VoIP Security

Project Team

Kurt Nishi
David Smreczak
Kevin Vaccaro
Gene Yahnes
Celestin Zimulinda

Project Background

- Customer provided carrier class SIP enabled Application Layer Gateway/Firewall
- Customer provided test plan
- Open source User Agents
- Proxy server (Siemens)
- Hands-on training
- Ethereal sniffer

Project Goals

- Assemble, install and configure gateway/firewall
- Obtain, configure, test, and document open source User Agents
- Distill down the initial customer test plan
- Establish a stable test bed
- Setup, test, and document the various User Agents
- Capture and document protocol traces of SIP calls thru firewall

Test Process

- Assemble, install and configure the firewall for SIP calls (Hands-on training)
- SIP User Agents had to be obtained, installed, documented, and configured in the test bed
- Successful and failed SIP protocol traces of the calls were to be captured and documented using Ethereal
- Cataloging of the traces

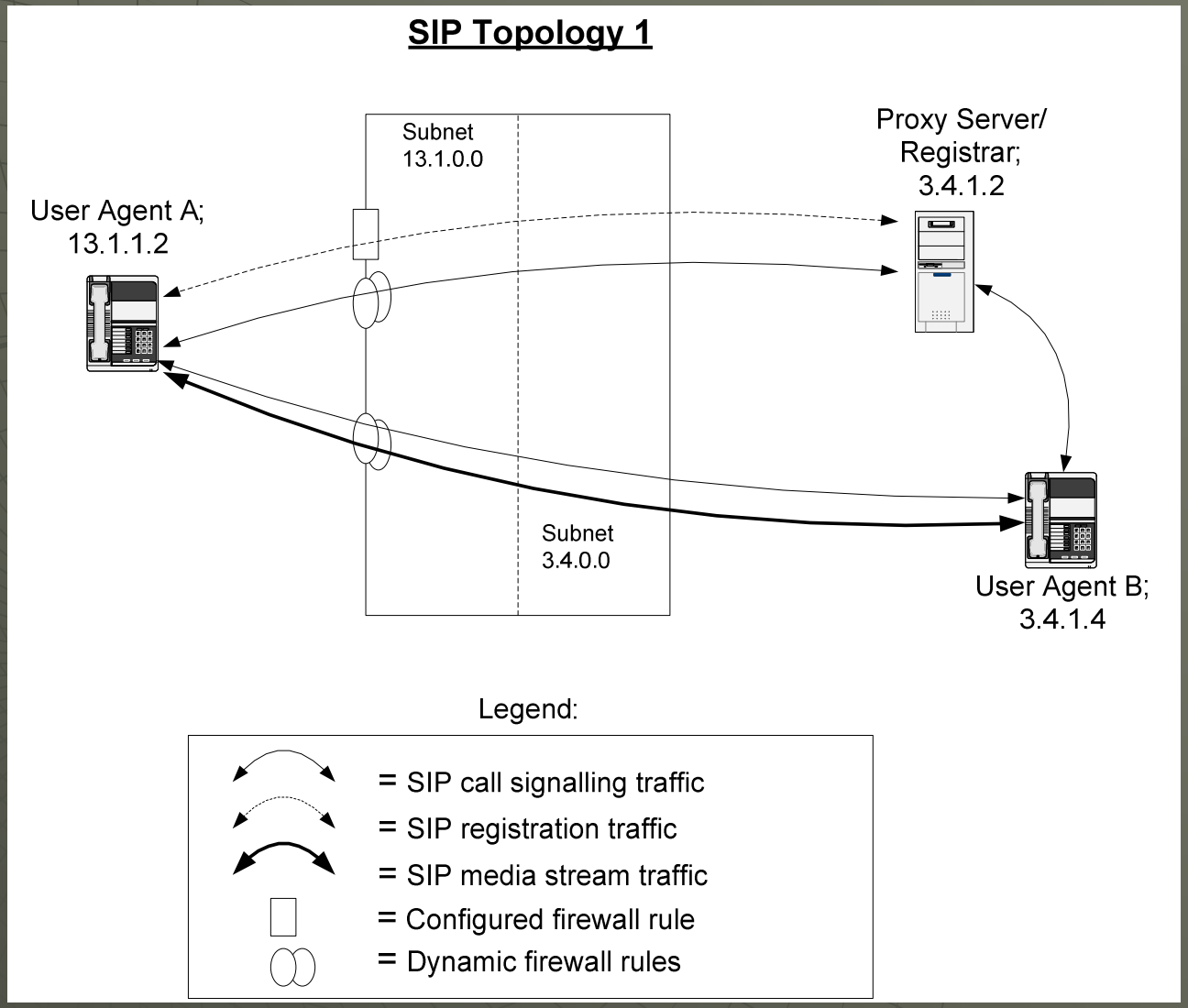
User Agents

- **Express Talk requires**: Windows 98/ME/2000/XP/2003, Pentium 500MHz or above with at least 32MB RAM (64MB for 2000/XP/2003); a sound card that supports full-duplex audio, a microphone, and a headset or speakers.
- **X-Lite requires**; Sound Card with microphone input, Microphone, Speakers and VoIP provider.
- **SJPhone requires**: MS Windows XP, 2000, and 98/ME, and Linux, Mac OS X. However, Windows 2000 users need to install Microsoft Installer 2.0 before installing SJPhone. A full-duplex sound card with a microphone and speakers, or any USB phones.

Test Plan

- Tests 1 – 3 verify that three different Open-Source SIP User Agents can register with a local proxy.
- Tests 4 – 6 verify that three different Open-Source SIP User Agents can register with a remote proxy.
- Tests 7 – 9 verify that two identical Open-Source SIP User Agents can send and receive all the mandatory SIP methods in compliance with RFC 3261.
- Tests 10 – 12 verify that two identical Open-Source SIP User Agents can establish an RTP media stream.

Test Bed


SIP Topology 1
Subnet
13.1.0.0
Proxy Server/
Registrar;
3.4.1.2
User Agent A;
13.1.1.2
Subnet
3.4.0.0
User Agent B;
3.4.1.4
Legend:
= SIP call signalling traffic
= SIP registration traffic
= SIP media stream traffic
= Configured firewall rule
= Dynamic firewall rules

User Agent Cataloging

User Agent	Initial Setup information	Call set up information
1.Express Talk v. 1.03 by NCH Swift Sound	**Step 1**: Microphone Connection and Record Volume	Supports NAT by using uPNP to acquire the public NAT address, assigns UDP port 5161 to the external address
	Step 2: Soundcard and Playback Volume	
	Step 3: Talk Mode and Audio Quality options - headset v. speaker phone and quality v. bandwidth	
	Step 4: SIP setup - register for a sip number or use computer IP directly	
	Step 5: SIP details - enter: display name, SIP number/UserName, SIP server (Proxy and Domain), SIP password	
2. SJPhone v1.6	Audio Wizard – establish hardware connections – microphone and speaker Use DirectX – sound options	Enter Sip Phone URL of destination phone
	Select playback and recording devices and system audio settings	
	Test speakers – volume levels Test microphone – volume levels	
	Verify Finish – (Used default settings)	
	User Information – enter name	
	Call Options – Incoming calls – automatically accept incoming calls; outgoing calls – Use following host address?	
	Profiles – create new profile – define name; profile type = Call through SIP Proxy;	
	Initialization tab in profile options – uncheck account and password; check Full Address of Record, saved, required.	
	SIP Proxy tab – enter Proxy domain (IP address and port (5060))	
	OK – Initialize – Enter Sip URL: “sip:*@ipofproxy”	
3. X-Lite soft phone 1.0.1	SIP server Username Password VoIP Number SIP Port Codec Type and Packet Size	In order for this soft phone to work some configuration parameters must be done What configuration parameters are asked for. I thought that was what column 2 was for.
	The ports are 5060 and 8000-8005 UDP.	

Express Talk (Register) trace

- No. Time Source Destination Protocol Info
- 3 0.000819 13.1.1.2 3.4.1.4 SIP Request: REGISTER sip:3.4.1.4
- Frame 3 (393 bytes on wire, 393 bytes captured)
- Ethernet II, Src: 13.1.1.2 (00:00:39:07:2d:ac), Dst: 13.1.1.1 (00:01:c6:10:15:40)
- Internet Protocol, Src: 13.1.1.2 (13.1.1.2), Dst: 3.4.1.4 (3.4.1.4)
- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
  - Request-Line: REGISTER sip: 3.4.1.4 SIP/2.0
    - Method: REGISTER
    - Resent Packet: False
  - Message Header
    - Via: SIP/2.0/UDP 13.1.1.2:5060;rport;branch=z9hG4bK34048
    - Max-Forwards: 70
    - To: <sip:13.1.1.2@3.4.1.4>
      - SIP to address: sip:13.1.1.2@3.4.1.4
    - From: <sip:13.1.1.2@3.4.1.4>;tag=1183884
      - SIP from address: sip:13.1.1.2@3.4.1.4
      - SIP tag: 1183884
    - Call-ID: 954213422-4048-RICENOTEBOOK16@13.1.1.2
    - CSeq: 3 REGISTER
    - Contact: <sip:13.1.1.2@13.1.1.2:5060>;expires=0;q=0.90
      - Contact Binding: <sip:13.1.1.2@13.1.1.2:5060>;expires=0;q=0.90
    - Content-Length: 0
    - User-Agent: Express Talk 1.03

Project Summary

- Original scope of test plan had to be revaluated in light of some initial testing with SIP-Communicator User Agent
- Working with customer we established an extension to the existing test plan
- Established a stable test bed with repeatable test results
- Documented and created an on going catalog of User Agent behavior thru firewall

Future Plans

- Revisit test plan and solicit input from customer and others on directions
- Obtain necessary tools to run tests, software and or hardware
- Layout a project plan and timeframe for tests plans and set milestones

Conclusion

- Project established a strong foundation for further testing on the firewall
- Now have reference material for user agents and their behavior
- We were able to identify bugs for the customer and document them effectively