



University "Politehnica" of Bucharest
Doctoral School of Electronics, Telecommunications and Information Technology



RO-LCG 2015 Conference

Analysis of the Security Solutions Implemented in Current Internet of Things Platforms

Ștefan-Ciprian ARSENI

Octavian FRATU

Alexandru VULPE

Simona HALUNGA

George SUCIU



Agenda

IoT Concept

IoT Architecture

Current security of
several IoT Platforms:

HomeKit
(Apple)

IoTivity
(Intel)

AllJoyn

Sen.se

Xively

Conclusions

Internet of Things - concept

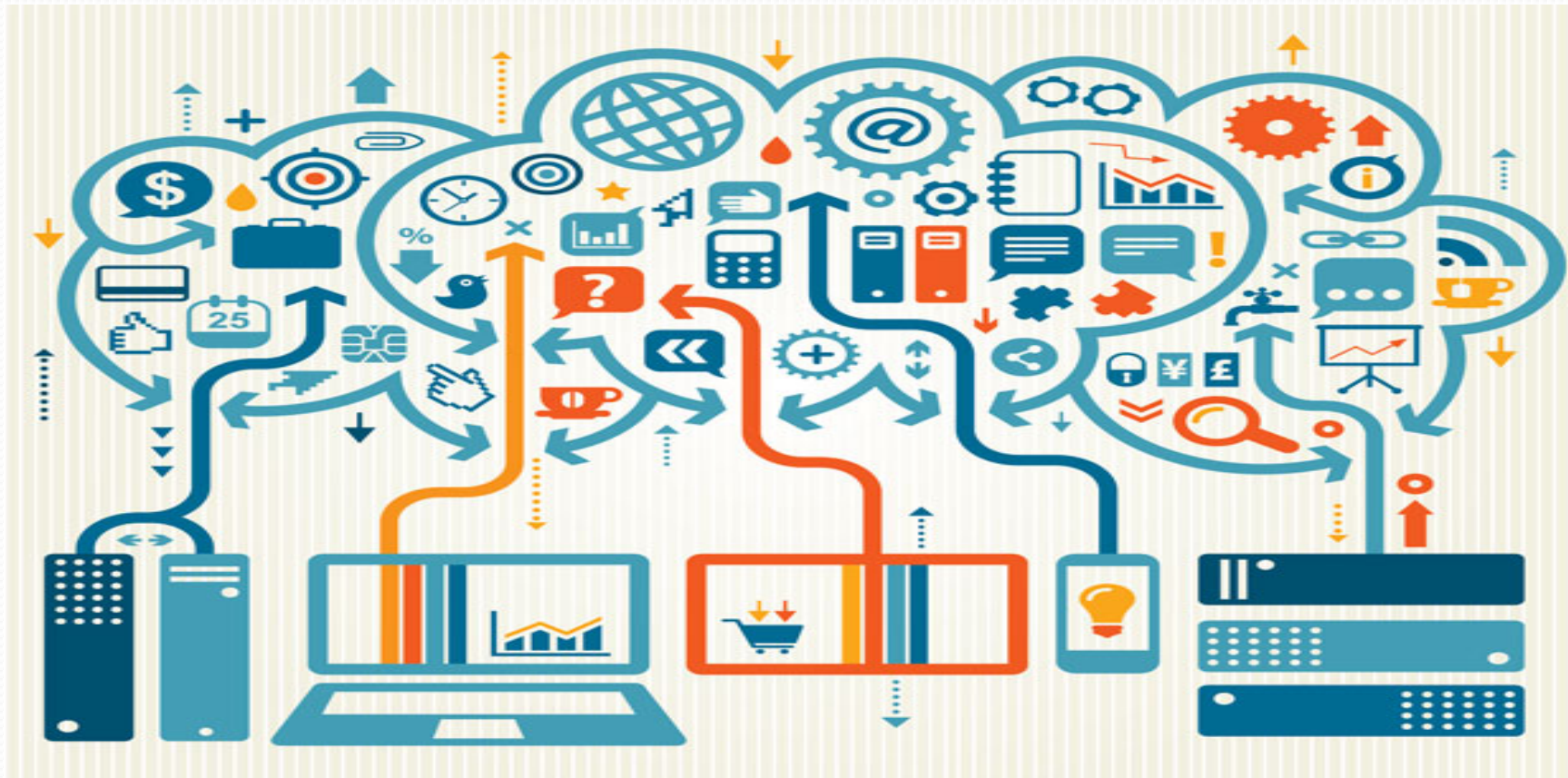
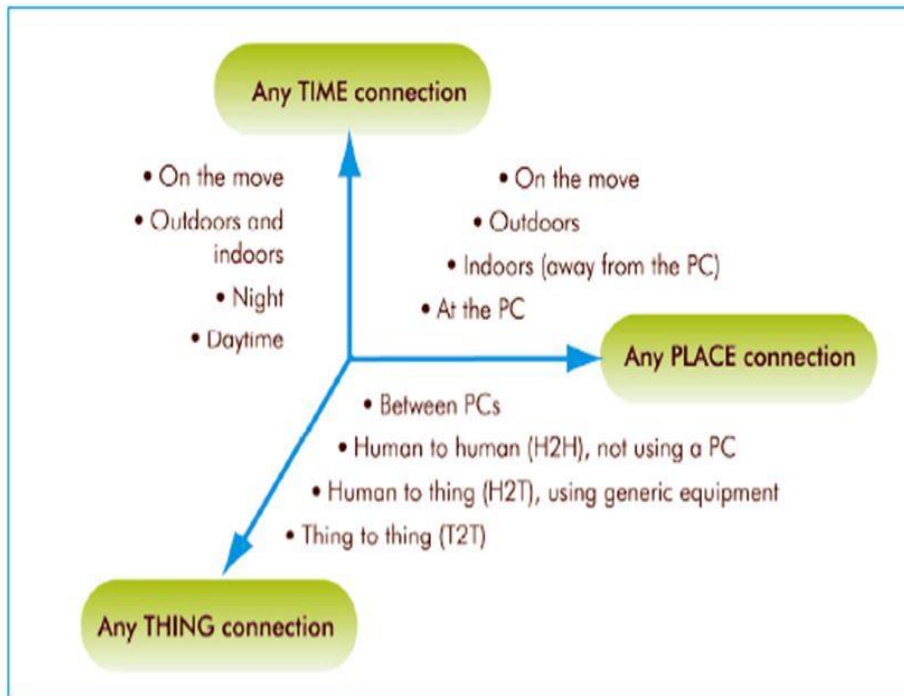


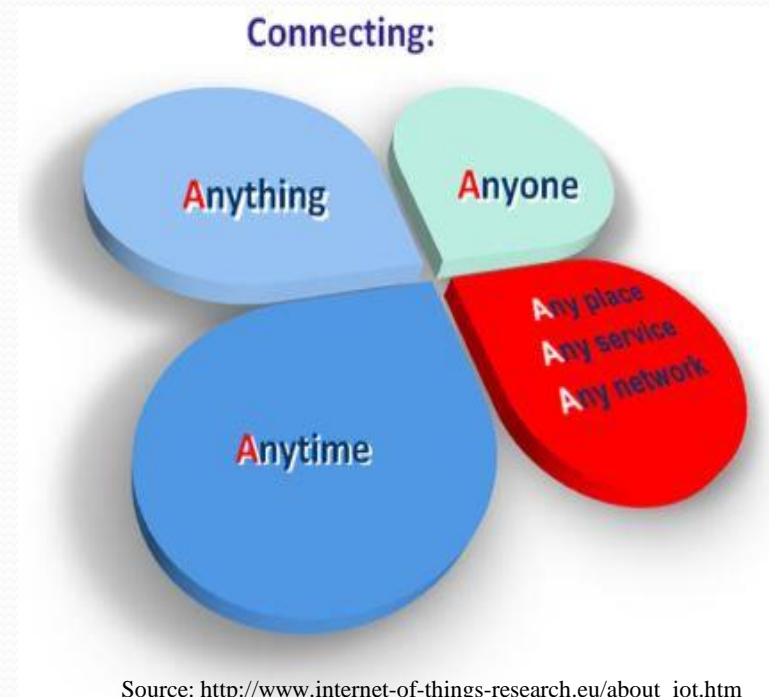
Image source: <http://www.rfcode.com/data-driven-data-center/bid/351906/An-Internet-of-Things-Future-is-Already-Here-What-Does-it-Mean>

- Technology-driven society
- Interconnected world

Internet of Things - definition



Source: ITU, adapted from Nomura Research Institute.



Source: http://www.internet-of-things-research.eu/about_iiot.htm

Internet of Things - architecture

- Domain Model

 - Implements IoT concepts

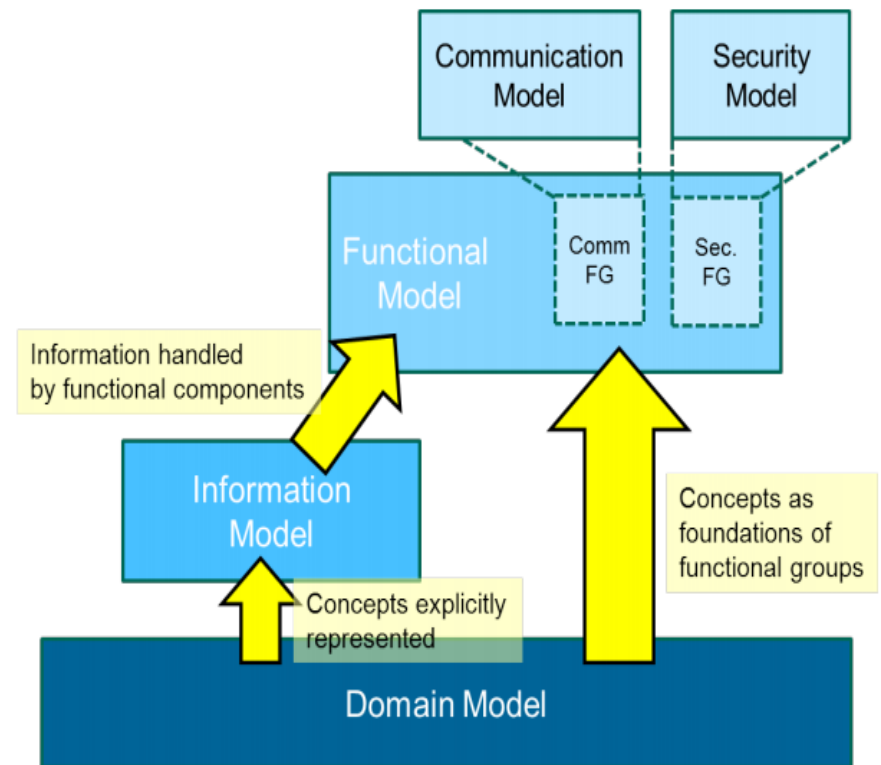
 - Creates the connections

between concepts

- Information Model

 - Defines the data structure

(attributes, relations)

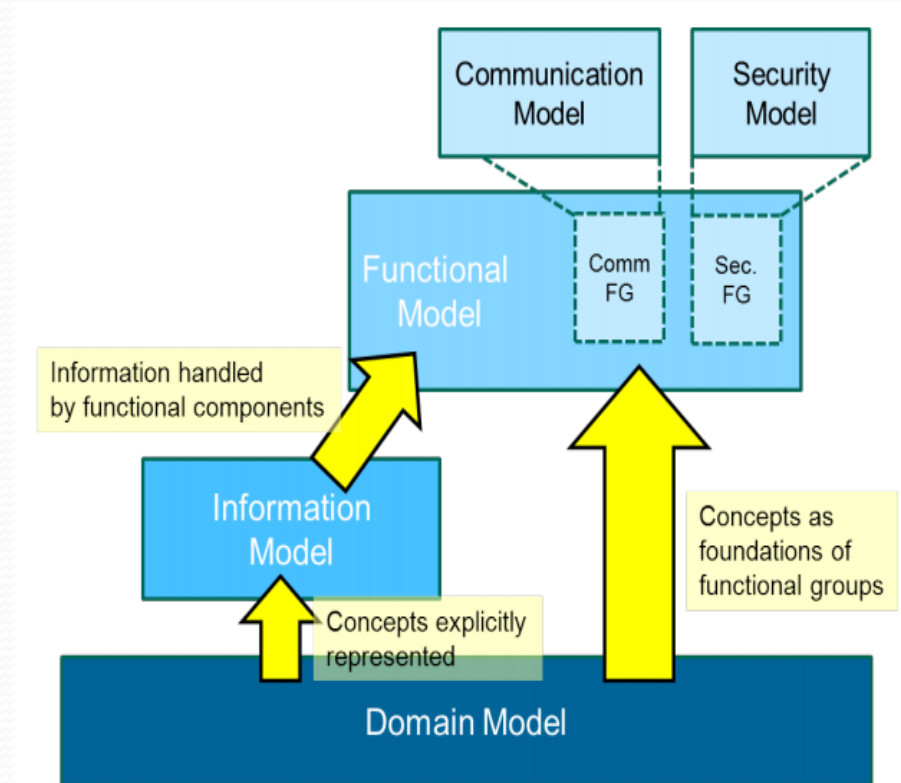


Source: Deliverable D1.3 of the project „Internet of Things – Architecture (IoT-A)”, available at: <http://www.iot-a.eu/public/public-documents/documents-1>

Internet of Things - architecture

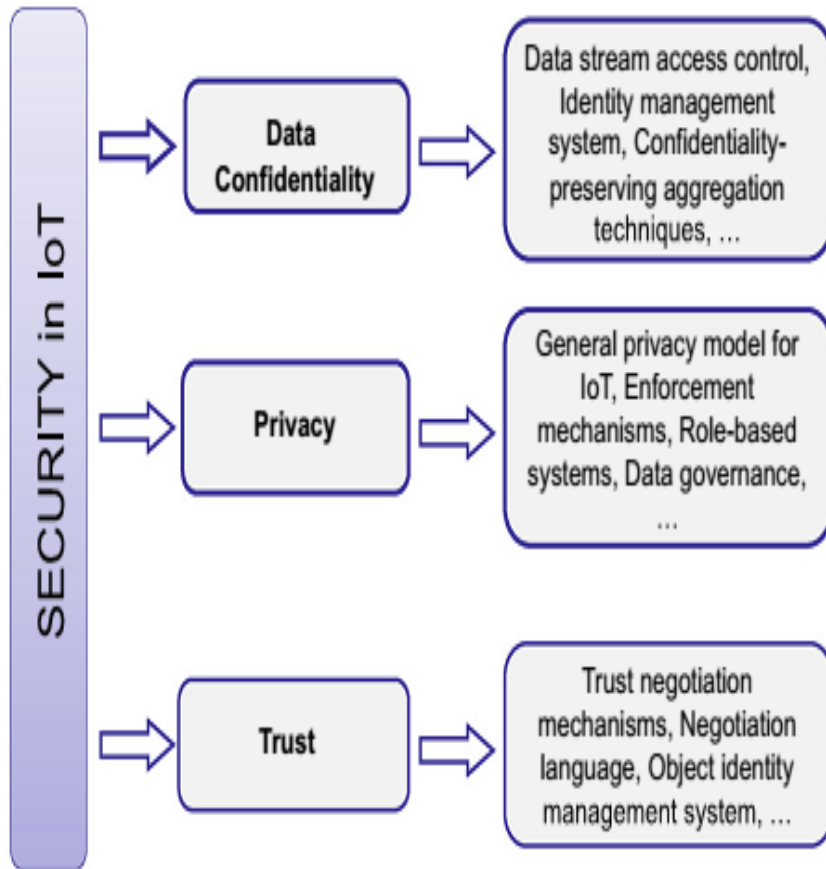
- Functional Model

- Functional Groups
- Communication Model
- Security Model



Source: Deliverable D1.3 of the project „Internet of Things – Architecture (IoT-A)”, available at: <http://www.iot-a.eu/public/public-documents/documents-1>

Internet of Things - security



Source: Deliverable D1.3 of the project „Internet of Things – Architecture (IoT-A)”, available at: <http://www.iot-a.eu/public/public-documents/documents-1>

- Key factors:
 - Scalability and heterogeneousness of platforms
 - Data anonymity
- Security → critical step in the process of extending IoT on a large scale

Internet of Things - Platforms

– HomeKit –

- Designed by Apple, is like a new network protocol → allows users to control home appliances or access certain services
- Integration into a smartphone → diversity of applications.
- Allows grouping of resources based on common features.



Internet of Things - Platforms

– *HomeKit (security)* –

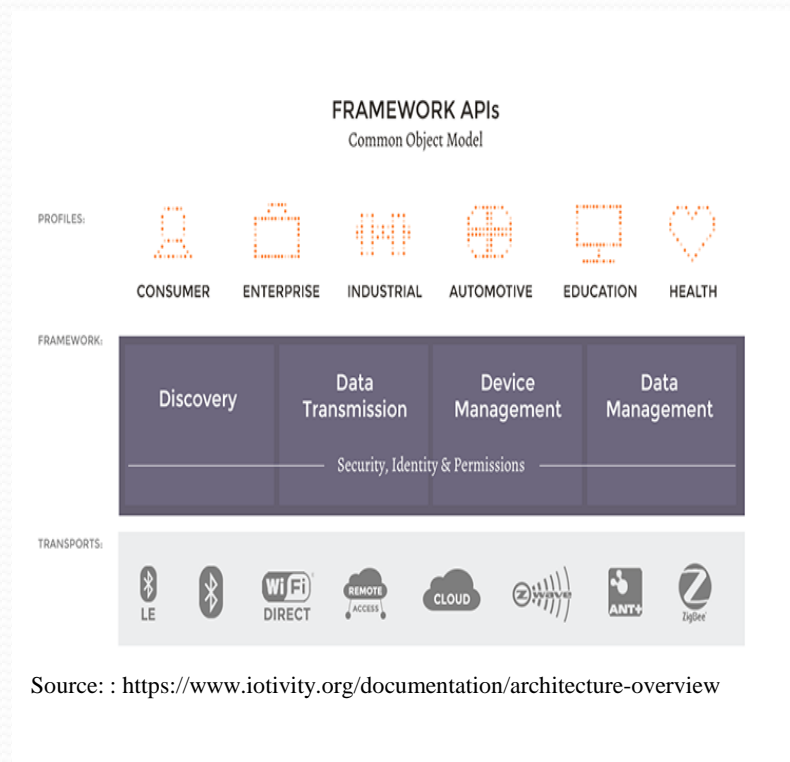
- Secure pairing of devices → ensures users they are the only persons controlling the device.
- Scene definition → control over multiple devices in the same area.
- Problem: weakness of the central controller.



Internet of Things - Platforms

– *IoTivity* –

- Developed by Intel → currently proposed as a good architectural model by the Open Internet Consortium
- Implements only CoAP (Constrained Application Protocol) and not also HTTP, as application level protocol.
- Open-source project focused on security and simplicity → projected rapid development and adoption



Source : <https://www.iotivity.org/documentation/architecture-overview>

Internet of Things - Platforms

– *IoTivity (security)* –

- Project under development → in current form it doesn't support complex security mechanisms
- Still, it has the possibility of integrating security methods through a variation of the “tinydtls” protocol, that needs to be activated before integration

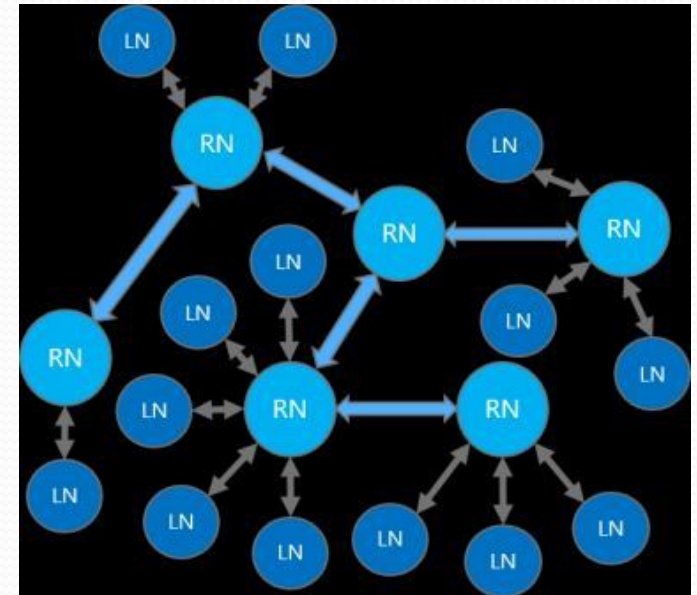
FRAMEWORK:



Internet of Things - Platforms

– AllJoyn –

- First designed by Qualcomm, now driven by AllSeen Alliance (cross-industry consortium composed of more than 185 companies such as Microsoft, Sony or LG).
- AllJoyn devices describe their capabilities via service interfaces on a virtual bus.
- Two types of nodes:
 - Routing Nodes (RN) → talk to any node
 - Leaf Nodes (LN) → talk to RN or LN through RN





Internet of Things - Platforms

– *AllJoyn (security)* –

- Similar to other frameworks → implements security at application level only, leaving the other levels unattended.
- At connection an authentication demand is triggered → various options:
 - PIN codes;
 - PSK (Pre-Shared Cryptographic Key);
 - ECDSA (Elliptical Curve Digital Signature Algorithm).
- After a successful connection, the confidentiality and integrity of data transmitted is assured by integrating cryptographic algorithms (such as AES).

Internet of Things - Platforms

– *Sen.se* –

- First designed for industrial use, now available to regular users
- Infrastructure that continuously collects data received from connected devices.
- Designed to handle a huge amount of incoming data.
- Platform as a Service





Internet of Things - Platforms

– *Sen.se (security)* –

- Ensures only the authentication of devices.
- Does not protect the entire communication plan.
- Authentication of devices is being done based on a Sen.se key, that is specific and unique to each user.
- Problem: Sen.se key is stored in online user profile → level of user data protection = level of IoT platform protection.

Internet of Things - Platforms

– Xively –

- IoT Platform focused mainly on companies and the assurance of business processes.
- Offers users specialized processes for
 - Managing and defining devices;
 - Controlling the deployment lifecycle or products.





Internet of Things - Platforms

– *Xively (security)* –

- Ensures security by providing a private cloud infrastructure for the protection and availability of data.
- Even though data exchanges are done via Web Services, the platform integrates the HTTPS protocol.
- For securing the device authentication process, there are used some API Keys, specific for each user.
- Allows a dynamic alteration of access rights over a resource.
- Problem: API Keys accessible in the user online profile.

Conclusions

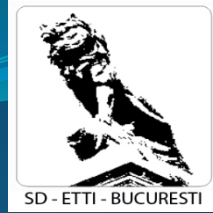
- A good security implementation in a platform ensures that users would be fully satisfied with their experience and assured that all data exchanged between devices is secure.
- Due to the constraints of embedded devices/sensors, stronger security mechanisms are harder to be implemented → users need to choose between local IoT platforms or ones that are provided as a service.

Acknowledgment

The work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU/187/1.5/S/155536.



University “Politehnica” of Bucharest
Doctoral School of Electronics, Telecommunications and Information Technology



Analysis of the Security Solutions Implemented in Current Internet of Things Platforms

Thank You!

Ștefan-Ciprian ARSENI

Octavian FRATU

Alexandru VULPE

Simona HALUNGA

George SUCIU





University "Politehnica" of Bucharest
Doctoral School of Electronics, Telecommunications and Information Technology



Contact:

stefan.arseni@radio.pub.ro