Defcon Capture the Flag: Defending Vulnerable Code from Intense Attack

Crispin Cowan

WireX Communications, Inc. http://wirex.com/

Immunix™ is a Linux system hardened with several DARPA-funded security technologies to produce a highly survivable server appliance platform. The Immunix technologies include:

StackGuard: A C compiler enhancement [7] that emits programs resistant to buffer overflow attacks [10, 8].

FormatGuard: A similar C compilation technique [4] that emits programs resistant to printf format string vulnerabilities [11, 2, 9].

RaceGuard: A kernel enhancement [6] to detect and stop temporary file race attacks [1].

SubDomain: A mandatory access control scheme [5] that lets the kernel enforce the set of files that can be accessed by each *program* .

LSM (Linux Security Modules): To enable rapid technology transfer, we have built the Linux Security Modules system [13, 12] which enables arbitrary access control policy modules to be loaded into standard Linux kernels. LSM has been accepted into the development Linux 2.5 system, and will be a standard feature of Linux 2.6. SubDomain is now an LSM module, and RaceGuard is being ported to LSM.

Combined, these technologies make it very difficult for an attacker to break into an Immunix server, despite the presence of *unpatched vulnerabilities* , while also preserving a high degree of compatibility with standard Linux systems.

The Defcon Capture-the-Flag (CtF) contest is the largest open security hacking game. The 2002 game was designed to make it particularly difficult for defenders to defend their servers by forcing players to host software known to be vulnerable. Our DISCEX III paper [3] describes our experience playing an Immunix server in this game: we placed second overall, and no one was able to take control of the Immunix server.

Our DISCEX III exhibit is comprised of various server appliance systems based on Immunix. In addition to being self-defending server appliances protected with Immunix technologies, these appliances also feature an easy-to-use web-based GUI that allows even non-technical staff to install and operate sophisticated servers in minutes. Exhibits will include:

Trend Micro InterScan/Immunix Secured Solution: WireX and HP have teamed up to create a family of Security Servers based on Immunix. This product is the first in the family, providing virus scanning services for e-mail servers and web clients, and is available for purchase through HP and Trend Micro sales channels.

Secure Webmail Appliance: Made to order for USTRANSCOM, this appliance provides a web-based interface to e-mail servers. The appliance can either be its own mail server, or can be a front-end for a Microsoft Exchange server, including providing access to Microsoft calendaring functionality.

Live-fire Penetration Tests: We will also demonstrate live-fire security attacks that show Immunix at work fending off these attacks.

References

[1] M.Bishop and M. Digler. Checking for Race Conditions in File Accesses. *Computing Systems* , 9(2):131–152, Spring 1996. Also available at url http://olympus.cs.ucdavis.edu/ bishop/scriv/index.html.

[2] Kalou/Pascal Bouchareine. Format String Vulnerability. url http://plan9.hert.org/papers/format.html, July 18 2000.

This work supported in part by DARPA contracts N66001-00-C-8032, F30602-01-C-0172, F30602-02-C-0219, and F30602-02-C-0214.

[3] Crispin Cowan, Seth Arnold, StevenM. Beattie, , and Chris Wright. Defcon Capture the Flag: Defending Vulnerable Code from Intense Attack. In *DARPA Information Survivability Conference and Expo (DISCEX III)* , Washington, DC, April 22-24 2003.

[4] Crispin Cowan, Matt Barringer, Steve Beattie, Greg Kroah-Hartman, Mike Frantzen, and Jamie Lokier. FormatGuard: Automatic Protection From printf Format String Vulnerabilities. In *USENIX Security Symposium* , Washington, DC, August 2001.

[5] Crispin Cowan, Steve Beattie, Calton Pu, Perry Wagle, and Virgil Gligor. SubDomain: Parsimonious Server Security. In *USENIX 14th Systems Administration Conference (LISA)* , New Orleans, LA, December 2000.

[6] Crispin Cowan, Steve Beattie, Chris Wright, and Greg Kroah-Hartman. RaceGuard: Kernel Protection From Temporary File Race Vulnerabilities. In *USENIX Security Symposium* , Washington, DC, August 2001.

[7] Crispin Cowan, Calton Pu, Dave Maier, Heather Hinton, Peat Bakke, Steve Beattie, Aaron Grier, Perry Wagle, and Qian Zhang. StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks. In *7th USENIX Security Conference*, pages 63–77, San Antonio, TX, January 1998.

[8] Crispin Cowan, Perry Wagle, Calton Pu, Steve Beattie, and Jonathan Walpole. Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade. In *DARPA Information Survivability Conference and Expo (DISCEX)* , January 2000. Also presented as an invited talk at SANS 2000, March 23-26, 2000, Orlando, FL, url http://schafercorp-ballston.com/discex.

[9] Tim Newsham. Format String Attacks. Bugtraq mailing list, url http://www.securityfocus.com/archive/1/81565, September 9 2000.

[10] "Aleph One". Smashing The Stack For Fun And Profit. *Phrack*, 7(49), November 1996.

[11] "tf8". Wu-Ftpd Remote Format String Stack Overwrite Vulnerability. url http://www.securityfocus.com/bid/1387, June 22 2000.

[12] Chris Wright, Crispin Cowan, Stephen Smalley, James Morris, and Greg Kroah-Hartman. Linux Security Module Framework. In *Ottawa Linux Symposium* , Ottawa, Canada, June 2002.

[13] Chris Wright, Crispin Cowan, Stephen Smalley, James Morris, and Greg Kroah-Hartman. Linux Security Modules: General Security Support for the Linux Kernel. In *USENIX Security Symposium* , San Francisco, CA, August 2002. url http://lsm.immunix.org.