Local Weather to Cool Supercomputer

The US Department of Energy’s Lawrence Berkeley National Laboratory is planning to use the weather in the surrounding San Francisco Bay area, rather than a typical expensive system, to cool a powerful exascale supercomputer the facility hopes to build during the next decade.

One of the DOE’s major computing-related goals is to develop exascale machines—which perform at 1,000 petaflops ($10^{18}$ floating-point operations per second)—by 2020.

The agency hasn’t yet determined how to design an exascale system, in terms of the processors, storage, networking, and programming approach it would use.

Berkeley Lab officials, though, have already determined that using the San Francisco Bay area’s generally moderate temperatures would adequately cool their Computational Research and Theory facility, which would house the supercomputer, 95 percent of the time. This approach would provide adequate cooling all the time if the exascale system produces less heat than expected, officials say.

The system would send water into a cooling tower that pulls in outside air. This would cool the liquid, which would then circulate through the exascale system.

Typically, supercomputers generate so much heat that they require elaborate, costly cooling systems.

Start-up Develops Encryption for the Cloud

Start-up security company Porticor has developed a novel split-key encryption technology for protecting data in the cloud. This addresses a key concern for cloud computing users: how to secure their own data when it’s stored on another organization’s cloud-based system.

Public-key-infrastructure technology has long protected data sent over the Internet between users’ own systems. In PKI, data is encrypted via a public key and only decrypted by a user with the associated private key.

This process is more complicated in the cloud. The main issue is where users could securely store cryptographic keys. Storing them in the cloud makes them vulnerable to hackers, and storing them with a security vendor requires trust in the vendor and its systems.

Porticor’s Virtual Key Management Service encrypts information via its Virtual Private Data application, using advanced algorithms such as that specified by the 256-bit-key Advanced Encryption Standard.

The system works like a safe-deposit box, in which the bank has one key, the user has another, and both are required to open the container.

In the Virtual Key Management Service, the user can’t decrypt a dataset without the key that Porticor has, and Porticor can’t decode the information without the user’s master key. In addition, the master key handles encryption of both keys. This keeps Porticor from being able to read private data, but also makes users completely responsible for the master key’s safe storage and handling.

The Virtual Key Management Service functions between the storage system and Porticor’s cloud-based server and thus can encrypt all data requested by users.

Porticor says its approach will work with all cloud systems.

McAfee: Unique Malware Samples Surpass 75 Million

According to security vendor McAfee, concerns about malware becoming an increasing problem are true. Its Threats Report: Fourth Quarter 2011 stated that the unique number of malware samples it found late last year exceeded 75 million.

The report said that although the amount of new malicious software grew more slowly in the fourth quarter of 2011 and the amount targeting PCs actually declined, mobile malware attacks increased to their highest level yet. McAfee said the Android mobile OS was a major target.
The growing threat to mobile systems is a particular problem because users increasingly conduct sensitive personal and business transactions via wireless technology.

The company said malware has become more sophisticated and targeted and now is likely to affect almost any type of computer, device, platform, or organization.

Other findings of the McAfee report for the fourth quarter of 2011 were

- data breaches via malware, hacking, and leaks of information from sources inside organizations have doubled since 2009;
- after a period of decline, threats from botnets have increased;
- hackers created an average of 9,300 new malicious websites per day, compared to 6,500 in the previous three-month period;
- 73 percent of the problematic sites originated in the US, 17 percent in Europe and the Middle East, and 7 percent in the Asia-Pacific region;
- an average of one in every 400 URLs was malicious, and there were more than 700,000 malicious URLs;
- the number of spam incidents continued to decrease, although many of the existing attacks were highly sophisticated; and
- the biggest network threat was represented by exploits of Microsoft Windows RPC vulnerabilities, followed by SQL-injection and cross-site scripting attacks.

App Lets Blind People Type on Smartphones

A team of Georgia Institute of Technology researchers has developed an application that could help blind people type on smartphone touchscreens without requiring additional, costly, hard-to-use equipment.

Postdoctoral researcher Mario Romero said he and his colleagues developed the BrailleTouch system for visually impaired users, who typically require expensive, bulky, or balky equipment—such as Braille or voice-activated keyboards—to type on touchscreens.

BrailleTouch users push combinations of six touchscreen buttons to type characters. The system then speaks the typed letter for confirmation.

After more testing, the Georgia Tech researchers plan to make the application available without charge for use with Apple iOS and Google Android phones.

Romero noted that the Braille-based system is so fast that some sighted people might also want to utilize it, particularly because users don’t have to look at the phone while typing. During tests, he noted, some subjects typed faster using the app than they could on traditional QWERTY keyboards.

Simulator Using Gaming Technology Could Reduce Flooding Casualties

New technology could quickly create 3D simulations of tsunamis,
Think You Know Software?
PROVE IT!

How well do you know the software development process?
Rise to the challenge by taking the CSDA or CSDP Examination.

With more and more employers seeking credential holders, it’s a great time to add this unique credential to your resume.

WWW.COMPUTER.ORG/GETCERTIFIED

The SINTEF-ICT scientists have developed an approach that uses computer graphics cards to accelerate the process.

Gaming technology involving elaborate virtual worlds has led to the development of powerful graphics cards that handle the necessary multimedia rendering. The SINTEF scientists used such cards in their natural-disaster simulations. In addition, they have developed code that speeds up the cards’ work.

The researchers say their approach can run so many calculations in parallel that the hardware generates less heat than if previous serial approaches were used. The system requires less cooling and thus is less costly to run and is more energy efficient.

The technique could be used for purposes other than simulating natural disasters, such as accelerating the discovery of underwater petroleum reservoirs.

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