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 US-TRANSCOM, 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**


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.


