

Security Prediction: Faster Networks will be Favorable for Host-Based Intrusion Detection Systems

By Gene Kim, Chief Technology Officer, Tripwire Security Systems Inc.

We are a networked world in the process of becoming even more networked. Businesses are finding ways to use the Internet to save money and time, and to improve communications with partners, customers, and subsidiaries around the world. At the same time, consumers are using the Internet to do banking, buy groceries, and plan vacations.

Imagine these networks as roads that carry speeding data. As more motorists hit the roads, the risk of an “incident”, such as being hacked, increases. Generally, the Internet’s benefits outweigh its hazards, but its worth noting that the risks related to information security are increasing.

The factors increasing risk include: faster networks; sophisticated attacks; an increasing number of servers around the world, all carrying heavier loads; the need for 100% system uptime and availability; and, a lack of system administrators to keep it all working smoothly. All of these conspire to make intrusion detection and information security more challenging in the future – and more important than ever. In order to understand how all of these factors interact and impact security, let’s take a look at each one.

Faster Networks

Maintaining a secure network is becoming more challenging by the minute. Bandwidth is expanding as organizations struggle to keep up with requirements for greater throughput, and the exploding constellation of e-commerce activity is straining networks to capacity. Meanwhile, vendors continue to innovate and end-users continue to invest in hardware and software to expand their network capabilities.

This explosion in technology and capacity creates a challenge for some current security technologies, such as network-based intrusion detection systems (NIDS). NIDS sniff the traffic on a network looking for strange requests, called attack signatures. Attack signatures are patterns common to attacks or specific to a cracking attempt.

However, as networks grow faster, NIDS are unable to keep up with the deluge of network traffic. In addition, many networks are using routing switches that prevent NIDS from being able to scan all traffic from a single location. This presents challenges for system administrators trying to construct a centralized NIDS box to keep track of critical network choke points. So to function at all, the NIDS must either decrease the number of signatures its scans for or scan selectively. Neither of which meets the needs for comprehensive, reliable security.

Sophisticated attacks

NIDS and virus software look for attack signatures, and this is a strategy that will work some of the time. If someone tries a well-known exploit on your network or sends a known virus, chances are that it will be caught. After all, the attack signature and virus detection approach rely on the ability to know about a certain type of attack *before* it happens -- in other words, the technology must know the attack or virus in order to detect it.

What happens if a new attack or a new virus is used? The real-time tools will fail.

Both a NIDS and virus software are essential components of well-planned security because they guard against the known, including the entire class of “script kiddie” exploits readily available on Internet sites. The trouble is that new exploits and new vulnerabilities are discovered everyday by attackers whose motives are unknown. Tools that protect your systems against the new, as well as the old, are essential.

Need for integrity and availability

In the last year, we have seen unprecedented media coverage of high profile failures at e-commerce sites, such as unavailability for hours at a time. We have seen scores of government web sites defaced, some politically motivated, and others with motives less obvious. These represent failures of integrity and availability. When e-commerce sites or other infrastructure reliant upon computer networks go down (telecommunications, aviation), it is embarrassing and inconvenient. But more important, these outages have an immediate effect on stock price, reputation, and future earnings potential.

The realizations that e-commerce sites must be available at all times and that networks must be fail-proof are escalating security from an IT-only concern to a management problem. Maintaining the integrity and availability of web servers and networks are bottom-line issues for company executives, shareholders and business partners. Executives want to know that risk is being managed in a cost-effective, comprehensive manner utilizing the best options available, and partners and shareholders want to know that its safe to do business with an organization.

Shortage of System Administrators

Often, the scarcest resource within an organization is not money or technology, but capable people. Larger and faster networks, with high needs for integrity and availability, in an increasingly hostile environment call for more system administrators. This staffing challenge affects small and mid-size companies in particular.

Military parlance portrays this situation best. The “defenders” of corporate networks are outnumbered 1000:1 by “attackers”. Classically, the playing field is leveled by technology. But what happens when there are not enough troops to run the newest weapons? Clearly, either more troops must be found or new technologies deployed that require less administrative support.

The state of intrusion detection today

Our quick examination has revealed a seemingly tough situation for network security in the future. But with a combination of the right tools and actions, including a well-defined security policy, a well-configured firewall, a vulnerability scanner and an intrusion detection system (IDS), there is a pleasant ending.

There are two main categories of IDS — network-based and host-based — and together they are a formidable team. The value of a NIDS is that it functions in real-time. The strength of a host-based IDS is that it takes a digital snapshot of a machine in a known, clean state using File Integrity Assessment (FIA) technology. With an FIA tool, an administrator can quickly compare baseline data to current files to identify any changes, additions or deletions. A host-based tool also enables you to determine the scope of damage and what you need to do to bring your servers back up and running.

In addition, the host-based FIA tool is the only way to determine exactly what data has been disrupted, no matter what the cause. It can discover alterations in replaced binaries and detect the addition of rootkits, sniffers, and other backdoors left behind after an initial reconnaissance intrusion. This is an effective approach because most intrusions occur over time with hackers taking possession of perimeter machines first—leaving rootkits and sniffers—then using these devices to penetrate deeper into the network during subsequent attacks.

And revisiting the personnel issue, a host-based tool also provides a “force multiplier” – once you have an inventory of damage and a baseline to work from, all available system administrators can contribute to the recovery effort.

What the future holds

The future of intrusion-detection and information security points to the development of more flexible technologies that work together to protect the multiple parts of a network. Security entails more than just one part of a network, with each part only as strong as the weakest link – a strong reason why end-users want the best tool for each function and seem to prefer best-of-breed solutions.

Moving forward, organizations that build a multi-layered defense and maximize the time of available system administrators will meet the challenges of an increasingly difficult security environment. After all, being able to confidently answer the question, “Is my server the same this morning as it was last night?” is the key to maintaining integrity and availability in a digital world.

Gene Kim is co-founder and CTO of Tripwire® Security Systems (TSS) in Portland, Oregon. He has a strong engineering and development background in networking and computer security. With Dr. Eugene Spafford, he developed the Tripwire intrusion detection software product in 1992 while at Purdue University's COAST Laboratory. At TSS, he leads the development effort for the Tripwire family of computer security products. Mr. Kim is widely published on computer security, operating systems, and networking in Usenet, ACM, and IEEE publications.