Anna Sperotto

Intrusion detection systems protect our networks against misuse. The networks are becoming increasingly faster, however, making the current generation of detection systems ineffective. For high-speed networks, Anna Sperotto introduces a new approach.

Intrusion detection systems at high speeds

"You find the Internet and computer networks everywhere these days. More and more data travels by electronic highway, and more and more information is stored electronically. An interesting situation for the bad guys. It means that misuse of networks happens a lot more than you think."

"Naturally, before you can take any action against network misuse, you have to know when it's occurring. This is why the end of the eighties saw the development of intrusion detection systems. These are computer-based systems that detect unauthorized access to information systems and networks. For example, spam mail, worm virus attacks, or programs that generate so much traffic they bring a system to its knees."

"To determine whether there is misuse of a network, the intrusion detection system scans the data flows entering and leaving the network. Each data flow consists of small packets of data. The detection system makes a copy of each packet and subjects it to a thorough check. If the system finds anything wrong, it notifies the network manager, who can then take action."

"This works fine for most existing networks, but networks keep getting faster. With high-speed networks, copying and checking data packets is slower than the normal throughput speed of the network. This means that, with these networks, you can't check all the data moving in and out. So we have to find a new approach."

"That's why I'm working on the development of an intrusion detection system for these faster networks. We're talking about speeds of between 1 and 10 gigabits a second. Although such speeds are still mainly achieved in Internet backbones, they're to be found in an ever-greater number of computer networks. Take the link between the University of Twente and the Internet for example."

"Because high speed networks don't allow the individual checking of data packets, I have to find a new method for collecting information from a data stream. I'm therefore using an inventory of the information in a complete stream. This inventory is referred to as a 'flow'. The information at my disposal is the duration of the communication, the number of data packets transmitted, the size of the data packets in bytes, the sender and the receiver."

"The best way to think of my approach is that of someone who has to check a long letter in a very short space of time. You need to imagine that each word is one data packet. As there's not enough time to read each word, you have to make an inventory of some sort. Based on the number of words, the length of each word, the names of the sender and receiver, and time of sending, you have to decide whether it's a personal letter or, say, a piece of junk mail."

"If you check a complete data stream this way, you obtain no information about the content. You're only examining patterns. Using statistical techniques, I look for deviations in these patterns. Supposing someone scans your network, with the intention of misusing it. This person contacts all the devices in the network in a short interval of time. What you observe is an increase in the number of flows during that interval. This is the kind of deviation from the norm that I detect with the aid of statistics. We've already demonstrated that this method can be used to detect spam mail."

'With high-speed networks, copying and checking data packets is slower than the normal throughput speed of the network.'

"The most difficult part of developing an intrusion detection system is to decide how sensitive to make it. You don't want the system to think there's attack when there isn't one, or report problems that aren't there. But what you don't want above all is for misuse to go undetected."

"I'm working mainly on the detection side of the problem. As soon as there's evidence of misuse, a message is sent to the system manager, who can then take appropriate action. The next stage is to ensure that the system takes action automatically as soon as there's an intrusion."