NETWORLD+INTEROP PRESENTS InteropNet Labs

Official Media Sponsor NetworkWorld

InteropNet Labs Wireless LAN Security Initiative Overview

By Karen O'Donoghue, Naval Surface Warfare Center, iLabs Team Lead

The InteropNet Labs Wireless LAN Security Initiative is once again exploring the current state of security in wireless networks, expanding on earlier efforts at NetWorld+Interop Las Vegas 2002 and NetWorld+Interop Atlanta 2002. Basic security services including authentication, data integrity, privacy, and denial of service are explored as they apply to the wireless environment.

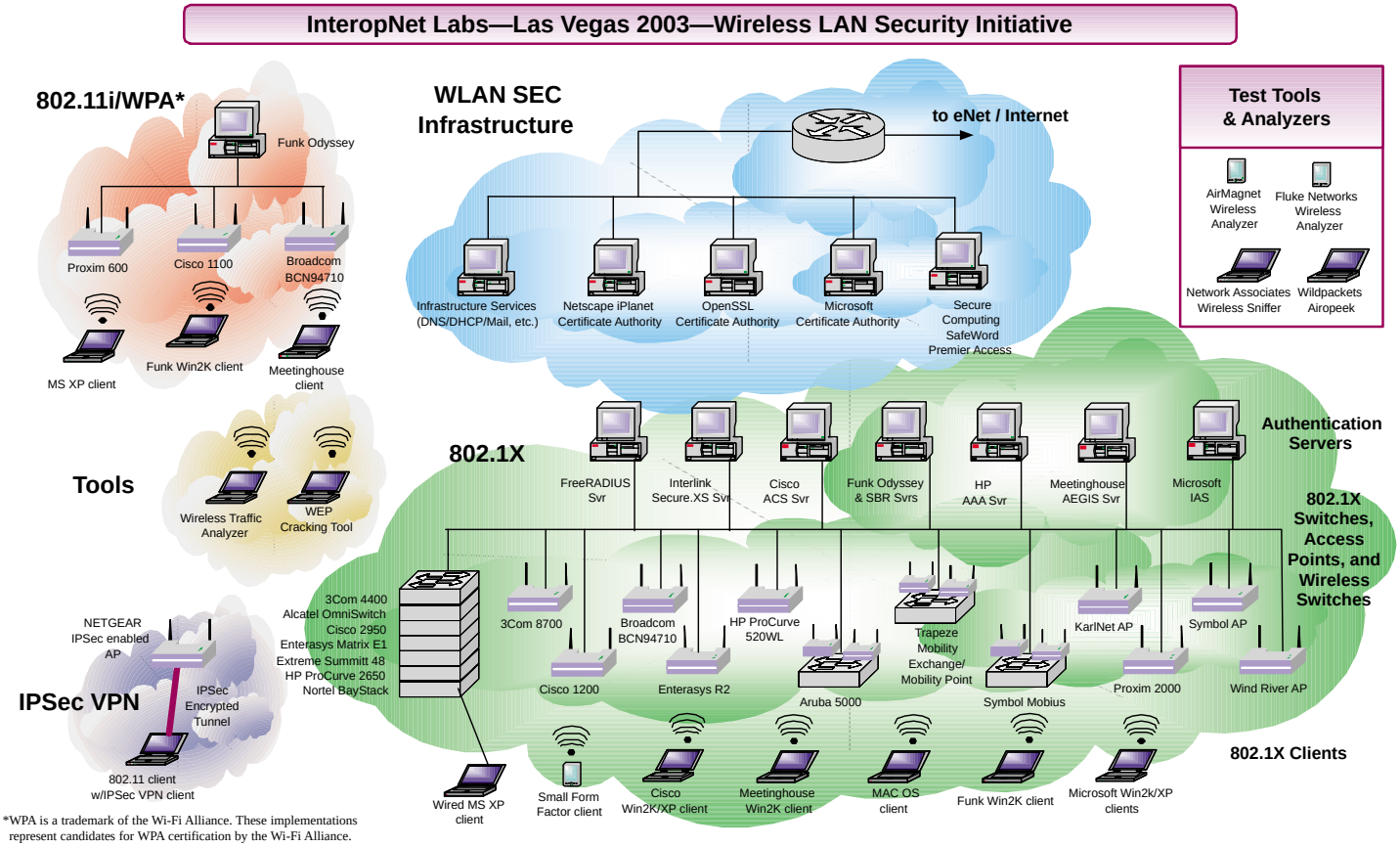
The primary goal is to promote security solutions that are interoperable and non-proprietary (meaning any component in the chain between end user and network can be swapped out with a different vendor's component and not impact the security or usability of the system). To this end, this initiative had two thrusts: 1) To promote interoperability of products implementing the IEEE 802.1X standard by hosting an open ad-hoc test event; and 2) to educate enterprise network managers about the alternatives available for securing wireless LANs.

We invited vendors of IEEE 802.1X supplicants, authenticators, and authentication servers to Belmont, California, for an ad-hoc interoperability test. After three days of testing, a wealth of lessons were learned about the state of interoperability including product bugs, specification interpretation, and basic deployment issues. Detailed results were fed back to the participants and generalized results and lessons learned will be available to NetWorld+Interop attendees during a Birds-of-a-Feather (BoF) session on Tuesday, April 29, 2003.

The second goal of the WLAN Security initiative has been addressed by the definition of four demonstration areas at the show to illustrate concepts to attendees: 1) Tools; 2) IEEE 802.11i/TKIP/WPA; 3) IEEE 802.1X; and 4) IPsec.

The first demonstration area contains a number of tools that illustrate the vulnerability of a wireless network. An ongoing trace of network traffic on various wireless links using a network analyzer product demonstrates the ease of doing basic things like capturing passwords passed in the clear. Also, in a demonstration of a commonly available tool for breaking WEP keys, we highlight some of the product improvements that reduce the impact of widely reported problems with WEP.

The second demonstration area looks at initial implementations of the emerging Wi-Fi Protected Access specification, which is based on Draft 3.0 of the IEEE 802.11i specification. This interim specification addresses a number of weaknesses in the current 802.11 standard providing users with more robust security as they await the final IEEE 802.11 solution. In this demonstration, a number of products still in development give some early insight into the 802.11i/WPA effort.



*WPA is a trademark of the Wi-Fi Alliance. These implementations represent candidates for WPA certification by the Wi-Fi Alliance.

The third demonstration area investigates the operation and interoperability of 802.1X in both the wired and wireless environments. Multiple clients (supplicants) are connected to the network through a variety of authenticators (wireless 802.11 access points, wired Ethernet switches, and the emerging class of products being referred to as wireless switches). These clients are authenticated by a number of Authentication Servers using various EAP types including MD5, TLS, TTLS, and PEAP.

The fourth demonstration area shows how an IPsec VPN solution can be deployed to provide wireless security. In this demonstration, one of the new combination 802.11 access point and VPN tunnel concentrator devices is being shown as one way to secure a wireless connection. White papers are available to discuss the different security models, benefits, and drawbacks of using IPsec as a wireless security tool versus the other approaches being shown in the iLabs.■

Participating vendors

3Com Corporation
Alcatel Internetworking
Aruba Wireless Networks
Broadcom Corporation
Cisco Systems
Enterasys Networks
Extreme Networks
Funk Software
Hewlett-Packard Company
Interlink Networks
KarlNet, Inc.
Meetinghouse Data Communications
Microsoft Corporation
Netgear, Inc.
Nortel Networks
Perfigo, Inc.
Proxim, Inc.
Riverstone Networks
Secure Computing Corporation
Symbol Technologies
Trapeze Networks
Wind River Systems

With support from:

AirMagnet, Inc.
American Power Conversion
Avocent Corporation
Fluke Networks
Hewlett-Packard Company
Ipswitch, Inc.
Network Associates
WildPackets, Inc.
VMware, Inc.

iLabs Class Schedule NetWorld+Interop Las Vegas 2003

MONDAY, April 28

5:00pm–6:00pm	WLAN Security	Room N116
5:00pm–6:00pm	Advanced Internetworking	Room N112
5:00pm–6:00pm	IP Storage	Room N115

TUESDAY, April 29

10:15am–11:15am	Advanced Internetworking	Room N115
11:45am–12:45pm	IP Storage	Room N115
1:15pm–2:15pm	WLAN Security	Room N115
2:45pm–3:45pm	WLAN Security Panel Discussion	Room N115

WEDNESDAY, April 30

10:15am–11:15am	Advanced Internetworking	Room N115
11:45am–12:45pm	IP Storage	Room N115
1:15pm–2:15pm	WLAN Security	Room N115
2:45pm–3:45pm	Advanced Internetworking Panel Discussion	Room N115

THURSDAY, May 1

10:15am–11:15am	Advanced Internetworking	Room N115
11:45am–12:45pm	IP Storage	Room N115
1:15pm–2:15pm	WLAN Security	Room N115
2:45pm–3:45pm	IP Storage Panel Discussion	Room N115

iLabs Wireless LAN Security Initiative Team

Karen O'Donoghue, iLabs Team Lead, Naval Surface Warfare Center
Matthew Gast, iLabs Instructor, Trapeze Networks
Bill Clary, iLabs Engineer, Phase Seven Laboratories
Craig R. Watkins, iLabs Engineer, Transcend, Inc.
Chris Elliott, iLabs Engineer, Cisco Systems, Inc.
Gerard Goubert, iLabs Engineer, InterOperability Lab, UNH
Jan Trumbo, iLabs Engineer, Opus One
Joel M. Synder, iLabs Engineer, Opus One
Margrete Raaum, iLabs Engineer, University of Oslo
Petter Bjørbæk, iLabs Engineer, University of Oslo
Sandy Turner, iLabs Engineer, Los Alamos National Laboratory

With Support from:

Eddy Harvey, Hewlett-Packard Company
Paul Congdon, Hewlett-Packard Company
Sandler Rubin, Secure Computing Corporation
Gilbert Goodwill, Wind River Systems, Inc.
Christian MacDonald, Funk Software, Inc.
Doug Moeller, Vista Broadband Networks