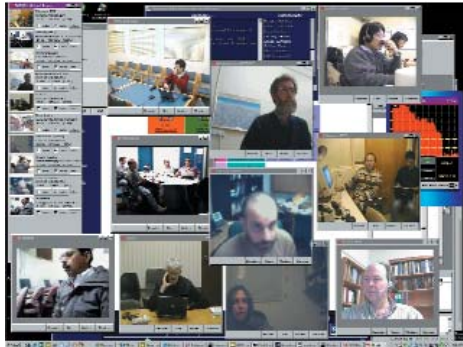


VIDEOCONFERENCING BY THE NUMBERS

USING TODAY'S VIDEOCONFERENCING TECHNOLOGY TO LINK MORE THAN THREE or four remote sites can be prohibitively expensive. But physicists from Caltech have devised a method that enables people located at as many as 40 sites around the world to confer affordably. The new setup employs a network of servers, scattered across 27



Web conferencing lets more people meet.

countries, that brings people together from different sites in one "virtual room" on the Internet. This approach eliminates the expensive hardware at each site that conventional systems require; instead, it can use cheap commercial webcams and microphones. It should thus allow some users to join videoconferences who couldn't afford to otherwise. A user simply downloads software written by the Caltech group and logs in to a Web site; each of the other attendees appears in a separate window on the user's desktop. More than 5,000

scientists from 88 countries are already using the system, which a team led by Harvey Newman and Philippe Galvez originally developed as a means of communicating with colleagues. The researchers have recently started up a company, VRVS Global in Pasadena, CA, to commercialize the technology.

DIGITAL DOORMAN

Electronic door locks secure everything from offices to dormitories, but wiring them up to send and receive data can be expensive. So Cambridge, MA-based CoreStreet has developed a wireless identity verification system, due out by year's end. Current systems use wires to gain secure access to a central database. But with CoreStreet's system, authorization information is stored at each lock. To periodically update that information, the system uses proprietary algorithms to generate a tiny, encrypted wireless message that informs each lock who has permission to enter. By eliminating wiring, says Phil Libin, CoreStreet's cofounder and president, the system "allows you to control access to things you can't right now," including airplane cockpits and trucks transporting hazardous cargo.



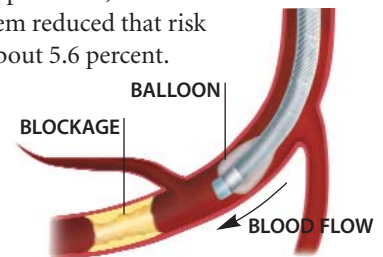
Tests take the "fingerprints" of seemingly indistinguishable microchips.

IDENTITY ANTITHEFT

THE MICROCHIPS IN SMART CARDS AND OTHER DEVICES OFTEN STORE DIGITAL keys—long strings of 0s and 1s—used to authenticate users and encrypt data in secure transactions. But specialists know that pirates can steal the keys by analyzing the chips' hard-wired connections. MIT computer science professor Srini Devadas might have found a virtually unbreakable scheme: let the chip itself act as the key. At the microscopic scale, circuits are never identical, even on chips manufactured the exact same way, and signals take different times to propagate through silicon and metal paths. Devadas has designed a very simple chip that includes a huge number of paths and a circuit that acts as a stopwatch. By timing the delays along a few hundred of the paths, Devadas can generate a unique fingerprint for each apparently identical chip. That fingerprint—recorded when the chip is made and stored in a database—can act as a key to, for instance, unlock proprietary software, or authenticate an online transaction. Devadas says the secure chip would cost about as much as those used in smart cards but offer much higher security. He and his coworkers have filed a patent and are in discussions with electronic-products manufacturers and smart-card companies about production of the chip, which could be on the market in one to two years.

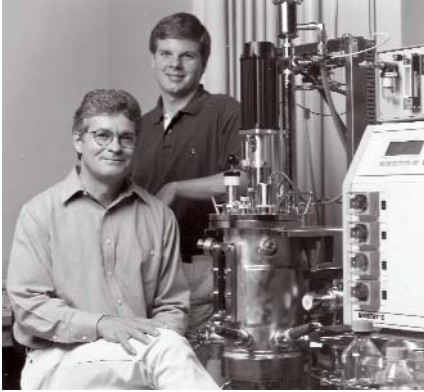
HEART HELPER

OPENING CLOGGED ARTERIES WITH balloon angioplasty saves many heart patients' lives, but the procedure has its own risks. During surgery, bits of the gunk blocking the blood vessel may break off and can cause heart attacks. Velocimed of Minneapolis, MN, is seeking U.S. Food and Drug Administration approval for a system that could reduce that danger. In the system, the artery-opening balloon is inflated upstream of the blockage, so even if gunk breaks off, there's no moving blood to carry it downstream. The trick is a tunnel through the balloon that lets doctors insert a "stent" that props the artery open and suck out any loose material with a syringe before they remove the balloon. With traditional angioplasty, up to 16.5 percent of patients suffer cardiac events such as heart attacks within 30 days of stent placement. But in a small European trial, Velocimed's system reduced that risk to about 5.6 percent.



This artery opener reduces angioplasty's risks.

COURTESY OF VELOCIMED (HEART); COURTESY OF SRINI DEVADAS (IDENTITY); COURTESY OF PHILIPPE GALVEZ (VIDEOCONFERENCING)



Protein makers Jim Swartz and Jim Zawada.

CELL-FREE PROTEINS

PROTEIN-BASED DRUGS ARE A FAST-GROWING CLASS OF NEW MEDICINES, BUT they cost 20 to 100 times more to make than conventional drugs. One reason is that proteins can only be made by living cells, which are not very efficient producers. Researchers at Stanford University believe they can cut costs by doing away with the cells and instead exploiting the protein-making machinery inside them. Chemical engineer Jim Swartz and his colleagues have come up with a way of growing bacteria, busting them open, pulling out their innards, and adding a soup of chemicals that mimics the inside of a cell. Also tossed into the mix are amino acids (proteins' building blocks), enzymes, and strands of DNA that encode the protein to be churned out. With no cells to keep alive, all those parameters can be fine-tuned for protein production. Swartz says the method can boost protein production five- to 10-fold and cut up to 80 percent of the capital costs. The researchers founded Fundamental Applied Biology in San Francisco, CA, to commercialize the technique.



With a swipe of this device, you can print directly onto e-paper.

E-PAPER PRINTER

ELECTRONIC PAPER, MADE OF CHARGE-SENSITIVE "INK" PARTICLES EMBEDDED in a thin plastic film, promises lightweight, flexible displays that consume minimal battery power. But e-paper has typically required a layer of electronics behind the film to turn the particles on and off, adding bulk and cost. Now researchers at the Palo Alto Research Center have developed a handheld device that can print information from a computer directly onto e-paper; the device activates the ink particles electrostatically as it's swiped across the paper's surface. PARC researchers plan to use the device initially to print on large e-paper whiteboards. In the future, the device could also be used to scan information from the whiteboard into a computer. "The idea of a scanning wand in conjunction with electronic paper is a really important step," says Nicholas Sheridan, electronic-paper pioneer and research director at Ann Arbor, MI-based PARC spinoff Gyricon. PARC has multiple patents pending on the technology.

PROGRAMMABLE WINDOW

A huge electronic display on a skyscraper facade can be interesting to passing pedestrians, but if you're inside the building it simply blocks your view. Researchers at MIT's Media Laboratory and Department of Urban Studies and Planning are developing a transparent display that doesn't entirely block incoming light. The group is adapting a commercially available film used in electronic window shades, a high-tech alternative to blinds or curtains that lightens and darkens when electricity is applied and removed. The display will be a matrix of small separate pieces of the film. A grid of tiny wires will connect the pieces to a computer, which will be able to compose letters and figures in gray-scale patterns. Because the film at its darkest blocks only 40 percent of incoming light, and because only some of the pieces in the matrix will be darkened at any given time, people sitting behind the display will still be able to see out. Project coordinator Carlo Ratti says the technology might be seen on the streets within a year.

CURVY SECURITY

TO KEEP MESSAGES SECURE, THE COMPUTERS THAT RUN wireless networks must do some complicated math to authenticate every Internet-enabled cell phone or wireless personal digital assistant that contacts them, and the devices must do the reverse, which can tax their batteries. Sun Microsystems senior staff engineer Hans Eberle and his team at Sun Labs are addressing that problem by creating a microprocessor that can be plugged into network computers to quickly authenticate messages from a range of wireless gadgets. The numerical "keys" used to authenticate most



Sun's chip (big black square) secures messages.

electronic messages today are generated by multiplying prime numbers; but to foil hackers, these numbers must be very large, containing up to 1,024 digital bits. Eberle uses a technique called elliptic-curve cryptography that instead derives keys from complex geometrical curves. The complexity of the curves makes the keys more difficult to break, so the same level of security can be achieved with smaller keys that require less computation to use. Eberle's chips can establish secure connections at the rate of 7,000 per second—the "fastest reported," he says. Sun's product groups are evaluating the microprocessors for inclusion in the firm's server computers.

COURTESY OF SUN MICROSYSTEMS (CURVY); COURTESY OF THE PALO ALTO RESEARCH CENTER (E-PAPER); COURTESY OF JIM SWARTZ (CELL-FREE)