Towards an architecture for safe secure and privacy preserving IoT

Bill Karakostas, VLTN

CHARIOT WORKSHOP
Rome, 11 October 2018
CHARIOT?

[Image of a cow pulling a cart, with a red prohibition sign over it.]
CHARIOT?

This is the kind of CHARIOT we have in mind!
Turbocharging IoT Safety, Security and Privacy!
Agenda for the Presentation

- Safety, Security and Privacy related IoT Risks
- The CHARIOT vision
- An Architecture for Safe, Secure and Privacy Preserving IoT
- An IoT practical demonstration video to trigger ideas and elicit responses
- Wrapping up
IoT can introduce Security and Privacy Risks to User Organisations

**Security Risks:** Insecure IoT can be used by malicious actors as a computational platform to launch cyberattacks (such as Distributed Denial of Service-DDOS) to other systems including those of the user organisation.

**Privacy Risks:** IoT data carrying private content can fall into the wrong hands if not properly secured, incurring privacy violations (e.g. user personal data and other privacy sensitive information)
Security risks inherent in IoT

Risks of Open Environment - Physical Exposure
IoT systems are out in the open usually and vulnerable to physical attacks.

Wide Range of Security Capabilities:
A mixture of systems and devices with diverse security capabilities and practices from stringent to non-existent! Resource Constraints among Devices. Devices can be unprepared or unable to adequately protect themselves. For example, many IoT devices cannot implement strong cryptographic functions and thus vulnerable to spoofing and replay attacks.

Remote Management: It offers opportunities for adversaries to launch various network-based attacks, and makes the detection and mitigation of these attacks more difficult and costly.
Invalid IoT data (i.e. deliberately or accidentally altered), can cause the industrial controller systems to carry out unsafe functions, creating risks for assets and human lives.
What the industry recommends*

*Develop specialized *integrity monitoring* tools for industrial control components.*

*Incorporate encryption and authentication techniques in future systems*

*Johnson, R.E.; , "Survey of SCADA security challenges and potential attack vectors," Internet Technology and Secured Transactions (ICITST), 2010 International Conference*
The CHARIOT ‘Solution’

• The CHARIOT ‘Solution’ represents a best of breed research solutions that will be specific to safety security and privacy concerns that are unique to IoT.

• It addresses the integrity of IoT data both at the deployment and configuration stage and at the operational stage (runtime).

• These include Cognitive systems, sensor monitoring, the Blockchain, real time Fog and Cloud Big Data analytics.

• The project will demonstrate its approach in a number of key application domains (buildings management, rail safety, physical& cyber security monitoring of airports) and will develop a best practice architectural guide/methodology for making IoT more trust-worthy, that applies also to other industrial domains.
Introducing the CHARIOT Concept

IoT Gateway

Configuring-authenticating-filtering

Installation time-Runtime

THE CHARIOT SYSTEM

IoT Network

sensors

sensor data

Firmware validation/Blockchain

CHARIOT ‘Engines’

Trusted sensor data

Industrial system Gateway

Industrial system
A video demonstration follows now!
Some interesting points (hopefully) raised by the video

Have you spotted any?
Knowing the characteristics of the sensors you are connecting…

….too many sensor types, many of unknown Provence, not fully tested (hardware, firmware, software,…)

Securely connecting to Cloud servers

Are your IoT data securely transmitted to the Cloud?
Are they securely stored once there?

https://us.io.seeed.io/v1/node/GroveAirqualityA0/quality?access_token=0382563496d030ddc572827b2df6e7e2

Get the analog reading of air quality. The air quality sensor is designed for comprehensive monitoring over indoor air conditions. It’s responsive to a wide range of harmful gases, such as carbon monoxide, alcohol, acetone, thinner, formaldehyde, and so on. Due to the measuring mechanism, this sensor does not output specific data to describe the target gases’ concentrations quantitatively. But it’s still competent enough to be used in applications that require only qualitative results, like auto-refresher sprays and auto-air cycling systems. If exposed for a long time to pollution, it will be damaged.

Request method: GET

Returns:
- HTTP 200 { "quality": [int value] }
  - quality: int value, analog reading of this sensor, please use the data as a comparative quantity, because it is a qualitative result.
- HTTP 400 { "error": "failure reason here" }
Firmware updating

Can you trust the firmware your sensor is running?

Can you be sure that it runs the latest firmware?

Do you have a secure method to ensure that only authorised/latest firmware is uploaded to your sensor (remotely) – and only that?
Wrapping up…

IoT brings potentials for significant productivity gains to organisations… but also significant safety, privacy and security risks.

CHARIOT introduces a multifaceted approach to tackle the above problems as singular solutions are unlikely to have the needed impact.

CHARIOT therefore tackles several critical IoT Problems:

• At installation/configuration time: ensuring sensors are connected and managed by IoT gateways operating encryption, digital keys and firmware version management
• At runtime, authenticating sensors with help from Blockchain technology
• At runtime, inspecting, analysing and filtering sensor data to ensure that only trusted sensor data reach the industrial system.
• Employing machine learning/analytics that operate both in the local Fog for fast responses and on the Cloud for learning sensor data patterns from huge volumes of sensor data.

CHARIOT is therefore the intelligent ‘shield’ that stands between the IoT system and the critical IT assets of organisations, and ensures that IoT is a friend- not a foe!
Thank you for listening!
Any questions?