VmSat
(VoIP monitoring & Security assessment tool)

College: Pune Institute of Computer Technology, Pune

Team Members:
Krishna S. Ghodke
Saurabh A. Gawande
Roshan R. Ghumare
Sumant D. Kukkar

Sponsored By:
GREAT SOFTWARE LABORATRY PVT. LTD. (GS Lab)
(www.gs-lab.com)

Contact: vmsat.pict@gmail.com

External Guide
Mr. Avinash Shenoi
Mr. Vivek Relan

Internal Guide
Mr. Tushar Rane
I] Idea and concept behind the Project:

The deployment of Voice over Internet Protocol (VoIP) instead of traditional communication system has helped in huge reduction in operating costs, as well as enabled adoption of next generation communication services using IP infrastructure. There exist many vendors which provide VoIP services. But a comprehensive monitoring/assessment mechanism is required to verify the claims made by vendor company to client organization.

Considering the above requirements we propose a “VoIP Monitoring and Security Assessment Tool” (VmSat). This tool monitors, analyzes and tests the VoIP infrastructure and services provided. The first part of this tool monitors and performs the analysis of the real time VoIP traffic for troubleshooting the infrastructure. It provides various quality metrics for voice traffic in terms of bandwidth utilized, delay, jitter, packet loss, R-Factor and MOS. It provides comprehensive remedial reasoning for quality deterioration. The second part of the tool assesses the VoIP infrastructure against security threats. VmSat provides several most generic attack templates and launches attacks (flood attacks, message attacks etc) within the system to identify the vulnerabilities present in the system. Robustness of SIP protocol implementation is assessed through rigorous checks. VmSat also provides most comprehensive and generic Meta language to assist in generating any custom attacks. It consists of a plaintext format like an English sentence which provides great flexibility to the user. Once vulnerabilities are identified it provides remedial information that enables security professionals to perform appropriate actions.

Following are the application of VmSat:

- To aid owners/users of VoIP infrastructure to test, audit, and uncover security vulnerabilities in their deployments.

- To aid third parties to test, audit, and uncover security vulnerabilities in the VoIP infrastructure of owners of said infrastructure who contract with or otherwise expressly approve said third parties to assess said VoIP infrastructure.

- To aid producers of VoIP infrastructure to test, audit, and uncover security vulnerabilities in the VoIP hardware/software/systems they produce.

- For use in collective educational endeavors or use by individuals for their own intellectual curiosity or aggrandizement.

Thus user can rely on this tool to penetrate the VoIP deployment for finding vulnerabilities in the network.
II] Salient Features:

1. Real Time Monitoring:
   - Proactive monitoring of Bandwidth utilization and QoS metrics such as Jitter, Latency, Packet loss.
   - ITU standard E-Model based MOS calculation.
   - Pictorial representation of the call flow, plotting all the SIP requests/response that took place from start to end of call. This comes in handy for debugging error calls.
   - Call categorization such as complete, incomplete, unanswered, error, good and poor quality calls.
   - Flexible filtering of data based on IP address and caller name.
   - Alarm generation on vital parameters viz., Too many consecutive incomplete calls, SIP Errors, High Average Delay, Jitter and Packet-Loss.
   - Web Based User Interface for platform independence.

2. Power-Off and System-Crash situations:
   Power-Off and System-Crash situations for both Server & Clients are handled. It helps the administrator to identify the reason of the Failed or Incomplete calls.

3. Infrastructure Discovery:
   Discovery of the SIP components viz, SIP Server, SIP Client.

4. Attacks:
   Three categories of attacks for Vulnerabilities detection:
   - Protocol Checks
   - SIP Message attacks (Bye, ReInvite, Replay)
   - Flooding attacks (DoS attacks)

5. Attack Templates & Meta language:
   - VmSat provides several generic attack templates which are used to perform attacks. It intakes customized datasets from the administrator.
   - A Meta language is constructed using LEX and YACC which provides the mechanism to the user for generating various attacks, through user mindset.

6. Configurable SIP Packet Generator:

7. Comprehensive Reports:
   The reports give the administrator a quick and most probable reason for quality deterioration and the vulnerabilities present in the VoIP infrastructure.
III] Technological Specification:

1. VmSat is implemented in Java.
3. XML is used for developing state machine for call flow and scenario generation of the VoIP calls (for SIP Protocol). Use of XML allows extension of scenarios. XML helps to provide compliance with wide variety SIP implementations.
4. Web-based UI in JSP, AJAX javascript, servlet allowing remote access.

IV] Implementation Strategy:

Diagram 1 shows the position of VmSat in VoIP infrastructure. VmSat sniffs the traffic flowing through the SIP Proxy using a trunk/mirror port of the switch.

Diagram 2 shows the architecture of VmSat. It has two phases:

1. Traffic Monitoring
2. Vulnerability Assessment

Traffic Monitoring [Diagram 3]

Traffic Monitoring and analysis is implemented by sniffing the packets over network using ‘Jpcap’ (a packet capture library). The call traffic is identified using a XML parser and call quality is determined by analyzing the captured RTP packets against various parameters. All the data is stored in MySQL database. A platform independent web based GUI provides the administrator to view the results.

Traffic Monitor includes two threads:

Thread 1: Sniffer
Algorithm:
1. Capture the packets.
2. Identify the protocol of packet.
3. Dissect the packet and extract necessary information required as per protocol (SIP or RTP).
4. Insert the information objects in Queue.

Thread 2: Processor
Algorithm:
1. Delete the information object from Queue.
2. Differentiate information object as per protocol and submit it to respective processor.
3. Calculate & analyze information object and generate information.
4. Store necessary information in database.

Snapshots of GUI of Traffic Monitor are shown in Diagram 4.
**Vulnerability Assessment** [Diagram 5]

Implementation of security assessment involves performing various checks and attacks against the deployed infrastructure. These attacks are performed by user using a predefined template on a web based interface. In addition, a facility is provided that enables user to write custom attacks using a Meta language, implemented using LEX and YACC.

**Working of phase:**
1. SIP components (SIP servers, clients’ soft phones etc) in the system are discovered and information is stored in `config.db`.
2. User provides the attack details through input system.
3. Attack system initializes attack parameters by using `config.db`.
4. Attack is launched.
5. System identifies status of attack by consulting with `symptoms.db`, which contains predefined parameters about attack for recognition.
6. Attack is stopped by using stopping condition for respective attack.
7. Based on status of system after attack, reports are generated which provides complete description of vulnerabilities found along with recommendation.

**VI] Commercial viability:**

**Need in the market:**

Cost-based analysis of industry usage of VoIP services shows the growth of VoIP market. Most of VoIP providers have adopted SIP implementation; however, corporations have not been deploying the technology because of its inherent security weaknesses. Our project helps the VoIP providers as well as users to overcome these security hurdles. Thus the contribution of the project towards VoIP market can be estimated on the basis of huge market value of the VoIP services, which is growing fast every year. This proves the importance of project in terms of market value and usage. Hence, the need of product is justified.

**Alternatives:**

Though different alternatives exist for VmSat, VmSat is one of its kinds which provide both Traffic Monitoring and Vulnerability Assessment. Existing products don’t provide language or customized attack, so it is difficult for the user to find out various other vulnerabilities present in the network. The *Meta Language* (plain English language format) feature of VmSat provides greater flexibility to the user for performing attacks, thus helping him to find out any new vulnerability in the network or protocol implementation which he can think of.
Diagram 1: VoIP Infrastructure Overview

Diagram 2: Architecture of VmSat
Diagram 3: Design of Traffic Monitor
Diagram 4: Snapshots of Traffic monitor
Diagram 5: Design of Vulnerability Assessment
VII] References:

Books:
1. VoIP Hacking Exposed by David Endler and Mark Collier
2. VoIP Practical Security by Thomas Porter
3. VoIP Security by James Ransome and John Rittinghouse
4. SIP Demystified by Gonzallo Camarillo

URL:
1. www.hackingvoip.com
2. www.voipinfo.org
3. www.asteriskguru.com