accenture

Strategy | Consulting | Digital | Technology | Operations

Securing the Internet of Things

Executive Summary

High performance. Delivered.

The Internet of Things (IoT) could supercharge industrial value creation by enabling a nonstop variety of new business models and applications. But it can also expose industries and consumers to unanticipated security issues. Emerging from the convergence of IT systems and operational technologies like smart sensors and actuators, the IoT covers everything from wireless heart monitors to autonomous cars. While few doubt its transformative power, many recognize the new security risks that arise when businesses incorporate the IoT at the edge of their networks. In fact, businesses surveyed by the World Economic Forum identified cyber-attack vulnerabilities as their most important IoT concern.[1]

Threat hotspots include critical aspects of operational security, the diverse number of communication protocols in use today, vulnerable software patches and unsecure access management practices. Hovering over all of these are the privacy expectations of consumers, who are becoming more aware of the online threats they face.

To secure applications while also pursuring value-creation abilities, digital enterprises should consider the following suggestions:

Engineer trust into connected products.
Apply "secure by design" principles throughout a product's development, from concept ideation to series manufacturing instead of addressing security issues at the end of the cycle. Designers should also build in operational controls when originally configuring systems to verify that all component behaviors conform to expected operational norms, and undertake a complete analysis of a system's threat-versus-risk profile. Engineering responses should focus on eliminating undesirable outcomes (e.g., breached customer data).

Adopt a new operational mindset.
Monitor the IoT's operational and security health continuously—a big data challenge that requires a big data solution. Furthermore, an IoT system might depend on other such systems, so design for failure survival and focus on resiliency, starting with anomaly detection capabilities enabled by machine learning and effective responses.

Develop contextualized threat models.
Build tailored threat models that take into account key business goals, the underlying technical infrastructure, and potential threats that can disrupt the business. Such models can help to prioritize IoT security threats and uncover blind spots.

Apply mobile and cyber/physical system (CPS) security lessons.
Consider the lessons learned and the growing pains endured by mobile networks and CPS arenas. In some ways (i.e., embedded systems), they are precursors to the IoT.

Adopt privacy by design (PbD) principles.
Establish access and authorization rights to data sets as they are collected, and co-locate these rights with relevant data sets when moved or stored.

Track and use emerging standards.
Understand emerging standards from collaborative organizations and consider joining standards bodies to exploit rapidly evolving technology innovation.

Continue to educate system users.
Educate users regarding increasingly sophisticated phishing and social engineering attacks.

The IoT promises to deliver substantial productivity improvements over the coming decade, but very few IoT assets feature adequate security, something many business leaders likely do not know. As a result, many companies expect to run what they presume are high integrity applications in what they don't realize are low integrity environments.

ABOUT ACCENTURE

Accenture is a global management consulting, technology services and outsourcing company, with more than 323,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.

Contributors

Allan Haughton
Accenture Digital: Digital Mobility/IOT Security Lead

Michael Teichmann
Accenture Security: IoT/IIoT Security Capability Lead

Pablo A. Vaquero
Accenture Security: Security Offering Development —Mobile/IOT Security Lead

References

[1] World Economic Forum, in collaboration with Accenture, Industrial Internet of Things: Unleashing the Potential of Connected Products and Services