IoT
Simple, Ubiquitous, Dangerous

The proliferation of IoT demands a new look at old security thinking

TOPSPIN SECURITY

Simple, Ubiquitous, Dangerous

TOPSPIN SECURITY

Contents

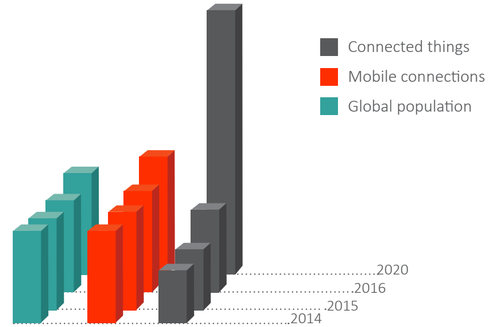
Contents:

IoT: Massive Market, Massive Security Liability

From Barbies to bridges, from home thermostats to power plants, from baby monitors to advanced healthcare scanners – IoT is part of our day-to-day reality.

According to Gartner, by the end of this year 6.4 billion “connected things” will be in use worldwide. That’s nearly one device for every human on the planet. By 2020, Gartner predicts, the devices will far outnumber us, with over 20 billion connected.

The massive proliferation of IoT devices presents a new world of security challenges. In this e-book, we’ll take a look at these vulnerabilities, and how advanced technologies can help resolve them.



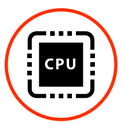
Sources:
GSMA, The Mobile Economy 2015 | Gartner, IoT November 2015 | Geohive.com

Why is IoT Security Inherently Different?

Why is the IoT ecosystem so dramatically different from a security point of view?

Fragmentation

There is still no single security standard or group of standards for IoT devices. Moreover, many IoT devices cross over traditional industry boundaries: is a refrigerator that can automatically order food an appliance, a communications device, or a payment device?

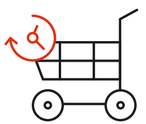


Limited resources

IoT devices by definition have limited resources. They're designed to perform specific functions with low power consumption, minimal CPU cycles, and low memory requirements. This prevents onboarding of traditional security tools like antivirus, application whitelisting, and more advanced kernel-based analysis tools.

Software stack

The incredible variety of IoT devices is matched by an equally incredible variety of software stacks. Devices use different operating systems, infrastructure protocols, and communication mechanisms. What's more, they often run proprietary protocols on top of the transport layer.



Time to market

In a competitive and emerging market like IoT, time to market is crucial. This means that proper security design of mission-critical elements like encrypted transmission and key management - as well as QA of communications channels and interfaces - can fall by the wayside. The results? Flawed security architecture, insecure interfaces, unencrypted data transmission, unknown backdoors and other vulnerabilities.

Vulnerability Scanning and Penetration Testing Aren't Enough

Designed to assess computers, computer systems, networks or applications for weaknesses or known vulnerabilities, vulnerability scanning can be effective for traditional network topologies. In the IoT realm, however, the sheer volume of devices - multiplied by the massive number of possible vulnerabilities, configurations and operating systems - makes vulnerability scanning clumsy and not cost effective.

Similarly, penetration testing for IoT devices is tedious and can be expensive. This is because testing requires detailed information about the number of different IoT devices in the organization, which software packages are installed on which device, what protocol each uses for communication, and whether there are known backdoors for each.

Even if all IoT devices are successfully scanned and tested, and vulnerabilities found – the solution is often firmware updates, which present serious administrative and technical challenges to organizations of any size.

Drill Down: IoT Security in Sensitive Industries

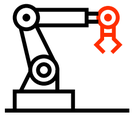
How is IoT used, and why are IoT devices so vulnerable, in these key industries?

IoT in Healthcare

Healthcare organizations have undergone a technological revolution in recent years. Today, caregivers share more information via more devices to raise standards of care while lowering expenses. Everything from MRI machines to personal insulin pumps are now connected and vulnerable. Digital medical records are stored on these IoT devices, and are increasingly valuable for identity theft, ransom, and other illicit purposes.

IoT in Automotive

The connected car is not new. Smartphones connect seamlessly to vehicles, and in-vehicle navigation and infotainment are standard. But a new generation of V2X (vehicle-to-everything) applications, combined with IoT sensors embedded in and communicating with the vehicle, radically change the vehicle systems security landscape. Now, vulnerabilities in vehicle-connected IoT devices - driver wearables, for example - or in-car IoT sensors can provide a backdoor for hackers into critical vehicle systems.



IoT in Industrial Control

IACS (Industrial Automation and Control Systems) and SCADA (Supervisory Control And Data Acquisition) devices such as sensors, wireless transmitters, RTUs, PLCs, and OITs are embedded in countless industrial and critical infrastructure systems worldwide. These legacy IoT devices can act as gateways into highly-sensitive and strategic systems. Yet many were simply never designed for security – leaving, for example, critical communication protocols like HTTP, FTP, and Telnet open and accessible.

IoT Visibility in the Network – Another Challenge

Asset management poses another key challenge in the IoT ecosystem. The exact interfaces of IoT devices, and how they communicate with internal or external environments, are not always known – especially in large enterprise networks.

In many enterprises, thousands of IoT devices – from enduser-facing devices like cameras and printers to full-scale industrial control systems - operate round the clock and communicate with an internal backend platform or directly to the Internet.

To manage and control these devices, the enterprise needs clear knowledge of their location, to where they connect, who and from where they can be accessed, what kind of protocols are being used, and more.

TopSpin – A New IoT Security Paradigm

To meet the challenges of the IoT paradigm, TopSpin's DECOYnet changes the way organizations map and protect their IoT assets - delivering maximum visibility and sophisticated deception-based security:

Deception

TopSpin learns and maps complex network topography – including IoT devices - to keep ahead of attackers. Leveraging deep network insights generated during mapping, TopSpin's DECOYnet solution intelligently sets decoys across entire networks which mimic relevant IoT devices. Then, using a unique targeted placement technique, DECOYnet strategically plants mini-traps (breadcrumbs) on endpoints and network assets.

DECOYnet proactively lures attackers away from actual organizational assets. Publicizing themselves throughout the organization and generating realistic traffic, DECOYNet mini-traps attract and divert attackers, who believe they are accessing real IoT assets. DECOYnet closely monitors all network activity, analyzing communication between IoT assets and remote locations, alerting security staff when an attack is in progress, and providing a complete forensic trail of attacker activities.

In TopSpin's deception paradigm, attackers targeting IoT devices are convinced that they've found exactly what they're looking for, and look no further.

Visibility

DECOYnet leverages continuous passive scanning and analysis to identify all IoT devices in the enterprise. Then, differentiating between human and automatic activities and using advanced anomaly identification, DECOYnet detects when IoT devices communicate with the Internet or with other systems inside the enterprise.

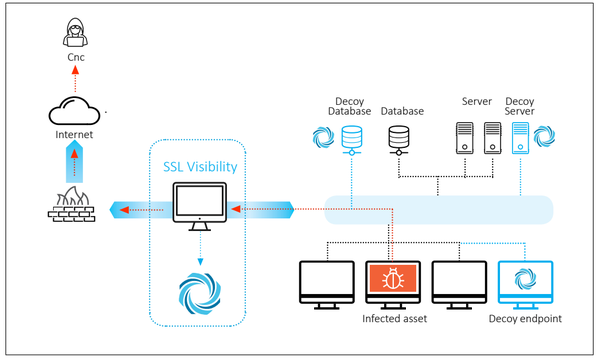
With DECOYnet, security teams create a mapping of the organization's IoT assets – including a complete report of protocols and ports being used, communication channels, network activities, data transmitted, and exfiltrated data.

DECOYnet's deception-based approach eliminates the need for expensive dedicated security software for individual connected devices. This is notably important for high-value, low-volume devices like MRIs or industrial control systems – and on the opposite end of the scale – for high-volume, low-value assets like insulin pumps, IoT printers, and other enduser-facing IoT devices.

About TopSpin

TopSpin empowers security professionals to go on the offensive against APTs and other sophisticated network threats. Our solutions learn network topography and sniff all egresses to keep ahead of attackers. Using our deep network insights to intelligently plant mini-traps (breadcrumbs), TopSpin identifies attacks early and diverts attackers to a decoy network. Then, we track Command and Control communications and catch attackers in the act.

Already deployed in major enterprise networks throughout North America, TopSpin's DECOYnet solution detects the presence of malware and attackers that have infiltrated network defenses.
Learn more at **www.topspinsec.com.**



For more information:

contact@topspinsec.com
www.topspinsec.com

TOPSPIN SECURITY