Improving network firewalls

April 16 2010

A firewall is the safety barrier between a computer network and the outside world. Individuals, companies and large organizations alike rely on a firewall being robust enough to fend off hackers attempting to break into a computer system. However, managing the firewall rules that decide between online friend and foe has proved to be complex, error-prone, expensive, and inefficient for many large-networked organizations, according to a research team writing in the *International Journal of Internet Protocol Technology*.

Muhammad Abedin of the University of Texas at Dallas and colleagues explain that just one error in the set of rules controlling a firewall can open up a critical vulnerability in the system. Such security problem can allow intruders to access data and programs to which they would otherwise be barred potentially leading to breaches of privacy, industrial sabotage, fraud, and theft. The researchers have now developed a method for analyzing the activity log files of corporate firewalls. Their analysis can determine what rules the firewall is actually applying to incoming and outgoing network traffic and then compare these with the original rules to spot errors and omissions.

Since the advent of the internet, firewall technology has rapidly gone through several generations of innovation and research in a short period of time, and has delivered many powerful and cost-effective services. However, no firewall is perfect and there is always the possibility of human error or computer bugs that can inadvertently open routes allowing malicious users to access off-limits systems or network components.

Previous researchers have developed analyses of firewall rule sets in an effort to discover potential security problems. However, these static approaches ignore the Firewall log files which change constantly but can provide a rich source of data on network traffic. Analysis, or traffic mining, of log files could potentially offer a much more rigorous way to assess the protection a Firewall is providing.

"By comparing the extracted rules with the original rules, we can easily find if there is any anomaly in the original rules, and if there is any defect in the implementation," the researchers explain. "Our experiments show that the effective firewall rules can be regenerated to a high degree of accuracy from just a small amount of data."

The approach also has the advantage of detecting anomalies that lead to omissions in the logs themselves, as such "shadowed" entries are revealed as gaps when the extracted rules are compared to the original rules.

More information: "Analysis of firewall policy rules using traffic mining techniques" in *International Journal of Internet Protocol Technology*, 2010, 5, 3-22

Provided by Inderscience Publishers