Protecting the Promise of the Internet of Things

The promise

We at Cisco are fully committed to the Internet of Things (IoT). We believe that the IoT will alter our society through advances in medical care, automation in manufacturing, dependable, efficient utilities and so much more.

Breast cancer kills 500,000 women annually around the world, and early detection can greatly increase the odds of survivability. Imagine wearing clothing that could detect the early signs of disease. The iTBra does just that. It is a wearable diagnostic device that detects the drop in metabolic activity that indicates cancer growth. Data from the sensors is fed from the device to the cloud for analysis and early detection.

That’s not the IoT of the future. It’s the IoT of now.
The challenge

The Internet of Things must be secured for it to fulfill its promise. Easier said than done. There are two hallmarks to the IoT that make securing it a monumental task: inherent vulnerabilities and scale.

The insecurities in IoT devices are the stuff of headlines and doomsday predictions, and it’s no surprise. IoT devices are affected by:

- Security immaturity/unfamiliarity from manufacturers
- Insufficient system resources to run native security
- Market/competitive pressures, especially on commodity devices, that force cybersecurity functionality to be removed

The reasons for a device not being able to secure itself are irrelevant from a security perspective. A vulnerability is a vulnerability is a vulnerability. A vulnerability is an opportunity for an attacker to exploit the device to gain access to your network. After an attacker is on your network, malware can be installed, intellectual property can be stolen, or any number of scenarios can occur. These threats are also in the now. We’ve already seen how attacks against the IoT can result in:

- **Equipment damage:** A cyberattack against a European steel plant damaged a multimillion-dollar smelter. The malware forced the operators to immediately shut the equipment down for safety reasons, bypassing a longer controlled cooling process.1
- **Critical infrastructure disruption:** Power was lost for up to six hours in some parts of an eastern European country when a power utility lost control of the power grid because of a multifaceted attack. The attack included malware that took down the management systems used to operate the grid.2
- **Healthcare disruption:** UK hospitals were forced to reschedule surgeries, cancel appointments, and divert major trauma cases while the hospital shut down systems to deal with a malware infection.3

We expect that there will be 30 billion connected “things” by 2020. That’s a lot of devices to defend. The simple fact is that enterprises are exposed now. A simple Shodan search will easily prove that. And we can’t passively wait for the problem to fix itself.

Tomorrow’s solutions today

The good news is that action can be taken today without reinventing the wheel. The challenge must be tackled on four critical fronts:

- **Software-based segmentation:** Traditional VLANs have their place, but they can’t scale to match the load imposed by the IoT. Scalable, extensible software-based segmentation with enforceable policy based on device type, user type, location, time of day, and so on means organizations have more visibility, control, and automation to protect the business and adapt to the unexpected.
- **Visibility and analysis:** Device, application, and user discovery coupled with packet analysis and behavior-anomaly threat detection across your environment transform the network into a sensor that quickly detects and remediates threats before business operations are affected.
- **Secure remote access:** Greater connectivity means greater cost reduction and efficiency for remote and mobile users and third parties, but this also introduces risk. Secure end-to-end remote access keeps communications protected and gives control over user access after users are connected to the network.
- **Advisory and technical services:** Every organization needs guidance and advice at some or all phases of a project. The likelihood of success is greater when services are engaged from the beginning of a project.

Software-based segmentation

Why segment IoT devices? Segmentation puts those devices out of the reach of attackers and prevents these devices from being used as pivot points to move through the network if they are compromised.

Network segmentation is a well-established security best practice. VLANs have been in use for decades, and they still have an important place. However, when we consider securing 30 billion things, the sheer scale of the IoT makes creating enough VLANs impractical, if not impossible.

Software-based segmentation uses factors such as location, device type, user role, and so on to create policy that is enforced throughout the network-anywhere.
And it is easily adapted as your environment evolves. Third-party technology integrations mean more control over your network, stronger security automation, and more value from other technology investments.

**Visibility and analysis**

Threats evolve as quickly as the new technologies that attackers strive to exploit. This means that there is limited time between threat detection and your response. You need to detect new devices, protocols, applications, and users as they attempt to get on your network—anywhere on your network. You also need to detect and block threats before they can affect your business.

An automated, multilayered capability to analyze the network traffic throughout your network, as well as traffic entering and exiting your organization, to detect anomalies, block threats, identify compromised hosts, and even help prevent user error is required to defend among a variety of threat vectors. Rule-based detections will ferret out the latest known threats; protocol analysis helps prevent human error; anomaly detection uncovers new threats and will identify “patient 0.” Malware command and control traffic is blocked for your in-house and mobile users, and web traffic is continuously inspected for suspicious behavior.

**Secure remote access**

It’s no surprise that many equipment vendors, such as industrial and healthcare equipment vendors, require remote support in their support contracts. Remote support saves the vendors on operational costs when they don’t need to send a technician on-site, and remote support can reduce downtime for customers as the technicians get to work while still on the phone with the customer. There are some drawbacks, though:

- Remote access means that sensitive networks—for example, an industrial control network—can be reached from the Internet.
- Customers have equipment from multiple vendors, which means access needs to be granted for each of the vendors separately, creating more holes in the defenses.
- Customers often have no idea what devices are actually communicating with in the customer’s environment or even whether the vendor’s network is introducing security threats into the customer’s network.

Secure the communications from the remote party to the network and employ segmentation, visibility, and analysis to make sure remote users do not introduce threats. This approach makes sure that remote users may only access the systems for which they are allowed access for the job they are intended to perform.

**Advisory and technical services**

Despite the technological advances that the IoT represents, the human factor is the most important. Technology is just a tool. People are needed to secure IoT environments. The proper planning and guidance will greatly improve the likelihood of establishing a successful IoT security program.

The most important first step is knowing where you want to go. Employing advisory and technical services to assess risk; develop a readiness plan; and deploy, operate, or build an incident response plan greatly increases the chances of successful project delivery and ongoing service support to your business.

**Bringing it all together**

The threats you face are dynamic, and your defenses should be, too. Imagine that a contractor connects a laptop infected with a worm to your network. The worm immediately attempts to propagate itself, and an automated response kicks in where:

1. The malicious traffic is detected and blocked.
2. The laptop is quarantined from the network.
3. The user account is disabled.
4. Your user console can visually display that your critical systems were never in danger.

You manage the entire process without it affecting the business because you were prepared and executed your prepared incident response plan.
Why Cisco?
Cisco has been in the business of designing, deploying, and securing networks for more than 25 years. We build the equipment, invent the technologies, and develop the standards that helped make the Internet possible, as well as any other kind of network that you can think of. Who better to help you meet the challenge of the IoT head on?

Let’s talk, and we can tell you how we can help you make the most of a secure IoT.

The last thing operators of critical networks want to hear about is automated cybersecurity. It might be fine for IT networks, but certainly not for most industrial networks, and we know this. You can automate as much or as little as you want. It’s your network, and you control it. We help you do it more easily and securely.

References