



## Press Releases

### The Latest in Computer Security Revealed at WPI International Workshop

Contact: [WPI Media & Community Relations](#)

WORCESTER, Mass. - More than 180 computer security experts, half of whom traveled from outside the United States, converged on Worcester Polytechnic Institute for the 1999 Workshop on Cryptographic Hardware and Embedded Systems (CHES), Aug. 12-13. The popular workshop provided a forum for real-world system and design issues.

Conference organizers Cetin Koc of Oregon State University and Christof Paar of WPI point out that many consumer products are gaining computer-like capabilities. E-commerce and other electronic communications demand that sensitive data, such as credit card numbers, must be protected from prying eyes. The tool for protecting information, called cryptography, will be required in these products, using embedded systems that offer relatively little computational power.

The challenge of adding cryptography to hardware devices and embedded systems led to the development of the WPI workshop. In its inaugural year, international experts presented new results on efficient implementation of cryptographic algorithms and attacks, as well as other practical issues in system design such as random number generation.

Among the highlights of the conference was a talk by Adi Shamir, a co-inventor of the RSA code used to protect e-commerce. Shamir called the security of the world's leading web browsers into question with a new fast factoring attack.

The most eagerly awaited contribution to CHES involved not only a fast way to make a code, but also a fast way to break one. The RSA public-key cryptosystem, which is widely used in web browsers such as Netscape Communicator and Microsoft Internet Explorer, is based on the problem of factoring large numbers. It is an acronym based on its inventors (Rivest-Shamir-Adleman).

Fortunately for consumers and businesses, up until now, factoring algorithms have been slow and memory intensive processes. But at the workshop, Shamir, from Israel's Weizmann Institute of Science, shed light on an ingenious way to speed up part of a factoring computation known as sieving. A sieve procedure consists of repeatedly running through a long list of numbers and finding which small integers divide those in the list. Using optoelectronics, Shamir's new device, called TWINKLE, offers a 500-1000 times speedup over the fastest workstations on the market in this crucial stage of factoring. This development has grave implications for electronic commerce: Due to U.S. export laws, the strongest exportable public-key systems are restricted to 512 bits. If and when the device is actually built, these systems can be easily broken. The systems, Shamir pointed out, "protect 95 percent of today's e-commerce on the Internet," and thus render them "very vulnerable."



Security Needs: WPI professor of electrical and computer engineering Christof Paar, left, discusses computer security with Brian Snow, middle, of the U.S. National Security Agency and his fellow conference organizer, Cetin Koc of Oregon State University.



Code Breaking: Adi Shamir, second from right, a world-renowned cryptographer, shares his insights with attendees of CHES

Brian Snow of the U.S. National Security Agency emphasized the need for more research in assurance technology.

"The scene I see is products and services sufficiently robust to counter many, but not all, of the 'hacker' attacks we hear so much about today, but not adequate against the more serious but real attacks mounted by economic adversaries and nation states," Snow noted. "We will be in a truly dangerous stance: We will think we are secure, and act accordingly, when in fact we are not secure."

Experts continue to search for answers to computer security. Another development at CHES involved improved methods for generating random numbers. Nearly all real-world cryptosystems need random numbers. Unfortunately, this is an extremely difficult problem, since computers are designed to be completely predictable.

At CHES, scientists from Italy's Ugo Bordoni Foundation offered a cost-effective idea based on sampling noisy semiconductor junctions. Normally in circuit design, engineers try to reduce noise. However, by building noisy circuits on purpose, one can use the noise as a source of random numbers. In addition, researchers from Bell Labs Innovations provided a variety of new, practical techniques including one based on chaos theory, which appears to be particularly cost-efficient.

Of course, efficiency of performance is just as crucial as cost. Sandia National Labs researchers presented a design for a new computer chip that can encrypt up to 10 gigabits of data per second, satisfying all but the most demanding of applications. In addition, one can use three of the chips together to handle Triple-DES encryption with no loss of performance. The DES, or Data Encryption Standard, algorithm is the most widely used bulk encryption method, having been a U.S. government standard since 1977. Since DES itself is now considered inadequate to protect against attackers, Triple-DES is gaining in popularity.

CHES provided a vital forum for scientists and engineers working in practical cryptography to meet and share ideas. As time passes, more and more consumer products will handle sensitive data, making the need for practical cryptography even more critical. Therefore, CHES will become an annual event, with next year's event to be held at Oregon State University.

For more information on CHES, contact Paar at 508-831-5061 or 831-5840; e-mail [christof@ece.wpi.edu](mailto:christof@ece.wpi.edu); or visit the CHES Web site at <http://ee.wpi.edu/Research/crypt/ches/>.

