

## The Economics of Information Warfare - Poking Layered Security with a Stick By Mark Wells and Woody Thrower

War is in large measure won or lost based on economic power. Information warfare is no different.

No security system is impenetrable. The ideal information security system causes the cost of an attack to exceed the benefit. A multi-layer security system significantly increases the resources required to compromise the organization. Industry best practices focus on the concept of security in-depth. Layered security creates a defensive barrier that is many times greater than the sum of the individual parts, and exponentially increases the cost to the attacker, therefore increasing the security of the organization.

Stick, an "IDS stress" tool, overwhelms network IDS by simulating a large number of attacks without actually performing them. It was built by reverse-engineering the attack signatures used by Snort (an Open Source network IDS) to generate network traffic that triggers those signatures. Since all network intrusion detection systems operate similarly, Stick can flood any network IDS with false-positives. In some cases, it can even completely disable the IDS.

Stick demonstrates the danger of security based on only one defense mechanism, in this case – the network intrusion detection system. The medieval equivalent of Stick is storming a castle with dancing minstrels carrying wooden swords. They make a lot of noise, and look like attackers at first glance, but are only a distraction.

The recent extortion of E-Commerce companies indicates that many organizations do not apply security indepth. This may then result in the loss of information that is worth significantly more than the attacker's cost in obtaining it.

A fundamental inequality of information war is that an attacker with limited expertise, time, and a free dialup Internet connection can cause an organization to lose millions of dollars, its reputation, and ability to conduct business. Organizations must increase the cost of attacks far beyond this point.

Network IDS acts as an early warning system, much like a guard in a watchtower. Properly functioning IDS can help identify points of attack, harden other defenses, and gather forensic data. If minstrels distract the tower guards, other security systems must still be in place. For example, the distraction is pointless if the real attackers still can't get across the mote (or firewall).

Firewalls, vulnerability assessment, and anti-virus software are still effective even when the network IDS fails. A properly configured firewall can block most unsophisticated attacks before a network IDS even sees it. Vulnerability assessment can identify weaknesses and help to eliminate them. Without weaknesses, real attacks fail even if they are not detected. Anti-virus software still detects Trojan horses and viruses even if IDS does not detect delivery, vulnerability assessment does not prevent it, and firewall doesn't block it.

A security measure like a firewall, IDS, vulnerability assessment, or anti-virus, when used alone, is not as effective as when those measures are used together as part of an in-depth security solution. Consequently, security measures used piecemeal, make it easier for an attacker to be successful because it lowers his total cost. A comprehensive security solution incorporating a firewall, network and host intrusion detection, vulnerability assessment, and anti-virus, create a security solution that is expensive for an attacker to defeat.