VANTAGE POINT

Baroudi Group

March 2002

Keep e-commerce secure by disconnecting your servers from the Internet

Eric Livingston, Lead Analyst, Security

While it sounds strange, disconnecting your e-commerce servers from the Internet is exactly what SpearHead Security Technologies would have you do - using their NetGAP line of security products. NetGAP technology allows communication to continue while creating an un-crossable physical gap between the Internet and an organization's internal network.

SpearHead's CEO, Buky Carmeli, developed GAP technology after recognizing that a very large proportion of internet attacks are carried out through deliberately malformed or misused network protocols. Examples include Teardrop attacks, WinNuke, Smurf attacks, DNS spoofing, SYN floods, and the infamous “Ping of Death”. In these cases, attackers alter or use protocols in unintended and unforeseen ways, to damaging effect.

These attacks are effective because prior to their introduction, network devices such as firewalls and servers are not expecting them and have no defense against them. It's only after patches are released that most devices become immune to them, and the interim between the introduction of an attack and the deployment of its corresponding OS or firewall patch can be a very vulnerable time for susceptible organizations.

NetGAP technology is inherently immune from all the above attacks, and from innumerable attacks of this form to come. Essentially, NetGAP “unwraps” TCP/IP traffic, separating the data from the protocol information, then “re-wraps” the data up in a new, independent TCP/IP protocol for travel on the LAN. Packets from the Internet never actually make it to the internal LAN - they are stopped and stripped down inside the NetGAP device, which sits physically between the LAN and the Internet.

A NetGAP device is an approximately router-sized piece of hardware that accepts two Ethernet connections: one to the Internet, and one to the LAN. Inside the device are two independent computers (a Trusted CPU and an Untrusted CPU) that share no hardware between them aside from SpearHead's dual-window memory region to which both CPUs have access, but never simultaneously. The Untrusted CPU is directly connected to the Internet, and is responsible for brokering TCP/IP traffic with clients, while the Trusted CPU manages connections with internal systems. The two CPUs share information by reading and writing data to the shared memory regions inside the device, at up to 120Mbps.

The Untrusted CPU (the internet-side) is protocol-aware, able to decipher and do stateful inspection of HTTP, HTTPS, FTP, SMTP, DNS, and POP3. (This is extensible, with IMAP and SQL on the way, and can be bypassed using simple port-forwarding rules for unrecognized protocols.) The Untrusted CPU can also decrypt and examine SSL-encrypted data, if desired, using on-board hardware by Rainbow Technologies. The CPU denies traffic it doesn't recognize and traffic that does not adhere to RFC specifications. Shenanigans related to such things as malformed packets, malformed protocol headers, and fragmentation, are stopped in their tracks by this CPU, which strips all TCP/IP protocol information out of the packets, ensures RFC integrity of the data portion of the traffic, digitally signs the payload data with a 1024-bit key, and places it in the shared memory region for pickup by the trusted CPU.

The Trusted CPU authenticates the data it picks up from the shared memory region using the digital signature (to prevent a cracked Untrusted CPU from passing along bogus data). It then creates a new TCP/IP connection with the appropriate internal target system, and places the validated payload data into the stream. Originally encrypted SSL data from the Internet can be re-encrypted at this time for internal security or left unencrypted in a secure internal LAN environment.

The Trusted CPU can also perform RADIUS and LDAP based authentication and authorization of users, ensuring that only valid connections are created on the internal LAN. Importantly, this security check occurs on the Trusted side of the NetGAP device, which is not physically accessible from the Untrusted side, ensuring immunity from cracking attempts originating from the Internet.

NetGAP technology ensures that unknown future protocol-based attacks can never impact protected systems. Any malformed or misused protocol information at the TCP/IP or application level (such as FTP, HTTP, etc) is simply thrown out by the NetGAP device, and is not forwarded onto the internal LAN. This is inherently more robust than a firewall, which forwards packets as-is. If a firewall does not detect a future malformed-packet attack, that packet will be forwarded as-is to internal systems that might succumb to the attack. The NetGAP device, however, does not forward packets - it actually strips the payload data out of the packet stream, passes the data over a “wall”, and re-wraps it in an entirely new data stream, thus ensuring that all data is passed to the internal LAN in perfectly formed packets every time.

In addition to this iron-clad protocol-level protection, the NetGAP device also has a built-in firewall and IDS to stop basic intrusion attempts, Denial of Service attacks, and the like. For Distributed Denial of Service and other bandwidth-saturating attacks using legitimately formed packets NetGAP can do little more than any other protective layer, in that it will go down first, acting as a “fuse” that protects internal systems from debilitating levels of network traffic. On the internal side, the NetGAP device is able to throttle the traffic going to the back-end servers in order to maintain good performance for connections that do make it through during such an attack. NetGAP is also scalable - several devices can act in unison as a load-balanced cluster for high-bandwidth operation.

Baroudi Group believes that SpearHead has introduced important technology addressing all forms of current and future recognized-protocol-based attacks. By completely separating internal TCP/IP traffic from external TCP/IP traffic, vulnerabilities related to exploiting the TCP/IP protocol are rendered harmless. For higher-level protocols such as HTTP, POP3, FTP, and others, stateful inspection of these protocols protects against most misuses of these applications as well, such as SYN flooding and buffer overflows. Baroudi Group believes strongly that ever-more-stringent security will be required as more and more of our financial, governance, transportation and economic infrastructures rely on automated systems vulnerable to malicious, targeted attacks. Because NetGAP technology is complementary to traditional rules-based firewalls, Baroudi Group believes that organizations doing business on the Internet should give it serious consideration.