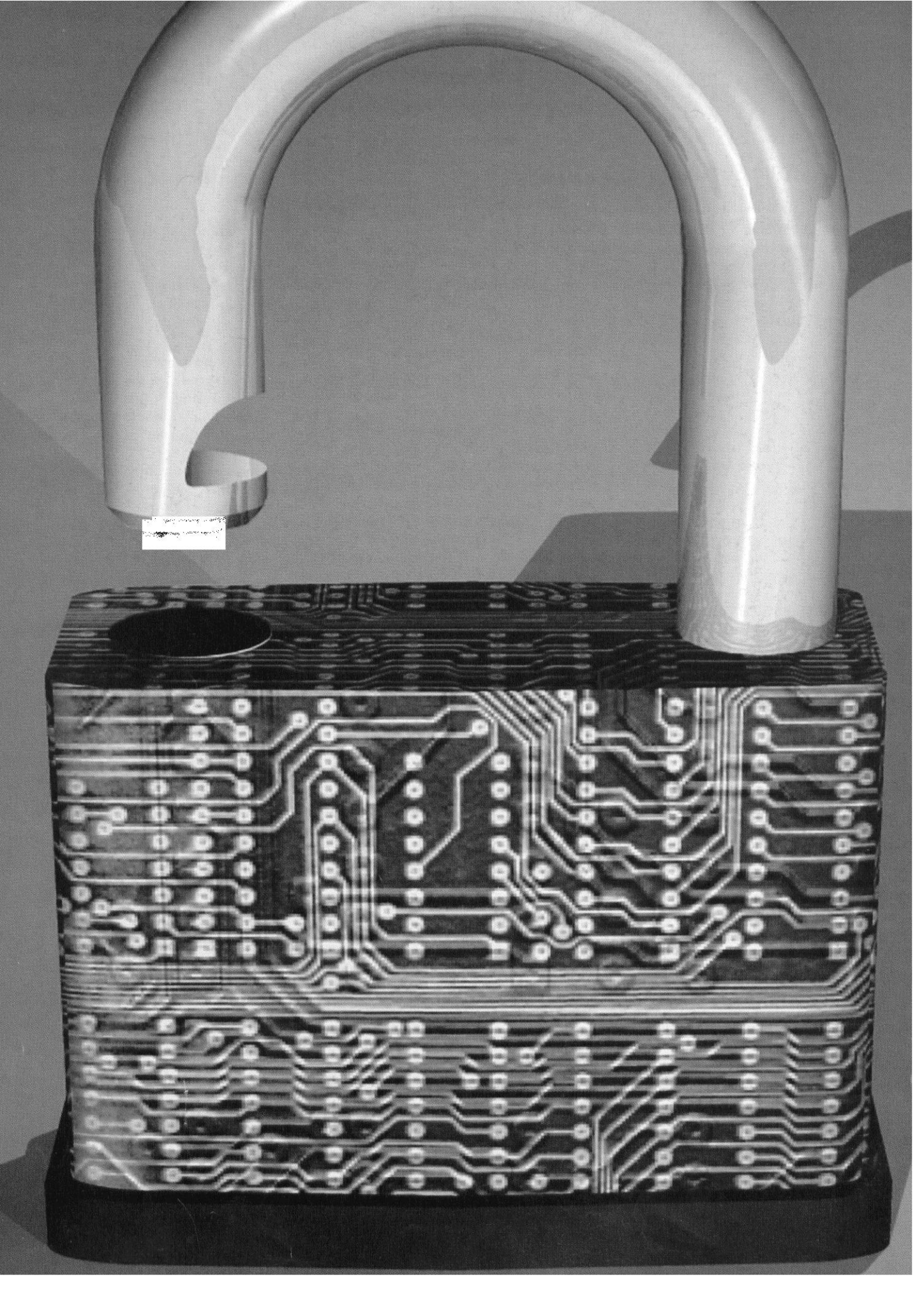

Guest Editors:
Ravi Ganesan
Ravi Sandhu

Securing Cyberspace

As you read these words your computer or communications systems may be under attack. If your personal or corporate cyberspace has been penetrated, what damage could a malicious intruder cause? Destroy your customer records? Steal the customer records and sell them to your competitor? Intercept communications between your troops during battle? Forge your digital signature? Alter your credit or medical records? ■ A simple thought exercise like this should quickly convince you that the potential for damage caused by violation of your cyberspace is limitless. The "old world" of paper-based information, or information contained on isolated computers, had a fairly well-developed threat model and we basically knew how to protect ourselves. In a fully connected cyberspace, the threats to our organizational and personal cyberspaces are much greater, and all the threats have not even been discovered, leave alone protected against.

The development, and especially deployment, of security technologies has not kept apace of the heightened threats a distributed connected environment presents. However, (before you rush to disconnect your workstations from your network!), we do wish to reassure you that there is good news. Practical distributed systems security is maturing and it is becoming increasingly possible to adequately secure our cyberspace.

One key to this maturity is the increased attention the security community is paying to the practical concerns of commercial environments and, for that matter, to those of a typical government or "less top secret" military establishment.

In the past, security was often exclusively viewed from the perspective of:

- The highly structured and rigid concerns of a top-secret military establishment leading to mandatory access controls;
- The free-flowing academic research environment driven by individual researchers providing discretionary access controls, or;
- Through the lens of a cryptographer who reduced a messy practical problem to clean mathematical abstractions concerning communications security.

Unfortunately, this has resulted in inadequate attention to the security concerns of commercial environments. Consider operating systems: for too long the choices have been to either purchase a highly secure multilevel operating system that is expensive to buy and maintain, or to purchase an operating system that out of the box has little or no security. Unlike a top-secret defense environment that can present a business case to justify the expensive highly secure option, most commercial environments cannot. Ironically, many current top-secret installations treat security as a people problem by running a system high (i.e., all users are trusted to see the highest level of data processed in the system) rather than by using multilevel operating systems to properly segregate data among a mixed user population. Similarly, in a 'national security environment' intercepted communications are a major issue, and hence much work in cryptography is devoted to a model in which communications are intercepted. As a result, it is often not recognized that in typical commercial environments, it is usually easier for an attacker to focus his attention on the endpoints—the strongest encryption system is useless if the encryption keys are stored on vulnerable computers, or implemented in the form of weak passwords. The bottom line is the threat model underlying most security work was largely inappropriate to that of any non-top-secret-spare-no-expense-on-security environments.

This situation is changing. Distributed systems make commercial environments more vulnerable than ever before, and hence the demand for security technologies by this sector of the marketplace is rapidly increasing. The growth of technologies such as electronic commerce mandates the duplication of security paradigms implicit in the paper world—signatures, and hence their expansion fuels the demand for new security technologies—digital signatures. To help catalyze and better focus this new direction toward practical security technologies, the ACM Special Interest Group on Security, Audit and Controls (SIGSAC), Bell Atlantic, and George Mason University have jointly started the ACM Conference on Computer and Communications Security. The inaugural conference was held last November and the second conference will take place this month in Fairfax, Virginia.

This issue features four articles, preliminary versions of which appeared at the first conference. The first article, by Ross Anderson, is a revealing eye-opener that dramatically underscores the significant gaps between the nature of practical security problems and the theoretical models of those researching and building security models. It reiterates a principle those of us who have managed tight security budgets in the real world are always acutely aware of: Do not spend money to carefully secure the attic windows when your front door is wide open. Most threats to cyberspace today are decidedly low-tech. In your rush to implement the latest greatest security technology, do not neglect these problems.

Among the attacks that can often be mounted in a low-tech fashion are denial of service attacks. In these attacks, an intruder does not necessarily steal information but instead, for profit or for pure malicious delight, disrupts all your operations, for example, by flooding your network with messages. Roger Needham examines one example of such attacks. This article on denial of service is especially valuable as it calls attention to a class of attack to which our cyberspace is much more vulnerable than we sometimes realize.

Changing pace, Ralf Hauser addresses a problem that is rapidly becoming of extreme importance to anyone who sells software: how do you protect against software piracy? His article on software licensing examines some solutions and describes an approach based on the concept of trying to help "honest system administrators keep their users honest." While this approach does not protect against dishonest system administrators or skilled hackers who

Distributed systems make commercial environments more vulnerable than ever before, *and hence the demand for security technologies by this sector of the marketplace is rapidly increasing.*

rely on sophisticated Trojan Horses to circumvent licensing agreements, the proposed scheme will make it very hard for users in a typical environment to cheat. As such it is an example of "adequate" security for a given realistic threat model.

The final article, by Gus Simmons, is in our opinion required reading for anyone who produces, buys, or uses products that implicitly or explicitly make any promises about security. It illustrates how a seemingly secure protocol can have extremely subtle problems that compromise the security of the system in a very unsubtle and dramatic fashion. It is also a stark reminder to all that the state of the art in proving or certifying security properties is at best an inexact science, and a reminder that even the most convincing arguments for the security of a product or standard are far from absolute guarantees. Unfortunately, "proven security" is in the same category of desirable oxymorons such as "reliable software." Naturally, just as we must continue our efforts to build reliable software, we need to continue proving security properties. An educated buyer, however, will look beyond claims of security by the producer to factors such as the length of time a security product or standard has been in existence, whether its internal mechanics have been publicly available to be scrutinized by the security community, and the strength of assurance techniques that have been applied to produce evidence for security.

We hope you will find these four articles relevant and intriguing. They are a sample of the techniques and technologies that go into building and deploying security products and services that will make cyberspace a more safe, productive, and enjoyable place to live and work. ◘

Ravi Ganesan *is Senior Manager at Bell Atlantic's Center of Excellence for Electronic Commerce. email: ravi.ganesan@bell-atl.com*

Ravi Sandhu *is an associate professor in the Information and Software Systems Engineering department at George Mason University. email: sandhu@isse.gmu.edu*