INTEROP LABS

In association with: NetworkWorld | NetworkWorld Lab Alliance

VOIP: WIRELESS & SECURITY

Over the past seven years, the InteropLabs (iLabs) team has tracked and tested Voice over IP (VoIP) from an initial plethora of protocol options to the industry-wide standardization on the Session Initiation Protocol (SIP). Over the years, we've set up SIP proxies, tested handset interoperability, and deployed advanced calling features. At Interop Las Vegas 2007, we're looking at the issues surrounding full deployment in an enterprise—specifically, how SIP fits into an overall security policy and how it can work in conjunction with your 802.11 (Wi-Fi) wireless networks.

Bringing together VoIP and Wi-Fi, two of the hottest networking topics today, seems like a perfect fit. You've already integrated your voice and data networks with VoIP; why not continue that convergence on your wireless networks? It is a great idea, but making it all work requires attention to detail.

Making that first VoIP call from a wireless handset is a major milestone, but the next step, scaling it up to hundreds or thousands of phones across your wireless network, is another thing altogether.

Depending on whom you talk with, you might be told to limit yourself to 10 simultaneous calls or less per AP. Is this really true? If so, what are the limiting factors? Does it make a difference which Wi-Fi technology (a/b/g) you use?

The iLabs team has built an impressive large-scale test environment where all these questions are being answered for an array of the top wireless vendors. Through the use of advanced test equipment and RF isolation chambers, the team subject access points (APs) to hundreds or thousands of concurrent calls to see where call quality breaks down.

Making a VoIP call over Wi-Fi involves sending lots of small time-critical data packets across a medium beset by loss and interference. Making this work in anything less than ideal conditions requires serious quality of service (QoS) mechanisms.

The IEEE's 802.11e QoS standard (and the Wi-Fi Alliance's Wi-Fi Multimedia (WMM) specification based on 802.11e) allows handsets, controllers, and APs to assign a high priority for VoIP packets, ensuring the lowest possible latency, jitter and loss. Expanding on last year's testing, the iLabs team will demonstrate the dramatic impact the use of this standard can make, as well as the growing number of devices that support it.

Integrating SIP into your overall security policy is not always an easy task. By allowing VoIP access to the Internet your users have the potential to greatly reduce your voice calling costs, while adding functionality and better voice quality. But all this comes at a price: You need to secure VoIP traffic at your perimeter, between stations, and across the Internet.

You probably already known that voice traffic consists of a stream of digitized samples sent across the network. What you may not know is that it's trivially simple for anyone who can access that network to listen to your call. In an VoIP-over-Internet context, that means that your ISP, the ISP of the person you're calling, and any network provider in the middle can intercept voice traffic at any time. Even malware on your own networks can render your calls vulnerable to eavesdropping.

The standards-based solution is the Secure Real-Time Transport Protocol (SRTP), an extension to RTP that encrypts media traffic from end to end. In the iLabs, we've brought together VoIP handset, softphone, and server solutions that implement SRTP to demonstrate their interoperability and determine where more work needs to be done.

At last year's iLabs, we investigated firewalls with basic SIP-awareness, but that level of awareness doesn't protect you from attacks that use legal SIP messages, or slightly malformed ones. That's where SIP-aware intrusion detection systems/intrusion prevention systems (IDS/IPS) come in. These devices have a deep understanding of the protocols and malicious uses found in the wild. IDS can flag any suspect traffic; IPSs take things a step further and actively block malicious traffic, adding another layer to your overall security solution. In the iLabs, we've set up several IDS/IPS appliances, an open source solution, and a router with IPS extensions, each protecting a virtual enterprise. We are then subjecting each "enterprise" to SIP-based attacks to see how well they defend their enterprise.

The iLabs are made possible by the tireless work of volunteers from all over the world and across industry, education, and government. This year's VoIP: Wireless & Security team members are:

- **Jim Martin**, *VoIP Team Lead, The Daedelus Group*
- **Jed Daniels**, *VoIP Instructor, Network Physics*
- **Craig Watkins**, *Transcend, Inc.*
- **Hege Trosvik**, *University of Oslo, USIT*
- **Jeremy McNamara**, *NuFone, Inc.*
- **David Newman**, *Network Test*
- **Karl Auerbach**, *Internetworking Labs*
- **Bill "WEJ" Jensen**, *University of Wisconsin- Madison DoIT*
- **John Balogh**, *Pennsylvania State University*
- **Matthew Gast**, *Trapeze Networks*
- **Chris Stradtman**, *GreenPoint Communications*

The iLabs team searches the industry for the best products and solutions to demonstrate the topic under investigation and works closely with the vendors to both educate the Interop attendees and improve the products themselves. Our thanks to the following vendors for their participation and support:

APC
Aruba Networks
AudioCodes
Avaya
Avocent Corporation
Belkin International
Check Point Software Technologies
Cisco Systems, Inc.
CounterPath Solutions, Inc.
Digium
D-Link Systems, Inc.
Extreme Networks, Inc.
Fortinet, Inc.
Grandstream Networks, Inc.
Hewlett Packard Development Company, LP.
Ingate Systems
Juniper Networks, Inc.
Motorola, Inc.
Mu Security
Network Physics
NuFone, Inc
OpenSER.org
pbxnsip Inc.
snom technology AG
SpectraLink/Polycom
Trapeze Networks, Inc.
Veriwave, Inc.
WildPackets

In addition to the iLabs demonstrations on the Interop show floor, the iLabs offers more free education in the form of daily classes and whitepapers. See the signage in the iLabs booth for class times and locations. The following whitepapers are available electronically in the iLabs booth and online at: http://www.opusone.com/voip/

- What is SIP?
- What is ENUM?
- Getting Started with SIP
- Migrating to SIP
- SIP Resources
- VoIP and 802.11
- SIP and the PSTN
- SIP and Border Security
- VoIP and VPNs
- What is SRTP?
- VoIP Wireless Call Scalability

InteropLabs – Las Vegas 2007 – VoIP: Wireless & Security

VeriWave WaveTest WT90

Aruba 70 / Aruba 6000
Aruba 70 / Aruba 6000
Cisco 1200 / Cisco 2006
Cisco 1200 / Cisco 2006
D-Link DWL-2230P / D-Link DWS-3227P
D-Link DWL-2230P / D-Link DWS-3227P
Extreme 350-2 / Extreme WM2000
Extreme 350-2 / Extreme WM2000

VeriWave WaveTest WT90

VeriWave WaveTest WT90

HP RP220 / HP 4000
HP RP220 / HP 4000
Juniper SSG5
Juniper SSG5
Motorola Symbol 300 / Motorola WS5100
Motorola Symbol 300 / Motorola WS5100
Trapeze MP-422 / Trapeze MX-216
Trapeze MP-422 / Trapeze MX-216

VeriWave WaveTest WT90

Test Tools & Analyzers

- VeriWave WT90, WT20
- WildPackets
- Network Physics NP-2000
- Wireshark

VeriWave WaveTest WT20

D-Link, Spectralink, D-Link, Spectralink

Over The Air

Aruba 70 | Cisco 1200 | D-Link DWL-2230P | Extreme 350-2 | HP RP220 | Juniper SSG5 | Motorola Symbol 300 | Trapeze MP-422

Walk-In Faraday Cage

Wireless Scalability

Legend

- SIP Aware Firewall
- Wireless Switch (802.11e or WMM)
- SIP Server
- IDS/IPS Device
- SIP Phone
- Wireless SIP Phone
- Wireless Access Point

Linux Based Attack Tools
Windows Based Attack Tools
Mu Security Mu-4000

Wireless QoS

Attack Detection and Mitigation

Enterprise 1

- Check Point UTM-1 450
- Asterisk SIP Server
- Cisco SIP Phone

Enterprise 2

- Juniper IPS200
- Asterisk SIP Server
- Cisco SIP Phone

Enterprise 3

- Fortinet Fortigate 500
- Asterisk SIP Server
- Cisco SIP Phone

Enterprise 4

- OpenIDS (Snort)
- Asterisk SIP Server
- Cisco SIP Phone

Enterprise 5

- Cisco 7206 IOS Router
- Asterisk SIP Server
- Cisco SIP Phone

Media Security

- Asterisk SIP Server
- OpenSER SIP Server
- Grandstream SIP Phone
- snom SIP Phone
- CounterPath SIP Phone
- Pbxnsip SIP PBX
- snom SIP Phone
- CounterPath SIP Phone
- AudioCodes Media Gateway
- POTS phone
- Ingate Firewall
- Avaya SIP Server
- Avaya SIP Phone
- snom SIP Phone
- Avaya SIP Phone
- snom SIP Phone