

Security in Storage: A Call for Participation

Jack Cole, US Army Research Laboratory

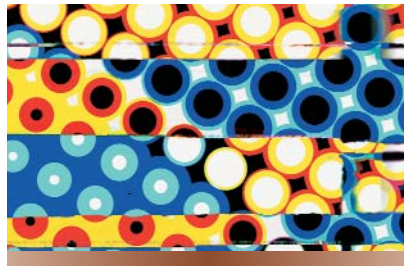
Protecting stored information for individuals, corporations, and governments has become more challenging than ever. Today's environment presents challenges that traditional storage farms, kept in protected enclaves, were never equipped to manage.

Factors that have led to greater exposure of both storage media and stored information include

- the widespread use of portable personal storage;
- the vulnerability of these devices to loss, theft, or capture; and
- third-party management of corporate storage.

If activities that rely on storage technology are to be viable, industry and government leaders must develop a comprehensive systems approach to storage security. One aspect is the development of standards.

In 2001, the IEEE began to explore the theoretical and practical aspects of designing, building, and managing secure storage systems by sponsoring an annual Security in Storage Workshop (<http://ieeiea.org/sisw/>). At the same time, the organization ramped up other activities related to the development of security in storage standards (<http://ieeiea.org/projects.html>). Participation in the area of security in storage can be rewarding, both personally and as a contribution to society.



CHANGING USES OF STORAGE

Personal portable storage devices that transiently connect to one another and to stationary systems offer great convenience, and such storage is often embedded in popular mobile devices, each with significant storage capacity.

With USB flash drives replacing floppy disks at a time of greater concern for security, sneakernet bandwidth has gone up considerably. Add to this mix the rise of mobile banking and other fiscal uses of personal portable devices with embedded storage, and the risks increase dramatically.

Portable, personal storage

The aggregate capacity of personal portable storage has exploded during the past few years, exceeding the capacity of the largest single institutional storage sites. Consider just one device: the Apple iPod was initially used to store music but is now used to contain pictures, calendar memos, dental records, and all sorts of other data.

Apple Computer shipped five million iPods in the second quarter of this

year (<http://arstechnica.com/journals/apple.ars/2005/4/13/55>), in capacities ranging from 4 to 60 Gbytes. Without knowing the distribution of models, but supposing that the units had a 20-Gbyte average capacity, the aggregate storage capacity of this one product was the equivalent of 100 petabytes (10^{17} bytes).

To appreciate this capacity, consider that NASA's Earth Observing System Data and Information System, the world's largest scientific data system, has accumulated only 4 Pbytes of data since the launch of the flagship satel-

The IEEE offers many opportunities to help provide better security in data storage.

lite five years ago ("NASA's Data Could Fill Library of Congress 300 Times," NASA Goddard News Release, 12 Feb. 2005; www.spaceflightnow.com/news/n0502/12data/).

Compare this to the sale of 100 Pbytes in a quarter-year of one portable storage device—not accounting for capacity or numbers of similar products sold by Apple competitors or past sales by Apple and its competitors combined. This also does not account for the vast array of other portable storage devices sold such as PDAs, Blackberrys, cell phones, USB flash drives, digital cameras, microdrives, and the like.

Recognizing the growing importance of portable storage, John Webster, senior analyst and founder of the Data Mobility Group, recently questioned, "Is It an iPod or Portable Storage in Sheep's Clothing?" (*Storage Networking World Online*, 25 Apr. 2005; www.snowonline.com/storage/insider/ipod_04-25-05.asp?s=6518).

"I read somewhere last week that data 'at rest' was not as big a security threat as data 'in flight,'" Webster wrote

Standards

in the article's mock diary entry. "I think that what the writer was really trying to convey was that data moving around in a network or exposed to network intrusion was at greater risk to theft than data parked somewhere on a disk drive.

"I wonder if the writer would care to reconsider that statement," Webster continued. "Data on an iPod may be parked on its internal drive, but it is movin', baby." After describing how his dentist backs up his office data on an iPod that he carts back and forth from home to office, Webster went on to say, "My dental records identify me. My dentist carries me with him when he goes home at night. I'll probably even be with him (digitally speaking) when he takes his kids to the beach."

USB flash drive

The storage industry has witnessed explosive private and corporate use of personal storage devices such as USB flash drives. These devices serve much the same function that floppy disks and Zip drives once did, but at much higher capacities—up to 4 Gbytes.

Floppy and Zip disks didn't require authentication before being read or written by a host, but USB flash drives have arrived in the marketplace at a time when security has become a greater issue. Enterprises are now beginning to require authentication of such devices before mounting by a host is permitted.

However, what happens when an infected transient storage device is connected to a system on a corporate network, or when such a device containing corporate intellectual property is lost at an airport?

Mobile banking and e-commerce

In many parts of the world, consumers can pay parking meters using a cell phone or conduct mobile banking transactions using various wireless devices. The European Mobey Forum (www.mobeyforum.org) deals with global financial industry issues and encourages using mobile technologies for services. Mobile banking is also taking off in Asia and other areas,

where businesses and consumers use handheld devices with embedded storage to manage staff salaries, mortgage payments, and charges for more mundane things like groceries and parking fees (www.cnn.com/2005/TECH/03/31/spark.mobile.banking).

Third-party storage management

Many IT professionals concerned about cost containment choose to outsource information management to

Many adverse conditions have emerged that present new challenges for security in storage.

companies that specialize in data storage. But how well are an information owner's interests protected when third parties manage data in consolidated storage facilities beyond the owner's control?

A storage provider can manipulate information from multiple unrelated organizations without regard to data ownership, moving the information over common storage area networks and saving it within different portions of the same device. This creates a new security risk because the merged information becomes vulnerable to threats from both the outsourcing organization and its other customers.

Adverse conditions

The "Storage Risks" sidebar provides examples that demonstrate the risks that can adversely impact the confidentiality and integrity of data. In all these real-life circumstances, the use of encryption would have provided protection to critical information without posing a hazard to human life, enabling identity theft, or risking public release of sensitive data. Encryption allows the possibility of key destruction, which is a quick and easy means of denying unauthorized access to information that is lost, stolen, or captured.

IEEE ACTIVITIES

The IEEE approaches security in storage—and other areas of information assurance—by integrating all tools and products at its disposal. IEEE security in storage activities, led by the IEEE Computer Society, include

- public events such as workshops and forums;
- full-use and trial standards;
- guides;
- best practices;
- publications, including proceedings, individual articles, and working-group notes; and
- public policy activities such as formulation of policy statements and education of policy makers.

The IEEE Task Force on Information Assurance (TFIA, <http://ieeetfia.org>) and the IEEE Information Assurance Standards Committee (IASC, <http://ieeieia.org/iasc/>) work together to sponsor workshops and forums, develop standards, publish proceedings and articles, and contribute to the development of public policy.

The TFIA and IASC collaborate closely with the IEEE Software and Systems Engineering Standards Committee (<http://standards.computer.org/sesc/>), the IEEE Technical Council on Software Engineering (www.tcse.org), the IEEE Mass Storage Systems Technical Committee (MSSTC; <http://msstc.org>), and the IEEE Storage Systems Standards Committee (<http://iee-sssc.org>).

Task Force on Information Assurance

The TFIA sponsors workshops on information assurance (<http://iwia.org>), critical infrastructure protection (<http://iwcip.org>), and security in storage (<http://ieeieia.org/sisw/>), and it cooperates with related workshops. The Task Force also cosponsored a recent presentation of the President's Information Technology Advisory Committee report, *Cyber Security: A*

Crisis of Prioritization (www.todaysengineer.org/2005/Aug/cybersecurity.asp), to the US Congress.

The TFIA, working with the MSSTC, will sponsor the 3rd International IEEE Security in Storage Workshop (www.ieeeia.org/sisw/2005) on 13 December in San Francisco, held in cooperation with the 4th Usenix Conference on File and Storage Technologies.

Information Assurance Standards Committee

The IASC sponsors several standards related to security in storage, all of which have working groups that are open to the community.

- *IEEE Std. P1667—Standard Protocol for Authentication in Host Attachments of Transient Storage Devices* (<http://grouper.ieee.org/groups/1667/>),
- *IEEE Std. P1700—Standard for Information System Security Assurance Architecture* (<http://issaa.org>),
- *IEEE Std. P1619—Standard Architecture for Encrypted Shared Storage Media* (<http://siswg.org>), and
- *IEEE Std. P1619.1—Standard Architecture for Encrypted Variable Block Storage Media* (<http://siswg.org>).

The present treatment of stored critical information, especially personal portable storage, provides inadequate protection. Through many means, the IEEE is examining the issue of security in storage and working to make technologies and standards available that advance the interests of society and protect its many critical functions.

Activities include research and idea sharing through workshops, the devel-

Storage Risks

Data owners need assurance that their intellectual property, privacy information, and military secrets are safe even when storage media or complete devices are lost. Although these cases are well known, largely unreported are the losses of personal portable devices such as iPods, PDAs, and cell phones—even though they may contain data just as critical as information kept on centralized systems.

Theft

December 2002: TriWest Healthcare Alliance, a records company within the US Department of Defense's TriCare system, announced the theft of computers and files from its Phoenix offices. Those systems contained the confidential and personal files of more than 500,000 members: active-duty military personnel, retirees, and their families. The stolen data included names, addresses, Social Security numbers, and other personally identifiable information such as diagnoses.

January 2004: Airlines Reporting Corp., an airline-owned transaction processing company, reported that two computers, one containing airline ticketing data, had been stolen. The stolen data included confidential customer information.

May 2005: Long-distance carrier MCI investigated the loss of employee data after a laptop was stolen from an MCI financial analyst's car. The laptop contained names and Social Security numbers of about 16,500 employees. A company spokesperson said the machine was password protected but didn't indicate whether the employee data were encrypted.

Loss

December 2004: Bank of America announced that tapes containing personal information on 1.2 million federal employees were lost in shipment. Customers affected included members of Congress.

May 2005: TimeWarner reported that tapes containing personal information for 600,000 current and former employees were lost in shipment.

June 2005: CitiFinancial notified some 3.9 million US customers that computer tapes containing information about their accounts—including Social Security numbers and payment histories—had been lost. Parent company Citigroup said that the courier UPS lost the tapes on their way to a credit bureau.

July 2005: Boston's Iron Mountain, the world's largest data-archiving company, reported that it had misplaced data backup tapes belonging to City National Bank of Los Angeles.

Capture

January 1968: The *USS Pueblo*, a US Navy spy ship gathering intelligence signals off the coast of North Korea, was captured, and a crew member died in the process of physically destroying critical information.

April 2001: A US Navy EP-3E surveillance aircraft was forced to land in China after colliding with a Chinese F-8 fighter. Although the crew apparently succeeded in destroying information before capture, the incident highlighted the vulnerability of military data.

opment of standards and guidance for protecting information, and educating policy makers to utilize these technologies and standards. The IEEE welcomes participation from any interested parties. ■

Jack Cole is the lead for technology exchange at the US Army Research Laboratory's Center for Intrusion Monitoring and Protection. Contact him at jack.cole@ieee.org or visit <http://msstc.org/cole>.