Monitoring and Regulation of Private Internet Servers

Prepared for the USSS, New York Electronic Crimes Task Force
Quarterly Meeting, April 11, 2002
By: Daniel Von Kohorn

Assistant Special Agent in Charge, Robert N. Weaver, invited me to address this meeting of the New York Electronic Crimes Task Force. His presentation at last month's United Nations session on Global E-Commerce was an impressive and encouraging summary of the current state of national information security initiatives. Today, I would like to amplify Agent Weaver's report and focus on some of the realities which make it increasingly more difficult and more necessary to improve the security of private Internet servers if we are to minimize national exposure to information-based attacks.

We are aware now, more than ever, of non-traditional risks to national infrastructure, and less trusting with our exposed critical infrastructure. This infrastructure has changed substantially in the last ten years, and now includes millions of copper, fiber, and satellite doorways for both wanted and unwanted electronic guests. National and electronic security practices are evolving accordingly.

Each of the 115 million global hosts of Internet content, applications, and services controls some degree of Internet traffic and information integrity, and collectively these hosts control much of the American infrastructure and economy. Without proper administration, each host becomes susceptible to vulnerabilities, representing a potential and ever-changing risk. Whenever one entity is able to control a large number of machines simultaneously, the additive nature of these risks can become overwhelming. Meanwhile, the sophistication of security abuse has increased through the automation of infiltration techniques. Individuals who understand a tool's controls, but may have limited knowledge of the internal mechanisms, are now implementing many attacks. Some infiltration tools are designed to automatically traverse web servers, attempt break-in, and propagate to increase the hacker's control over more network servers.

Open source and commercial code is constantly being developed to improve both security and services. This innovation in information services results in a constantly evolving server security landscape. In order to deal with this problem, public and commercial services such as IRC and CERT (http://www.cert.org/faq/cert_faq.html#A2) publish known security vulnerabilities and associated patches. While beneficially educating server administrators, these boards also inform hackers. Hackers have developed very efficient methods of identifying and exploiting known vulnerabilities through web traversal engines. These engines are constantly being updated, and their speed in identifying and exploiting weakness is increasing rapidly. We should consider it a wake-up call to know that the time between public notice and hacker adoption into web traversal engines can be as little as one day. It is almost certain that some of the more sophisticated engines log system data to return to precisely the right population of servers for newly identified vulnerabilities.

There is, in effect, a race between the hackers and the network administrators every time a new security flaw is identified. When hackers win this race, they position themselves with r/w/x access to system files as well as the ability to execute high volume requests for foreign IP addresses (denial-of-service attacks). A notable example of this type of attack was the Smurf Attack on

Monday and Tuesday, February 7-8, 2000, when reachability fell to 88% and packet loss reached as high as 16%.

What is the risk we are willing to accept? What threshold of potential attack do we consider an acceptable risk? These are questions for Congress, but the country's policy-makers should know that there are tools we could use to manage these risks.

All networked systems, from PCs to e-businesses to national defense systems, are susceptible to a certain degree of attack. Critical risks exist when the threshold to a critical system is exceeded, and typically this requires a substantial level of coordination by attacking machines. The infiltration tools described earlier are the primary technique for coordinated attacks of third party servers, and represent the motivation for proactive monitoring and regulation of server administration. Server susceptibility is typically a function of server administration, meaning patches and upgrades. The timing and selection of applied patches and upgrades is critical to maintaining the integrity of server control.

Server monitoring traditionally consists of the set of practices administrators routinely follow to maintain operations. *Cyberthreat Response and Reporting Guidelines* was recently published as a joint effort of the FBI, the Secret Service, and *CIO Magazine* to specify best practices for internal cyberthreat responses. However, it is also now possible for *external* processes to aid in server monitoring and administration. The new systemic nature of vulnerability exploitation of private servers creates a need for corresponding systemic monitoring.

The tools of those who use and those who monitor the Internet are becoming increasingly sophisticated. These new tools also raise legal questions of first impression: who may monitor the Internet, and how?

My firm made some progress in designing a system to monitor external hosts, alert administrators to their vulnerabilities and fixes, and track aggregate risk thresholds for 'geographic' areas of the web. Two levels of monitoring achieve both a 'surface' evaluation as well as vulnerability testing. If this system were applied properly, noncompliance with a minimum standard of server maintenance would trigger signals of risk. Cumulative risk signals could be measured against the thresholds of various national interests, providing intelligence about the specific nature and magnitude of various types of cyberthreats. Private server administrators who repeatedly or substantially violated the established minimum standards could be alerted; in extreme cases, penalties for violation could be imposed. This model would provide an early warning system for, and substantial deterrent to, many forms of coordinated information-based attacks.

However, as a private sector organization, our ability to do anything more than manipulate and convey public information is very limited, and further, legal counsel advised us that to do so would violate a number of laws. The government, on the other hand, has the authority to set up Internet monitoring.

In *Katz v. United States*, the Supreme Court found that what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. *See* 389 U.S. 347, 351 (1967). The first level of the relevant information required for active monitoring is knowingly exposed to the public. Therefore, the collection of such information by government officials does not violate the Fourth Amendment. After the collection and analysis of this information, most servers will not require anything other than periodic re-visitation. However, other servers will exhibit meaningful risk characteristics.

The documentation of certain risk characteristics could be construed as evidence of criminal negligence if it could be shown that administrators knew, or should have known, that their lack of administration exposed their servers to computer fraud.[1] When this is established, a second level of monitoring could be initiated that is more informative.

This second level of monitoring would enable specific security vulnerabilities to be tested, and specific fixes to be prescribed. Automation of the monitoring tools would mirror in many ways the automated exploit tools of the hackers, however, the procedure would include prescribing of a combination of solutions rather than exploitation. Finally, non-compliance with minimum standards would represent criminal negligence.

While these findings are a basis for Internet monitoring by the government, they do not provide adequate grounds for effective private monitoring. One alternative we considered would be to make the monitoring service a subscription, where server administrators would authorize our firm's activity. However, this would only be effective for the administrators who are proactive about their security management, and sidesteps the real problem of negligent administrators who unwittingly enable hackers to use their servers for attacking third parties.

Within the next few years, it will become necessary to monitor and regulate a minimum standard of server administration. This monitoring and regulation will need to be implemented by a government agency. In practice, proactive monitoring of Internet servers can offer an early warning system, but also represents a means to enforce compliance with security standards. This combination of results would provide important new national security intelligence and reduce the frequency and magnitude of systematic unauthorized access to network servers, including large-scale information-based attacks.

That concludes my prepared statement, and I would be happy to answer any questions you may have either here or via e-mail.

Thank you all very much

Daniel A. Von Kohorn
Chief Technical Officer
Technology Partners (Holdings) LLC
570 Lexington Ave
New York, NY 10022
Phone: 212-759-3022
Fax: 212-759-9184
E-mail: dan@vonkohorn.com
http://tphllc.com

---

[1] The Computer Fraud and Abuse Act, originally enacted in 1984, sets forth conduct constituting fraud and related activity in connection with computers. *See* 18 U.S.C.A. §1030. This statute is meant to be expansive. As stated in the Senate Report of 1996, S. Rep. 104-357, "Congress must remain vigilant to ensure that the Computer Fraud and Abuse statute is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime."