December 11, 2001

The Lego Approach to Counter Cyber-Terrorism:

Researchers Release Computer Intrusion Detection System With Configurable Components

Santa Barbara, Calif.--A team of UCSB computer science professors have created and released a comprehensive computer intrusion detection system--a powerful tool to counter cyber-terrorism.

We are all familiar with cyber assaults caused by infectious agents such as worms, viruses and the flooding that leads to denial of service. Worms, such as the recent Code Red, are self-contained infectious agents, while viruses attach to another program. Denial of service attacks, like those on CNN among others in February 2000, flood servers with spurious service demands leading to denial of requests by legitimate users.

So far, the worms, viruses, and denial of service attacks that have made headlines have been solo missions devised by hackers to create mischief.

But cyber security issues have become national security issues because of the pervasive use of computer and network technology, fundamentally affecting for instance:

control of air traffic;
operation of the power grid;
disposition of goods including inventory maintenance and parts order and delivery, pertaining especially to the vast array of military hardware;
command, control, and coordination of a host of defense units from missiles, to individual ground troops, to planes, to a fleet of ships.
Imagine a coordinated cyber attack on more than one of the above, launched not just by a person or two, but by a team. The US Department of Defense has. It awarded the trio of UCSB computer scientists--Richard Kemmerer, Giovanni Vigna, and Kevin Almeroth--$4.3 million last February to proceed with development of their computer security system.

A first prototype of the system is now available free of charge at http://www.cs.ucsb.edu/~rsg/STAT. (Vigna cautions would-be downloaders that what's there is a university prototype, not a "polished" commercial software package).

The security system is an intrusion detection application package with a core technology and various adaptations to specific uses in the form of intrusion detection sensors. And most significantly the system provides for communication between individual sensors and to a central monitor--enabling detection of and response to a pattern of attacks aimed at different targets.

"Today," said Vigna, "if the system administrator at UCSB notices a problem, he picks up the phone and calls

the system administrator in San Diego and says, 'Hey, are you seeing this stuff?' Much of the interaction and response to intrusion is based on human ad hoc interaction." What's key to national security is a centralized reporting of and response to locally detected intrusions, so that an overall pattern of attack can immediately be detected.

For surveillance against an intruder targeting a single computer or terminal, there is the basic sensor USTAT, which stands for "Unix-based State Transition Analysis Tool." Further adaptations include NetSTAT for local area networks and WinSTAT for Windows-based operating systems. Another adaptation (AlertSTAT) adds alert correlation capability, which aggregates individual alerts to provide the overall pattern of intrusion. MetaSTAT enables centralized monitoring and control of a web of sensors. Through MetaSTAT it is possible to reconfigure remotely the intrusion detection sensors.

Kemmerer gives an example that shows the latter's importance. "As soon as we ascertain we have a new worm attacking, we can tell all the individual sensors what it looks like.

"Overall, this computer security system is general," said Kemmerer, "and that is its real value. We can identify a new attack, express in our language what it looks like, and generate code that will detect the attack, and then load that into systems without bringing them down. That is important. Often times when a new attack is identified, and one generates a signature for it, it is necessary to bring down the systems and completely reinstall them in order to incorporate identification of that signature into the security analysis."

Vigna calls it "the Lego approach to intrusion detection." "We provide the components that can be configured any way you want," he said. "Other systems are monolithic. One great virtue of ours is its flexibility."

Kemmerer, who has worked on computer security for over 25 years, began focusing on intrusion detection around 1990. He devised the essential detection sensor in the early '90s. Vigna joined him four years ago and got the idea for the Lego approach. Instead of building the core technology into each application, they have built a stand-alone core and the individual components. They have just released the core and the components this fall.

Kemmerer describes two kinds of intrusion detection: one is anomaly detection and the other misuse detection.

The anomaly approach builds up a history of normal use patterns and constructs usage profiles for a given user or job category, say, a bank teller who does specific things in a specific sequence. Deviations from the profile then raise an alarm. There are two main problems with this approach: (1) high probability of false alarms, which in turn undermine human attention and therefore effectiveness, and (2) inapplicability to unpredictable users, such as university professors.

Misuse detection looks for a profile of known possible attacks. The problem is that new attacks have not yet been profiled.

The idea behind their core technology, according to Kemmerer, "is to abstract out a pattern from the various

kinds of attacks." The patterning raises the probability of detecting a new attack because of its resemblance to the abstracted categories of previous attacks.

The STAT intrusion detection system looks in real time at every packet of information received by a computer or system. In other words, it's not just 10 percent of the bags that are being sampled, but every one.

Almeroth, the third co-principal investigator on the recently funded Hi-DRA High-speed, Wide-area Network Detection, Response, and Analysis $4.3 million grant from the Army Research Laboratory (as part of the Department of Defense University Research Initiative [URI] program) has recently joined the team as an "in-the-network" expert. This will allow the team to expand its focus to network centric attacks, such as those on routers.

Previous releases of the STAT system have been deployed by the U.S. Navy and Air Force and by some corporations.

Note:Professor Kemmerer can be reached at 805-893-4232 and kemm@cs.ucsb.edu; Professor Vigna at 805-893-7565 and vigna@cs.ucsb.edu; and Professor Almeroth at almeroth@cs.ucsb.edu

Images

Media Contact

Tony Rairden
trairden@engineering.ucsb.edu
805.893.4301