MIT software aims to thwart cyber hackers

August 28 2008

(PhysOrg.com) -- In response to the chronic cyber threat of hackers, MIT Lincoln Laboratory researchers are developing a software tool to identify the most vulnerable points in a computer network. The tool aims to make it possible for system administrators to focus on parts of a network that are most prone to attack, instead of securing all parts of the network.

U.S. government and defense computer networks are attacked all the time, says Richard Lippmann, leader of the work and a senior staff member in Lincoln's Information Systems Technology Group. In an attack known as Titan Rain, between 2003 and 2005 a series of breaches of U.S. government computers may have captured sensitive information about military readiness.

NetSPA (for Network Security Planning Architecture) uses information about networks and the individual machines and programs running on them to create a graph that shows how hackers could infiltrate them. System administrators can examine visualizations of the graph themselves to decide what action to take, but NetSPA also analyzes the graph and offers recommendations about how to quickly fix the most important weaknesses.

NetSPA relies on vulnerability scanners to identify known weaknesses in network-accessible programs that might allow an unauthorized person access to a machine. But simply being aware of vulnerabilities is not sufficient; NetSPA also has to analyze complex firewall and router rules to determine which vulnerabilities can actually be reached and exploited

by attackers and how attackers can spread through a network by jumping from one vulnerable host to another.

"It's a matter of what the attacker can get to and in what order," says Kyle Ingols, a computer scientist in Lippmann's group who is working on NetSPA, along with Seth Webster (who is focusing on ways to make the system more automated) and MIT graduate student Leevar Williams (whose master's thesis is on visualizing attack graph data). It takes a long time to patch all hosts in a network. "If you spend time patching vulnerabilities the attacker can't get to first," Ingols says, "you've left your network exposed longer."

NetSPA aims to solve that problem. "Instead of patching or fixing or blocking a thousand hosts," Lippmann explains, "we could say there are 10 critical hosts and patch those first."

This insight sounds obvious, but applying it to real systems can be a huge challenge. A network comprised of thousands of computers may have dozens of filtering devices such as firewalls and routers, and each device may have 200 or more different filtering rules. The multitudinous combinations of possibilities are far too many to track down by hand, and are even very complex for a computer algorithm to compute. The original version of NetSPA, in fact, could handle networks of only about 17 machines before the modeling complexities made it too slow to be useful.

Since then, however, the Lincoln Laboratory researchers have developed ways to speed NetSPA up. For instance, firewalls may have rules that treat a number of different machines on the same network in the same way. Rather than modeling each of those machines individually, the software uses the same model for all of them, saving significant computing time. The researchers have also developed new types of attack graphs and efficient algorithms to compute these graphs.

NetSPA also has the potential to discover unforeseen avenues of attack. For example, a network might have had to share data with an outside vendor several years ago, so the system administrator added a rule to allow access from that vendor's IP address. Someone forging that address could exploit that long-forgotten permission.

The researchers have received one patent for NetSPA, and have another pending. They're currently testing the tool on different networks, and developing ways to make it easier to use.

Already the software has garnered some attention. In May, a group of MIT students won $10,000 in the MIT $100K Entrepreneurship Competition for creating a business plan for a proposed company, CyberAnalytix, that could commercialize NetSPA (Lippmann and Ingols are technical advisers).

Provided by MIT