

New Chips Stop Buffer Overflow Attacks

Chip makers are designing a new generation of microprocessors to stop buffer overflow assaults, exploits that hackers often use to attack and extract data from PCs or servers.

AMD's Athlon-64 chips for notebook and desktop computers and its Opteron processors for servers include features that provide buffer-overflow protection. However, the feature won't work until it is supported by operating systems, said Richard Brunner, an AMD Fellow in software architecture. "We've been working with [OS] ven-

dors to get them to take advantage of the hardware features," he explained.

Intel offers buffer-overflow protection in its Itanium chips for servers and will do so in future chips. Microsoft will support the buffer-overflow features in its Windows Server 2003 service packs scheduled to be released in the first half of 2005. Different Linux flavors also plan to work with this technology.

A buffer overflow occurs when a program or process tries to store more data in a buffer than it was designed to hold. The extra information can overflow into other memory sections,

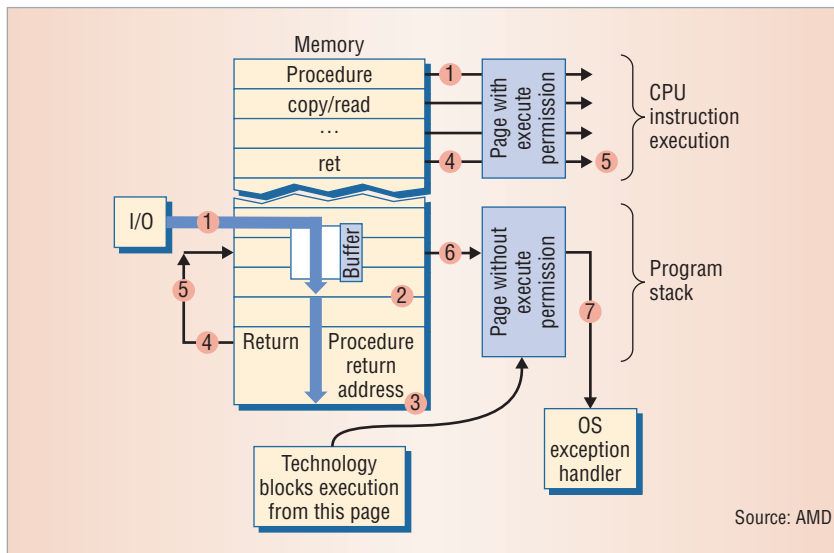
corrupting or overwriting data stored there. Systems could then execute malicious instructions inserted by a hacker into the data. The Slammer and Blaster worm PC attacks in 2003 and the Slapper worm that infected many Linux-based Web servers in 2002 involved buffer overflows.

Operating systems that support the buffer-overflow prevention approach mark certain data in memory with a bit that identifies them as executable or nonexecutable. If hackers try to force a computer to execute code from a section of memory designated as nonexecutable, the processor will send an OS exception that causes Windows to generate a page fault that closes the application.

The AMD chips let users turn off the new security feature for legacy programs not written to work with the technology so that the applications can continue to function. Intel chips will work in a similar manner, according to company spokesperson Howard High.

This type of protection is important, and OS vendors should support it, noted Carl D. Howe, cofounder and analyst at Blackfriars Communications, a market research and consulting firm.

According to Howe, buffer-overflow prevention currently is limited almost exclusively to Intel-compatible systems, although there are a few other implementations. ■



Source: AMD

AMD is gaining support for a feature in its microprocessors that helps stop buffer-overflow exploits, a way that many hackers attack PCs or servers. First, (1) a computer copies input data, which includes a virus, into the buffer on the program stack. (2) The data overflows the buffer and overwrites another stack. (3) Data overwrites the original procedure return address to point to data in the buffer that actually contains CPU instructions. (4) When the procedure finishes, the return instructions transfer control to the procedure return address and thus (5) to the buffer. (6) The CPU tries to execute the buffer instructions, including the virus. (7) AMD's technology blocks execution of the instructions, and the CPU generates an OS exception that causes Windows to generate a page fault that closes the application.

News Briefs written by Linda Dailey Paulson, a freelance technology writer based in Ventura, California. Contact her at ldpaulson@yahoo.com.

Editor: Lee Garber, *Computer*,
l.garber@computer.org

Two Companies Make the Hard Drive Wireless

A company has developed a device that utilizes wireless universal serial bus (USB) interconnect technology to let multiple users write to and access data on the same external hard drive. This can help users in small companies or households share data without setting up expensive storage area networks or installing cabling.

The Network Storage Link by Linksys, a Cisco Systems division, connects to an external hard drive on one end and to a router on the other. Multiple PCs or laptops with wireless adapters or cards could then connect to files stored on the drive via the router and the NSL.

A machine without a wireless adapter or card could use a USB cable to connect to the NSL and thus communicate with an external drive, noted Linksys spokesperson Karen Sohl. Or a user could connect a computer without wireless capabilities to a router via an Ethernet cable. The user could then communicate with an external drive via the router and the NSL, which contains USB and Ethernet ports.

For cable-free data communications, the NSL uses wireless USB, which works with the same protocol and architecture as a traditional wired USB except that it runs over ultrawideband. UWB is a low-power, short-distance, radio-based technology that transmits large amounts of data over a wide range of frequency bands.

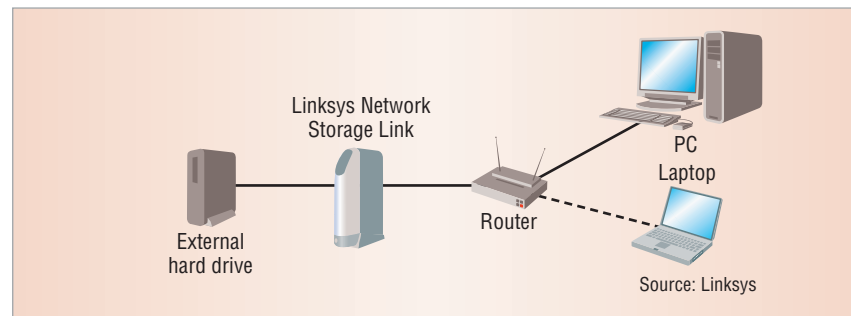
Linksys has teamed with drive maker Maxtor to develop a common set of instructions so that their products will work together. However, the NSL will work with any vendor's external drive that also uses the instruction set, said Sohl.

NSL includes an optional file management system that coordinates enhanced tasks such as setting up user permissions and giving users their own sets of files to work with.

Philip Marshall, director of wireless-

technology research for the Yankee Group, a market analysis firm, said it

is not clear yet how big a market there will be for the new technology. ■



A laptop links wirelessly, or a PC links via wires, to a router that connects to Linksys's Network Storage Link. The NSL then acts as a link between multiple laptops and PCs on one hand and an external hard drive on the other. This provides an inexpensive way for multiple users in a household or small business to share data without setting up an expensive storage area network.

Spam-Plagued Researchers Develop Antispam Technique

Computational-biology researchers have used a pattern-discovery application created for protein studies to develop an algorithm that enables e-mail systems to automatically and accurately identify spam.

Isidore Rigoutsos and Tien Huynh of the Bioinformatics and Pattern Discovery Research Group at IBM's T.J. Watson Research Center developed the Chung-Kwei system, named after a mythical Chinese figure known for protecting valuable property from evil.

During testing, the system's main algorithm—which is part of IBM's larger SpamGuru project (www.research.ibm.com/spam/filtering.html)—correctly identified 96.5 percent of incoming spam messages and falsely identified only one out of 6,000 non-spam messages.

The two IBM researchers developed Chung-Kwei based on the Teiresias pattern-discovery algorithm that Rigoutsos created in 1996 to look for patterns in

protein and nucleic acid sequences and in other strings of biological material. Chung-Kwei analyzes the patterns of characters used in both spam and regular e-mail and generates a database of patterns found only in spam.

The database can grow as the system analyzes more e-mail. The system examines e-mail for patterns also found in its spam database. It then computes a score for messages based on the number and prevalence of spam-related character patterns they contain. The system identifies messages as spam based on their scores.

Individual users or network administrators can train the algorithm by exposing it to new spam messages with different character patterns so that it won't be fooled by spammers' tricks, such as replacing the "S" in words commonly used in spam with an "\$."

To improve Chung-Kwei's filtering performance, researchers trained it on 66,000 spam and 22,000 nonspam

News Briefs

messages, Rigoutsos said. In this process, researchers used some of the many unsolicited messages they regularly receive.

Current antispam applications generally use several techniques to recognize unsolicited mail, such as identifying whether the sender's address has been spoofed or finding a sender's presence on lists of known spammers or trusted contacts.

Paul Hoffman—director of the Internet Mail Consortium, which hosts many mailing lists related to Internet mail standards—expressed no confidence in spam filtering. “We haven't seen a filtering technology that spammers haven't figured out how to circumvent,” he said.

But John R. Levine, chair of the Internet Research Task Force's Anti-Spam Research Group, said the

Chung-Kwei approach is “a very clever way to do mail filtering within the limits of what mail filtering can do. But spam filtering at its best is only a stop-gap. Even really good filtering makes mistakes now and then.”

IBM says it plans to commercialize the system eventually, probably in its Lotus software products. First, however, Rigoutsos said, the company must test it in a live, real-world setting. ■

Using Computers to Accompany Musicians

The next time technically savvy musicians need an accompanist, they may turn to their computers.

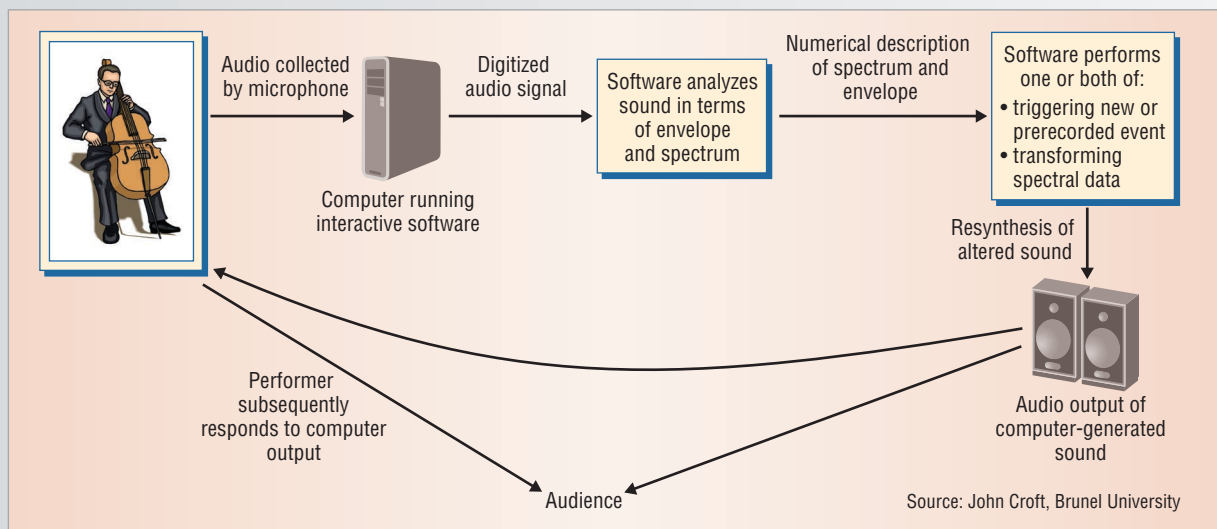
Researchers at the UK's Brunel University have developed a set of specialized software objects that react to played music and enable a computer to quickly provide far more complex accompaniments than have been available in the past. The Brunel researchers have developed these objects to work within the Max/MSP programming environment, developed by multimedia-software vendor Cycling 74 and the Institut de Recherche et Coordination Acoustique/Musique (Institute of Research and Coordination of Acoustics/Music).

Upon receiving played music as input, the Brunel software separates it into components—such as pitch, tempo, and volume—and then uses complex, probabilistic algo-

rithms that generate an accompaniment based on a wide range of parameters, explained John Croft, a music lecturer at the school. Users can program Brunel's system to affect the nature of the accompaniment, including its degree of “improvisation.”

Traditional computer-generated music-accompaniment technologies include simple loop machines, which continuously repeat part of a musical piece that has been played. Other techniques make random choices of sounds from a predefined range of possibilities. However, more powerful processors and sophisticated software have enabled faster and more complex approaches, said Croft.

Brunel's software is still in the early stages of development, he noted. The university plans to make its software available commercially in mid-2006.



Brunel University has developed software that produces real-time, complex, improvisational-sounding accompaniments to live musicians. The software analyzes and reacts to various complex elements of music—such as the spectrum of different pitches that make up a sound and the envelope that represents the way a sound fades or otherwise changes over time—to produce accompaniments.