Bringing trust to the internet of things

IoT Security Evaluation

Your best companion to face IoT cyber-security threats and their consequences

RED ALERT LABS
IoT Security

IoT requires a feasible distributed trust strategy to overcome the drawback of existing security models. Applying trust to IoT is no longer about designing and developing individual models, but is about how to provide a pool of security models covering the whole IoT infrastructure which includes IT and physical infrastructures (devices, sensors, etc.).

Our IoT security evaluation laboratory will allow you to achieve this latter by performing a full examination of your products, architectures or systems going from Chip to Cloud based on a unique, specific and methodic expertise in all IoT verticals.

Manufacturing · Industrial · Transportation · Housing · Education · Communication

Entertainment · Healthcare · Finance · Oil & Gas · Retail · Law enforcement

Unique and specific IoT security evaluation approaches //

Red Alert Labs IoT security laboratory will help you in:

Determining the degree of compliance and assurance level of your products, infrastructure or systems with a stated security model, security standard, or specification

Providing a proof of the level of security based on our unique expertise in the IoT domain for all verticals in an independent approach

1) IoT Security Assurance Level & Compliance

Basic (Consumer/Enterprise)	**Substantial** (Consumer/Enterprise/Industrial)	**High** (Industrial/Critical)
• highly efficient • fast (1-5 days) • focuses on common baseline of security requirements • addresses specific security aspects of IoT products/solutions • covers common attacks and known IoT vulnerabilities	• highly efficient • fast (5-15 days) • focuses on business-line risks defined for each Security Profile • considers the threat model relevant to a type of IoT product/solution and its specific operational environment • covers a wider panel of IoT attacks and vulnerabilities	• a highly efficient and comprehensive approach • supports you during all the stages of the evaluation process • focuses on specific security profiles • covers state-of-the-art attacks and unknown IoT vulnerabilities

Red Alert Labs S.A.S.
Paris Area, 3 rue Parmentier,
94140 Alfortville, France

www.redalertlabs.com
contact@redalertlabs.com
+33 9 53 55 54 11

Bringing trust to the internet of things

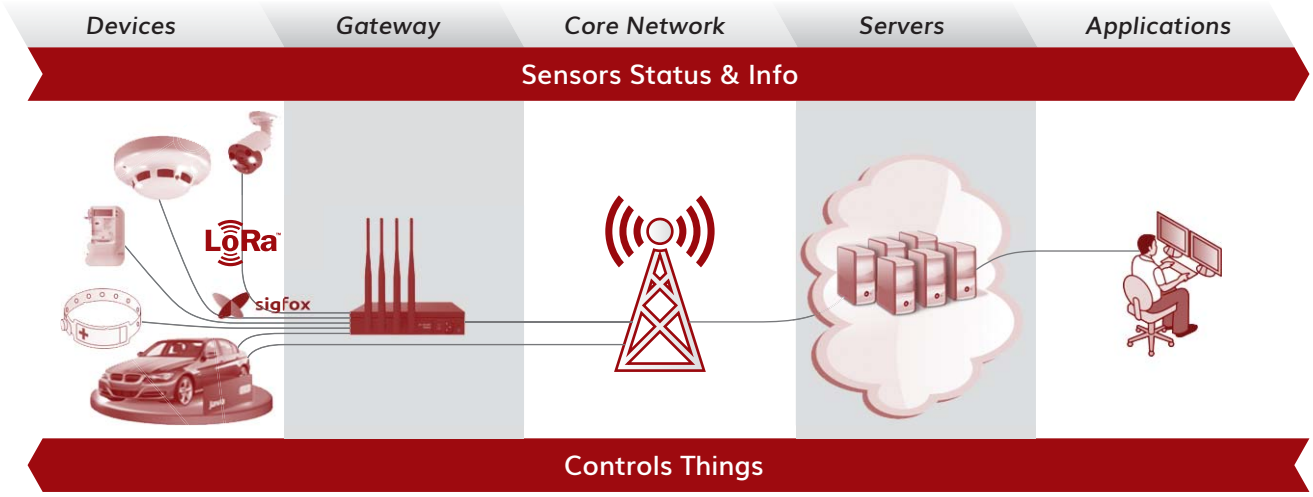
EUROSMART
IEC 62443
OWASP
GSMA
CSPN
IoTSF
ETSI
CC

2) IoT Independent Security Approach

Black Box	Grey Box	White Box
• simulates real world scenarios • attacker has no knowledge of the interior workings of the product, infrastructure or system • partly exhaustive & least time-consuming • fast identification of the first level of security • fast patching	• simulates real world scenarios • attacker has limited knowledge of the internal workings of the product, infrastructure or system • exhaustive & partly time-consuming • identification in a semi-comprehensive way the level of security • fast patching	• detailed investigation of internal logic and structure of the code of a product, an application or system while covering a wider area • allows businesses to be on their highest guard • most exhaustive & time-consuming • identification in very comprehensive way the level of security & design errors • detailed security patching

We secure all your IoT environment //

Based on several types of penetration testing methods, our evaluation services will provide details on exploitable vulnerabilities (in a prioritized, tangible manner) of your products, infrastructures and systems from Chip to Cloud while covering the device, service, application and network domains.



1) Hardware Analysis & Assessment

- IoT device reverse engineering
- IoT device disassembling
- Mapping out components
- Uncovering known and unknown vulnerabilities

2) Software Analysis & Assessment

- Encryption analysis and obfuscation techniques
- Reverse engineering firmware binaries
- 3rd party libraries and SDKs
- Debugging binaries to gain sensitive info

3) Signal and Communication Protocol Enumeration and Analysis

- Device infrastructure and protocols (Zigbee, Wifi, etc.)
- Communications captures (Radio, Bluetooth, etc.)
- Analysing cryptographic protocols
- Analysing interaction with external components

4) Mobile Applications

- Data storage (ex: sensitive data)
- Transport data (ex: information disclosure)
- Authentication/Authorization (ex: certificate validation)
- Session management (ex: resiliency)
- Data validation (ex: through IPC channels)

Red Alert Labs S.A.S.
Paris Area, 3 rue Parmentier,
94140 Alfortville, France

www.redalertlabs.com
contact@redalertlabs.com
+33 9 53 55 54 11