The phony goat gets the worm

March 28 2006

IBM researchers have designed a new way to detect and thwart attacks on computer networks. Code named "Billy Goat," the intrusion detection tool provides both early detection of worm attacks and fewer false alarms than other sensor systems.

The tool masquerades as a collection of servers on a network. Actual servers do not communicate with Billy Goat, but criminals who randomly attack servers are likely to stumble over it. As soon as Billy Goat is attacked, it identifies the attacking systems and fences them off electronically, isolating worms and viruses before they can propagate.

"Billy Goat uses a unique approach to detect malicious software by responding to requests sent to unused IP addresses, presenting what from a worm's-eye view looks like a network full of machines and services," says Dr. James Riordan, the lead designer of the system at IBM's Zurich Research Lab.

"In other words, Billy Goat creates a virtual environment for the worms. Such virtualization, by providing feigned services as well as recording connection attempts, helps Billy Goat trick worms into revealing their identity. This method allows the system to reliably and quickly identify worm-infected machines in a network."

Source: IBM