A University of Michigan academic team has developed a prototype system for providing antivirus protection via the Internet. This security-as-a-service approach is an example of cloud computing, an increasingly popular technique in which applications and services are offered via the Internet, rather than via programs loaded onto in-house PCs or servers.

The University of Michigan team’s CloudAV system would let users avoid having to keep and update complex antivirus software on their own computers. Instead, security providers would handle this on their systems.

The technology also places fewer demands on a device’s CPUs, memory, and power source than traditional approaches, noted researcher and doctoral student Jon Oberheide.

The technology would thus let mobile devices run heavy-duty antivirus programs, which they can’t do now because of their limited processing power and memory.

The optimal setting for CloudAV is in an organization’s local-area network or in an ISP’s network, Oberheide said.

Rather than scan entire systems, CloudAV analyzes applications and files only as users encounter or try to open them.

CloudAV analyzes files via multiple, simultaneously running antivirus programs from different vendors that identify malware by comparing it to known malware’s code strings or by its behavior once on a computer.

Using multiple antivirus programs is more likely to catch problems than running a single application, according to Oberheide.

Presently, users generally can run only one antivirus application at a time on their computers because of performance constraints and program incompatibilities. CloudAV avoids this problem by running each program in its own virtual machine. The system then scans every file with each antivirus program.

Because each application is in its own virtual machine, a hacker successfully attacking one antivirus program won’t affect the other applications or the host system.

Unlike traditional antivirus software, CloudAV caches scan results and shares them with other users on an organization’s network. This prevents redundant analysis, accelerates performance, and reduces both bandwidth consumption and analysis time.

CloudAV also uses retrospective detection. On its servers, the system stores the files that protected devices within an organization access. When security providers release code signatures for newly identified viruses, the system can rescan stored files to see if they include the malware.

Although CloudAV has advantages, it also creates an important problem, said Jon Ramsey, security vendor SecureWorks’ chief technical officer. Because the application must inspect data in the cloud, he explained, Internet congestion could delay the process.

And multiple antivirus vendors might not permit a commercial CloudAV version to run their applications at the same time, he added.

Moreover, he said, many users might not want to have their systems protected via the Internet because of security and reliability concerns.

Licensing costs might make simultaneously running multiple antivirus programs expensive, so organizations would have to decide whether the enhanced protection is worth the additional cost, Oberheide noted.

The University of Michigan research team is testing CloudAV’s effectiveness and continuing its work on the system.
Third-Generation RFID Is on Its Way

Companies have begun releasing products utilizing a new, more-functional generation of RFID that uses special tags as sensors to process and send business-related information within inexpensive, scalable, self-healing mesh networks.

RFID tags on products or other items contain data that a reading device scans, via radio technology, to obtain information about or identify the objects. The tags typically have been used for inventory tracking or to control access to vehicles or buildings.

The technology’s first generation was used mainly for identifying objects, while the second added item-location capabilities. Early tags were passive, using signals from RFID readers to power up. Newer technologies use active tags, which have their own battery power. The added power increases their communication range.

The third generation of RFID—called wireless-sensor-network (WSN) technology—works with active tags. They gather information and then send it from tag to tag over a mesh network until it reaches the location at which the data will be processed.

The new RFID approach is scalable, self-healing, and less expensive, said Allen Nogee, principal analyst for wireless technology and infrastructure at In-Stat, a market research firm.

MIT Works on a Tree-Powered Network

Scientists at a bioenergy startup are working on a forest-fire-detection sensor system powered by the tiny amounts of electricity that trees generate.

Voltree Power, owned in part by MIT research scientist Andreas Mershin and MIT senior chemistry student Christopher Love, has developed the Early Wildfire Alert Network system.

EWAN would include temperature and humidity sensors scattered throughout a forest. They would be powered by energy-efficient batteries recharged by the electric current found in trees.

The MIT researchers determined that trees produce between 5 and 100 nanowatts of electric current at 59 millivolts, generated by the pH imbalance between the plant and the soil it grows in. A device that uses this power to charge the sensor system slowly and steadily could generate up to 100 microwatts of power at 2.4 volts.

EWAN’s environmental readings would help observers determine whether there is a high risk of fire in a forest or where fires are likely to start. The system could also help researchers develop better models for predicting fire outbreaks.

EWAN’s sensors, which would be between 20 and 40 meters apart in a forest, would communicate with one another via a custom, low-power ZigBee (IEEE 802.15.4) wireless mesh network.

Voltree chose mesh technology because it is inexpensive, uses little power, and is maintenance free, said Mershin.

The system thus could work in large remote areas, like those where forest fires frequently start.

An EWAN network would use various redundant paths in the network to carry the signal via multiple hops to a transmitter, which would send the data for analysis.

Testing of the system is tentatively slated to begin next spring on a 10-acre plot of US Forest Service land in the state of Idaho’s Boise National Forest.

The network would send data from sensor to sensor until the information reaches a Forest Service Remote Automated Weather Station equipped with a satellite link to an interagency fire-coordination center in Boise. Weather experts would then analyze the data and advise firefighting agencies how to best deploy their resources in anticipation of problems, explained Mershin.

The system would trigger a fire alert if the sensors detect temperatures above a preestablished level, said Voltree CEO Stella J. Karavas. ■
Researchers Make Holographic Breakthrough

A University of Arizona research team has achieved a breakthrough in rewritable, erasable, and refreshable holographic systems that could enable 3D displays that show moving images, such as TV programming or video.

Another possible application would be medical imaging, said assistant research scientist Pierre-Alexandre Blanche. For example, he explained, this type of holographic display could let a surgeon see data from a body scan and then change the viewing angle as needed.

In holography, light cast on and scattered from an object falls onto a recording medium. A second light source also illuminates the recording medium so that interference occurs between the two beams. This yields a 3D image of the object.

Current holographic technology can’t show moving images because it writes data too slowly. Also, the inorganic crystalline materials it uses don’t enable the erasing and rewriting of information because they generate images via an irreversible chemical reaction, Blanche said.

The University of Arizona team made its holographic display with a photorefractive polymer that enables the writing, erasing, and rewriting of images.

The ambient or laser-created light that enters the system generates charges in the display medium. These charges generate an electrical field that changes the medium’s index of refraction. This lets the system change the images it shows, which enables the display of moving pictures.

Currently, the researchers’ test system can’t change the nature of the light source quickly enough to show moving images well. They are thus experimenting with faster lasers.

Another problem with current holographic technology is that growing enough of the crystalline material to form a large display is difficult and expensive. The University of Arizona’s polymer material comes in sheets that can be applied to a large screen surface.

The researchers’ current prototype monochrome holographic display has an active area of $4 \times 4$ inches with a writing time of between one and two minutes. Blanche said the image persists for about two hours.

Movies or TV programming would require a display system that could refresh images every $1/30$ of a second.

---

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