Privacy-Enhancing Technologies

Stephen A. Weis
Independent Consultant

The sixth annual Workshop on Privacy Enhancing Technologies (PET) was held in Cambridge, England, from 28–30 June 2006. The workshop included sessions focusing on real-world privacy, cryptography, multiparty computation, and traffic analysis. This year's PET workshop was colocated with the Workshop on Economics of Information Security (WEIS) and the Workshop on Trustworthy Elections (WOTE).

Sun Microsystems's Susan Landau delivered a keynote speech on the current state of data-collection privacy. Expressing concern over recent developments, such as the US National Security Agency's wiretapping program, Landau called on researchers to consider the ethical and societal impact of their work with regard to individual privacy. She praised Pugwash organizations (www.pugwash.org) that educate scientists on ethical issues.

Richard Clayton of Cambridge University presented a notable talk detailing how to circumvent the "great firewall of China" with which the Chinese government censors the Internet for its citizens. Based on a paper coauthored with Steven J. Murdoch and Robert N.M. Watson, also from Cambridge, Clayton described how China's firewall searches for forbidden keywords such as "falun" (as in the Falun Gong group banned in China) inside TCP packets. Upon detecting a censored word, the firewall forges TCP reset messages to both ends of the connection. Standard TCP implementations honor the forged reset messages and shut down the connections. The firewall then automatically forges reset messages to both parties for about 20 minutes.

Yet, TCP stack implementations can easily detect and safely ignore the forged reset messages. If both ends of the connection ignore the forged reset packets, the forbidden traffic proceeds unmolested. Clayton described how sending messages containing verboten words to users inside the firewall triggers the 20-minute "cool down" period.

Clayton suggested that if TCP stacks ignored forged reset packets by default, Chinese users could circumvent the firewall with plausible deniability—they wouldn't be running any special software.

Simson Garfinkel of the US Naval Postgraduate School and David Malan of Harvard University, presented a paper discussing disk data sanitization. Garfinkel and Malan tested several standard sanitization tools on various file systems and measured how much data could be recovered. They also tested simply filling a disk with one big file as a sanitization technique. As the title of Garfinkel and Malan's paper states, "One Big File Is Not Enough" to sanitize a disk because they reliably recovered file names and, often, slack space in spite of sanitization attempts.

Anonymizing mix networks, particularly Tor (http://tor.eff.org), were the subject of multiple talks during the workshop. Tor inventors Roger Dingledine of the FreeHaven project and Paul Syverson from the US Naval Research Laboratory presented several mix network-related papers. Their paper, coauthored with Andrei Serjantov, also of the FreeHaven project, described alpha mixing, which lets users in a mix network like Tor specify performance and anonymity trade-offs on a per message basis.

The University of Waterloo's Ian Goldberg also presented a formal proof of security for the Tor authentication protocol. Tor uses its own custom protocol, rather than a well-established authentication protocol. Goldberg showed that Tor's custom authentication protocol is in fact secure in the random oracle model and under standard cryptographic assumptions.

Overall, the conference offered a broad range of both theoretical and practical privacy-enhancing constructions, attacks against existing schemes, and policy-framework analysis. The breadth of privacy-related topics covered at PET 2006 made it an interesting, accessible, and educational conference to attend. The seventh PET workshop is scheduled to take place in 2007 and will likely be held in the US. □

***Stephen A. Weis** is a software engineer. His research interests include cryptography, information security, and privacy. Weis has a PhD in computer science from the Massachusetts Institute of Technology. Contact him at sw@saweis.net.*