IoT Test Lab Whitepaper

How to Avoid the Internet of Insecure Things

Executive Summary

This whitepaper reviews the technical challenges facing the Internet-of-things (IoT) industry and explores potential quality and security issues against the current myriad of competing industry standards defining the open specifications, security and connectivity protocols.

> *"… the increasing digitization and automation of the multitudes of devices deployed across different areas of modern urban environments are set to create new security challenges to many industries."*
> Gartner on IoT Security

The paper also outlines the innovative solution that Test and Verification Solutions (T&VS) has established to create an IoT lab and certification process, with an aim to verify the quality and security of IoT products against the latest international standards. The IoT certifications include:

- T&VS IoT Network Certification
- T&VS IoT Security Certification

T&VS offers flexible engagement models based on a global footprint and partnerships with selected equipment suppliers.

Test and Verification Solutions

Engine Shed, Station Approach

Temple Meads, Bristol

BS1 6QH, United Kingdom

t: +44 (0)117 903 1100

e:iot@testandverification..com

twitter: @testandverif

T&VS
Test and Verification Solutions

Introduction

The Internet of Things refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems. Conservative estimates suggest that by 2020 over 200 billion connected sensor devices will be in use. Gartner states that IoT product and services suppliers will generate incremental revenue exceeding $300 billion by 2020.

2. IoT Testing Challenges Quality Assurance & Security

The consumer "Internet of Things" is now a reality. Connected devices create an increased level of intrusion, generating new types and unprecedented quantities of data, raising potential quality and security issues. Some examples are given below.

Quality Assurance (QA)

- The Nest home thermostat recently had a fault where the heating would deactivate and not be turned back on by the homeowner, until Nest provided a patch.
- Petnet is a smart pet feeder with features including intelligent sensor technology. A recent incident saw a third-party server service failure, had been down for around 10 hours and did not have redundancy backups. Causing pet feeds to be missed.
- A smart home smoke alarm fault in 2014 where the alarm could be deactivated by waving at the device, meaning the house was not being monitored for smoke.

Security

- A recent study revealed that over 70 percent of the IoT devices and sensors examined were susceptible to one or more of the vulnerabilities in the OWASP Internet of Things Top 10
- Osram Lightify smart bulbs that security experts found could enable hackers to breach home Wi-Fi networks.
- At Black Hat 2015, security researchers demonstrated how they could hack into a Chrysler Jeep Cherokee's network of IoT devices and sensors and remotely disable the Jeep even as it drives down the highway.
- SecurView cameras used for home security or even baby monitoring had faulty software that let anyone who obtained a camera's IP address look through it and possibly listen as well.

IoT Standards

There is a range of competing current and emerging IoT standards causing fragmentation in the market. Some of the competing IoT standards and consortiums are shown below.

onem2m	Open Interconnection Consortium	Wireless IoT forum
IETF	ZigBee Alliance	Industrial Internet Consortium
ITU	AllSeen Alliance	GSMA
IEEE	AllJoyn	Thread

If you are delivering an IoT solution, how do you know which standard is relevant to your product or is even future proof? T&VS takes an active role and understands the different industry standards, and has

built a certification process against selected key standards, so that any IoT product can be ensured it conforms to the latest industry best practices.

3. Solution – T&VS IoT lab and Certification Process

T&VS IoT lab and certification process allows companies to ensure their products conform against the latest industry standards and rigorous testing best practices.

T&VS IoT Lab

The facility has the capability to re-create real world scenarios in a controlled manner. For example, the lab can simulate a wide range of network conditions including: RF testing, cell handovers, low signal strength, protocol analysis, moving between 2G, 3G and LTE or wifi. The following communication protocols can also be verified:

- Mobile (GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G))
- Wifi (Based on 802.11n (most common usage in homes today)
- Bluetooth (Bluetooth 4.2 core specification)
- BZigbee (ZigBee 3.0 based on IEEE802.15.4)

and other less common connection protocols:

- Z-Wave (Z-Wave is a low-power RF communications technology)
- 6LowPAN (key IP (Internet Protocol)-based technology is 6LowPAN
- Thread (new IP-based IPv6 protocol aimed at the home automation env)
- NFC – (standard ISO/IEC 18000-3)
- SIGFOX – (wide-range technology, in terms of range between WiFi & cellular)
- Nuel – (sub-1GHz band, very small slices of the TV White Space spectrum)

IoT - Network Interfaces & Connectivity – Certification (1)

The T&VS IoT Network certification allows IoT providers to ensure their solution will work against a wide range of networking connection and connectivity protocols. The certification can be tailored to meet specific requirements. The following latest industry guidelines were considered when building the T&VS Network IoT certification including (but not limited to):

- GSMA IoT connection efficiency guidelines
- onem2m connection standards

IoT – End-2-End Security – Certification (2)

The following latest industry guidelines were considered when building the T&VS Security IoT certification including (but not limited to):

- GSMA IoT security standards
- Onem2m security standards
- OWASP Internet of Things Top 10
- Online Trust Alliance's IoT Trust Framework

The T&VS IoT lab can test a range of security conditions and scenarios, including:

- Authentication / authorisation
- Encryption model
- Software / firmware
- Cloud interface
- Physical security.

4. Engagement Model

First step is for T&VS to fully understand your IoT product and deployment model. T&VS would then recommend the required test sets and certification modules. The client then chooses their preferred execution model:

- Equipment and resources are supplied to execute the certification at your premises.
- Execution is performed offshore at our Bangalore IoT lab, with a lead person assigned onshore (in UK) to manage the engagement.
- Access to our facility and equipment for you to execute the testing at our UK IoT lab.
- The facility and resources executed nearshore in our UK IoT lab.

5. Why T&VS IoT?

- The cost for establishing and managing an ongoing, up-to-date, internal IoT enabled test capability is high.
- Flexible resourcing models can help reduce the impact of the ever-changing world of IoT quality, security and standards.
- IoT testing experts can ensure your products conform to the latest quality and security standards and international testing best practices
- Global offices have the capability to create any number of engagement models that are flexible to meet your requirements and budget.

6. Conclusion

There are currently many technical challenges facing the IoT industry. The 'Internet of insecure things' will become reality unless IoT device and solution providers start to ensure the quality and security of their products, which in turn will start the slow process of rebuilding consumer confidence.

> Every animate and inanimate object on Earth will soon be generating data, including our homes, our cars, and yes, even our bodies.
> Anthony D. Williams, in The Human Face of Big Data (2012)

T&VS IoT lab and certification process helps enables companies to ensure their products conform against the latest industry standards and QA & security testing best practices.