Care Interrupted—Top Five Vulnerabilities in Medical Devices

Matt Neely, Director of Strategic Initiatives, SecureState

 As medical science advances, so does the equipment used to deliver care. In the modern day hospital, more and more medical devices, such as IV pumps, ventilators, MRI, CAT Scan, and X-Ray machines are attached to hospital networks. Putting medical devices on the network provides a large number of benefits, such as supporting telemedicine and the easy transfer of test results to electronic medical records (EMR) systems. However, putting these devices on a network also introduces a number of risks. Through performing penetration tests [1] on hospital networks and medical devices, SecureState [2] has found that many of these commonly used devices are insecure and can be easily broken into.

Top Five Vulnerabilities in Medical Devices

1. *Denial of Service Vulnerabilities*—Among the most serious weaknesses found in these devices are flaws that allow attackers to crash a device or cause it to disconnect from the network. These devices are often very delicate, so basic denial of service attacks can crash them. We've seen cases where a flood of traffic, which any modern day desktop or laptop could handle, crashed a medical device. A device susceptible to this form of attack may simply disconnect from the network or could stop functioning altogether, interrupting the care being delivered to the patient. Denial of Service attacks can be an inconvenience in many other industries, but when we’re talking about the healthcare industry, this could directly impact a

patient's health depending on how badly the medical device fails.

2. *Weak and Default Passwords*—Medical devices commonly have weak passwords set on them or have built-in back door passwords [3]that cannot be changed by the hospital managing the device. This means that attackers can easily guess the passwords used to protect the device and gain access. Vendor built-in default passwords pose a special challenge because these credentials often give attackers access to diagnostic and configuration information that can aid in more advanced attacks.
3. *Missing Security Patches*—Medical devices running on Windows or Linux operating systems are often missing critical security patches. Medical devices are often not patched once they are deployed and are commonly years behind on critical updates. Compounding this issue, many devices are still running Windows NT and Windows 2000, which are no longer supported by Microsoft and, therefore, no longer get security patches for new vulnerabilities. Often times, these missing patches leave these devices vulnerable to computer viruses such as Conficker, which downloads additional malware like keystroke loggers to a device and traditionally adds infected systems to a botnet. Additionally, these missing patches allow attackers to easily break into these devices using readily available tools such as Metasploit.
4. *Unencrypted Management Traffic*—Management interfaces used to remotely administer and sometimes operate the device are frequently unencrypted. Similarly, when these devices send data to a central monitoring and EMR system, this traffic is often not encrypted. This means that attackers who are monitoring the network can steal passwords used to log into the device, hijack connections, and view and alter patient information sent to and from the device. This is of particular concern for devices using WiFi networks.
5. *Web Application Vulnerabilities*—A growing number of network attached medical devices have web interfaces used for status updates or remote management. Often times, these interfaces are not securely coded and contain web vulnerabilities, such as cross-site scripting (XSS) and SQL injection. These vulnerabilities vary in the type and complexity, but could allow an attacker to log into a device without providing a password. That person could then change settings on the device or access private information.

Many Risks and Insufficient Guidance

As you can see, these vulnerabilities pose a number of risks to patient care. Most concerning is that many of these devices can be taken offline, shutdown, or infected with a virus when an attacker isn't even targeting them. When SecureState has investigated infections of these devices, we often find the virus was accidently introduced into the network. Also concerning is the idea of attackers targeting on one of these systems, using these common vulnerabilities to crash medical devices, change settings, and view and manipulate patient data.

Recently the FDA released draft guidance [4] for hospitals and device manufactures to secure medical devices. Although this guidance is a good start, it is too high-level to be truly useful and does not provide actionable information hospitals and device manufactures can use to improve security. As an example, the FDA guidance

mentions encryption, but does not provide any guidance around selecting secure algorithms or performing key management, which are critical to properly implementing encryption. Additionally, the agency does not recommend types of security tests that should be performed on devices, which can be used to verify that implemented security controls are actually working.

In a future series of blog posts on medical device security, SecureState will discuss these types of vulnerabilities in more depth and provide our recommendations on how medical device manufactures, hospitals, and regulators should address them.

Links:
[1] http://www.securestate.com/Services/Profiling/Pages/Internal-Attack-and-Penetration.aspx
[2] http://www.securestate.com/
[3] http://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01
[4] http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356186.htm