Firewalls for Embedded Applications

Alan Grau, President of Icon Labs

 In the past few years embedded devices, including industrial controls and monitoring systems, have taken a huge leap forward in connectivity. Over half of the embedded devices released this year will be connected to the Internet, exposing them to a wide array of cyber-threats. Despite this fact, almost none of these devices will include a firewall to protect against Internet-based threats. Firewall technology is the foundation for network security in home and corporate networks, yet firewalls are virtually absent in embedded systems.

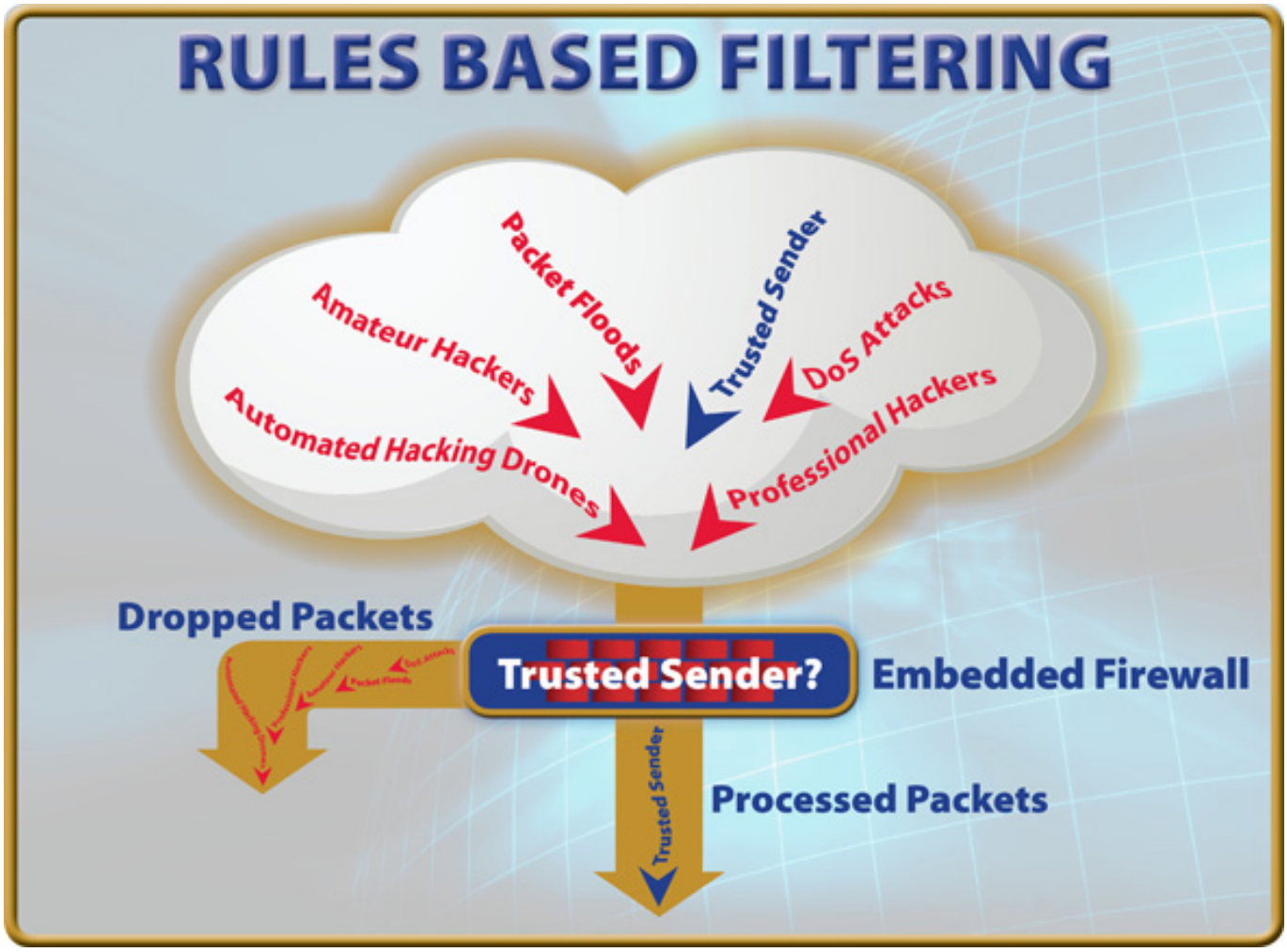
Attacks against embedded devices
The number of attacks against embedded devices continues to rise. An Arbor Networks Security Report showed a 1000% increase in attacks from 2005 to 2010 and a 102% increase just from 2009 to 2010. Reported attacks on embedded devices include:

• Hacking into a car’s computer and disabling its brakes, stopping the engine, and controlling other functions; even overriding the driver’s commands.
• Video conferencing systems were hacked by researchers, allowing eavesdropping and potential corporate espionage.
• Printers reprogrammed with malicious firmware causing it to forward documents to a remote computer, or to run continuously, heating up and physically damaging the printer.
• Pacemakers hacked by researchers.
• Computerized IV drips shut off due to a DoS attack in a lab setting.
• Embedded devices failing from packet floods.

Protecting against attacks
A firewall protects an embedded device by controlling which packets are allowed to pass through for processing by the device. There are three types of filtering provide by Floodgate:

• Static filtering: filters packets based only on the information in the packet. This includes filtering based on port number, protocol, IP address, etc.
• Dynamic filtering or Stateful Packet Inspection (SPI): filters packets based on the state of the connection, allowing packets to be blocked or rejected based on the

connection state as well as the filtering rules.
• Threshold-based filtering: keeps statistics on the packets received and monitors for threshold crossings based on configured time intervals and threshold levels. If the number of packets received from a specific IP address during any time interval exceeds the configured high-water threshold, future packets from that IP address will be blocked, blocking packet floods and DoS attacks.

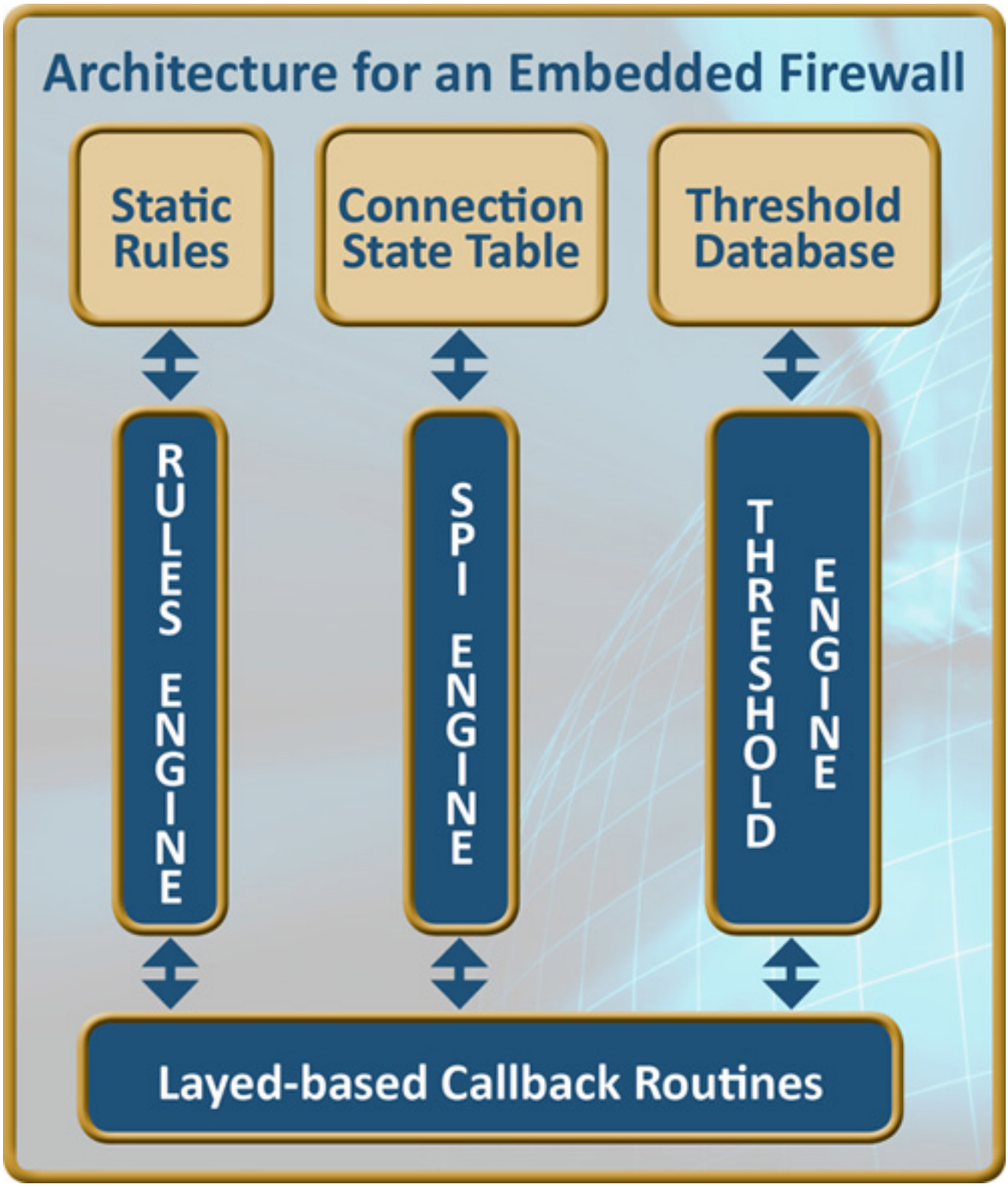


Depending on system requirements, an engineer may elect to use one, two, or all three filtering methods. All too often embedded devices are deployed without any firewall protection. This is generally based on the assumption that an embedded system, as a non-Windows device, is not vulnerable to the same attacks as a PC, or embedded devices will not be attacked. Recent attacks have shown that this is simply not true.

Firewall requirements for embedded systems
To be effective, an embedded firewall must be small,efficient, andeasily integrated with the operating system and TCP/IP stack of the embedded device. Ideally, the firewall would also support all three filtering methods.
Embedded devices often do not have the memory, available CPU cycles, or other resources found in desktop or enterprise systems. As a result, traditional firewall technology does not work well in an embedded environment. Engineers need a firewall designed specifically for embedded systems.

A firewall for embedded systems

Floodgate is a firewall product designed by Icon Labs to meet the specific requirements of embedded applications. Floodgate provides static filtering, threshold-based filtering, and Stateful Packet Inspection to protect embedded devices from Internet-based threats. Floodgate has a small footprint, low CPU processing impact, and is easily integrated with any embedded IP stack.



Summary

Despite the growing awareness of risks, most embedded devices still do not include a firewall. A typical desktop or enterprise firewall is just too big and requires too many resources to function in an embedded environment. Until recently, only a few limited solutions were available leaving engineers with a difficult and time consuming task if they wished to implement an embedded firewall. Icon Labs' new Floodgate firewall solves these problems, making it easy and affordable to add an embedded firewall to a wide variety of embedded devices.

Alan Grau is the President of Icon Labs. You can reach him at alan.grau@iconlabs.com [1]

Links:
[1] mailto:alan.grau@iconlabs.com