Crossroads
The ACM Student Magazine

Introduction

by ***William Stevenson***

In the eighth issue of *Crossroads*, published in April 1996, we explored the topic of "Computer Security." It is humorous to note that we featured an article entitled, "Computer Security Past and Future" by Michael Neuman and Diana Moore. In it, the authors concluded:

> "So what should be done next? (1) Continue work on defensive and offensive tools to secure and defend a site, (2) organize better laws and response teams to aid in the capture and prosecution of intruders, and (3) educate the entire Internet community. Every person, from the general user to the advanced applications programmer, should know what types of holes make systems or applications vulnerable to attack and the enormous liability data loss can mean to a company or individual. We hope that this issue will educate readers on the types of issues that are currently being dealt with in the field of computer security [1]."

One might say that our success at following this eight-year-old advice has been at best mixed, but progress has been made in each of the areas that the authors outlined. This issue discusses several tools for securing sites, and more generally, computer and infrastructure systems. Laws have been mixed in their successes, but the legal system historically has run at a slow and steady pace, and it is important to carefully consider the potential impact of legislation. The Internet community is, for the most part, more sophisticated than that of years past, but there are also many more novice computer users than before, and the attackers of computer systems have also grown in sophistication.

Our first article, "Computer Security and Intrusion Detection" by Khaled Labib serves as an overview of computer attacks, and discusses the notion of Intrusion Detection Systems (IDSs) — software systems that monitor the network and act when potential attacks are detected. Labib first dissects the typical computer attack, and then uses the discussion to motivate the need for IDSs. He follows by describing the algorithms used in implementing IDSs and analyzes their performance on various historical metrics.

A new concern that was not prevalent last time we explored computer security is that of wireless networking. The past few years have brought with them substantial deployment of wireless LANs, and coverage will inevitably expand even more in the coming years. Andrea Bittau "exposes" many of the security risks of wireless networks, particularly in the Wired Equivalent Privacy (WEP) protocol, in his article, "WiFi Exposed." Bittau gives an overview of the 802.11 wireless networking protocol suite and discusses how connections operate, both with and without a WEP implementation. He covers various attack scenarios, leading to the conclusion that WEP is inadequate, and concludes with advice on how to secure a network, both with infrastructure changes and with emphasis on awareness of the potential for attacks.

Next, secure commerce is discussed with a twenty-first century twist: biometric authentication. In their article "DNA Smart Card for Financial Transactions," Sofia Gleni and Panagiotis Petratos discuss the formation of a multi-dimensional authenticator based on the combination of a cryptographic smartcard and biometric information about the cardholder. The authors give a brief description of biometric data and its representation, and discuss the motivation for multi-factor authentication that employs such data. While described in the context of usage for financial transactions, biometrics can be used for things as basic as logging in to a workstation.

Finally, in their article "A Distributed Security Scheme for Ad Hoc Networks," Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia, Nirali Mody, Sugata Sanyal, and Ajith Abraham discuss the implications that limited bandwidth and power, common factors in ad hoc networks, have on the security of a wireless network. Taking these concerns into account, the authors detail modifications to the existing Ad hoc On Demand Vector

(AODV) protocol that address certain Denial of Service attacks without incurring extra overhead and give an analysis of the performance of the modified protocol. Please stop by our website at **http://www.acm.org/crossroads** for additional articles on Computer Security, and be safe!

References

1
Neuman, M., & Moore, D. "Computer Security Past and Future." *ACM Crossroads*, vol. 2, num. 4. April 1996.

Biography

William Stevenson (**billstevenson@acm.org**) is a Ph.D. student in the School of Information Sciences and Technology at the Pennsylvania State University, from which he holds a Master's degree in Computer Science. His main research interests are in Cognitive Science and High Performance Scientific Computing. In his spare time, Bill enjoys cooking, the outdoors, and playing with his new G5. He has served as Editor in Chief of *ACM Crossroads* since July 2001.