Security Measures for Converged Networks

June 2005

Author: Ramana Mylavarapu
# Table of Contents

I. **Introduction** ..............................................................................................................................................3

II. **Converged Services Security Threat Analysis** .........................................................................................3

   - **Infrastructure Risks** .................................................................................................................................3
     - Unauthorized Remote Access .......................................................................................................................4
     - Denial of Service Attacks ............................................................................................................................4
   - **Unauthorized Remote Access** .................................................................................................................4
   - **Denial of Service Attacks** .........................................................................................................................4
   - **OS, Support Systems and Applications Attacks** ..................................................................................4
   - **Technological Frauds and Social Engineering** ....................................................................................4
   - **Subscription Frauds** ...............................................................................................................................4
   - **Ignorance and Imperfect System Management** ..................................................................................5
   - **Protocol Vulnerability, Buffer Overflow, Flooding** ............................................................................5
   - **Intermediate Routers** .............................................................................................................................5
   - **Signaling Servers** ....................................................................................................................................5
   - **VoIP System Risks** ..................................................................................................................................6
     - **Replay, Insertion and Distortion** .........................................................................................................6
     - **Spam, Virus and Worm Attacks** ...........................................................................................................7
     - **Identity thefts** .........................................................................................................................................7
     - **Diverting Voice Streams** ......................................................................................................................7
     - **Interception, Monitoring or Eavesdropping** ....................................................................................7
     - **Rogue Proxy / GK** ......................................................................................................................................7
     - **Tampering Call Detail Records** ...........................................................................................................7
     - **Anonymous/ Malicious and Spam Calls** ............................................................................................7
     - **Caller ID blocking / Tampering** ...........................................................................................................7

III. **Remedial Measures** ................................................................................................................................8

   - **Border Element Security** .......................................................................................................................8
     - **Firewalls Specially Designed for VoIP Gateways** ..............................................................................8
     - **SIP Protocol Robustness** .....................................................................................................................9
     - **QoS Considerations** ..........................................................................................................................9
     - **Intrusion Detection and Prevention Systems** ....................................................................................9
     - **VoIP Security** .......................................................................................................................................10
       - **Secure Provisioning** ............................................................................................................................10
       - **User Authentication** ...........................................................................................................................10
       - **Signaling Security** ................................................................................................................................10
       - **Media Security** ..................................................................................................................................11
       - **State of Adoption** .............................................................................................................................12

IV. **Intoto’s Product-line for Secure Converged Networks** .............................................................................13

V. **Conclusion** ...............................................................................................................................................15
I. Introduction

In today’s converged networks, several forms of information--data, voice, audio, video and multimedia, are transmitted over a common network infrastructure. These services are accessed by consumers through integrated communication access devices. Operation support systems are built to provision these services, operate and manage the network from a common management infrastructure. In order to achieve manageability the network elements in access, edge and core of the network are migrating to TCP/IP based. Thus, convergence is possible due to availability of Internet service at low cost data bandwidth, consolidation of usage charges and toll charges, QoS assurance through protocols, open standards and availability of inexpensive and fast RISC/DSP processors.

While the end user benefits from high quality services at lower costs, service providers inherit IP security risks with converged services. During the early phases of deployment, service providers were concerned about quality of service considerations such as voice quality and latency, and the interoperability of the systems. As converged services become more mature and being deployed in a larger scale, the focus is shifting towards security measures, one of the core issues to be considered for undisrupted converged services.

II. Converged Services Security Threat Analysis

IP networks are based on open standards and prone to threats for various reasons. An attacker tries to access servers to gain access to vital information of an organization or misuse voice services by unauthorized access. The attackers/fraudsters can be corporate insiders, customers, or any outsider who knows how to exploit the weaknesses of the organization’s system and policies.

Infrastructure Risks

IP-based services are also prone to vulnerabilities. Voice services are highly critical and equally subject to attacks. Like IP services, VoIP networks are vulnerable to Denial of Service attacks, worms, viruses, etc.
VoIP network elements that can transmit the attacks are access devices like soft phones, terminal attacks, VoIP media servers, proxies, etc. The operating systems used for building these equipment is same as that of IP networks, which are also prone to attacks. Protocols used for VoIP service access and call control can also be exploited, resulting in network element failures that make the service unreliable. A robust security defense system takes care of these specific threats as well.

Some of the infrastructure risks are as follows.

**Unauthorized Remote Access**

Attackers may gain unauthorized assess to the network elements. This would result in modifying the equipment configurations, customer sensitive information such as billing records, entitlements, etc. This results in customers losing confidence on the service provider and the service.

**Denial of Service Attacks**

Like any other IP network element, the VoIP network elements are subject to DoS attacks. The attacks are targeted on the core devices such as PBXs, servers and media gateways which serve a large number of end points and customers.

**OS, Support Systems and Applications Attacks**

Most systems are built on popular operating systems which can be vulnerable to attacks. Access devices such as IP phones, VoIP TAs and gateways are based on operating systems which are embedded or Windows/UNIX/Linux-based. Embedded operating systems are more secure than the PC-based operating systems. Applications that run these devices are prone to vulnerabilities.

Other equipment such as voice mail servers, LDAP servers, Web servers, databases used in provisioning the service are also subjected to attacks. Any malfunction or overloading of these servers would result in poor service.

**Technological Frauds and Social Engineering**

External fraudsters or insiders of an organization get access to the network equipment and make phone calls through the system or sell the service illegally to others. An insider intrusion is more intense than external intrusion for the obvious reason that the people who maintain the systems would be involving in committing the fraud. The insiders who are technically knowledgeable try to discover shortcut methods to access the system and configure it. This will result in a hacker to learn internal procedures by packet sniffing.

**Subscription Frauds**

Subscription frauds happen when a fraudster customer applies for the service and tries to misuse the service by making calls to international destinations, premium rate services or call sales within short time frames, resulting in large telephone bills. The fraudster may collude with insiders and exploit the weakness of the systems and access the services for which he/she is not authorized. The fraudster later disputes the calls and does not pay for them. This fraud results in leakage of revenue or large outstanding amounts due to disputed bills.
Ignorance and Imperfect System Management

While providing services and assisting customers, operations personnel who are fully aware of the system and its configuration may inadvertently create security holes in the system. This may result in hackers accessing the systems with less effort. Some examples for this risk are improper configuration of customer accounts, security access policies, trivial authentication information like login, enabling remote access and leaving it open, etc.

Protocol Vulnerability, Buffer Overflow, Flooding

Attacking the network elements with genuine or imperfect signaling and bearer protocol traffic may result in traffic overloading beyond its dimensioned load, losing its function partially or fully. The header/message contents which are less or greater than the recommended sizes may result in the software overwriting/corrupting valid data in the system. This may result in system crash or malfunctioning. UDP flooding using chargen and echo services provided by the system. Ping of death, IP reassembly attacks, smurf attack, etc. The excess traffic will result in the server responding slow to the actual VoIP call setup requests which results in poor call completion rates and artificial call attempts and network congestion.

Intermediate Routers

The routers that come in the path while accessing the service are also vulnerable for the attacks. While providing VoIP service, access to the servers in the Internet will be needed. The access could be to initiate remote configuration download, resync of the device or offering inward calls. There is a possibility of spoofing the server address and make the device believe that it is a genuine server and accept whatever malicious information it provides. The firewall in the router provides application layer gateway (ALG) functionality for the signaling protocols. The firewall should be able to support multiple sessions and statefully maintain the sessions. Any imperfections in the ALG functionality will result poor VoIP service. The ALG should allow inward call requests to the devices only from the device registered server/endpoints and it should dynamically allow inward media packets only on call set up. These media sessions are to be disabled on connection tear down.

Signaling Servers

The signaling protocols are designed for ease of implementation, interpretation and analysis, therefore they cannot be secure themselves. A SIP proxy or redirect server / H.323 Gatekeeper enables call setup between two clients. The SIP proxy adds addressing information for statefully controlling the call and both clients will communicate through the proxy.

The security risks in a signaling servers are:

Client Impersonation

The SIP protocol enables registration of multiple contacts for a given user. The ‘To’ and ‘From’ header fields will be different to enable several contacts for a user. By impersonating the client, a fraudster can register his own contacts and make the incoming and voice mail notifications to the redirected contact addresses.

Server Impersonation

The client registers with a genuine server. The call setup requests are intercepted by a fake server and a spoofed response is sent to the client which tells the client that it shall send its call setup request to a new server. The calls from the client will be failing or they get connected to attacker’s endpoints. The same
approach can be adopted for register requests from client to server. The register requests get redirected to a fake server. This results in a client getting connected to an unknown server and sharing the server’s credentials.

**Message Tampering**
A proxy server enables call set up and exchange of information between clients for call set up and media streaming. If compromised, the proxy server which is considered to be a trusted intermediate element can know the media session encryption method and the keys. It could change the security options for specific calls, redirect the media streams to a fake device or make the media stream unreachable to the actual destination. The media streams will be decrypted for wiretapping / eavesdropping.

**Session Tampering / Hijacking**
After a call is established, messages exchanged for session renewals, codec negotiations requests during call and forging of messages are possible. When a client expects a session renewal message periodically, the SDP information is tampered to divert the media stream to a fake device for wiretap or the request is declined by sending a fake BYE message for the request or abruptly sending a BYE when the conversation is going by forging a message.

**Signaling Requests Resulting in DoS Attacks**
The proxy servers process registration requests and call setup requests from the clients. They are reachable over a standard port number. Flood of such requests can be simulated by the attackers by possessing a valid account but spoofing source IP addresses. The attacker can register for multiple contacts and setup call requests to the device which result in server forking of multiple connections to these contacts. SIP requests with record route headers will result in server maintaining multiple transaction. Flooding the server with call setup requests simultaneously from multiple devices will result in server overload and denial of service.

**VoIP System Risks**
The VoIP services are based on the TCP/IP protocols over Internet. The networks are becoming more and more complex, and the attackers equally are working on how to exploit them. Some of the attacks on VoIP networks are discussed below.

**Replay, Insertion and Distortion**
The signaling and voice packets exchanged are intercepted and replayed, some extra information is appended to the packet or the information is altered and the packet is sent over the network again. The packet looks like a genuine packet and the receiving end point processes it. This attack is possible due to physical layer and network layer security. The packets can be captured using simple L2 sniffers and altered. Tools such as Voice Over Misconfigured Internet Telephones (VOMIT) are used to introduce extraneous voice packets. This kind of man in the middle attack is possible by providing IP address to the device using a rogue DHCP server in the LAN. The traffic in and out of the device is routed through the equipment that provided the IP address. If the configuration information that is downloaded by the device is not secure, then the man in the middle attacker can change the configuration information. This technique allows recording a conversation and playing it back intelligently when a call is received by the same person to the other party. The person’s voice is synthesized based on the conversation recorded and played back to the others. Rogue RTP packets can be generated and sent with the same IP address, UDP port number of an ongoing conversation and make server/ device to process junk packets which will overload the DSP and overload the server.
Spam, Virus and Worm Attacks

These attacks which are common in IP network endpoints are possible on VoIP devices as well.

Identity thefts

The user credentials of another user are stolen and used for gaining illegal access to the VoIP service. The VoIP device identity such as MAC address, serial number, etc., is stolen to gain access to the service. The same can also be used to insert, alter or distort voice streams. The user identity theft can result in the attacker modifying user settings such as forwarding all calls to another number where the voice mail/auto answering machines can record the messages meant for the user.

Diverting Voice Streams

The device which is in conversation can be asked to send the voice frames to an equipment used for a man in the middle attack by sending a change in Gateway MAC address using ARP protocol. This then voice packets are sent to the fake gateway.

Interception, Monitoring or Eavesdropping

Specialized equipment which follows the signaling messages in real-time and the associated voice streams logs them in a centralized server and recorded. The information collected can be processed to generate the call detail record and the associated conversation. This technique which is generally used by law enforcement agencies can be misused by attackers for unlawful activities.

Rogue Proxy / GK

By altering the phone configuration information, incoming calls can be diverted to a rogue server. The server handles incoming calls to the device and the server acts as a fake device and tries to answer incoming calls and diverts the call to a voice mail server.

Tampering Call Detail Records

The gatekeepers/servers generate partial and complete Call Detail Records (CDRs) for the calls made through them. These records are emitted by the servers and sent over the Internet to a billing center. While sent, this information is collected and altered real-time to the advantage of the user. The record is identified based on the user ID and Call ID for that call and modified. By this method, no one will be able suspect that the information is altered as there is no loss of information except for the possibility of a slight delay in the transmission.

Anonymous/ Malicious and Spam Calls

An attacker can make calls to a VoIP phone from public call offices or pay phones and create nuisance to the customer. This makes it very difficult to trace the attacker. The software should be able to authenticate the inward caller / filter the calls based on caller phone number or name. The software should dynamically build a list of spam calls and make it available to the user for scrutiny.

Caller ID blocking / Tampering

Caller ID restriction can be enabled per call whereby the caller ID/name are blocked by specifying privacy options during call setup. The caller ID can be altered to mislead the called party. This makes it very difficult to trace the actual caller.
III. Remedial Measures
VoIP devices, gateways, servers, voice mail and unified messaging systems, billing systems of the VoIP network shall be equipped with software that can detect and prevent infrastructure attacks. The network shall be secure enough to overcome VoIP system risks. The complexity of this software varies on the type of the device, its usage/application and criticality in the network. The remedial measures recommended here are focused on the converged network elements.

- Organize the corporate network by using L2 switch hierarchy. Maintain a separate virtual LAN network for handling VoIP within the corporate LAN. This will prevent packet loss, jitter, free from attacks in the internal network
- The voice traffic need to be encrypted to avoid sniffing of the signaling and voice packets.

Border Element Security
Access to the VoIP servers is provided through Session Border Gateways (SBCs). SBCs are the network elements which are most prone to the infrastructure and VoIP service attacks. SIP proxies and media servers are behind the SBC.

Firewall and NAT Traversal, Topology Hiding
The Firewall provides access to the devices for registration and making calls through the VoIP servers. The Firewall dynamically opens and closes multiple ports for signaling and takes care of unsolicited incoming sessions. NAT traversal provides communication of both signaling and media from devices having private IP addresses.

DoS and Flood Attack Detection
The SBC shall detect the DoS attacks, UDP, ICMP and TCP flood attacks discussed above.

Signaling and Media Security, Theft of Service Prevention
Signaling security is based on MD-5 authentication and TLS/IPSec. Media security is based on secure RTP/IPSec. The type of security is negotiable through SIP signaling or through provisioning process.

Granular Access Control
Stateful with granular access control policies and also provides a facility for administrator to create application specific policies.

Session Admission Control, Rogue RTP Detection, Policing and Shaping
The SBC shall allow the media traffic to go through valid sessions and apply traffic management rules and police the traffic to avoid excess traffic. Similarly the SBC shall provide the desired QoS by shaping the traffic in the egress.

Firewalls Specially Designed for VoIP Gateways
These firewalls have higher capabilities over conventional firewalls since they are part of the VoIP Gateways/ IP PBX systems. The firewall can provide necessary security to these elements and also detect frauds real-time in the distributed networks, which is not possible in legacy PSTN systems that adopt centralized fraud management systems.

The following are the firewall’s capabilities:
• Real-time fraud detection based on trends, user profiles, suspicious activities, unauthorized service access etc. generation alerts for remedial action
• Detailed logs of the activity and analysis for insider frauds
• Emergency call handling
• Automatic detection of malicious / spam calls and blocking
• Detection and prevention of intruders for unauthorized service access

SIP Protocol Robustness

Robustness of the SIP protocol stack should be ensured before deployment in public networks. PROTOS-07 Test Suite provides message templates for test cases for baseline robustness of SIP stack:
http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/
The test suite provides message templates (INVITE and CANCEL) of about 4.5K types for each message type. These messages potentially crash the protocol stack of the end point. The SIP clients and servers should be able to process the message and either discard or generate a corresponding SIP error response message to the requester.

QoS Considerations

The VoIP servers need to identify the type of traffic flowing through them.

• Traffic management rules are to be used to classify the traffic based on the applications and ensure desired bandwidth for each flow. The classifier need to support classification based on 5-tuple, packet length, DSCP/ToS.

• The traffic management components -- traffic policing and traffic shapers-- are to be used for achieving this. The recommended policing scheme is token bucket policing and ingress prioritization.

• The traffic shapers support RED/WRED queuing schemes to avoid latency in traffic flow. The recommended traffic shaping schemes are token bucket shapers and Class-Based Queuing (CBQ) algorithms.

• DiffServ based classification is more efficient to prioritize and shape the voice streams. This needs enforcement of end to end DSCP marking through various network elements in the Internet.

Intrusion Detection and Prevention Systems

It is recommended to have an intrusion detection system for a VoIP infrastructure that provides Web access, provisioning and billing systems in order to detect attacks and intrusions based on signatures. This system shall not pose delays and jitter in VoIP signaling and voice traffic flowing through the network.
VoIP Security

Secure Provisioning
The VoIP devices shall be provisioned securely over TLS based standards such as TR-69. The configuration file download and Firmware shall be over SSL-based https. The device shall establish the trust of itself and server based on digital certificate stored in the device.

User Authentication
The device shall support http digest authentication scheme for SIP signaling security. This scheme is based a challenge-response paradigm. The REGISTER, INVITE and BYE are to be protected with this http digest authentication scheme.

Signaling Security
The security schemes are either configured through secure provisioning or negotiated by SIP OPTIONS method. The following security schemes are recommended.

**SIP Signaling over TLS**
- The device sets up a TLS connect with the server for registration and call setup. The client authentication of the server is by maintaining server’s certificate in the device. The device can optionally maintain its own certificate provide it to server when asked.
- The scheme has built-in message integrity and confidentiality. The scheme is robust and immune to reply attacks. The signaling is over TCP and SIP can enforce of TLS security end-to-end.
- SDP during call setup can be used over TLS connection to securely negotiate keys for secure RTP.
- The device needs to discover whether it is behind NAT or in front of a router. If it is behind NAT, it needs to keep the TLS connection always active for receiving incoming calls. As the TLS has alive sessions, sending SIP REGISTER messages is not needed (unlike SIP over UDP behind NAT).
- The device when it is in front of a router, the firewall in the device needs to allow TLS connections only from the SBC/ SIP server.
- The scheme is recommended for consumer VoIP devices like IP Phones, WiFi phones, PDA, TAs.

**SIP Signaling over IPSec**
- The device exchanges key with server using Internet Key Exchange (IKE). Mutual authentication of the client and server is done using pre-shared secrets and RSA/DS x.509 certificates.
- Provides rekeying of session keys periodically. Provides security encapsulation (ESP/AH) protocols. ESP and AH make use of session keys and provide connectionless integrity, source authentication and anti-replay service.
The scheme is connectionless, SIP signaling can be in UDP. The device does not need to discover whether it is behind NAT or in front of a router.

The SBC detects whether the device is behind NAT and provides low SIP register expire intervals to enforce the device to send register requests fast enough to keep the UDP session active in the intermediate router(s).

When it is in front of a router, the firewall in the device needs to allow TLS connections only from the SBC/ SIP server.

The IPSec session established for signaling can also be used for media. Alternatively, SDP during call setup can be used over TLS connection to securely negotiate keys for secure RTP.

The scheme is recommended for SMB VoIP devices like IADs/ IPPBXs/ Media Gateways. The following are the imperatives for IPSec based implementation.

- Processors with sufficient power or crypto hardware accelerators required to reduce encryption/decryption latencies
- Maintain persistent tunnel for media traffic
- Key refresh periodically
- Voice traffic prioritization important
- UDP encapsulation to ensure that IPSec protected traffic traverses NAT/Firewall devices
- Adapt to the IP address changes in the peer, in the access point or NAT devices in the peer network

Media Security

The media (RTP) and media control protocol (RTCP) security schemes are either configured through secure provisioning or negotiated by SIP SDP method. The following security schemes are recommended.

**SRTP**

- SRTP provides confidentiality, message authentication and replay protection to the RTP/RTCP traffic. The RTP standard provides the flexibility to adapt to application specific requirements with the possibility to define profiles in companion documents.
- SRTP is used within multimedia sessions to ensure a secure media data exchange. SRTP does not define key management by itself.
- SRTP is a "bump in the stack" between RTP and transport layer. It intercepts RTP packets and then forwards equivalent SRTP packets. Intercepts received SRTP packets and passes an equivalent RTP packet up the stack.
- Ensures confidentiality of RTP payloads and integrity of RTP packet. Encryption applied to payload and authentication applied to header and payload.
- Master key used for confidentiality and integrity protection. Salting keys used to protect against pre-computation and time-memory tradeoff attacks
The following approaches will be adopted for SRTP key management.

- Through Configuration file download: The keys for encrypting the RTP payload will be specific to each device and will be downloaded to the cell phone during provisioning process. The key can be changed periodically by initiating configuration file download.

- Through SDP: This is possible if the SIP signaling is secure over TLS or IPSec.

- MIKEY:
  - It describes a key management scheme that addresses real-time multimedia scenarios. The focus lies on the setup of a security association for secure multimedia sessions including key management and update, security policy data, etc.
  
  - MIKEY also supports the negotiation of single and multiple crypto sessions. Traffic Encryption Generation Key (TGK) and derives traffic encryption key (TEK) for the media traffic and media control traffic. This is especially useful for the case where the key management is applied to SRTP, since here RTP and RTCP may be secured independently.

  - Deployment scenarios for MIKEY comprise peer-to-peer, simple one-to-many, and small-size interactive group scenarios.

The scheme is recommended for consumer VoIP devices. MIKEY is used in the cases where the signaling security is not adopted except digest authentication.

**RTP/RTCP over IPSec**

The IPSec session used for SIP signaling can be used for transportation of RTP/RTCP. AES CTR/CBC algorithms (faster than 3DES) are to be be used for reducing media traffic latency.

The scheme is recommended for SMB VoIP devices.

**State of Adoption**

The following schemes are adopted for security of Infrastructure and VoIP elements.

**Residential VoIP Gateways**
- Stateful Inspection Firewall
- DiffServ QoS
- Digest authentication for SIP signaling
- Signaling security over TLS
- Media security with SRTP pre-configured keys through secure provisioning
- Moving forward, key exchange over TLS (MIKEY)

**Business VoIP Gateways**
- Stateful inspection Firewall with SMB class features
- IPSec VPN
- Traffic Management
• Digest authentication for SIP signaling
• Signaling as well as media security over IPSec and IKE
• Only media security using MIKEY

IV. Intoto’s Product-line for Secure Converged Networks

Intoto’s iGateway convergence product line offers full featured, integrated, open standards based, certified, interoperable and field proven convergence devices, SBM and enterprise gateways that provide routing, security and SIP based gateway and proxy functionality. These products address the requirements of consumer devices, business class routers, SBCs and SIP servers deployed in typical voice networks. The product features are constantly enhanced to cater to address evolving threat challenges and emerging VoIP feature requirements.

iGateway RGS Plus – Wireless Router with VoIP TA

The following are the features of this consumer device.

• Routing and WLAN (802.11a/b/g)
• SIP based VoIP gateway
• Supplementary services
• SIP over TLS
• Basic Firewall: ICSA certified Stateful Inspection w/ NAT and ALGs
• Wireless LAN security (WPA2/802.1x)
• DiffServ QoS with priority scheduling
• Simple Web-based management
**iGateway RGS Pro-V – Wireless Router with VoIP TA and IPSec VPN**

The following are the features of this Consumer device:

- Features of iGateway RGS Plus
- Basic IPSec VPN: ICSA certified and VPNC certified

**iGateway SecureICP- SME Router with VoIP Gateway and Proxy**

The following are the features of this business class gateway device.

- Routing and WLAN (802.11a/b/g)
- SIP based VoIP gateway
- SIP proxy, registrar and redirect server
- Supplementary services
- SIP over TLS
- SIP over IPSec
- Media Security over IPSec
- SME Firewall: ICSA certified Stateful Inspection w/ NAT and ALGs
- SME IPSec VPN: ICSA certified and VPNC certified
- Wireless LAN security (WPA2/802.1x)
- Application based Traffic management and DiffServ QoS
- SSL based provisioning and remote software upgrade
- Simple Web-based management
Security Measures for Converged Networks White Paper

iGateway SecureEnterprise- Enterprise Firewall and VPN Gateway
The following are the enterprise class gateway for core networks.

- Routing
- Enterprise Firewall: ICSA certified Stateful Inspection w/ NAT
- Enterprise IPSec VPN: ICSA certified and VPNC certified
- VoIP Firewall for SBCs
- High Availability and Virtual Firewall and VPNs
- Symmetric Multi-processor (SMP) support
- Application based Traffic management and DiffServ QoS
- Simple Web-based management

V. Conclusion
Converged services deployment shall include the proper security measures such as voice services privacy through encryption, reliability through redundancy, network element security by protecting the servers from attackers and vulnerabilities, while regularly estimating the threats to the network through security audits. The network elements from the consumer access devices to the core of the network shall be made immune to these security risks and the core elements are to be monitored for risk identification through intrusion detection systems. The success of converged networks greatly depends on the efficiency of the systems in the perimeter, border and core of the converged networks.