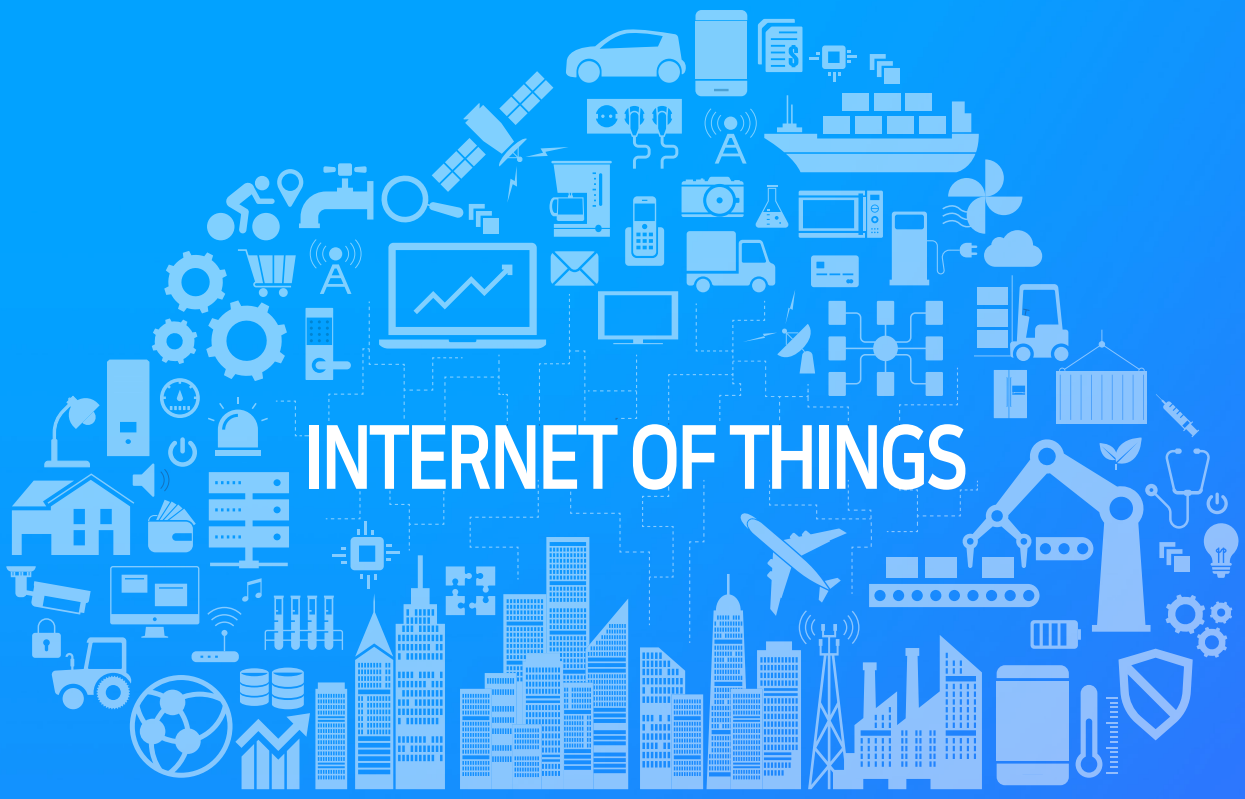
dellfer

Why IoT Security Needs a Rethink



Why IoT Security Needs a Rethink

THE CRITICALITY AND RISKS OF IoT CONNECTIVITY

Having an always-on connection to the internet is a requirement today for many branded consumer products. Because consumers value the internet's convenience and superior experience, manufacturers that embrace this fact can achieve sustainable competitive advantage. Imagine the consumer, sitting at a movie theater with his or her family, and using a mobile phone to turn down the thermostat in one's home to save on electricity costs. For the thermostat manufacturer that can enable this convenience, this type of feature could mean the difference between losing and winning a sale.

From wearables such as heart rate monitors to home electronics to connected or self-driving cars, the pressure for branded and industrial product manufacturers to design connectivity into their products for more value is extremely high. That pressure is driving the growth of IoT connected devices to estimates of current day 5 to 8 billion growing to between 20 to 50 billion devices by 2020.

This innovation comes at a cost for branded product manufacturers. Focused for years on consumer and public safety, this always-on internet connection exposes the stark possibility of security, not safety, issues. Cybersecurity attacks are often the product of a root software vulnerability, and the fact is IoT connected devices expose themselves to hacking more than the average enterprise business software product. Yet the stakes are much higher in the IoT environment, where security can mean the difference between damaged life and death, brand reputations, and continuing customer trust and loyalty.

IoT SECURITY TRADITIONALLY GREW FROM IT SECURITY

Since the appearance of Stuxnet in the late 2000's, the government has increasingly mandated security standards to strengthen existing safety standards in many critical infrastructure sectors. In sectors such as the automotive industry, private bodies are organizing to move the ball forward with best practices and updated standards for cybersecurity that will bolster well established safety standards.

Many of the initial security forays in ICS/SCADA, automotive cybersecurity and medical device equipment security has been with solutions that bring a traditional IT security view of the world and approach to the problem. Unfortunately, while some things such as a defense-in-depth continue to make sense in IoT environments given the lack of a silver bullet, applying traditional network security thinking to IoT is destined to fail for various reasons. Below we list our Top 8 Reasons why IoT security needs a rethink.

THE TOP 8 REASONS

1. The Outcome is Rarely Exfiltration

In IoT the hacking goals can be very different. The outcome may simply be system compromise and downtime. This would be more akin to ransomware, where a computing system can be made un-useable. For many attackers, simply running a buffer overflow attack that could crash or create an extended outage on a system would be success with major impact on individuals or society at large.

2. The Interfaces Are Different

Many IoT connected products are small and use entirely different interfaces than LAN-based products. The leading attack vector for data breach cyberattacks in IT security is a web application running over a browser. In contrast, many IoT connected devices are written in compiled languages such as 'C' and have both physical interfaces (such as OBD-II in cars) as well as virtual ones that need to be protected.

3. The Keys to the Kingdom Are Different

O*ne of the key objectives in an advanced cyberattack after* "infiltrating" a target is escalating administrative privilege to get to crown jewel data records. This facilitates a "lateral movement step" and may involve a privilege escalation action such as dumping a password file on an endpoint machine. While impersonation or credential theft can be utilized in IoT arenas, the goal is to get to a gateway or host that holds encryption keys or can generate downstream instructions that wreck havoc, not necessarily data records.

4. The Architectural Constraints Differ

Most traditional IT security solutions are architected for much richer resource environments. When you consider for example that the internal messaging network of a connected car is essentially an 8-byte "packet" size (CANBUS), the ideas of AES 128 or 256-bit encryption and standard IT security authentication options are out of reach. And with much of next generation IT security moving to big data and heavy log file analysis, it's clear IoT's limited bandwidth and storage sizes will be an issue.

5. Inability to Patch Due to Uptime and Reliability Needs

Perhaps the biggest difference in approach and mindset that dictates a rethink in security for IoT environments is the necessary patching cycle the software world and security industry depends on. It is, in fact, the leading piece of advice and best practice for enterprises with respect to preventing hacking infiltrations. Patching, software updating requiring a re-boot and the required system downtimes associated with such operations are non-starters in many industrial IoT environments. This means products have much longer lifecycles in un-updated states than systems that can be updated close to real time or frequently to adapt to changing adversarial patterns of attack.

6. Need for Greater Precision

One other big complicating factor with IT security solutions is that many are simply not precise enough for IoT environments given the stakes. Many IT security solutions are prone to high false negatives and false positives, but succeed because of a lack of alternatives or a compliance-oriented checkbox mindset. IoT requires a higher bar of efficacy. Protecting a self-driving car or ensuring that a nuclear facility is not compromised demands higher precision and prevention options.

7. Cost Structure

On the low end, endpoint or user-based security products cost between $10 to $80 per seat, but for those solutions and others, the overall sell price range tends to be between $75K to $250K for an initial deployment security solution. Venture-backed business models are architected with these types of assumptions in mind. However, in the heavily margin constrained world of consumer products, this type of pricing model does not always adapt well for manufacturers. Economic models must evolve to something different, particularly for products that require a high cost to deploy or maintain.

8. Embedded Supply Chain Component

IT security approaches do not fit well into complex supply chains between finished goods manufacturers and their suppliers common in IoT sectors. IT security solutions are designed for corporate enterprises,6 and most solutions do not prioritize an embedded component model of security.

THE FOUNDING PREMISE OF DELLFER

For the reasons listed above, Dellfer is focused on protecting IoT connected devices from hacking in its own lightweight and focused way. Rather than support a traditional bolt-on model of security, the company supports a view of inside out security, built intrinsically into products. A founding tenant is that technology be easy to apply but highly effective, a tough compromise in the security industry until now. Founded by leading experts in embedded systems and developer-centric security, Dellfer represents a new option for industrial IoT and consumer product manufacturers with cloud connected consumer products. We invite you to learn more at www.dellfer.com.

Dellfer enables product manufacturers to reliably secure their cloud and IoT connected products from zero-day hacking and advanced cyberattacks. Focusing on the automotive cybersecurity and other IoT markets, Dellfer offers ZeroDayGuard, the first execution integrity monitoring solution that can be added during the build process easily within seconds. ZeroDayGuard can prevent zero-day attacks against unknown vulnerabilities and instantaneously alert manufacturers to attempted and thwarted hacking events in seconds.
More information about Dellfer and ZeroDayGuard are available at www.dellfer.com.

951 MARINERS ISLAND BLVD,
SUITE 300 SAN MATEO, CA 94404

INFO@DELLFER.COM • WWW.DELLFER.COM