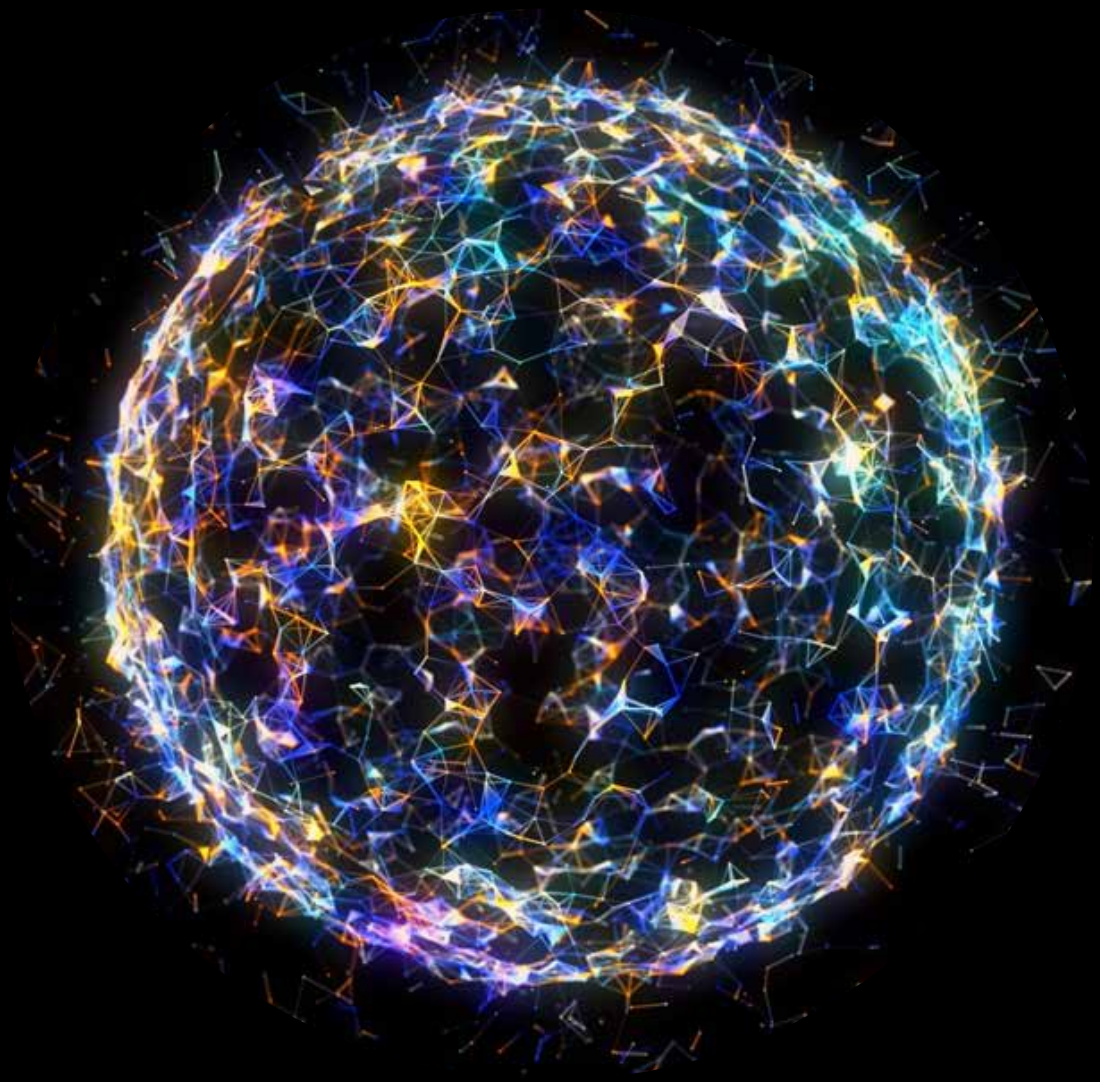
Deloitte.



IoT Security Testing

For private circulation only

February 2019

Risk Advisory

Contents

Overview

Over last few years, IoT devices and IoT enabled solutions have become significantly popular both for consumers and industries. IoT is not just about embedded devices, but also comprises an ecosystem of device hardware, system integration, connectivity, data storage, security, IoT platform providers, IT and communication service providers, and application development. A large number of major technology companies are competing with each other to establish themselves as the market leaders in providing solutions such as home automation, personal assistant, building management, workspace management, parking management, traffic management, healthcare management, etc. These companies are manufacturing and leveraging IoT devices to build solutions for the marketplace, and have been increasing their retail and distribution efforts. Currently, there are more IoT devices connected to networks than the number of human beings on the earth. These IoT devices carry a lot of sensitive data which remain insecure because of the lack of reliable security standards that can be implemented. This could seriously impact our network infrastructure including the security and privacy of consumers. IoT security has become the subject of strong consideration after a number of high profile incidents where a common IoT device was used to infiltrate and attack a larger network, hacking of internet-connected devices, surveillance concerns and privacy.

Therefore, it is important to adopt a holistic approach to secure these IoT devices and connected ecosystems right from the design stage to the ongoing monitoring during their use in the production environment.

Key challenges faced by organisations

Managing a range of complex protocols, interfaces, hardware and standards from around the world can be daunting for an organisation dealing with connected platform products (IoT). Organisations often feel like they are drowning in a sea of different domains such as hardware, firmware, web, mobile, and cloud, which ultimately becomes a roadblock for their usual business.

Typical challenges in IoT security testing faced by organisations are highlighted below.

Increase in Adoption	• Increased adoption and pervasion of IoT & IoT enabled devices across various industries and sectors • Increase in adoption of Cloud based solutions in various industries and sectors
Increase in Security and Privacy Concerns	• Increasing concerns related to security of devices and data privacy in the connected device world • Increase in cyber attacks and targeted attacks on IoT devices and solutions
Inadequate Security Measures	• Lack of inherent security and privacy measures embedded in IoT devices and services • Lack of knowledge of reliable Industry standards and regulations related to IoT device security compliance
Insufficient Expertise	• Lack of knowledge of protocols and interfaces used in IoT devices and products • Lack of professionals with strong expertise in IoT security and secure embedded design principles

How can we help?

IoT security architecture review

Security architecture is the most important pillar of your product in today's world of connected platform. Our IoT security professionals carry out a detailed architecture assessment of IoT solutions that encompasses devices, cloud, APIs, web and mobile applications from security stand point to make the solution more robust.

IoT device / embedded device penetration testing

Hardware and interface connectivity architecture of the IoT/embedded device carries the details of internal components that can determine the breadth and depth of IoT product's attack surface. A small loop hole in the physical security can compromise your complete IoT eco-system.

- Our cyber security professionals carry out an end-to-end security testing from an external hacker prospective on the IoT/ Embedded device to remediate flaws and give you confidence in your underlying embedded hardware.

IoT ecosystem penetration testing

While you are enjoying the success of your newly built connected product in the market, a suspect might take advantage of the unknown weakness of the product.

- Our cyber security professionals carry out an end-to-end penetration testing of the complete IoT ecosystem to remediate flaws and give you confidence in your product.

IoT device firmware security testing

In this connected device world, a suspect might connect to your IoT device/product and it’s ecosystem through a backdoor installed inside the firmware.

- Our cyber security professionals will assess your device's firmware and its upgrade process for any malwares/ vulnerabilities and review boot process from security prospective.

IoT Security Risk Assessment

Do you know that while your IoT sensor based CCTV camera is monitoring any suspicious activity, a suspect might be breaking in your CCTV camera?

- Our cyber security professionals carry out a detailed IoT risk assessment on your IoT sensor based devices to give you confidence on their security.

Security by Design and Privacy by Design for IoT Products & Solutions

Designing secure IoT hardware & Ecosystem is often the first step of designing a product/solution which can identify your limitations and security flaws.

- Our cyber security professionals will help you with their expertise in embedding security and privacy by design as part of Agile and DevOps methodology.

IoT Product Threat Modelling

Complexity of IoT and connected systems in the connected world sits on a very high risk which adversely distracts you from focusing on the entry points that matters.

- Our cyber security professionals will work closely with your team to develop comprehensive threat models of your entire system that can evolve and live with your complete product lifecycle and help you identify and mitigate the most critical issues.

IoT security by design implementation

Do you know that while implementing sensors on industrial machines for predictive maintenance, they can be easily hacked to corrupt or control data without authorisation?

- Our cyber risk professionals will highlight risks in this scenario, support the secure implementation of the connected product, and assist you in focusing on innovation.

IoT data security governance

Do you know data shared among connected vehicles encompasses a large chunk of personal yet highly sensitive information. This information includes driving habits, real-time location, entertainment preferences, and daily schedule of your connected medical fitness device data, such as calories, GPS location, heartbeat, and personal health information.

- Our cyber security professionals will help you gather data to establish a baseline to differentiate between normal aberration suspicious aberration. They will also play a stronger governance role by defining which data to secure to prevent unwanted breaches.

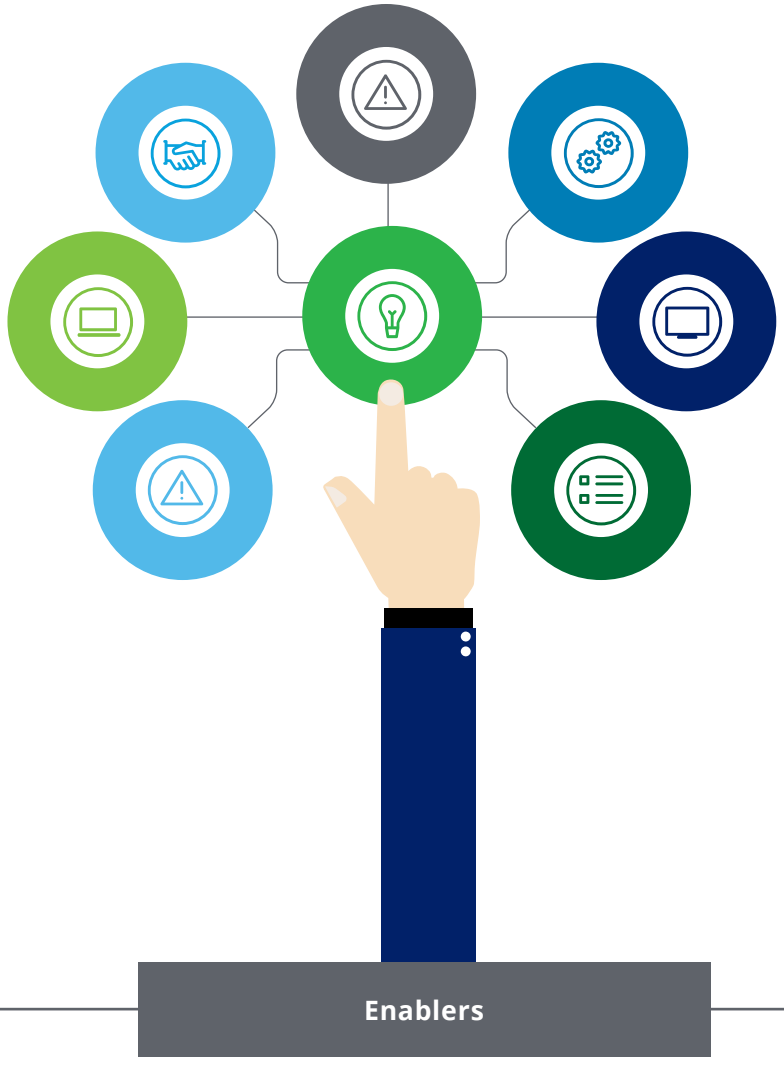
IoT security testing enablers

Cyber Intelligence Centre
Provides updates on IoT specific threats and vulnerabilities

Collaboration
Collaboration with the Deloitte Global team for knowledge and resource sharing

IoT Labs
equipped with tools and hardwares to conduct security testing for clients

Risk Ranking Framework
Suitable for vulnerabilities identified for IoT devices and embedded devices



Subject Matter Experts
Professionals coming with firmware development/ firmware testing / product testing with background and in-depth knowledge of embedded devices

Hardware & Software Tools
Specialised hardware, debuggers and software packages for IoT security testing

Proven Test Cases
Device or platform wise, interface or protocols wise test cases

Benefits of IoT Security Testing

Despite a complex IoT product architecture, IoT security testing (IST) is beneficial for various IoT activities across organisations.

01

Holistic view of current security posture of a product

IST provides the ability to look at the holistic current security posture of a product/device & its ecosystem from an expert's view.

02

Knowledge of vulnerabilities in the IoT product ecosystem

IST establishes its diverse specialists in identifying vulnerabilities/flaws in the circuit design and firmware.

03

Expert guidance throughout IoT product / service lifecycle

Eliminates the need for experts at different stages of the product lifecycle by experienced security professionals, with correct guidance on security of IoT devices throughout the product lifecycle.

04

Specialised IoT security architects

Eradicates the architecture level flaws with the help of secure architecture design principles implemented by our specialized Embedded and IoT security architects.

05

Increased customer confidence and comparative edge

Establishes a strong foundation of security throughout the IoT ecosystem, resulting in increased confidence of the management and investors into developing more secure IoT products.

Contact

Shree Parthasarathy
Partner
sparthasarathy@deloitte.com

Gaurav Shukla
Partner
shuklagaurav@DELOITTE.com

Gautam Kapoor
Partner
gkapoor@DELOITTE.com

Vishal Jain
Partner
jainvishal@deloitte.com

Maninder Bharadwaj
Partner
manbharadwaj@deloitte.com

Santosh Jinugu
Director
sjinugu@deloitte.com

Deloitte.