# THE USE OF APPLICATION SPECIFIC SECURITY MEASURES IN A MODERN COMPUTING ENVIRONMENT

By Ryan Permeh
eEye Digital Security

Current computer security practices tend to favor protecting the network as a whole, and avoid the specific issues regarding an application hosted on that network. For instance, a firewall that is configured to support SMTP (Simple Mail Transport Protocol) is rarely designed to deal with any specific implementation details pertaining to SMTP.

This leads to problems with granularity. A traditional solution requires that all external defenses force specific applications to deal with their own security implications. This practice has flaws because not all implementations of a specific service are created equal. By following bug reports and remote attacks on various applications, whether they are web servers, mail servers, IMAP/POP servers or even LDAP servers, you will notice a trend that would alarm any IT administrator.

We feel that it is worth considering the application of a set of "filtering" devices specific to any class of service that is hosted on a network. These devices can be implemented in hardware or software, and their purpose is to understand and protect the hosted service to a degree that traditional methods cannot.

## The Internet Threat Model

Attackers on the Internet tend to focus on gathering intelligence on a service, researching the specific implementations, and exploiting any known vulnerabilities to attack that service. Firewalls lock certain aspects of these exploits out, denying the chance to attack services for which the firewall is configured to block. Intrusion Detection Systems (IDS) alert network administrators of specific attacks against the services that firewalls allow through the border of the network, and potentially can alert firewalls to block future attacks.

This 2-tier approach of protecting services catches a large amount of the attacks against systems, but it has limitations on what it can achieve. The main problem with this traditional system of general protection is that it is a reactive strategy for protecting networks, and will always be lagging behind the cutting edge in security.

Traditional packet-filtering firewalls are able to block packets based on specific packet characteristics, such as TCP flags, source IP address, destination IP address, or TCP and UDP ports. They are able to stop packets that do not meet a certain configurable criteria. Even newer state based firewalls still only look at packet information contained in the IP, TCP, or UDP headers. They tend not to look at specific data contained in those packets beyond the headers, and tend not to discern anything related to a specific protocol. The other disadvantage of firewalls is that if they are used to protect public services, by the very nature of the services being public, they must be allowed access by the Internet at large.

Current Intrusion Detection Systems (IDS) in widespread commercial use are signature based. This means that the IDS only know to look for attacks that they have been programmed to catch. All new attacks have a "window of opportunity" between the time that an attack is developed and the time that patches are released, a signature is created for that attack by IDS vendors, and the signature is shipped to the network administrators.

This window of opportunity is dependent on numerous factors not in control of application developers, IDS vendors, or network administrators. These factors include disclosure by the hacker underground, leaks in application vendors, or improper bug reporting practices. Evidence of this can be seen in most major security related forums, such as bugtraq or ntbugtraq. Exploits are released for services everyday, sometimes before the vendor has a chance to provide a fix for the problem. There is also a large degree of underground activity, and some security problems are only found after having been actively used, sometimes for months, before they are noticed and released to the proper channels.

### Enter the Application Firewall

With the understanding that there are problems in the traditional model of protecting networks comes a new paradigm for securing specific services. It is not meant to be a replacement for Firewalls and IDS, but instead will be a complementary technology.

Application firewalls are systems designed to protect specific services from attack. At its basest form, an application firewall is a reduced application that allows filtering of input for a specific service to allow only desired input. By defining what is acceptable and what is not, it can abort abnormal sessions of a protocol and stop them from continuing on to the actual application.

If implemented correctly, this technique can stop not only specific vulnerabilities, but also general classes of vulnerabilities. This allows the application firewall to protect against new vulnerabilities before they are found and exploited. This philosophy should be implemented in service design, but rarely is.

A generic application firewall should take a "less is better" stance. It should be in place to limit the possible inputs to its service. It should understand the underlying protocol and be able to offer a higher degree of protection that a normal firewall. An application firewall will reassemble protocol state information beyond a normal firewall, and can block general classes of attacks (such as buffer overflow attacks and format string attacks) before they are handed off to the actual application for processing.

Also, in addition to blocking attacks, application firewalls can also be used to reduce the amount of possible information that an attacker can glean from the system it protects. This means that it should be able to stop or change banner information, often it should allow everything as if normal and just discard it before passing it on to the actual application.

It is important to note that application firewalls must also take special care to make certain that they do not implement any types of new security bugs into the system. The application firewall designer should survey the current state of security and should attempt to lessen the impact of the firewall on the overall system. In reality, a successful application firewall design should not interrupt any normal protocol transaction, while stopping abnormal ones from affecting the actual system.

### The New Model of Computer Security

We feel that security in layers is an important part of protecting your information assets. Firewalls and IDS systems are necessary pieces of the security infrastructure, but they are not infallible, nor are they 100% trustworthy. It is important to implement as many security practices as possible; if one system fails, another should pick up where it leaves off. Application firewalls overlap onto the domain of traditional firewalls and IDS systems, but offer a different type of protection that neither of them or both can offer.