PHYS.ORG

Protecting networks is just a game

July 27 2011

How can an organization detect the onset of an attack on its computer network giving it time to respond quickly and block any intrusion or compromise of its data? Modern firewalls and other technology are already in place, but these have not prevented major attacks on prominent networks in recent months. Now, information technologist Heechang Shin of Iona College in New Rochelle, NY, has used game theory to develop a defense mechanism for networks that is more effective than previous approaches.

Writing in the *International Journal of Business Continuity and Risk Management*, Shin explains that with the tremendous growth in numbers of computing and other devices connected to networks, information systems security has become an issue of serious global concern. He points out that each incident might not only cause significant disruption to services affecting many thousands of people but for a commercial operation can take as much as 1 percent of annual sales, per incident. That number amounts to tens of millions of dollars for the average publicly listed company, Shin says.

Shin has now developed an effective anti-hacking tool based on a game theoretic model, called defensive forecasting, which can detect network intrusions in real time. The tool, by playing a "game" of reality versus forecast, wins when reality matches its forecast and it sends out an alert to block the intrusion.

Importantly, the tool works on real-time data flowing in and out of the network rather than analyzing logs, an approach that can only detect network intrusions after they have taken place. The game theoretic model continuously trains the tool so that it can recognize the patterns of typical network attacks: denial of service attacks, such as a syn flood, unauthorized access from remote machines in which login passwords are being guessed or brute-force tested, attacks by insiders with "superuser" or system root privileges or probing attacks in which software carries out surveillance or port scanning to find a way into the system.

In order to measure the effectiveness of the tool, Shin compared the approach using the semi-synthetic dataset generated from raw TCP/IP dump data by simulating a typical US Air Force LAN to a network intrusion system based on a support vector machine (SVM), which is considered one of the best classification methods for network intrusion detection. Experimental results show that the tool is as good as or better than the one based on SVM for detecting network intrusion while the tool adds the benefit of real-time detection.

More information: "Identifying network intrusion with defensive forecasting" in Int. J. Business Continuity and Risk Management, 2011, 2, 91-104

Provided by Inderscience Publishers

Citation: Protecting networks is just a game (2011, July 27) retrieved 8 August 2024 from https://phys.org/news/2011-07-networks-game.html