Internet Security: Intrusion Detection & Prevention

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

Daily commerce on the Internet consists of billions of dollars worth of transactions. Unfortunately, the Internet has become the lurking grounds for electronic n'er-do-wells who are constantly jeopardizing the processes of business. Recent network events throughout the world have caused people to become more and more hesitant to transact business over broadly connected networked 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.

Many different agencies have participated in monitoring and opposing attacks by networked intruders. Groups such as the CERT Coordination Center and SANS have attempted to aid the user community at large in defending themselves against cyber invaders. Over the years, much has changed in end-user technology, the ways that we use the Internet, techniques used by attackers, and the volume of attacks seen by users. Supporting agencies and the user community must recognize these changes and must respond in-kind with a heightened sense of awareness down to the individual user level. New responses and response procedures must be devised in order to immediately counter hostile network behavior.

In order to develop appropriate responses, the community must recognize a few things about the trends in attack strategies. First, attackers are becoming more and more sophisticated in their methods. Automated techniques are being used to both seek out vulnerabilities in code, as well as deliver and spread an attack automatically "in the wild". This means that waves of viable attacks will occur more frequently and will spread at very high speed.

The Internet is based on mutual sharing of the development and use of a major infrastructure. Security on the network is also mutually dependent – if your neighbor's machine is not protected, it is more likely to launch a devastating attack against you. Advances in attack tool development allow a single attack strain to launch multiple attacks against singular targets. Individual users have a very difficult time protecting themselves and functioning normally in this type of environment.

Although firewalls typically form a rather secure outer boundary, they too are becoming easier to penetrate. Internet Printing Protocol (IPP) is an example of a technology that is nominally unthreatening to firewalls, but with some work can be turned into a real fire(wall) hazard.

Tools and techniques used for attacks are becoming much more sophisticated. Signatures left by attacking software are becoming much more difficult to detect through either operations analysis or through signature-based detection systems. Dynamic mutation of the attacking tools compounds the problem of detection.

Finally, there is an increased threat to the infrastructure of the Internet itself. Denial of Service attacks are the common example of how assailants can deplete the infrastructure of functional capability. Worms are another example of code that consume basic infrastructure resources. Attacks on DNS systems and overt attacks on network routers are just a few more problems facing those concerned with the overall infrastructure.

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. 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.

0-7695-2056-1/04 $17.00 (C) 2004 IEEE