Guest Editorial

Frederick M. Avolio
Trusted Information Systems, Inc.

If the hottest topic of the late 90s ends up being "The Internet"—and please notice people are ceasing to talk about the Information Superhighway and are just talking about the Internet again—then the hottest subtopic is computer and network security. (Okay, I mean besides the World Wide Web.) The Fifth USENIX UNIX Security Symposium, this past June, reflected this phenomenon. More than three quarters of the attendees were first-time USENIX attendees. For more than half, it was their first computer or network security symposium. They were there because their jobs demanded it, or because it was, for them, unexplored territory.

The papers submitted, and so those selected and presented, represented the needs of the new Internet community: three of four papers on one-time password research were presented, as were papers touching on IP encryption, privacy in general, and hardening of the base operating system. A few case studies of network use and abuse and protection were offered.

On the Uniform side of the symposium, I was moderator for a panel discussing techniques and mechanisms for assuring "privacy," and I commented that I looked forward to a day—soon, I hope—when privacy mechanisms in computer and network communications become as commonplace as the envelope in which I mail a bill or a personal letter. I would like my e-mail software, for example, to automatically send all of my e-mail encrypted, if it can for the addresses. If I have a public key on file for an addressee, the e-mail program will use that key. If I do not have one on file, the software will query the network and try to obtain a public key for the addressee. If and only if no public key was found for the individual, would the message be sent unencrypted. You see, in this way, it will become **commonplace** for me to use cryptology to send e-mail and out of the ordinary for me to send e-mail in the clear. Just as 90% of the postal mail I send is in sealed envelopes, with the occasional note scrawled on a postal card, 90% of my e-mail will be sealed. Most of the time I am not hiding any secrets. In no case am I trying to cover a crime. And yet, even with little to hide, the normal way for me to send p-mail is to do it in a sealed envelope.

And soon, I hope, this will be the norm for all of us. Cryptology will protect our business dealings, our friendly letters, our terminal connections, and our

file transfers, and authenticate our identity to our computer systems and to our correspondents and friends.

Henry L. Stimson, Secretary of State under Herbert Hoover, is quoted as having said, "Gentleman do not read each other's mail!" While this may be true, the World, and so the Internet, is populated by many who are neither gentlemen nor gentlewomen.

The papers presented in this volume represent extensions or additions to works presented at the USENIX UNIX Security Symposium. The authors, in each case, have expanded or revised their previous work. Each matches the different areas of interest represented at the symposium: The "user problem" and threats and vulnerabilities; user authentication in a time when only fools use reusable passwords across the Internet; encryption for privacy; and hardening the basic UNIX operating system. Each discusses topics that will continue to concern computer, network, and especially Internet users for the foreseeable future.