P-SCAN SERVICE INTRODUCTION

BY LCIE BUREAU VERITAS

IOT CYBERSECURITY ASSESSMENT
2 MAIN TYPE OF ASSESSMENTS

SECURITY MEASURES ASSESSMENT

Allow to verify the security requirements implemented by the device.

The level of implemented security features and practices depend on the risks associated to the device.

Example: in consumer IoT world

- From Basic to Substantial Advanced Bureau Veritas requirements (5 levels)

Conformity Evaluation

Documentation review
Code inspection
Audits
Functional tests of security requirements

Resistance to Attacks

Known vulnerabilities
Vulnerability scanning
Fuzzing Test
Robustness tests
Penetration testing

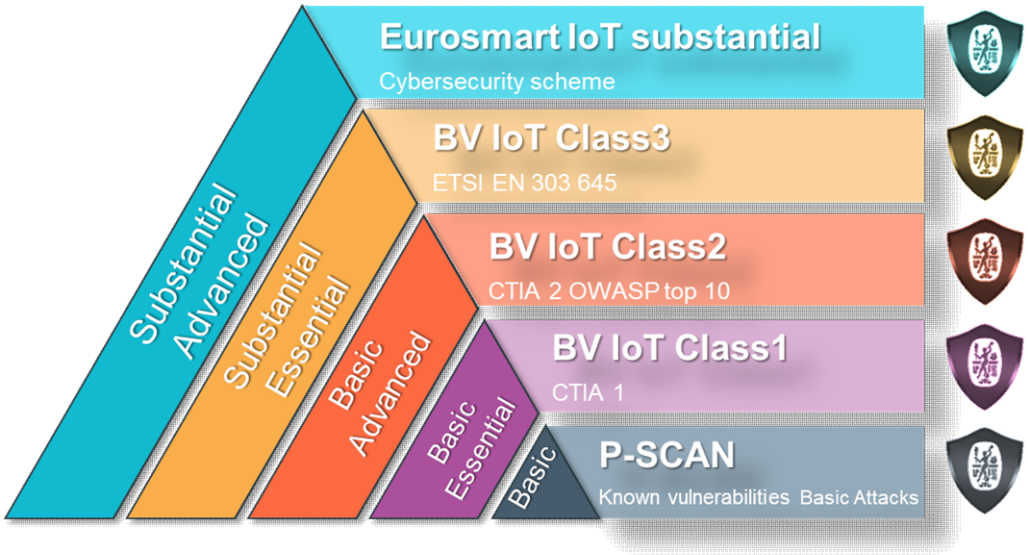
Allow to verify how resistant is the device to cyber attacks.

The level of evaluation simulate the level of the attackers:

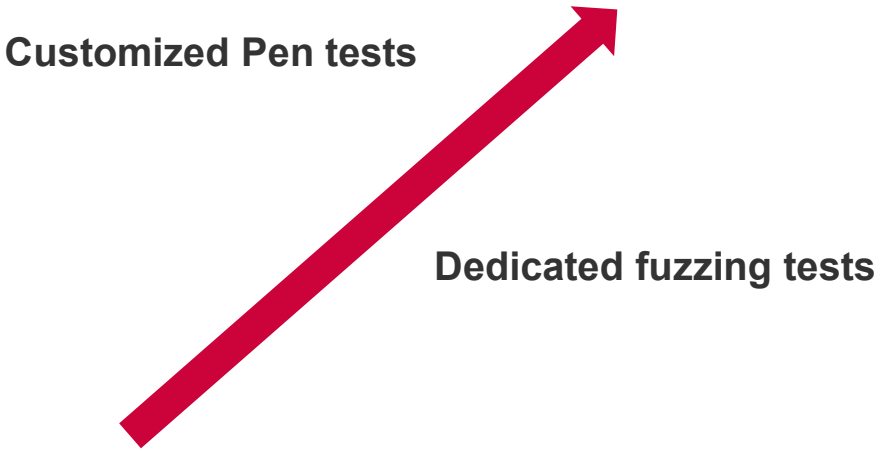
- From Basic : Known vulnerabilities; scanners
- To High : advanced pen tests

IOT CONSUMER MARKET
CONFORMITY VS RESISTANCE TO ATTACKS SERVICES

Bureau Veritas
Conformity assessment pass



Bureau Veritas
Resistance to attack path



The presence of known vulnerabilities on products is the starting point for both Conformity assessment and Resistance to attack approaches

VULNERABILITIES MANAGEMENT IS CRITICAL FOR IOT PRODUCTS

The vulnerability Management during the life cycle of a product is a high priority for cybersecurity regulations and certification schemes. e. g.

- ✓ Responsibility to ensure that no known vulnerabilities are included at product launch
- ✓ Need to have a vulnerability disclosure process in place while the product is available on the Market
- ✓ Capability to deliver security patches when new vulnerabilities are discovered

=> Remote access Vulnerabilities are even more important due to possible remote attacks

Coordinated vulnerability disclosure from the Basic Level

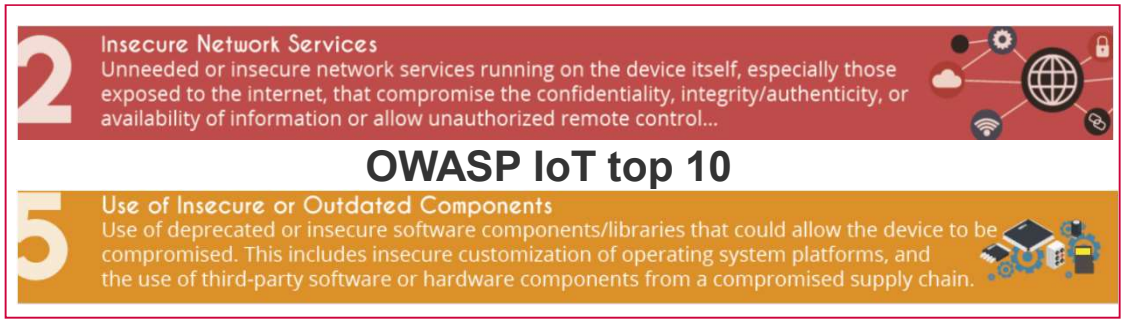
Cyber Security ACT

Keep SW updated, Implement a vulnerability disclosure policy, authentication & cryptography.

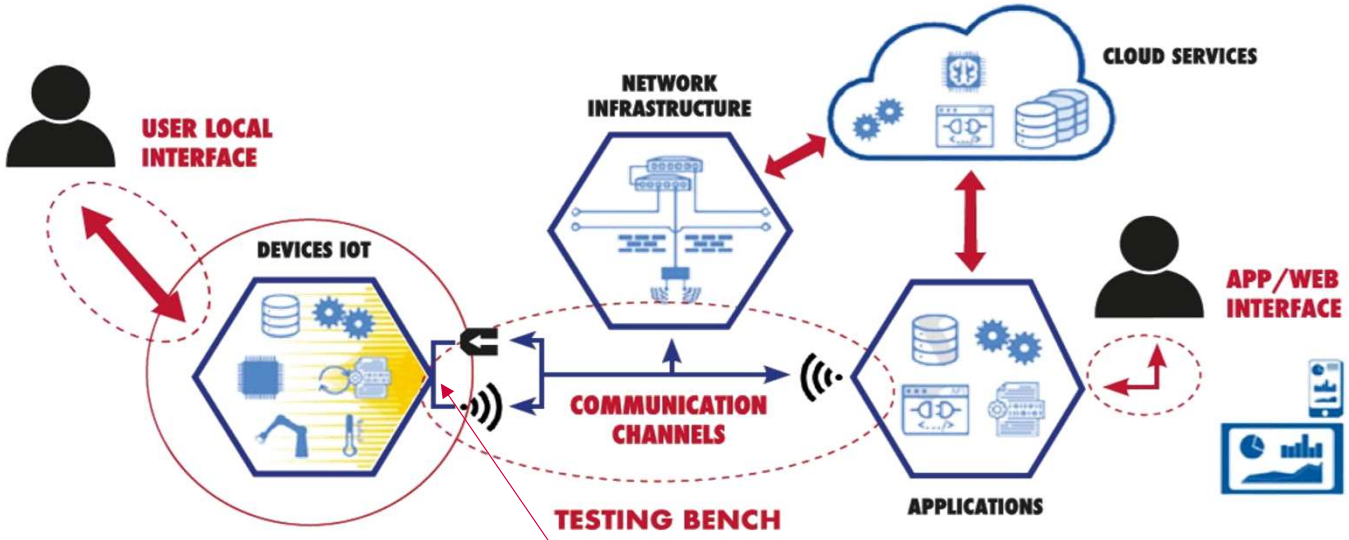
2) Implement a vulnerability disclosure policy
3) Keep software updated

UK code of conduit

5) Communicate securely &
6) Minimise exposed attack surfaces



IOT DEVICE SERVICE SECURITY
RESPONSIBILITY OF THE IOT DEVICE



Device Liability :

The responsibility of an IoT device manufacturer is to make sure that he has implemented the necessary measure to avoid security (incl. cybersecurity) defect. Especially he needs to follow the State Of The Art (SOTA) in cybersecurity matter.

Remote Access :

Making sure that Remote access interfaces are “vulnerability free” is the most important

P-SCAN SERVICE PRINCIPLES

P-SCAN is a Framework to detect vulnerabilities & protocol implementation defects for communication interfaces (Zigbee, Bluetooth, Wifi…) and TCP/IP Web interface

Automated

- Cost reduction
- Full reproducibility

Flexible

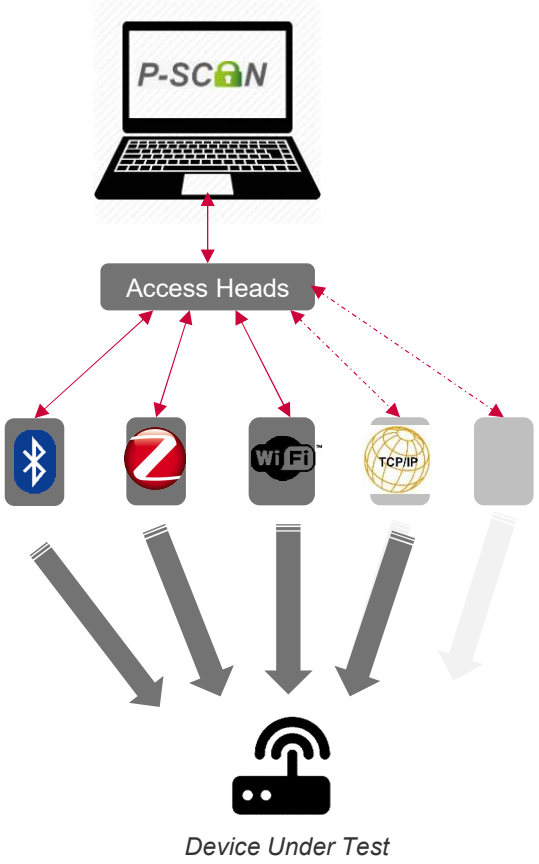
- Interaction with the communication interfaces of the product ⇔ Access heads
- Test libraries are enriched based on new vulnerabilities (CVE, Publications)
- Easy to plug new access head for additional protocols

Simple

- Minimum information is necessary from the device manufacturer « BlackBox Approach»

Certificate

- In case of successful assessment a certificate **Basic**  is delivered



P-SCAN BUREAU VERITAS TOOL
Vulnerability scanner for Low Layers

In the Cyber security world existing tools, software and scanners are IT focused.

They are not suitable for this IoT consumer product. Indeed connected objects often use simplified Operating System (OS) and communication protocols different from those used in IT

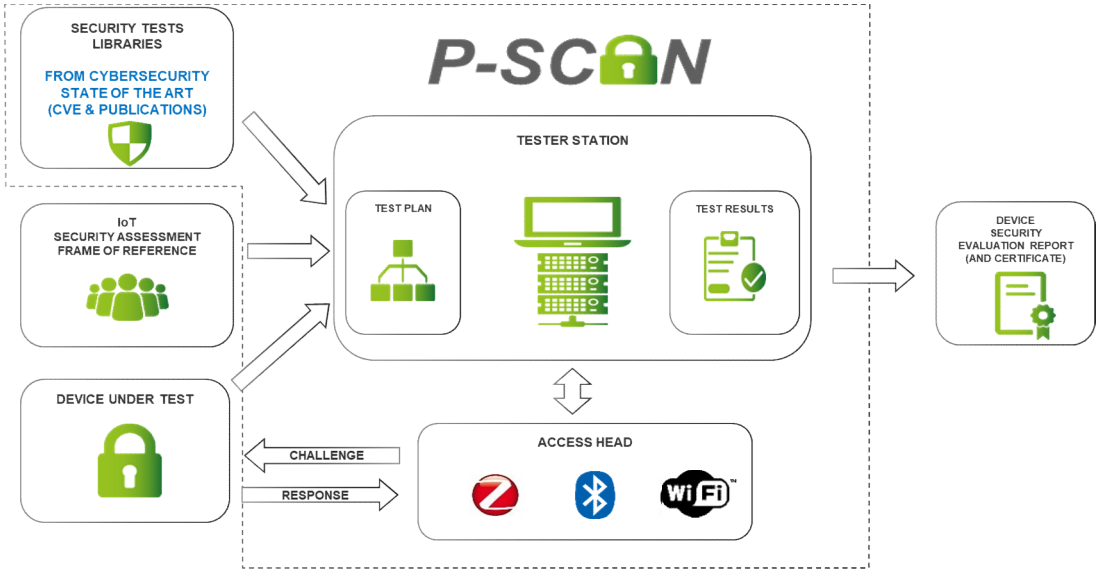
Especially, not automatic vulnerability scanner is available for Layer 1, 2 and 3 of the OSI. Existing are tools on communication layers only perform network scanning and / or limited Man in the Middle attacks.

Integration

BUREAU VERITAS

STRATEGIC PARTNERSHIP

leti cea tech



In order to cover this GAP

Bureau Veritas did create a vulnerability scanner

- For low layer communication technologies
- Applicable to the consumer IoT Market
- Cover Wi-Fi, BLE and ZigBee

LCIE

P-SCAN BUREAU VERITAS TOOL
Test Case Sample

WIFI#6 - FCH_CKM: TKIP-GTK Reinstallation Attack in the 4-way Handshake

FIELD	DESCRIPTION
Name	TKIP-GTK Reinstallation Attack in the 4-way Handshake
Description	This test case aims at exploiting a vulnerability present in the 802.11i amendment allowing the Group Temporal Key (GTK) to be reinstalled during the 4-way handshake using the TKIP protocol.
Test scenario	In this test case, the access head acts as an AP and performs the 4-way handshake first to install the GTK and then send ARP requests to increase the IV. Then, it reinstalls the GTK with IV=0 by sending again a message 3 and check whether the DUT replies with a message 4. Finally the access head replays the previous ARP request and checks that the DUT does NOT send an ARP response.
Expected behavior	The DUT shall not reinstall the GTK when receiving the second Message 3.
Success oracle	Success if the DUT does not reuse previously used nonce.
Related weaknesses	CWE-323: Reusing a Nonce, Key Pair in Encryption
References	• IEEE Std 802.11™-2016 • CVE-2017-13078 • wpa_supplicant v2.3 • see https://github.com/kristate/krackinfo
DUT/SUT prerequisites	DUT is in BSS station mode. DUT supports IEEE 802.11i amendment
Solutions and mitigations	Implement IEEE P802.11 countermeasures published on 2017/10/26 entitled "Addressing the Issue of Nonce Reuse in 802.11 Implementations".

WIFI#1	FCH_CKM: TKIP-PTK Reinstallation Attack / Delayed Plaintext Message 3
WIFI#2	FCH_CKM: TKIP-PTK Reinstallation Attack / Consecutive Plaintext Message 3
WIFI#3	FCH_CKM: TKIP-PTK Reinstallation Attack / Consecutive Encrypted Message 3
WIFI#4	FCH_CKM: TKIP-PTK Reinstallation Attack / Plaintext and Encrypted Message 3
WIFI#5	FCH_CKM: TKIP-GTK Reinstallation Attack in Group Key Handshake
WIFI#6	FCH_CKM: TKIP-GTK Reinstallation Attack in the 4-way Handshake
WIFI#7	FCH_CKM: TKIP-IGTK Reinstallation Attack in Group Key Handshake
WIFI#8	FCH_CKM: TKIP-IGTK Reinstallation Attack in the 4-way Handshake

Wifi Crack attack are well known wifi attacks

- P-SCAN do not implement only the basic scenarios but also corner cases

P-SCAN
Web interface Vulnerabilities

Web interfaces scanners have been used for a while in the industry especially in the IT world.
They are also useful to check vulnerabilities of these same interfaces when TCP/IP services are made available by the IoT product.
Bureau Veritas is using Nessus to check the Web interface when available on the product

D.U.T with Web I/F

Examples of vulnerabilities

11801 - HTTP Method Remote Format String
41028 - SNMP Agent Default Community Name
50686 - IP Forwarding Enabled
58751 - SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)
42263 - Unencrypted Telnet Server

For vulnerabilities identified on the device criticality is indicated based on the CVSS score

P-SCAN
Service summary

Example of Applicable Interfaces for a Smart Watch

D.U.T

P-SCAN Service will check vulnerabilities on the IoT device amongst the BLE, Wi-Fi, ZigBee and the Web interface depending on the available interfaces on the device.

P-SCAN is a Black-Box approach providing an immediate feedback on the communication channel vulnerabilities that are present on the device an can be used by attackers.

A test report is provided covering all interfaces verified.

In case of successful verification on the low layers interfaces (BLE, WiFi, ZigBee) and no TCP/IP vulnerabilities with critical or High severity :

A certificate **Basic** is delivered


BUREAU VERITAS
1828
L C I E
THANK YOU