Introduction to Internet Security

Joseph G. Tront
Electrical & Computer Engineering
Virginia Tech
Blacksburg, VA USA 24061-0111
jgtront@vt.edu

Randy C. Marchany
Computing Center
Virginia Tech
Blacksburg, VA 24061
marchany@vt.edu

Viruses are running rampant. Encryption schemes have been broken. Passwords have been compromised and account information has been intercepted. Recent events throughout the world have caused people to become very circumspect when it comes to transacting business over electronic media. Will this cause the Internet to be abandoned as a vehicle for transacting business? Without the ability to trust in the scrupulous behavior on both ends of a transaction, most prudent e-commerce operators and clients may decide to forgo the use of the Internet and revert back to old methods of doing business. To counter this trend, the issues of network security on the Internet must be constantly reviewed and appropriate countermeasures devised. At the same time, security measures must be appropriately devised so that they do not inhibit or in any way dissuade the intended e-commerce operation. As the use of wireless technology grows, the number of events and the far reaching effects of network security problems are likely to have an even larger impact on e-commerce.

The security issues affecting the e-commerce of large commercial enterprises are similar to those affecting the business of universities, the government, the .coms and most others using the web. As it turns out the electronic security issues that need to be dealt with in securing the Internet are very much the same as those occurring in general physical security operations. This session will focus on the types of security problems that can occur, the solutions for known problems, and strategies for circumventing these problems in the future. These include:

- Establishing and implementing minimum-security requirements in an e-commerce environment.
- Security breach detection and recovery: mechanisms to detect when critical data has been altered and knowing when to rollback to recovery data.
- Internet security education: training network developers and engineers how to design more secure systems.
- Certification of security compliant network appliances and how this process might affect use of the Internet.
- Network performance issues related to the use of security measures.
- Ensuring confidence in network security in order to alleviate client reservations towards using e-commerce.
- System software design that incorporates appropriate security mechanisms beneficial to e-commerce.
- Establishing standardized practices for network protection.
- Secure transactions and authentication/authorization.

Attendees are challenged to interact with presenters to seek out strategies that apply to their own network environments. Discussions initiated in this venue promise to produce a continuing channel of communication between those who participate.

Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03)
0-7695-1874-5/03 $17.00 © 2002 IEEE