The Art of Identification
Technology Review (02/28/07), M. Erard

Researchers at the Netherlands Institute of Cultural Heritage are working on a system that generates traceable "fingerprints" for works of art as a way to discourage the flourishing underground trade in stolen art and artifacts. The system, known as FingArtPrint, creates a fingerprint using two steps. First, a one-centimeter square of an original work of art is selected, and the color of every pixel in the area is mapped using a scientific-grade digital camera. Next, the roughness of the area is examined using a white-light confocal profilometer, a type of microscope that scans micron by micron, turning what appears to be two-dimensional into a three-dimensional landscape that is unique to the object. The color and roughness information is then combined to make a fingerprint that is stored in a computer database. To ensure the authenticity of an object, a curator or buyer would have to capture a fingerprint from the object and match it to the original fingerprint stored in the database. A test conducted by the research team showed that FingArtPrint was able to capture reliable fingerprints from a variety of works of art and could even distinguished between two sculptures made from the same mold. The system has an advantage over other techniques for verifying authenticity because it has no physical effect on the object itself. However, because FingArtPrint examines patterns of cracking or fading due to aging to create fingerprints, further aging after an original fingerprint is taken could make an original work appear to be a forgery.

Berners-Lee Gets Technical on the Hill
InternetNews.com (03/01/07), R. Mark

Internet pioneer Tim Berners-Lee spoke before the House Subcommittee on Telecommunications and the Internet on Thursday to tout the importance of network neutrality and the need to do away with DRM protection. Berners-Lee pointed out that network neutrality is accepted in other countries, and said, "I feel a non-discriminatory Internet is very important for a world based on the World Wide Web... The special care we extend to the World Wide Web comes from a long tradition that democracies have of protecting their vital communications channels." He said a slight compromise on the issue may be appropriate, but maintained that "we should err on the side of keeping a medium blank sheet." In his argument against DRM protections, Berners-Lee stressed that the growth of the Internet is based upon open standards, scalable architecture, and access to standards on a royalty-free basis. "E-commerce entrepreneurs have been able to develop services with the confidence that they will be available for use with an Internet connection and a Web browser," he said. Berners-Lee also noted that Apple's use of non-standard technology for its copy-protection scheme has led to slow growth, while its open-standard podcast component has grown significantly. Instead of using DRM, he suggested software that "let[s] people do the right thing," although he is not sure "if we will [ever] move to a totally DRM-free world."

Online Voting Clicks in Estonia
Wired News (03/02/07), J. Borland

The first national election to feature online balloting for all voters is being held in the Baltic state of Estonia. "No one has managed to prove that e-voting actually raises participation, so that remains unanswered," says National Electoral Commission secretariat A. Koitmae. "But this gives people another possibility." The system requires a national ID card equipped with an electronic chip that identifies the card holder, while card readers are available at low prices or for free; voter authentication is facilitated through two sets of PIN. The ID card is slotted into the reader, and the voter application displays a list of parties and candidates via Internet Explorer. A registered vote is encrypted and routed through a chain of relay servers to an archive until its decoding on Sunday. Many other countries, particularly the United States, are concerned about the security and reliability of e-balloting, and US critics are worried that voting systems that employ conventional Windows PCs and the open Internet could be compromised by outsiders as well as insiders. Estonian government services are already online, while wireless connections have spread to almost all city cafes, parks, bars, and commuter trains, so concerns about e-voting's security are somewhat muted. Political scientists are more optimistic of e-voting systems than computer scientists, as long as voters trust the system.

Fighting Bugs: Remove, Retry, Replicate, and Rejuvenate
Computer (02/07) Vol. 40, No. 2, P. 107; M. Grottke; K. Trivedi

The software faults or bugs responsible for system failures cannot be determined and isolated if the failure cannot be reproduced, and it is estimated that between 15-80% percent of all software faults detected after release are of a variety that are not spotted during testing for precisely this reason. These "Mandelbugs," as they are called, behave differently under apparently identical conditions for one of two reasons: Because there is a long delay between the activation of the bug and the final failure occurrence, complicating the identification of the user actions that triggered the bug and induced the failure; or because other software system elements--the operating system, the hardware, or other applications--can affect a bug's behavior in a specific application. One way of dealing with Mandelbugs is to retry a failed action by restarting the application, and this method can be enhanced via checkpointing, in which a snapshot of the application is regularly saved in stable storage. It is also possible to use a replication methodology that employs redundant resources. Performance degradation of software systems in continuous operation for a long duration can cause failures to occur more frequently, and this can be prevented through software rejuvenation techniques. Bugs related to software aging can cause errors to build up over time, while the activation rate of an aging-related bug can be affected by the total time that the system runs continuously. The two primary rejuvenation strategies are model-based approaches, which use analytic models to catch system degradation and rejuvenation, and measurement-based approaches where system properties that might show signs of software aging are periodically watchdogged. The costs of software rejuvenation include unavailability of a hosted Web site during a Web server's reboot, or the division of the workload among running servers in a multiple-server scheme.

Software Vulnerability Index Making Progress
IDG News Service (03/01/07), M. Hines

The Common Weakness Enumeration (CWE) project expects to publish the sixth iteration of their software vulnerabilities index in April, and says the final draft of the encyclopedia should be ready later in the year. The security experts involved in CWE continue to aggregate and organize the enormous amount of data on software flaws that they have collected, and lately they have focused more on testing commercial security scanning tools to determine their effectiveness. The applications target 45% of the 600 common vulnerabilities that have

been entered into the CWE index thus far. "We found that less than half of what we already have in CWE is covered by these tools, so this helps prove that there are a lot of known issues out there that aren't being addressed," says Citigal's S. Barnum. "We also thought that the tools would look for the same types of things, but they are actually very different, and there's not a lot of overlap; that's something that developers need to be aware of as they choose tools; you want to right set for aggregated coverage." A central resource on common flaws is viewed as a helpful tool for improving software quality, and project participants believe it could lead to a common language and standard procedures for addressing the loopholes in source code today. The Department of Homeland Security is sponsoring the CWE initiative.

Foolproof Quantum Cryptography
Technology Review (03/02/07), D. Graham-Rowe

Current quantum-cryptographic systems are hindered by the fact that sending information more than a short distance allows the encryption keys to be intercepted in a manner that is undetectable. When sending bursts of light over optical fibers, stronger pulses often contain more than one photon, meaning single photons can be intercepted without the transmitter or receiver being aware. Toshiba has developed an "unconditional security" system that allows stronger signals to be sent, using individual "decoy photons" sent along with the signals in order to detect eavesdropping. Using this system, eavesdroppers' attempts to block single photons and siphon off multiple photons from other pulses will result in more decoy pulses than the rest of the signal being blocked, and by measuring the ratio of decoy pulses that make it through to signals that make it through, an attack can be identified. This ability to detect eavesdropping allows stronger signals to be used, and therefore allows encryption keys to be sent greater distances. The new challenge confronting researchers is to create a system that more reliably produces single photons, which would eliminate the need for "decoy pulses." Toshiba envisions an array of quantum dots each measuring 45 nanometers in diameter and capable of emitting only single photons.

Black Hat Demonstrations Shatter Hardware Hacking Myths
eWeek (03/01/07), L. Vaas

At the Black Hat Briefings in Arlington, Va., two long-standing hardware security beliefs, that reimaging would remove a rootkit hit on a system and using a PCI card or a FireWire bus was the best way to search a PC's volatile RAM memory, were proven false in two demonstrations. The first demonstration exploited a way to subvert system memory through software, destroying the long-held conviction that "going to hardware" to secure incident response worked as a security failsafe. Following such an attack, the only way to correct the system's memory corruption would be to reboot, erasing all evidence of the subversion and leaving digital forensic teams unable to figure out, or prove in court or to auditors, what the attackers did on the company's computers. The second demonstration proved that rootkits can persist on a device, or firmware, rather than on only a disk, and can survive a machine being reimaged, and can even survive reformatting. Though these hacks are not widely known or frequently deployed, they prove that a significant number of assumptions about hardware security are false.