# Secure Computing on the Internet

Reliable Software Group
Computer Science Department
University of California
Santa Barbara, CA 93106
kemm@cs.ucsb.edu

*Prof. Richard A. Kemmerer*

## Abstract

The growth of the Internet during the past few years has been phenomenal. When it first started as the ARPAnet in 1969 there were four nodes. This increased to 23 nodes in 1971, 213 nodes in 1981, and more than 300,000 nodes in 1991. The Internet is currently serving tens of millions of people connected through millions of computers. Almost every business and government institution is connected to the Internet and the Internet is quickly becoming the primary infrastructure for exchanging information and carrying out business transactions.

As the Internet has become a major part of world-wide business, it has also become the major means for attacking hosts. The growing importance of the Internet and of network security issues has resulted in a shift of security concerns from operating system security to the security of the networks themselves.

When discussing security of the Internet there are many interesting topics to consider, including firewalls, network monitors, secure network protocols, and cryptography. Firewalls can serve as a first line of defense by controlling the information that can flow between a company's enterprise network and the external, potentially hostile, network [1]. Although firewalls are a reasonable first line of defense, they are only one part of a comprehensive defense strategy.

Network monitors are passive devices that sit on a local area network and record all or part of the information that flows on the network. They keep track of network-level security-relevant events and can be used as part of an intrusion detection system [8]. Network monitors can also be used to attack networks by eavesdropping or "sniffing" sensitive traffic containing passwords, email messages, file transfers, etc.

Using cryptography to encrypt the data flowing on a network has been successful in thwarting some sniffing attacks, as well as other attacks. However, the clear text information can often be recovered by attackers due to weaknesses in the security protocols being used. This can occur even though the encryption algorithms themselves are secure [7].

Each of these topics is interesting in its own right, and it would be possible to give an extended talk on each area. Unfortunately, the time for this presentation is limited; therefore, this talk will concentrate on what many people consider to be the most important area of Internet security and the one that needs the most immediate attention. This is the vulnerability of the World Wide Web (WWW) and approaches to making the web more secure.

Today most business and government institutions have a WWW presence and the web is fast becoming the primary source of information for people of all ages. The World Wide Web is considered to be a platform for building distributed applications on the Internet. This evolution is made possible by web browsers with processing capabilities and by programming languages like Java and JavaScript that allow web designers to embed real programs into HyperText Markup Language (HTML) documents. In particular, Java applets, which are designed to be downloaded from the web and run directly by the Java virtual machine within a browser, are increasingly being included in web pages to provide more sophisticated animation, client-server interaction, and other desirable features. Unfortunately, downloading and executing code from anywhere on the Internet brings security problems along with it. That is, the host computer is open to a variety of attacks, ranging from attacks that simply monitor the environment to export information, to attacks that change the configuration or the behavior of the host (e.g., modifying files or consuming resources), and finally to attacks that open a back door to let intruders get into the host.

Many security holes in web browsers have been discovered and brought to the attention of the public [2, 4, 5, 6]. Most of these holes have been patched; however, new holes or variations of the old ones are constantly being discovered.

Many of the attacks carried out so far require the attacker to have substantial capabilities, such as taking over a web server or a domain name server or assuming that the user will navigate only

through hyperlinks. These assumptions, therefore, often limit the likelihood of the attacks due to the low probability that the assumptions could be satisfied or because they require so much knowledge that only highly-skilled programmers could implement the attacks.

This talk describes some experimental attacks that have been carried out by the Reliable Software Group at UCSB. What sets these attacks apart from most of the others is that the attacks presented in this talk can be realized without assuming that the attacker has any capabilities beyond those granted to every user on the net and without assuming that the attackers are highly skilled programmers with complex software tools for carrying out the attacks.

Two attacks and how they were modified to contend with browser improvements that negated the original versions of the attacks will be presented. The first attack deals with the violation of privacy; it requires only that the victim downloads a honey-pot page that includes an attacker applet. The applet collects information and sends it back to the attacker's server. The second attack is as powerful as a "man-in-the-middle" attack, but it too requires only that the victim downloads a honey-pot page. The page includes an applet that can detect when the victim visits a certain site. When this happens, the applet displays an imposter page for that site in order to steal sensitive information, such as credit card numbers or personal identification numbers. The details of these attacks can be found in [3].

The web is constantly changing, and the browsers that are used for navigating the web are constantly being updated and improved. Most of the experiments described in the literature can no longer be reproduced using the latest versions of the web browsers. The main purpose of this talk is to provide a historical view of web browser security issues and to give samples of the kinds of problems that can result from either inaccurate and security-unaware designs or from poor implementations.

In order to discuss browser security issues it is necessary to summarize the browser and language features that are used. In particular, details on applet capabilities and features will be presented to establish the background for the attacks. Some previously known attacks will also be presented.

# References


[1] Brent Chapman and Elizabeth Zwicky, Building Internet Firewalls, O'Reilly & Associates, 1995.

[2] Drew Dean, Edward W. Felten, and Dan S. Wallach, "Java Security: From HotJava to Netscape and Beyond," Proceedings of the 1996 IEEE Symposium on Security and Privacy, (http://www.cs.princeton.edu/sip/pub/secure96.html).

[3] Flavio De Paoli, Andre L. Dos Santos, and Richard A. Kemmerer, "Web Browsers and Security," in Mobile Agents and Security, G. Vigna, Ed., Lecture Notes in Computer Science, vol. 1419, Springer-Verlag, June 1998.

[4] Digicrime, Online Security Experiments, Digicrime, Inc., (http://www.digicrime.com).

[5] Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach, "Web Spoofing: An Internet Con Game," Proceedings of the 20th National Information Systems Security Conference, Baltimore, MD, USA, October 6-10, 1997, (http://www.cs.princeton.edu/sip/pub/spoofing.html).

[6] D. Martin, S. Rajagopalan and A. Rubin, "Blocking Java Applets at the Firewall," Proceedings of the InternetSociety Symposium on Network and Distributed System Security, February 10-11, 1997.

[7] B. Schneier and P. Mudge, "Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)," Technical report, Counterpane Systems, June 1998.

[8] Giovanni Vigna and Richard A. Kemmerer, "NetSTAT: A Network-based Intrusion Detection Approach," Proceedings of the 14th Annual Computer Security Conference, Scottsdale, Arizona, December 1998, to appear.