anything he or she can think of to attempt to gain access to or disrupt the target system. While this is the most realistic and useful, some clients balk at this level of testing. Clients have several reasons for this, the most common of which is that the target systems are “in production” and interference with their operation could be damaging to the organization’s interests. However, it should be pointed out to such clients that these very reasons are precisely why a

“no-holds-barred” approach should be employed. An intruder will not be playing by the client’s rules. If the systems are that important to the organization’s well-being, they should be tested as thoroughly as possible. In either case, the client should be made fully aware of the risks inherent to ethical hacker evaluations. These risks include alarmed staff and unintentional system crashes, degraded network or system performance, denial of service, and log-file size explosions.
Regular auditing, vigilant intrusion detection, good system administration practice, and computer security awareness are all essential parts of an organization’s security efforts. A single failure in any of these areas could very well expose an organization to cyber-vandalism, embarrassment, loss of revenue or mind share or worse. Any new technology has its benefits and its risks. While ethical hackers can help clients better understand their security needs, it is up to the clients to keep their guards in place.

Acknowledgments

The author would like to thank several people: the members of the Global Security Analysis Lab at IBM Research for sharing their amazing expertise and their ability to make just about anyone understand more about security; Chip Coy and Nick Simich for their trailblazing work in defining IBM’s Security Consulting Practice at the very beginning; and Paul Karger for his encyclopedic knowledge of computer security research and for his amazing ability to produce copies of every notable paper on the subject that was ever published.

**Trademark or registered trademark of the O’Reilly Group, Microsoft Corporation, eBar, Inc., TPL, or TRADEC (R)TRADE Securities, Inc., or Cable News Network, LLLP.

Cited references and notes

3. The first use of the term “ethical hackers” appears to have been in an interview with John Patrick of IBM by Gary Anthony that appeared in a June 1995 issue of ComputerWorld.
10. Who can really determine who said something first on the Internet?
12. This strategy is based on the idea of raising the security of the whole Internet by giving security software away. Thus, no one will have any excuse not to take action to improve security.
14. For a collection of previously hacked Web sites, see http://www.2600.com/hacked_pages or http://declassified.alides.de. Be forewarned, however, that some of the hacked pages may contain pornographic images.
15. In 1965, Intel co-founder Gordon Moore was preparing a speech and made a memorable observation. When he started to graph data about the growth in memory chip performance, he realized there was a striking trend. Each new chip contained roughly twice as much capacity as its predecessor, and each chip was released within 18–24 months of the previous chip. In subsequent years, the pace slowed down a bit, but data density has doubled approximately every 18 months, and this is the current definition of Moore’s Law.

Accepted for publication April 13, 2001.

Charles C. Palmer IBM Research Division, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598 (email: cchapman@us.ibm.com). Dr. Palmer manages the Network Security and Cryptography department at the IBM Thomas J. Watson Research Center. His team work in the areas of cryptography research, Internet security technologies, Java security, privacy, and the Global Security Analysis Lab (GSAL), which he cofounded in 1995. As part of the GSAL, Dr. Palmer worked with IBM Global Services to start IBM’s ethical hacking practice. He frequently speaks on the topics of computer and network security at conferences around the world. He was also an adjunct professor of computer science at Polytechnic University, Hawthorne, New York, from 1993 to 1997. He holds four patents and has several publications from his work at IBM and Polytechnic.