



## TOPIC understanding VoIP vulnerabilities

### How Fragile is your VoIP Implementation?

For a long time, telecommunications networks and telephony services have been a part of the critical information infrastructure. They have always had high requirements for availability and Quality of Service (QoS).

The advent of VoIP (Voice over Internet Protocol), also called IPTel (IP Telephony), has brought telephony services to new networks. VoIP provides the same range of services over different transport protocols. From a reliability perspective, VoIP is no different from legacy telephony infrastructure.

In VoIP, telephony services are provided specifically over the IP protocol family. VoIP in itself does not imply in any way that the public and open Internet should be used as the transport network. Using IP networks does not automatically mean using the Internet.

The most common method of implementing enterprise VoIP is through private dedicated lines as opposed to using the public Internet to route the calls. This is partially because of the risks involved with the open and hostile Internet.

### Data and Telephony – Double the Threat

Looking at threats, attacks and vulnerabilities for VoIP, we need to consider it both as a telephony service and IP data service. Both of these domains come with their own sets of threats, attacks and vulnerabilities.

A VoIP service can be taken down by approaching it from a VoIP protocol standpoint, but it can also be attacked as any other IP network. The attack methods range from flooding the systems and networks with traffic to crafting malicious packets that may compromise the target systems and take them down.

Threat analysis and related vulnerability analysis will always reveal the true business risks involved with VoIP. If there are no vulnerabilities, there is zero risk of threats becoming realized. If vulnerabilities can be assumed to exist, the system can be attacked by using attack scripts, viruses and worms.

In real life every single piece of software will always have bugs and vulnerabilities. The number of bugs can be reduced dramatically through rigorous testing and verification. Often this is the only way to control the total business risks associated with VoIP.

### Most Vulnerabilities Caused by Implementation Mistakes

According to RFC3027, a vulnerability can be defined as: "A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy." Vulnerabilities can be introduced during various phases in the software lifecycle: requirements capture, design, implementation, or configuration.

Statistics from NIST (National Institute of Standards and Technology) show that more than 70% of all vulnerabilities discovered are caused by implementation mistakes, i.e. bugs introduced during actual coding. Bad design choices or insecure default configurations only amount to 20-25% of all reported vulnerabilities.

CODENOMICON Ltd.

Tutkijantie 4E  
FIN-90570 OULU  
FINLAND  
+358 424 7431

101 Metro Drive, Suite 660  
San Jose, CA 95110  
UNITED STATES  
+1 650 714 5460

info@codenomicon.com  
www.codenomicon.com



## TOPIC understanding VoIP vulnerabilities

### Vulnerability Type Input validation error

Year	2006	2005	2004	2003	2002	2001
# of Vulns	1586	3183	1374	681	977	815
% of Total	68%	66%	58%	54%	50%	49%

Source NIST, an Agency of the U.S. Commerce Department  
<http://nvd.nist.gov/statistics.cfm>

### Open Networks, Hostile Traffic

The greatest difference between traditional telephony and Next Generation Networks (NGN), where everything is built on top of Internet Protocol (IP), is the openness of the system.

In traditional systems an uptime of 'five nines' (99.999% uptime) could be measured by simulating traffic over an extensive period of time. The traffic used for these tests was for the most part normal. Little to none anomalous or malicious traffic was used.

In the Internet, no-one guarantees that the working environment contains only "normal" traffic. In fact, it is a certainty that there will be malicious attackers sending hostile traffic flows and corrupted packets in an attempt to disrupt services. Securing a Next Generation Network (NGN) that uses the open, public Internet requires finding and fixing all of the reliability flaws in all of the used software components. An attacker needs to find only one reliability or security flaw in order to take down the entire service.

### Service Disruption Equals Loss

The operation of any service can be disrupted, denied or altered in such a way that the original service is not available any more. The service disruption category of threats and vulnerabilities is one of the biggest reasons for revenue loss through downtime and maintenance costs.

The list of services that can be threatened will be under constant change as new services are introduced to IP telephony. Example telephony services today include: making and receiving calls, using voice mail, caller ID, international calling, telephone numbering, call waiting, call transfer, location services, encryption, lawful intercept, and emergency services. All of these can be disrupted by simple Denial of Service (DoS) attacks.

### Attacks – Brute Force or Intelligent and Targeted?

DoS situations arise from performance problems and software quality issues. The two main categories for DoS attacks are:

1. Load, stress and performance-based attacks
2. Robustness, torture testing, fuzzing, protocol-based attacks

In the first category, a DoS attack is performed by sending an excessive amount of network traffic to a target system. The focus is on rendering a particular network element unavailable by bombarding the interfaces that are open to the network.

The second category of DoS attacks employs anomalous messages where the traffic does not conform to any normal expectations. In this type of attack even a single well-



## TOPIC understanding VoIP vulnerabilities

crafted packet can shut down a service. Buffer overflow attacks constitute the best-known variant of protocol-based DoS attacks.

Attacks performed with anomalous protocol packets can lead to total system compromises. In a total compromise, an attacker "owns" the system and can control, monitor and reconfigure any services and processes on behalf of the intended users of the system. An example of a total compromise is a worm attack where a worm runs inside the victim's computer and impersonates the victim when creating new communication sessions.

### Defending VoIP with Proactive, Targeted Testing

Load-based DoS attacks are detected easily and can be mitigated by denying traffic from the malicious parties in cooperation with service providers and law enforcement agencies. The risks for these attacks can be reduced by providing more bandwidth, distributing incoming traffic through load-balancing, and by provisioning resources carefully.

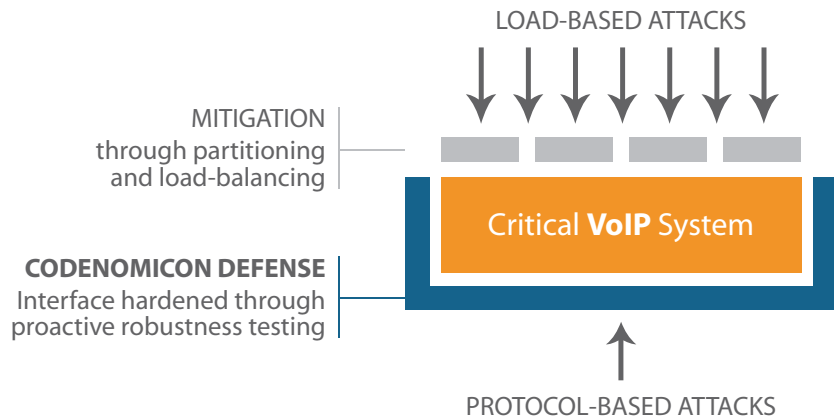
Attacks done through anomalous protocol messages are much harder to prevent and mitigate. When an attack of this type occurs, it is already too late to fix the bugs in the software. The victim can only do damage control and try to minimize loss.

The only way to prevent protocol-based attacks is to subject the used software to extensive negative testing even before any attackers get the chance to approach it. The robustness, security and overall quality of an implementation can be determined by bombarding it with tens of thousands of protocol messages that simulate potential malicious attacks.

Systematic, automated and repeatable robustness testing enables software vendors, operators, enterprises, and end-users to verify the security and quality of their VoIP implementations already at an early stage during adoption.

Many fuzzing tools on the market generate pseudo-random traffic, with little or no chance for repeatability and very poor test coverage. Robustness testing with carefully designed and prepackaged test suites can find flaws more efficiently and assuredly. This type of testing also fits extremely well into existing test automation systems.

### Protecting Against DoS Attacks



CODENOMICON Ltd.

Tutkijantie 4E  
FIN-90570 OULU  
FINLAND  
+358 424 7431

101 Metro Drive, Suite 660  
San Jose, CA 95110  
UNITED STATES  
+1 650 714 5460

info@codenomicon.com  
www.codenomicon.com



## TOPIC understanding VoIP vulnerabilities

### An Analysis of VoIP Interfaces

Example interfaces in VoIP systems that need to be tested from a robustness perspective:

- Signalling: H.323, SIP, SS7, SigComp, SCCP
- Media control: MGCP, H.248, Megaco
- Media: RTP, codecs, MPEG4 streams
- Platform/Transport: IPv4/IPv6, TCP, UDP, SCTP, TLS
- Device Management: SNMP, HTTP, SSH, Telnet, TFTP, NTP, DHCP

### PROTOCOL STACK

RTP	audio/video	MPEG4 streams		MEDIA PLANE
SIP	H.323	H.248	MGCP	SIGNALLING/MEDIA CONTROL
TLS				OPTIONAL ENCRYPTION
TCP	UDP	SCTP		TRANSPORT
IPv4	IPv6			IP LAYER
IPsec				OPTIONAL ENCRYPTION

### MANAGEMENT PROTOCOLS etc.

SNMP	HTTP	SSH	Telnet	TFTP	DHCP
------	------	-----	--------	------	------

### Codonomicon Test Tools for VoIP Robustness and Security

Codonomicon SIP UAS Test Tool  
 Codonomicon SIP UAC Test Tool  
 Codonomicon H.323 Test Tool  
 Codonomicon H.248 Test Tool  
 Codonomicon MGCP Test Tool

Codonomicon RTP Test Tool  
 Codonomicon Audio Test Tools  
 Codonomicon Video Test Tools  
 Codonomicon MPEG4 Test Tool

Codonomicon TLS/SSL Test Tools  
 Codonomicon IPv4 Test Tools Suite (IPv4, TCP, UDP, ICMP, IGMP, ARP)  
 Codonomicon IPv6 Test Tools Suite (IPv6, TCP, UDP, ICMPv6)  
 Codonomicon IPsec Test Tool

Codonomicon SNMP Test Tool  
 Codonomicon HTTP Server Test Tool  
 Codonomicon SSH1 and SSH2 Test Tools  
 Codonomicon Telnet Test Tool  
 Codonomicon TFTP Test Tool  
 Codonomicon DHCP/BOOTP Test Tool

CODENOMICON Ltd.

Tutkijantie 4E  
 FIN-90570 OULU  
 FINLAND  
 +358 424 7431

101 Metro Drive, Suite 660  
 San Jose, CA 95110  
 UNITED STATES  
 +1 650 714 5460

info@codonomicon.com  
 www.codonomicon.com



15 May 2006.b.01

# CODENOMICON technology briefing

## TOPIC understanding VoIP vulnerabilities

### Conclusion

VoIP networks must meet the same rigorous demands for availability as traditional telecommunications networks. Since open environments make VoIP systems more susceptible to protocol-based DoS attacks, proactive and upfront testing is essential for ensuring security, reliability and robustness.

New attack techniques are being developed constantly. This means that attacks are becoming increasingly harder to mitigate en route. Firewalls, IDS systems and other stopgap solutions can never stop all attacks. The most cost-effective solution is to harden the implementations themselves by means of automated negative testing.

The best defense against VoIP vulnerabilities is a great, proactive offense. You must test your software before someone else does.

### For More Information

For more information on protecting your VoIP implementations – or to learn more about the broad set of robustness and security testing tools offered by Codenomicon – please visit our website or contact one of our sales representatives.

CODENOMICON Ltd.

Tutkijantie 4E  
FIN-90570 OULU  
FINLAND  
+358 424 7431

101 Metro Drive, Suite 660  
San Jose, CA 95110  
UNITED STATES  
+1 650 714 5460

info@codenomicon.com  
www.codenomicon.com

page  
05