Researchers create next-generation software to identify complex cyber network attacks

March 17 2008

Researchers in George Mason University's Center for Secure Information Systems have developed new software that can reduce the impact of cyber attacks by identifying the possible vulnerability paths through an organization's networks.

By their very nature networks are highly interdependent and each machine's overall susceptibility to attack depends on the vulnerabilities of the other machines in the network. Attackers can take advantage of multiple vulnerabilities in unexpected ways, allowing them to incrementally penetrate a network and compromise critical systems. In order to protect an organization's networks, it is necessary to understand not only individual system vulnerabilities, but also their interdependencies.

"Currently, network administrators must rely on labor-intensive processes for tracking network configurations and vulnerabilities, which requires a great deal of expertise and is error prone because of the complexity, volume and frequent changes in security data and network configurations," says Sushil Jajodia, university professor and director of the Center for Secure Information Systems. "This new software is an automated tool that can analyze and visualize vulnerabilities and attack paths, encouraging 'what-if analysis'."

The software developed at Mason, CAULDRON, allows for the transformation of raw security data into roadmaps that allow users to proactively prepare for attacks, manage vulnerability risks and have realtime situational awareness. CAULDRON provides informed risk analysis, analyzes vulnerability dependencies and shows all possible attack paths into a network. In this way, it accounts for sophisticated attack strategies that may penetrate an organization's layered defenses.

CAULDRON's intelligent analysis engine reasons through attack dependencies, producing a map of all vulnerability paths that are then organized as an attack graph that conveys the impact of combined vulnerabilities on overall security. To manage attack graph complexity, CAULDRON includes hierarchical graph visualizations with high-level overviews and detail drilldown, allowing users to navigate into a selected part of the big picture to get more information.

"One example of this software in use is at the Federal Aviation Administration. They recently installed CAULDRON in their Cyber Security Incident Response Center and it is helping them prioritize security problems, reveal unseen attack paths and protect across large numbers of attack paths," says Jajodia. "While currently being used by the FAA and defense community, the software is applicable in almost any industry or organization with a network and resources they want to keep protected, such as banking or education."

Source: George Mason University

Citation: Researchers create next-generation software to identify complex cyber network attacks (2008, March 17) retrieved 25 April 2024 from https://phys.org/news/2008-03-next-generation-software-complex-cyber-network.html