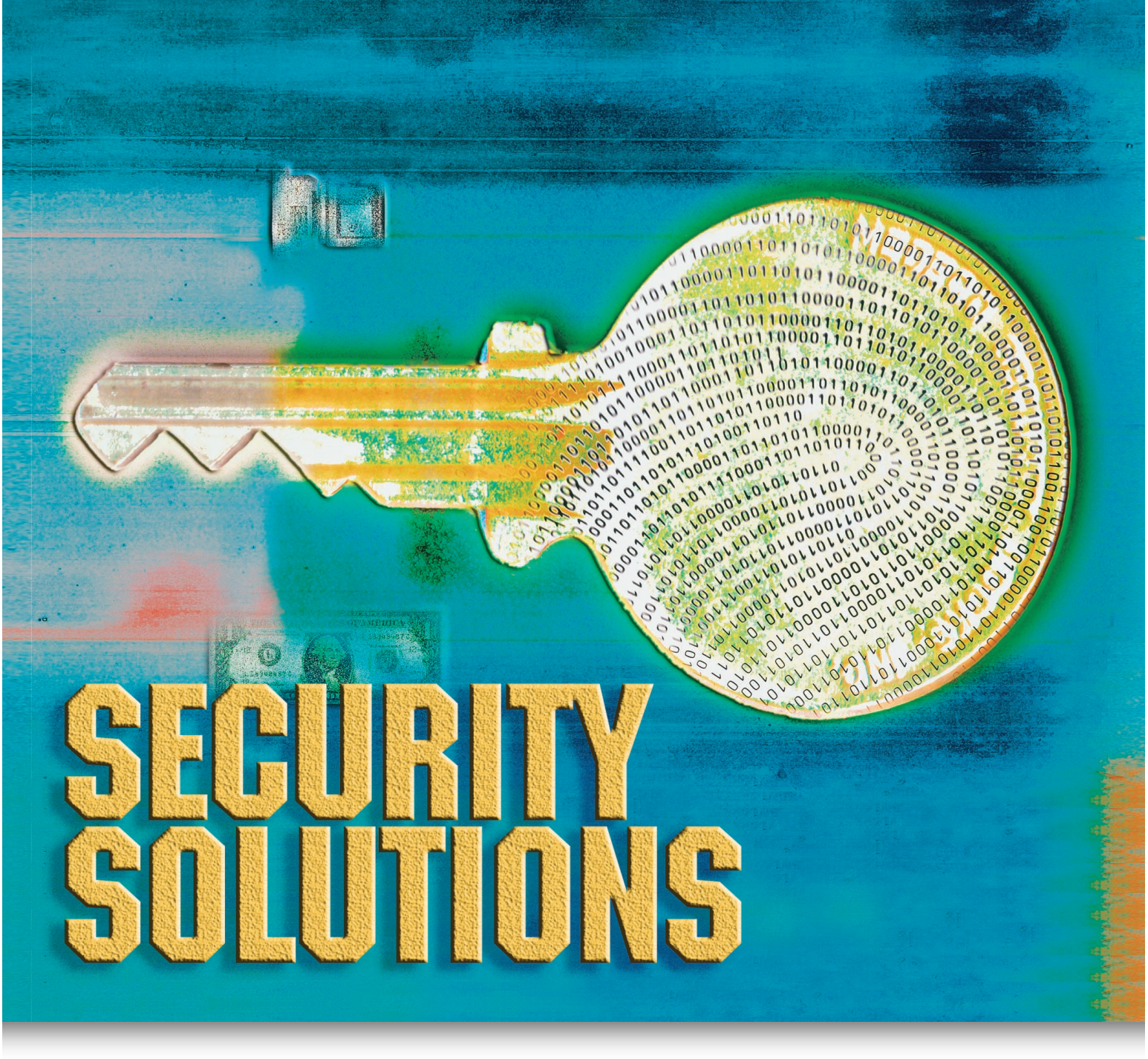

Li Gong and Ravi Sandhu

What Makes Security Technologies Relevant?

This issue of *IEEE Internet Computing* presents three articles exploring the theme of "Widely Deployed Internet Security Solutions." This topic highlights the three characteristics that we think define relevant security innovations today: deployability, orientation toward solving a problem, and suitability to the Internet environment.

DEPLOYMENT VERSUS RESEARCH

The focus on deployment reflects the frustration, shared by the majority of the computer security research community, over the glaring gap between state-of-the-art security research and state-of-the-art security practice. As a technology, computer security emerged with the development of time-sharing and multi-user systems. Security technology research remains an active academic field, attracting much interest from government, military, and commercial sectors. Despite this interest, the distance is huge between

1089-7801/00/$10.00 ©2000 IEEE

what is possible as demonstrated in research and what is practiced in the real world.

Although a tremendous amount of new research is published each year (see the sidebar "Security Research Resources" on page 41 for a list of relevant conferences, journals, and Web sites), the commercial adoption rate of this research is miserably low compared with adoption rates for other technologies, such as high-speed networking. In fact, you can count on one hand the number of innovative and effective security technologies that have been widely deployed in the past three decades:

- anti-virus software;
- onetime passwords, especially when used with a token card;
- firewalls;
- secure socket layer (SSL), which uses encryption and public-key systems; and
- Java security mechanisms (although they may be too new to be on this list).

Why such a gap exists is a mystery, and to attempt an analysis is beyond the scope of this article. Our emphasis on deployment for this special issue is a small effort toward narrowing this gap. In the end, we failed to attract articles that explain why certain security technologies are adopted while others are not—Any historians out there reading this?—but succeeded in getting articles that dissect and discover problems with a few emerging security standards.

SOLUTIONS VERSUS TECHNOLOGY

Our second focus, on solutions rather than merely technology, derives from our observation that the five technologies listed above solve some pressing problems:

- Viral attacks on DOS and Windows machines can cause serious damage, thus the need for anti-virus software.
- Passwords sent over the network have proven to be such easy targets of attack that many institutions have adopted onetime password systems.
- As more nodes were connected via the Internet, attacks on network protocols and host machine vulnerabilities also increased, and firewalls emerged as an effective countermeasure.
- In the early 1990s, when the lack of transaction security was deterring the commercial Internet's

Network Address Translators: Effects on Security Protocols and Applications in the TCP/IP Stack

Shiuh-Pyng Shieh, Fu-Shen Ho, Yu-Lun Huang, and Jia-Ning Luo

NATs implement a method for connecting a network with private IP addresses to the global Internet of unique IP addresses. NATs have been widely deployed in the past few years as a way to alleviate the shortage of address space in IPv4. Because they can hide the inside network topology from the outside world, NATs offer a level of security, but not when a protocol requires end-to-end IP addresses, as many security protocols and applications do.

Key Exchange in IPSec: Analysis of IKE

Radia Perlman and Charlie Kaufman

IPSec is a proposed standard for securing real-time communications on the Internet. It has been criticized for being overly complex, partially by allowing too many options for accomplishing essentially the same thing. Criticism has focused mainly on the part of the standard that addresses data packet encodings. The Internet Key Exchange part has its own complexities, which have not been as thoroughly studied—until now.

A Transport-Level Proxy for Secure Multimedia Streams

King P. Fung and Rocky K.C. Chang

Firewalls must offer secure traversal services to applications, but current techniques cannot meet the requirements of increasingly popular multimedia streaming applications. The authors propose an extension to the SOCKS transport-level standard proxy. The extension provides complete support for UDP-based multimedia streaming applications.

growth, Netscape introduced SSL to provide a reasonable level of security for online shopping. SSL's debut as an integral part of Netscape's browser, requiring no user administration, also drove its widespread adoption.
- Java is now used in devices ranging from cell phones, pagers, PDAs, and TVs, to desktop systems, servers, and mainframes. Enterprise applications, financial systems, and many other critical computing environments depend on Java not only for mobility and platform neutrality but also for strong security.

Inventing a security technology and turning that technology into a solution are two different things.

It is worth noting, however, that these five technologies—although they came out of commercial settings—benefited a great deal from prior research. Pattern matching, reverse engineering, fast indexing, and searching are key to anti-virus software. Cryptography in general, and one-way functions in particular, provide the foundation for onetime passwords. TCP/IP, pattern recognition, application-specific integrated circuit (ASIC) design, and virtual private networks (VPNs) underpin some modern firewalls. SSL is a fairly straightforward application of public-key systems, secure handshake protocols, and encryption. Java security traces its roots to operating system security, access-control algorithms, and object-oriented system design.

Nevertheless, inventing a security technology and turning that technology into a solution are two different things. For example, even though public-key systems existed at least as early as 1976, it was not until the early 1990s that the technology found its biggest application in SSL. Therefore, pushing for solutions instead of technologies is our way of nudging researchers to pay attention to the "last mile problem": How do we turn a great invention into an effective solution?

INTERNET VERSUS SPLENDID ISOLATION

Third, our theme focuses on the Internet—not only because the world is becoming more connected each day, but also because security issues manifest themselves more urgently in a networked environment. For example,

- Viruses, which used to travel on floppy disks (the pre-Internet with human routers), now reach us through e-mail.
- Onetime passwords eliminate the need to transport user passwords in clear text on an open network.
- Firewalls detect and prevent network-based attacks.
- SSL secures transaction information over the Internet.
- The Java security architecture provides a solid platform for Internet-based programming, including mobile code, applets, and agents.

Our concern here with today's networked environment does not imply that there are no longer security problems inside individual network nodes. In fact, in many aspects, security issues for a single node (for example, OS security, Java VM security) are technically more challenging than network security issues. However, it is more convenient—and convenience is what commercial systems look for—to assume that network nodes are controlled and trusted by their owners (which is not an unreasonable assumption in the case of cell phones and pagers) and to worry only about network-level security.

THE ARTICLES

All of the articles in this issue have the characteristics we were looking for: they focus on standards for wide deployment of security technologies. They describe practical solutions. The technologies they discuss fall within the Internet context.

The article "Network Address Translators: Effects on Security Protocols and Applications in the TCP/IP Stack," by Shiuh-Pyng Shieh et al. (pp. 42-49), studies the intrinsic conflict between the use of NATs to translate and hide network addresses and the essential requirement in some security protocols to carry and identify users' actual network addresses. The authors' conclusion that many protocols would not function properly in a NAT environment is significant, given NATs' widespread use.

The article, "Key Exchange in IPSec: Analysis of IKE," by Radia Perlman and Charlie Kaufman (pp. 50-56), identifies several problems with the IKE mechanism in IPSec, an Internet Engineering Task Force–proposed standard also included in

IPv6, and suggests several improvements.

The article, "A Transport-Level Proxy for Secure Multimedia Streams," by King P. Fung and Rocky K.C. Chang (pp. 57-67), examines the inadequacies of SOCKS, the IETF's firewall traversal standard, and proposes an extension for better multimedia streaming support.

We look forward to continued work in this area and to the day when computer security practice catches up with computer security research. ■

ACKNOWLEDGMENTS

We would like to thank all those who submitted their work, as well as the hard-working reviewers who made available their precious time to ensure the high quality of *IEEE Internet Computing* articles. We would also like to express our appreciation to *Internet Computing*'s editorial board for making this issue possible, and to the staff for ensuring smooth production.

Li Gong is a Distinguished Engineer at Sun Microsystems, and currently the Director of Engineering for peer-to-peer networking. He was Director of server products in Sun's consumer and embedded systems division, and prior to that, Chief Java Security Architect and head of JavaSoft's security and networking group. He is the founding chair of the Open Services Gateway Initiative (OSGi, http://www.osgi.org/) Java Expert Group. Gong received a BS and an MS from Tsinghua University, Beijing, China, and a PhD from the University of Cambridge, England. He is a member of *IEEE Internet Computing*'s editorial board and an associate editor of *ACM Transactions on Information and System Security.*

Ravi Sandhu is professor of information and software engineering and Director of the Laboratory for Information Security Technology (http://www.list.gmu.edu) at George Mason University. He is currently chair of ACM's Special Interest Group on Security Audit and Control (SIGSAC). Sandhu is the founding editor-in-chief of the *ACM Transactions on Information and Systems Security* (TISSEC), and a member of *IEEE Internet Computing*'s editorial board. He founded the ACM Conference on Computer and Communications Security and the ACM Symposium on Access Control Models and Technologies. Sandhu has authored more than 130 papers in research journals and conference proceedings.

Readers may contact the authors via e-mail at li.gong@sun.com and sandhu@gmu.edu.

Security Research Resources

Many conferences, journals, and Web sites publish the latest in security research. Some of these are listed below.

Conferences

ACM Conference on Computer and Communications Security • http://www.acm.org/sigsac/#CONF

ACM Symposium on Access Control Models and Technologies • http://www.acm.org/sigsac/#CONF

Annual Computer Security Applications Conference • http://www.acsac.org

European Symposium on Research in Computer Security • http://www.laas.fr/~esorics/

IEEE Symposium on Security and Privacy • http://www.ieee-security.org/

IEEE Computer Security Foundations Workshop • http://www.ieee-security.org/

IFIP Working Conference on Dependable Computing and Fault Tolerance • http://www.dependability.org/wg10.4/

Network and Distributed System Security Symposium • http://www.isoc.org/ndss01/

Usenix Security Symposium • http://www.usenix.org/events/sec2000/

Journals

ACM Transactions on Information and System Security • http://www.acm.org/tissec/

Journal of Computer Security • http://www.iospress.nl/

Internet Security Standards

Internet Engineering Task Force • http://www.ietf.org/
Links to Internet Requests for Comment and working drafts.

IETF Security Area Working Groups • http://www.ietf.org/html.charters/wg-dir.html#Security_Area

Computer Security Resource Center at the National Institute of Standards and Technology • http://csrc.nist.gov/
Links to news, policies, and U.S. federal standards (often widely used outside the U.S. federal government).

Public Key Cryptography Standards, RSA Laboratories • http://www.rsasecurity.com/rsalabs/pkcs/
Links to public-key cryptography standards documents, mailing lists, and news.