Shutting The Door On Shodan

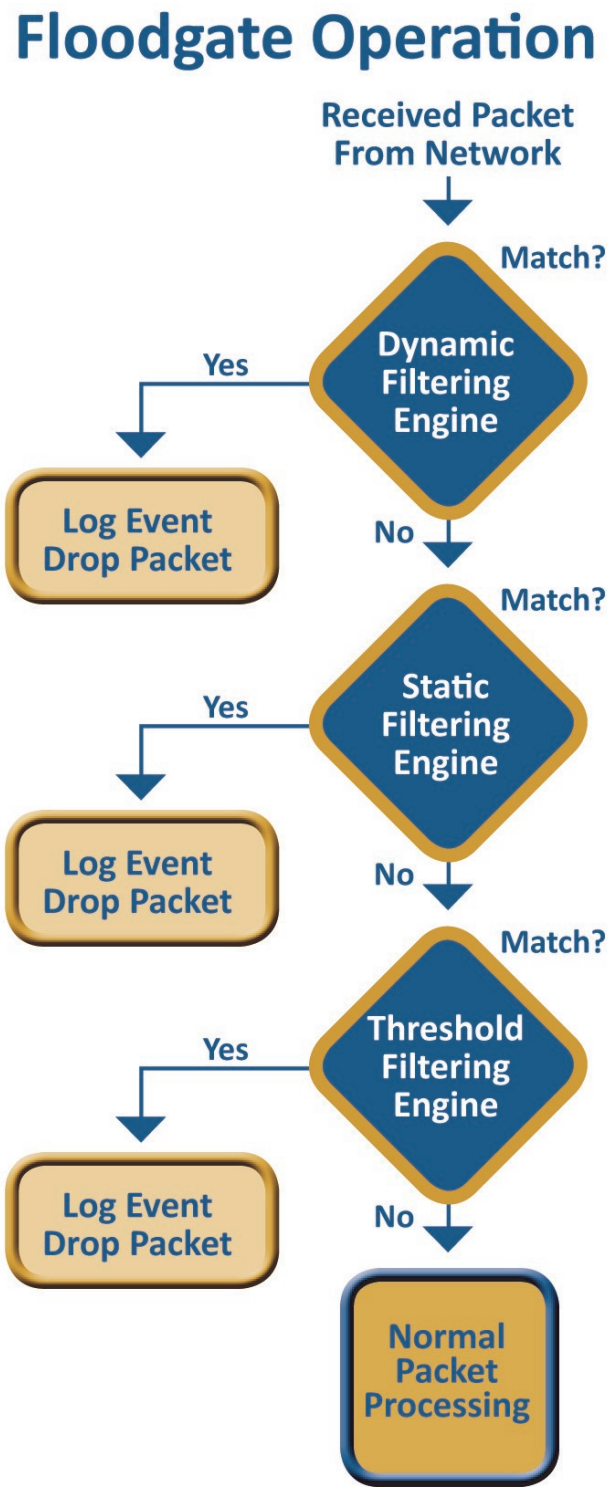
Alan Grau, Icon Labs

Shodan, “the scariest search engine on the Internet” according to *CNN Money*, is a search engine scouring the Internet looking for servers, webcams, printers, routers and all the other devices that are connected to, and make up, the Internet of Things. Searches on Shodan can find a stunning amount of information. Would-be hackers find critical systems to attack, search by city or GPS coordinates, and find detailed information on devices and their vulnerabilities.

Searches on Shodan have turned up countless web cameras, traffic lights and home automation devices, many with little or no security. Searches also exposed SCADA systems, gas station controls, and even command and control systems for a nuclear power plant. Shodan even allows searches for discovered exploits and vulnerabilities. Shodan provides hackers a simple, easy-to-use launching pad for attacks.

It is easy to look at Shodan as the problem — it provides easy access to the devices connected to the Internet. In reality, however, Shodan simply highlights the security vulnerabilities of many of the devices that comprise the Internet of Things (IoT). The real problem is not that Shodan finds insecure devices, but that so many devices lack real security.

Shutting the Door on Shodan



Ensuring that a device is not discoverable by Shodan or a botnet is an important first step in security for IoT devices. If hackers can't find the device, they can't attack it.

Shodan, like other search engines, crawls the Internet looking for information. Unlike other search engines, Shodan is looking for web connected devices. Once it finds a device it checks to see what services are available on the device, detecting things such as default passwords and known vulnerabilities and exploits. The Shodan home page boasts: "Expose online devices. Webcams. Routers. Power Plants. iPhones. Wind Turbines. Refrigerators. VoIP Phones." Shodan is able to do this because most IoT devices have little if any control over the packets they process.

Many IoT devices perform a fixed set of functions. These functions typically require communication with a small set of known devices and only utilize a small number of protocols and ports. For example, a SCADA system may control operations for an offshore oil rig. The individual devices in the SCADA system should only need to communicate to other SCADA devices located on the oil rig, and perhaps to a control computer located in a corporate server room. In addition, these systems only need to support SCADA specific communication protocols. Other Internet services such as HTTP, SSH and FTP are typically not needed by the device and should be turned off. Even if they are supported, they are not supported for general access — only a few other computers should utilize these services.

Adding a firewall to the IoT device provides the critical missing layer of security. A firewall controls the packets processed by the device and blocks all communication from unknown hosts, and closes unused ports and protocols. Since Shodan or the computers in a botnet would not be known trusted hosts, any attempts to discover the devices would fail. This essentially renders the device undiscoverable, closing the door on Shodan and botnets.

Security requirements for the Internet of Things

Ensuring that a device is not discoverable by Shodan or a botnet is an important first step in security for IoT devices. If hackers can’t find the device, they can’t attack it.

However, a comprehensive security solution needs to go further than just preventing discovery of the devices. A security solution for IoT devices must also provide the ability to control communications, detect and report attacks, or suspicious traffic patterns, and allow centralized control of security policies. These capabilities would provide a much higher level of security than most devices currently have and would protect them from the majority of cyber-attacks.

The security solution must provide:

- Control of the packets processed by the device.
- Protection from hackers and cyber-attacks which may be launched from the Internet, inside the corporate network or WiFi networks.
- Protection from DoS (Denial of Service) attacks and packet floods.
- Ability to detect and report traffic abnormalities, probes or attacks.
- Ability to manage and control changes to filtering policies.

Integrating security into the device

Many facilities and campuses have a corporate firewall designed to protect the internal systems from attack. However, the corporate firewall can be breached or bypassed by sophisticated hackers, or attacks may originate from within the corporate network. In some cases, an IoT device may not reside behind a firewall, leaving it vulnerable to cyber-attacks. Building protection into the device itself provides another security layer — the devices are no longer dependent on the

corporate firewall as their sole layer of security.

For new devices, enhanced security can be built into the device itself. This is the same approach taken with PCs today. While a PC may sit behind a firewall on a home or corporate network, it is also running a built-in firewall and other security software.

An integrated firewall provides a basic, but critical level of security for a networked device by controlling which packets are processed by the device. The embedded firewall resides on the device and is integrated into its communication stack. The communication requirements of the device are encoded into a set of policies defining allowable communication. The firewall enforces these polices, limiting communication to the required IP address, ports and protocols specified in the policies.

Since each packet or message received by the device is filtered by the firewall before passing from the protocol stack to the application, many attacks are blocked before a connection is even established, thereby providing a simple, yet effective layer of protection missing from most devices.

Blocking attacks with a firewall

In a system without a firewall, a hacker may attempt to remotely access the device using default passwords, dictionary attacks or stolen passwords. Such attacks are often automated, allowing a huge number of attempts to break the system’s password. However, by protecting the system with an embedded firewall configured with a whitelist of trusted hosts, the firewall can effectively block such attacks. The firewall blocks packets from the hacker before they are passed to the application to attempt to login.

Rules-based filtering provides a simple and effective tool to enforce communication policies, blocking communication from a non-trusted IP address, and isolating the device from attack.

Security Management

Building a firewall into a device provides a

foundation for security. Once deployed, it is critical to be able to manage the security policies on the device and for the device to report invalid access attempts and other security threats. This is achieved by providing integration with enterprise security management systems. The firewall should include a management agent enabling:

- Integration with enterprise security management systems.
- Configuration of filtering policies.
- Reporting of invalid login attempts and other security incidents.

Integration with the security management system allows network management personnel to be notified of security issues, allowing mitigation and preventing issues from proliferating throughout the network. This type of security management is standard policy for PCs and servers. IoT devices are no different — they need to support built-in security and integrate with existing security management systems.

Securing legacy devices – the “bump-in-the-wire” solution

Many legacy devices and systems are already in place, but lack adequate security. Upgrading these devices to improve security may be difficult and expensive. Some devices cannot be upgraded without being returned to the factory to be updated. In some cases, the manufacturer may no longer support the device, or may be out of business. Replacing these devices is often too expensive to be an option and newer devices may not yet be available with improved security.

For devices that cannot be easily or affordably replaced or upgraded, a “bump-in-the-wire” appliance solution provides the required security. This type of solution can protect legacy devices by creating a “secure enclave” in which these devices can operate and protect the current investment in the hardware. Only trusted devices should be deployed within the secure enclave. These devices can freely communicate with each other, but communication outside of the enclave is controlled for security. The “bump-in-the-wire” appliance provides security by enforcing communication policies, ensuring that only valid communication is allowed with the endpoints within the secure enclave.

Summary

Many of today’s IoT devices and systems are complex connected computers charged with performing critical functions. Firewalls provide the cornerstone of security both for PCs and for home or corporate networks. Including a firewall in IoT devices provides a simple and effective layer of security. These firewalls provide protection even if the corporate firewall and security is breached. A small embedded firewall, such as Floodgate from Icon Labs, can be used to protect devices from a wide range of cyber-attacks. By controlling who the device talks to, you can shut the door on Shodan and block attacks before a connection is even established.

1. http://money.cnn.com/2013/04/08/technology/security/shodan/ [1]

Alan Grau is the President and cofounder of Icon Labs *[2], a leading provider of security solutions for embedded devices. You can reach him at alan.grau@iconlabs.com* [3]

Links:
[1] http://money.cnn.com/2013/04/08/technology/security/shodan/
[2] http://www.iconlabs.com/
[3] mailto:alan.grau@iconlabs.com