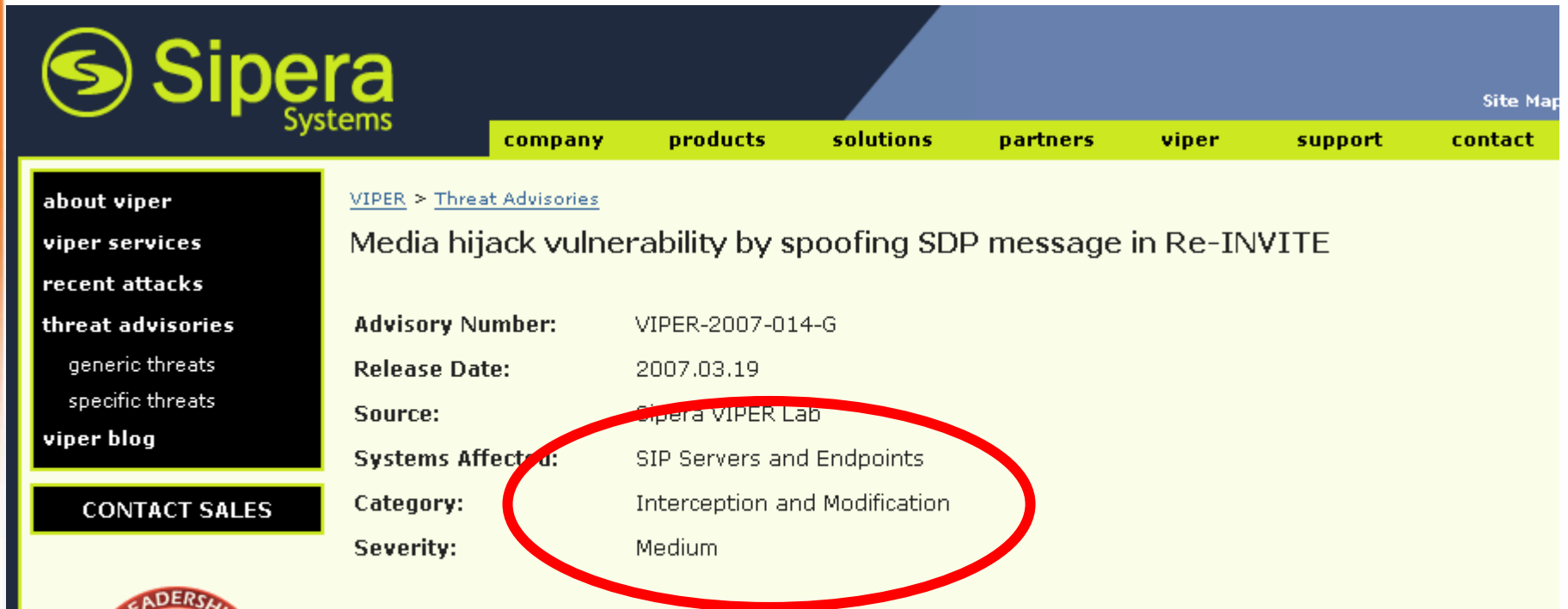
SIP call servers may provide feature to set call forwarding to some other number in case user is not available at his/her regular phone. Users can setup this forwarding by using specific feature access code. If this feature access is not properly authenticated an attacker may use this to forward calls made to victim's phone to attacker chosen destination.

Impact

Attacker can exploit this vulnerability to hijack calls to be made to victim, may use social engineering



Why Not Just .Connect Directly?



The screenshot shows the Sipera Systems website. The header includes the Sipera Systems logo and a navigation menu with links: company, products, solutions, partners, viper, support, and contact. A 'Site Map' link is also visible. On the left, a sidebar contains links for 'about viper', 'viper services', 'recent attacks', 'threat advisories' (with sub-links for generic and specific threats), and 'viper blog'. Below this is a 'CONTACT SALES' button. The main content area displays a threat advisory titled 'Media hijack vulnerability by spoofing SDP message in Re-INVITE'. The advisory details include: Advisory Number: VIPER-2007-014-G, Release Date: 2007.03.19, Source: Sipera VIPER Lab, Systems Affected: SIP Servers and Endpoints, Category: Interception and Modification, and Severity: Medium. A red oval highlights the 'Systems Affected' and 'Category' fields.

Sipera Systems

Site Map

company products solutions partners viper support contact

about viper
viper services
recent attacks
threat advisories
generic threats
specific threats
viper blog

CONTACT SALES

[VIPER](#) > [Threat Advisories](#)

Media hijack vulnerability by spoofing SDP message in Re-INVITE

Advisory Number: VIPER-2007-014-G
Release Date: 2007.03.19
Source: Sipera VIPER Lab
Systems Affected: SIP Servers and Endpoints
Category: Interception and Modification
Severity: Medium

Overview

SIP allows mid-call changes to IP address and port number where media is received by the UAs. Unless a trusted media anchoring proxy is used and endpoints reject invalid media redirected requests, an attacker can send RE-INVITE messages to the UAs and hijack the media streams for later reconstruction.