Security Assessment Report
DR100824C

SIEMENS OPENSCAPE VOICE v5 and OPENSCAPE BRANCH v1

3 May 2011

Miercom

www.miercom.com

Table of Contents

Executive Summary

Siemens' OpenScape Voice v5 and OpenScape Branch v1 are rated Certified Secure by Miercom Independent Testing Labs as of September 2010. Certified Secure testing involves subjecting the product to a rigorous battery of vulnerability analyses and scans as well as a complex set of exploits designed by a team of experienced security professionals. OpenScape Voice and OpenScape Branch proved they were resilient to system compromise. The Certified Secure rating is valid for a two year period while advancements in both security countermeasures and vulnerability exploits continue to be monitored.

OpenScape Voice and OpenScape Branch were tested without any additional security countermeasures employed. The internal countermeasures that are built into the firewall of OpenScape Voice were enabled during testing. The approach and methodology utilized in this test are based on knowledge that Miercom, in collaboration with leading security experts, has collected over several years through its work in VoIP pre- and post-deployment site surveys and security assessments.

OpenScape Branch proved its resiliency in its ability to sustain branch communications even after failure of connectivity to the main office.

This document provides an overview of the more noteworthy exploit attempts conducted. In some test cases, specific details were intentionally omitted to avoid the use of this information to reverse-engineer exploits for VoIP products. The products tested were configured in accordance with Siemen’s guidance, documented in their OpenScape Voice Security Checklist that in effect greatly enhances the resiliency of the systems. Siemens was afforded the opportunity to review initial findings, respond and repeat tests to ensure that potential vulnerabilities we tested were addressed in the Siemens approved secure voice system.

Miercom congratulates Siemens for OpenScape Voice v5 and OpenScape Branch v1 for achieving the Miercom Certified Secure Certification – the most comprehensive and challenging security certification in the industry.

Introduction

Siemens engaged Miercom to perform a security assessment on the OpenScape Voice v5 and OpenScape Branch v1. OpenScape Voice, a stand-alone software-based IP PBX, and OpenScape Branch, a server that connects and routes communications to multiple branch offices, were evaluated for their security countermeasures without the use of additional security gateways, firewalls and SBCs in the deployed topology.

The purpose of the test was to determine if there were any relevant security vulnerabilities that could be leveraged to the detriment of a customer using OpenScape Voice and OpenScape Branch. We compared the resiliency of OpenScape Voice and OpenScape Branch to that of other IP PBX and Unified Communications solutions on the market. Overall, the OpenScape products proved more secure than the majority of other products we have tested to date.

This report provides results that were used to qualify the products as Certified Secure. Siemens OpenScape Voice v5 and OpenScape Branch v1 achieved the Miercom Certified Secure rating which is reserved for products that score in the top 30% of a product class and can prove their resiliency to compromising security threats.

Methodology

To conduct the tests reported in this report, we used a combination of test tools including customized proprietary test scripts, commercial vulnerability scanning tools and open-source security assessment products. We used a VoIP network infrastructure typical of a mid-sized enterprise to support OpenScape Voice and OpenScape Branch as much as possible. We evaluated the viability of each attack and the risk of compromise of OpenScape products and recommended compensating measures to rectify or mitigate the suspect vulnerabilities. Additional details are shown in the OpenScape Deployment Diagram and How We Did It sections.

Use of the Data in this Report

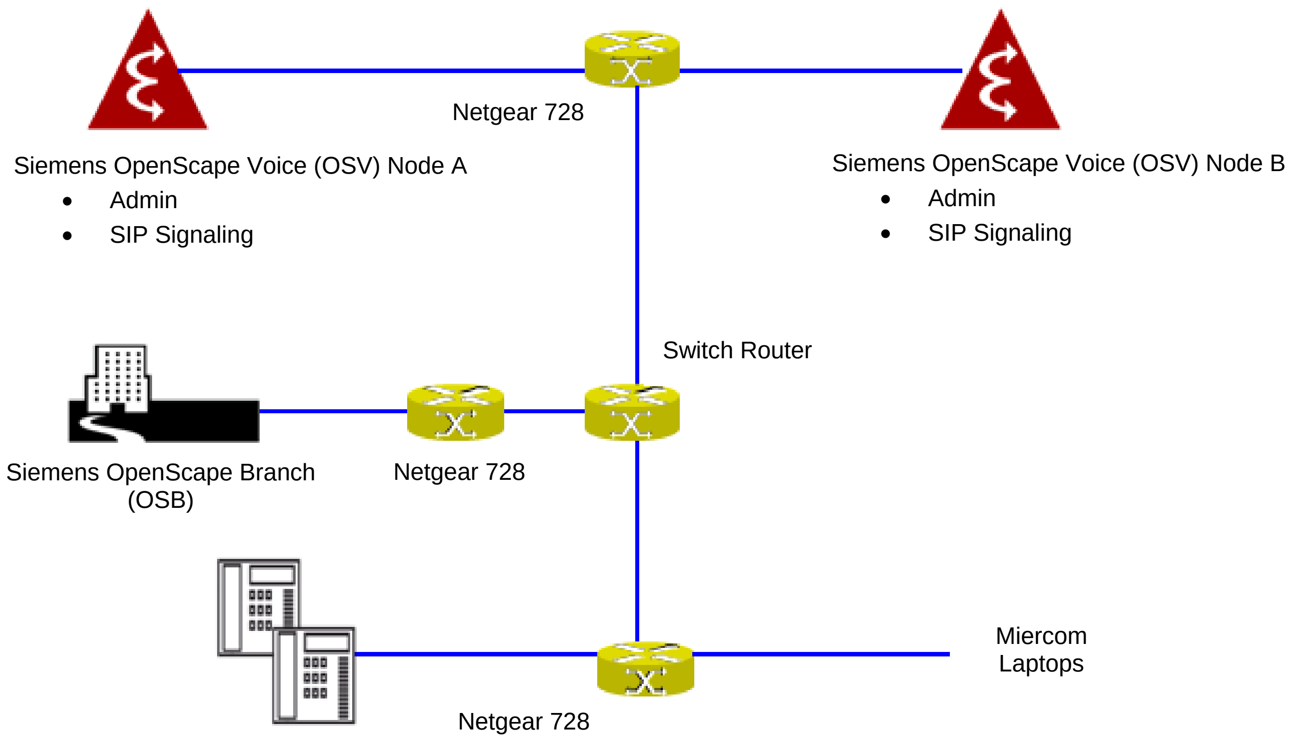
All tests conducted on OpenScape products were inside the internal network and network infrastructure security countermeasures, for the most part, were not utilized. We stressed the inherent resiliency of the hardened OpenScape system itself. Miercom does not offer a warranty of fitness or suitability for this product in a customer's environment based on this testing alone, without Miercom additionally conducting the site assessment and integration for the deployment. However, Miercom is confident and stands behind the findings for security resiliency that OpenScape Voice v5 and OpenScape Branch v1 have demonstrated in this testing.

OpenScape Deployment Diagram

A representative diagram for an enterprise network for OpenScape Voice and OpenScape Branch is depicted below. The OpenScape systems shown in this diagram were connected in a “High Availability” configuration that would be more typical in a larger enterprise configuration. The High Availability configuration consists of contingency measures to maintain availability in case the OpenScape system application fails. Each OpenScape server has eight Ethernet ports, in two sets of four, enabling fully-redundant network connections. The testing was conducted using OpenStage 60/80 SIP phones. Security assessment of the OpenScape Voice v5 and OpenScape Branch v1 were made without use of any security gateways, firewalls or SBC in the deployed topology.

Exact configuration and tools used in testing for this project is proprietary for the protection of the security testing program and the vendor being tested.

Miercom Testing: Physical Configuration

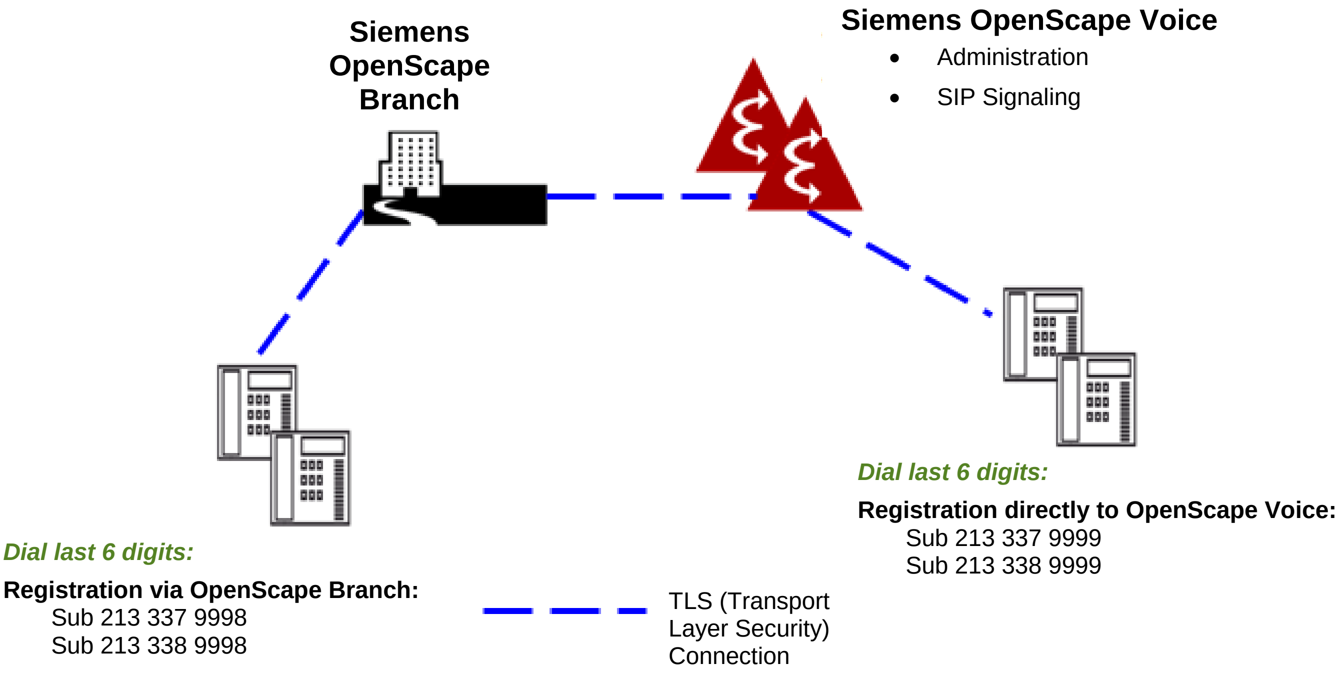


Dial last 6 digits:

Registration via OpenScape Branch:
Sub 213 337 9998
Sub 213 338 9998

Registration directly to OpenScape Voice:
Sub 213 337 9999
Sub 213 338 9999

Miercom Testing: Logical Configuration



How We Did It

The objective was to compromise the ability of the Siemens OpenScape Voice v5 and OpenScape Branch v1 to successfully deliver real-time voice communications and to gain surreptitious access to the OpenScape system for the purposes of placing unauthorized calls, or compromising and intercepting presumed secure VoIP communications. The OpenScape products were evaluated inside the internal network. The tests included in this report were conducted without external security countermeasures employed to the OpenScape systems as it is most desirable to assess the resiliency of IP PBX components first and then subsequently assess the additional protection provided by the underlying network.

We evaluated OpenScape Voice and OpenScape Branch while they were installed in a standard quality assurance test environment. We did a perimeter assessment to identify paths through the network that could be used to attack the systems by a potential attacker. We identified several paths (i.e. SIP signaling, the administrative interface, the OpenScape Branch) that merited exercising to look for flaws. We then exercised these paths as potential attack vectors that are further detailed within this report.

To conduct the tests contained in this report, we planned our attack in three stages: research, reconnaissance and attack execution. Preparation began weeks prior to the actual testing date, with tools, attacks planned and pre-tested prior to the start of actual testing. Preparations included researching public sources (Google, Bug Traq, CVE, security advisory) as well as Miercom internal research. The scanning and enumeration part involved learning the network topology, including services running, ports open/filtered, protocols, operating systems, program name and version numbers. The tools used for port-scanning and enumeration included Nmap, Netcat and Nessus. We performed several rounds of analysis on the phone-to-OpenScape data path to identify server-side issues. This involved rebooting the IP phones, making calls, and examining the internal state of the OpenScape servers using the operator console (ps, netstat, tcpdump, log analysis). Carefully selected Linux operator commands were used to identify potential weak points in the platform (netstat, uname, config files in /boot, lsmod, etc.).

SIP torture tests were conducted against the Linux kernel TCP stack. The endpoints were tested for any potential information leakage that could be used against the phone or to attack the OpenScape Voice and OpenScape Branch servers. Attempts to gain surreptitious access to the OpenScape systems were executed, along with attacks directed to the management interfaces (HTTP, SSH).

Penetration test tools used to run attacks/exploits, security scans including protocol interaction with mutated traffic, common vulnerability exploit tests, Denial of Service (DoS) and SIP server torture tests (RFC 4475) included proprietary test scripts and open-source security assessment products, BackTrack 4 and Mu Dynamic's Mu-4000 Service Analyzer. Mu Dynamic's (http://www.mudynamics.com) Mu Service Analyzer provides a complete service assurance solution for determining the reliability, availability and security of IP-based applications and services.

The Mu-4000 Service Analyzer actively and methodically probes for vulnerabilities using attack vectors. These vulnerabilities may exist as the result of an insecure protocol implementation, a known security flaw or even a bug in the beta code of the product. The Mu-4000 Service Analyzer was used to perform protocol mutations, published vulnerabilities and also external attacks using test cases and custom scripts. The Mu solution is highly automated with lights-out fault isolation. It can help speed the remediation of software flaws by providing actionable reports and complete data on any faults.

Splunk 4.14 is software that searches, monitors and reports on real-time streaming and historical IT information on the network. It searches logs, metrics and other data from programs, servers and network devices, then creates a searchable file from which it generates graphs, SQL reports and alerts. Splunk helps system administrators identify patterns, and diagnose and solve problems.

WhatsUp Gold by Ipswitch was used to scan the internal network so that we could discover what devices were present. This network management software helped us monitor which devices continued to stay online during our testing period. WhatUp Gold sends a periodic ping to the systems in its database to show availability. When a system goes offline, WhatsUp Gold displays what system has the offline status. The program offers remote view of an online system's CPU, memory and services status.

We used Nessus to scan each system in the OpenScape infrastructure to see what vulnerabilities were present. If Nessus finds vulnerabilities on a system, it will generate a short report displaying each vulnerable port. Once we were able to isolate the ports that were open, we could decide which attacks to use to bombard the exposed system.

We evaluated the viability of each attack and the risk of compromise to the SUT and recommended compensating measures to rectify or mitigate the suspected vulnerabilities.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Contact reviews@miercom.com for additional details on the configurations applied to the system under test and test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis study and test specifically for the expected environment for product deployment before making a selection.

Vulnerability Scans Conducted

A partial list of security scans, attacks and exploits included in this assessment:

Active port scans (TCP, UDP, other protocols)

TLS/SSL protocol attacks

SIP signaling attacks

RTP stream protocol attacks

TCP, UDP, and IP protocol (low level) attacks

Linux firewall attacks

Network tap (man in the middle) TCP attacks

Web server (HTML/HTTP) attacks

Address Resolution Protocol Attack Vectors

Dynamic Host Configuration Protocols (BOOTP, DHCP, DHCPv6) Attack Vectors

Distributed Network Protocol v3 Attack Vectors

Hypertext Transfer Protocol Attack Vectors

Internet Control Message Protocol Attack Vectors

Internet Protocol v4 Attack Vectors

Lightweight Directory Access Protocol Attack Vectors

Session Initiation Protocol Attack Vectors

Simple Network Management Protocol Attack Vectors

Secure Shell Protocol Attach Vectors

Secure Socket Layer/Transport Layer Security Attack Vectors

Transmission Control Protocol Attack Vectors

User Datagram Protocol Attack Vectors

TESTS RUN: IP v4, ICMP, ARP, UDP and TCP malformed

BackTrack 4 Attacks

BackTrack 4 is a Linux-based penetration testing tool. In our testing, this software was installed on a DVD-ROM so was booted from the DVD and run from it. BackTrack 4 has the abilities to gather and map network information, identify vulnerabilities, analyze Web applications, perform digital forensics and reverse engineering, and provide VoIP.

Test

The information gathering, vulnerability identification and penetration tool was used against the OpenScape Voice server and the OpenBranch server.

Observations

We were unable to gather any information or detect any vulnerabilities that would help lead to a successful penetration of the server.

Nessus Scans

Nessus was used to scan each system in the OpenScape Voice v5 environment for open ports. A single IP address or an IP address range may be inputted into Nessus to reveal vulnerable devices on the network. A system with open ports can pose a threat if they are not securely implemented.

Nessus Scan Against Node A Admin

Test

A Nessus scan was performed against the OpenScape Voice Administrator interface to find vulnerable ports.

Observations

The Nessus report revealed that the OpenScape Voice Administrator interface had port 22 or SSH (Secure Shell) open. SSH is used for secure communication between two network devices. SSH is secure because it communicates over an encrypted channel. In this network the SSH port on the Admin interface may be used for modifying or viewing configurations on the server from a remote location. It is highly unlikely that this open SSH port is a valid entry point, nor is it susceptible to eavesdropping because the communication channel is encrypted.

Nessus Scan against SIP Signaling

Test

A Nessus scan was performed against the OpenScape Voice SIP Signaling interface to find vulnerable ports.

Observations

The Nessus software could not identify any open ports during the scan. We conclude the SIP signaling interface on OpenScape Voice v5 is secure. It was not vulnerable in this situation.

Nessus Scan against OpenBranch

Test

A Nessus scan was performed against the OpenBranch interface to find vulnerable ports.

Observations

Nessus found that the OpenBranch interface did not have any open ports on the system.

SNMP Exploit

Test

We ran an SNMP MIB (Management Information Base) walk on the OpenScape Voice v5, as well as vulnerability scans.

Observations

We found SNMP to be enabled but it was not vulnerable to attacks in any way at the conclusion of testing.

Protocol Mutations and Vulnerability Scans

Protocol mutation attacks created by the Mu-4000 Service Analyzer were directed at the OpenScape Voice server and OpenBranch to test for vulnerabilities in protocol implementation. The mutation engine maps the attack surface (OpenScape Voice and OpenScape Branch servers) looking for fault conditions. These include highly specific, stateful test cases that are built based on the state, structure and semantics of protocols as well their interdependencies on other protocols.

The protocol mutation attacks described below included individual, unique deviation from the standard operation in a protocol implementation. Secure and robust targets should handle mutated packets by either dropping it or sending an error message, but an insecure target with protocol implementation flaws would respond abnormally, or not at all. We analyzed the OpenScape Voice server and OpenBranch for millions of stateful and stateless mutation possibilities for a particular protocol and all protocols on which it depends.

The open SSH port on the OpenScape Voice server was not vulnerable. We captured packets with ClearSight that were going to and from the Administrator interface and a machine that was connected to it via SSH. After reviewing, the packet captures that ClearSight produced did not show any private information that would help us successfully penetrate or eavesdrop.

A partial list of protocol mutation attacks performed follows.

DHCP Mutation Attack

Test

The DHCP mutation attack was run with 51972 different variants. Each variant/attack vector carried a single protocol mutation directed to the OpenScape Voice server. The different variants were implemented for DHCP decline, discover, inform, release, request, request renewal messages and included DHCP options.

Observations

All attack vectors were handled successfully and no faults were reported. The OpenScape Voice Server and OpenBranch dropped all mutated packets and sent error messages. No vulnerabilities in the DHCP protocol implementation at the OpenScape Voice server were detected.

FTP Mutation Attack

Test

We attempted to run an FTP mutation attack with 4,700 different variants/attack vectors. These variants were to be implemented for over 20 FTP messages/commands, covering access control commands, transfer parameter commands, connection type and FTP service commands, including FTP PORT, FTP ABORT, FTP DEL, FTP REST and others.

Observations

We were unsuccessful in establishing a connection with the OpenScape Voice and OpenScape Branch systems so that the attack on the FTP port could be run. Based on previous testing, Siemens has improved the security of their FTP protocol. No vulnerabilities were found with FTP.

ICMP v4 Protocol Mutation Attacks

Test

The ICMP v4 protocol mutation attack was run with 42,981 different variants/attack vectors. These variants were implemented in ICMP echo requests and ICMP fragmented echo request messages.

Observations

All attack vectors were handled successfully and no faults reported. The OpenScape Voice and OpenScape Branch servers dropped all mutated packets and sent error messages. No vulnerabilities in the ICMP v4 protocol implementation on the OpenScape systems were detected. ICMP v4 attacks against the SIP Signaling interface were not possible because it does not permit ICMP v4 requests.

IP v4 Protocol Mutation Attacks

Test

The IP v4 protocol mutation attack was run with 31,129 different variants/attack vectors. These variants were implemented in IPv4 datagrams and fragmented datagrams.

Observation

All attack vectors were handled successfully and no faults reported. The OpenScape Voice Server dropped all mutated packets and sent error messages. No vulnerabilities in the IPv4 protocol implementation at the OpenScape Voice server were detected.

ISAKMP Protocol Mutation Attacks

Test

The ISAKMP (Internet Security Association and Key Management Protocol) mutation attack was run with 1,882 different variants/attack vectors. These variants were implemented in ISAKMP information exchange (phase 1) messages.

Observation

All attack vectors were handled successfully and no faults reported. The OpenScape Voice Server dropped all mutated packets and sent error messages. No vulnerabilities in the ISAKMP protocol implementation at the OpenScape Voice server were detected.

SCTP Protocol Mutation Attacks

Test

The SCTP (Stream Control Transmission Protocol) Protocol mutation attack was run with 26,252 different variants/attack vectors. These variants were implemented in over 5 SCTP commands including SCTP abort, error, init and shutdown commands.

Observation

All attack vectors were handled successfully and no faults reported. The OpenScape Voice Server dropped all mutated packets and sent error messages. No vulnerabilities in the SCTP protocol implementation at the OpenScape Voice server were detected.

SIP Protocol Mutation Attacks

Test

The SIP (Session Initiation Protocol) Protocol mutation attack was run with 12,018 different variants/attack vectors. These variants were implemented in SIP ack, bye, cancel and SIP torture test messages (RFC 4475).During the SIP mutation attack, Mu analyzer acts as the SIP client and the OpenScape Voice server is the SIP server. The mutations used TLS v1 as the layer 3 transport protocol and IP v4 as the network layer protocol.

Observation

All attack vectors were handled successfully and no faults were reported. The OpenScape Voice and OpenScape Branch servers dropped all mutated packets and sent error messages. No vulnerabilities in the SIP protocol implementation at the OpenScape servers were detected.

Other Analysis Conducted

A summary of the compound exploits and other analysis conducted in the OpenScape Voice v5 and OpenScape Branch v1 Security Assessment:

Log Files Examined – Evaluation included the logs in the OpenScape products including messages emitted by certain SOAP software components involved in SIP login parameter processing. The presence of passwords or other sensitive information in log files was checked. In examining the log, we found no sensitive information.

Port scanning and Enumeration – Open source tool Nmap was used to scan the OpenScape server for any unused open ports, OS fingerprinting, version numbers, protocols supported, services running, and other information that could be used to attack the OpenScape Voice server. Only in-use ports were found to be open ICMP only at the Admin and Billing interfaces of the OpenScape Voice server. All ports except those in use were found to be filtered or closed. ICMP was detected to be disabled at the SIP signaling interface and majority of the port scans and enumeration attempts were successfully blocked.

Integer and Buffer Overflow Tests – These mutations add, insert or replace input with a large number of random bytes in an effort to cause the data to exceed the boundaries of its specified location. Overflow attacks exploit the method computers use to store integers, which are variables that represent real, non-fractional numbers. Humans represent integers in decimal format (using 10 numerals, 1-10), but computers store integers in binary format (using two numerals, 1 and 0). If the operation produces a value larger than the maximum integer size for the data, an integer overflow occurs. These potential integer overflow conditions were verified to not cause buffer overflows.

Fragmented attacks – Fragmented packets were used to infiltrate and cause degradation in server performance. Such fragmented packets can get past ACLs (Access Lists) in stateless packet filtering deployment and be further used to cause DoS. Teardrop, overlapping fragment attack and tiny fragment attack were tested with the OpenScape server. No vulnerabilities were found after the fragmented attacks were applied.

Denial of Service and Packet Filtering

Denial of Service (DoS) attacks were generated and directed at the OpenScape Voice SIP signaling, admin and OpenScape Branch to gain insights into reliability, availability and security of service in the face of DoS attacks or extreme amounts of service level traffic. While attacking the OpenScape servers, our objective was to saturate it to the extent that it could not respond to legitimate traffic, so that it would become unresponsive and slow, or that it would crash or reboot, which all can lead to failures at the SIP phones.

Metasploit, BackTrack 4 and the Mu Dynamics Mu-4000 Service Analyzer were used to configure 28 different DoS attacks with fixed and randomized source ports (IP and MAC addresses), TTLs, TCP sequence numbers, payload, user defined TCP header values, randomized protocol types and other values for the attack packets. Attack patterns included different start/end rate (packets /sec), duration of attacks and number attack iterations. Target availability and response time was verified at defined intervals during the attacks using ICMP.

The OpenScape Voice and OpenScape Branch servers were preconfigured and hardened to counter DoS attacks. The defenses included a Layer 3 integrated packet filter and traffic rate limiting. Incoming traffic was monitored using integrated IDS (Intrusion Detection System). The rate threshold configured to counter DoS attacks was set to 200 packets/ sec, so any IP address exceeding this dynamically got added to the blacklist and all subsequent messages from that IP were blocked for an administrator defined time interval. In this case, we found the block period to be 60 seconds.

A partial list of DoS attacks used and results are discussed below:

IKE v1 Aggressive Mode and IKE v2 Security Association Initialization DoS

Test

Attack UDP packets containing IKE v1 payload were used. The parameters defined included TOS (Type of Service) as value zero, TTL set at 64, randomized identifiers, IP options enabled and other IPv4 header settings. The source and destination port were set at 500 ISAKMP. Binary string with exchange type 04 was used for aggressive mode and exchange type 22 for IKE_SA_INIT. All three interfaces (SIP, billing and admin) were targeted for this attack.

This attack was repeated with a packet rate ranging from 199 packets/sec to 100,000 packets/sec and randomizing the source IP address with a 24 bit mask.

Observations

The attacks were blocked and the server log indicated that the IP addresses (static and spoofed random addresses) of the attack platform were blacklisted for 60 seconds. No calls were dropped and the SIP phones did not lose telephony.

DHCP Discover DoS

Test

Attack UDP packets containing DHCP Discover messages were broadcast from the attack platforms. The parameters defined included TOS (Type of Service) randomized, TTL set at 64, randomized identifiers, IP options enabled and other IPv4 header settings. The source port of the DHCP client was set to 68 and the destination port of the DHCP server was set to 67. Binary string payload with random hex digits and ASCII values were used. All three interfaces (SIP, billing and admin) were targeted for this attack.

This attack was repeated with packet rate ranging from 199 packets/sec to 100,000 packets/sec and randomizing the source IP address and MAC address.

Observations

The attacks were blocked and the server log indicated that the IP addresses (static and spoofed random addresses) of the attack platform were blacklisted for 60 seconds. No calls were dropped and the SIP phones did not lose service.

ICMP Source Quench DoS

Test

Attack IP packets containing ICMP source quench messages used to request the target to decrease traffic rate were sent from the attack platforms. The parameters defined included TOS (Type of Service) randomized, TTL set at 64, randomized identifiers, IP options enabled and other IPv4 header settings. The protocol field was set at 1 for ICMP protocol. Binary string payload consisted of ICMP type set at 04 and ICMP code at 00. All three interfaces (SIP signaling, admin, and OpenScape Branch) were targeted for this attack.

This attack was repeated with packet rate ranging from199 packets/sec to100,000 packets/sec and randomizing the source IP address and MAC address.

Observations

The attacks were blocked and the server log indicated that the IP addresses (static and spoofed random addresses) of the attack platform were blacklisted for 60 seconds. No calls were dropped and the SIP phones did not lose service.

ICMP Address Mask Request DoS

Test

These attack IP packets contain ICMP Address Mask requests. A host receiving address mask request should respond with the address mask field set to the 32-bit mask of the bits identifying the subnet and network, for the subnet on which the request was received. The parameters defined included TOS (Type of Service) randomized, TTL set at 64, randomized identifiers, IP options enabled and other IPv4 header setting. The protocol field was set at 1 for ICMP protocol. Binary string payload consisted of ICMP type set at 11 and ICMP code at 00. All three interfaces (SIP signaling, admin and OpenScape Branch) were targeted for this attack.

This attack was repeated with packet rate ranging from199 packets/sec to100,000 packets/sec and randomizing the source IP address and MAC address.

Observations

The attacks were blocked and the server log indicated that the IP addresses (static and spoofed random addresses) of the attack platform were blacklisted for 60 seconds. No calls were dropped and the SIP phones did not lose service.

IPv4 DoS Attacks

Test

The IPv4 DoS attack was run against the OpenScape Voice and OpenScape Branch servers. They were both attacked with 100,000 packets/second for a total of 1 minute and 955 milliseconds.

Observations

The attacks were blocked and the server log indicated that the IP addresses (static and spoofed random addresses) of the attack platform were blacklisted for 60 seconds. No calls were dropped and the SIP phones did not lose service.

SIP Register DoS

Test

These attack packets contain SIP register messages. The parameters defined included TOS (Type of Service) randomized, TTL set at 64, randomized identifiers, IP options enabled and other IPv4 header setting. The source and destination port number were set at 5060 SIP and then at 5061. The ASCII payload included added control and Hex digits. The frequency of the DoS attack packets was set at a ramp like profile (steady increase or decrease of attack packets). TCP header settings were set with varying flags, window size and urgent pointers. The SIP signaling interface and admin interface were targeted for this attack.

This attack was repeated with packet rate ranging from199 packets/sec to 100,000 packets/sec and randomizing the source IP address and MAC address.

Observations

The attacks were blocked and the server log indicated that the IP addresses (static and spoofed random addresses) of the attack platform were blacklisted for 60 seconds. No calls were dropped and the SIP phones did not lose service.

SIP Invite DoS

Test

These attack packets contain SIP invite messages. The parameters defined included TOS (Type of Service) randomized, TTL set at 64, randomized identifiers, IP options enabled and other IPv4 header setting. The source and destination port number were set at 5060 and then at 5061. The ASCII payload included added control and Hex digits. The frequency of the DoS attack packets was set at a step like profile (incremental increase or decrease of attack packets). TCP header settings were set with varying flags, window size and urgent pointers. The SIP signaling interface and admin interface were targeted for this attack.

This attack was repeated with packet rate ranging from199 packets/sec to 100,000 packets/sec and randomizing the source IP address and MAC address.

Observations

The attacks were blocked and the server log indicated that the IP addresses (static and spoofed random addresses) of the attack platform were blacklisted for 60 seconds. No calls were dropped and the SIP phones did not lose service.

SIP Torture Test DoS

Test

These attack packets contain SIP torture test messages. The parameters defined included TOS (Type of Service) randomized, TTL set at 64, randomized identifiers, IP options enabled and other IPv4 header setting. The source and destination port number were set at 5060 SIP and then at 5061. The ASCII payload included added control and Hex digits. The frequency of the DoS attack packets was set at a ramp like profile (steady increase or decrease of attack packets). TCP header settings were set with varying flags, window size and urgent pointers. The SIP signaling interface and admin interface were targeted for this attack.

Observations

The attacks were blocked and the server log indicated that the IP addresses (static and spoofed random addresses) of the attack platform were blacklisted for 60 seconds. No calls were dropped and the SIP phones did not lose service.

Attacks with Spoofed SIP phone IP Address

Description

Attacks were repeated with the source IP address of the attack packets spoofed to be the IP address of the SIP phones. The IP address of the SIP phones could be obtained by using open source tools like pingsweeps, nmap or from the SIP phone itself. The objective of this test was to blacklist the SIP phones IP address and thereby causing disruption in telephone service.

Test

The OpenScape Voice Server was configured for rate limiting threshold of 200 packets/sec. DoS attacks with spoofed source address of the SIP phone were directed to the OpenScape Server at a user defined packet rate.

Observation

With packet rate of the DoS attacks set at 10,000 packets/second, the spoofed IP address of the SIP phones was added to the blacklist for 30 seconds. Phones lost SIP signaling and telephone service was disrupted for 30 seconds (as long as the IP address is blacklisted). After the blacklist period expired, the IP addresses of the phones were removed from the blacklist and the phone came back up and telephone service resumed. Although this attack can render individual phones temporarily unavailable, the OpenScape Voice server successfully thwarted this attack from causing a widespread outage.

High Availability of OpenScape Voice Server

Description

Verify and assess carrier grade reliability and high availability of the OpenScape Voice deployment.

Test

The high availability of the OpenScape Voice application was demonstrated by deploying an OpenScape Voice cluster with two servers and implemented the use of VIP (Virtual IP address). One OpenScape Voice server node was intentionally made to fail and telephone service was observed for any disruptions.

Observations

OpenScape Voice server failover was simulated by dropping a link between the redundant OpenScape Voice server nodes. We observed that phones were still able to place calls.

Each cluster server node is assigned a VIP. Upon failure of one server node, the peer server node takes over the VIP of the failed server node and assumes session control for all devices assigned to that VIP.

Upon failure of OpenScape Voice Server A, VIP A was taken over by OpenScape Voice Server B. SIP phones lost telephony for a brief period (approximate average 30 seconds) - the transition time for failover of VIP A to OpenScape Voice Server B, and full telephony operation was restored and all traffic was being directed to the OpenScape Voice Server B.

Once the OpenScape Voice Server A was brought back on-line, it once again resumed the role of an active server, and full telephony operation was restored with VIP A taken over by OpenScape Server A.

Additional Notes

The security counter-measures of this VIP scheme were not evaluated. Since it is an integral part of the OpenScape Voice application, we recommend secure deployment of this hot standby topology, including use of authenticated keep-alive packets between the master and all backup servers.

Survivability of OpenScape Branch Server

Description

Verify and assess survivability of the OpenScape Branch deployment when it becomes isolated from OpenScape Voice cluster.

Test

The survivability of OpenScape Branch was demonstrated by intentionally disabling its WAN connection between the branch and to the OpenScape Voice server. Telephone service at the branch was observed for any disruptions.

Observations

OpenScape Branch survivability was simulated by disabling the WAN connection from the OpenScape Branch server to the OpenScape Voice server cluster. We observed that phones that were part of the OpenScape Branch server were still able to originate and terminate calls. OpenScape Branch sustained branch communications while there was no connectivity to the OpenScape Voice cluster.

Verification of Cryptographic TLS

Description

This test confirms the TLS-protected connections used for SIP signaling are configured to use sound cryptographic operating values. The SUT is checked for cryptographic algorithms used, key length and use of proper TLS protocol options. The likelihood of misconfigured TLS cryptographic parameters depends on the initial configuration at time of deployment, expertise of the installer(s), documentation, etc. If weak cryptographic algorithms, vulnerable or outdated TLS protocol options are used, it is possible the TLS protection mechanism can be compromised.

Test

The TLS cryptographic parameters were tested for use of strong keys and secure algorithms and the recommended TLS protocol settings.

Observations

Diagnostic tools were used to confirm proper TLS configuration for OpenScape Voice v5 was employed.

Packet Sniffing of SIP Voice Calls

Description

If packet traffic between the server and endpoints is not properly encrypted, sensitive information may be leaked, including but not limited to, details of the network infrastructure and the RTP audio stream during voice calls.

Test

Clearsight Analyzer version 6.9 was used to monitor the phone PC port for data leakage during endpoint initialization, as well as SIP traffic between the servers and endpoints during actual voice calls to verify Secure Real-time Transport Protocol (SRTP) and Secure TLS.

Observations

Packet captures were collected during SIP calls placed between endpoints with SRTP both disabled and enabled to verify the effect of encryption on the audio. With unencrypted RTP, clear audio was captured as expected. SRTP was then enabled, and new calls were placed. The audio stream was encrypted and appeared as white noise when replayed from the packet capture file (pcap). At the endpoints themselves, we were pleased to note that audio quality was not compromised as an effect of the encryption process.

TLS authentication of the SIP phones with the server was verified through analysis of packet captures taken during SIP calls. Packets were transmitted on port 5061, which demonstrated that TLS was in use, and deeper inspection of the TCP stream revealed no sensitive information from the encrypted data. We were impressed that no VLAN or TFTP server information was exposed, a security vulnerability we have seen on other UC solutions.

Viruses, Worms and Botnets

Description

These are specific variations of DoS attacks. The objective is to identify weaknesses that could affect reliability, availability, and security of the network. A botnet attack would be characterized by multiple systems attempting to access the OpenScape server, but with much higher than normal frequency, causing the system to become unavailable. Blacklist library size can play a key role in mitigating this type of attack. The Witty worm exploits a firewall application vulnerability, targeting systems that have employed proactive countermeasures, and includes a destructive payload. Infected hosts send packets as fast as an Internet connection will allow in order to propagate the worm. The Slammer worm also exploits similar buffer overflow vulnerabilities infecting hosts and randomizes destination IP addresses to enable further propagation.

Test

The Mu Dynamics Mu-4000 Service Analyzer was used to evaluate the effect of these attacks on the server's various interfaces. Interface availability was monitored, as well as any undesirable effect on operation. VoIP calls were placed throughout the test at a rate of one call per second, and the call completion rate was also monitored. By randomizing the source port and address during these attacks, the behavior of a botnet was emulated. Witty and Slammer worm DoS attacks were configured with random source and destination IPs.

Observations

These attacks were unsuccessful in disrupting the operation of the system. Real-time monitoring and post-test analysis of the server logs indicated successful blocking of the attacking source addresses. The OpenScape servers and interfaces remained available, and VoIP calls continued to be placed successfully during the attacks.

SIP Resource Exhaustion Test

Description

SSL/TLS test tools were used to connect to the OpenScape Voice server and determine if connection times out, or otherwise allows for a resource exhaustion attack. No protocol skill is required to execute this type of attack. It is possible a virus could crudely provide this exploit to cause a DoS attack. Such an attack, if successful, would consume all the SIP signaling resources of the SIP server and prevent legitimate calls from registering.

Test

SIP server port was identified. OpenSSL was used to establish a TLS connection to the SIP server and exhaustion test was conducted.

Observation

The OpenScape Voice Server implemented an inactivity time out of 2 minutes at the SIP signaling interface. This time out period is configurable and user defined.

Utilization of this time out mechanism for SIP signaling mitigates the ability of an attacker to establish illegitimate connections and consume resources.