RSAConference2016

Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

SESSION ID: CMI1-R08

Managing Security in Internet of Things Using API Management Platforms

Suhas Desai

VP – Digital Security, Aujas

@desai_suhas

#RSAC

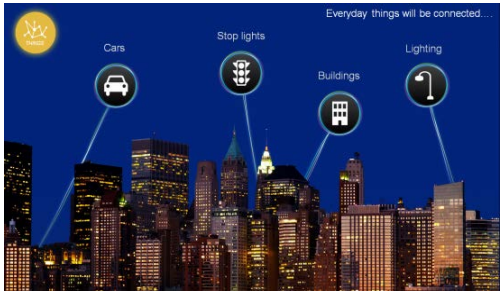
Agenda

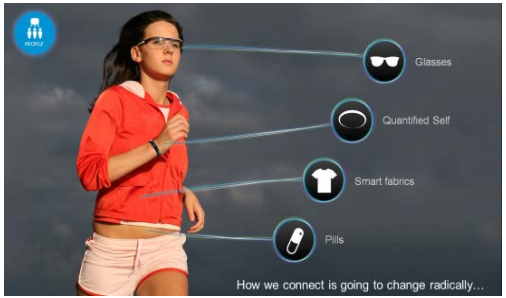
- What is digital and it's changing landscape
- How Internet of Things Eco-system works?
- What are security threats to IoT, consumer apps and Cloud
- What are common issues during API integration with IoT
- How to secure IoT eco-system through secure API integration

Digital Everywhere

Digital usage driving businesses to adopt and innovate “connected things”

Phytech has teamed up with ADAMA Agricultural Solutions to sell its plant-alert system to farmers in North and South America.





Source: Cisco Blog
Beyond Things: The Internet of Everything Takes Connections to the Power of Four – People, Process , technology and “connected things””

Hype

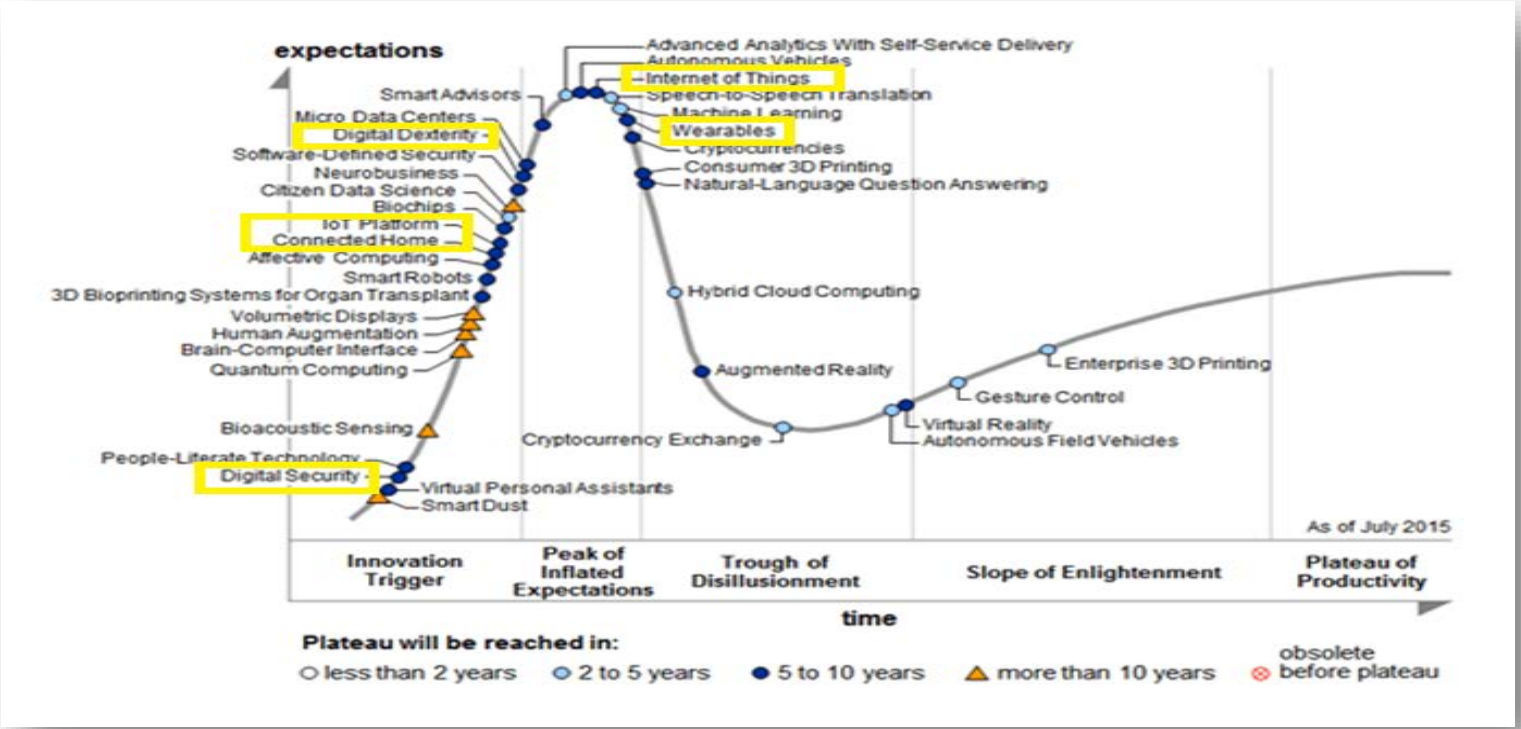


Figure 1: Gartner Hype Cycle – Emerging Technologies 2015

Source : Gartner

Trends - Connected Things and API

We estimate that while the total cost of ownership of vehicles will remain stable for consumers, the dramatic increase in **vehicle connectivity** will increase the value of the global market for connectivity components and services to **€170 billion by 2020** from just €30 billion today.
(Source - McKinsey & Company)

Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015

Monetisation of Cloud Platform (**PaaS**) as a Services and **APIs** access from the API Management Platforms are accelerators to connect the mobile, social and cloud apps to the Internet of things devices and enterprise data.

IoT Eco-System

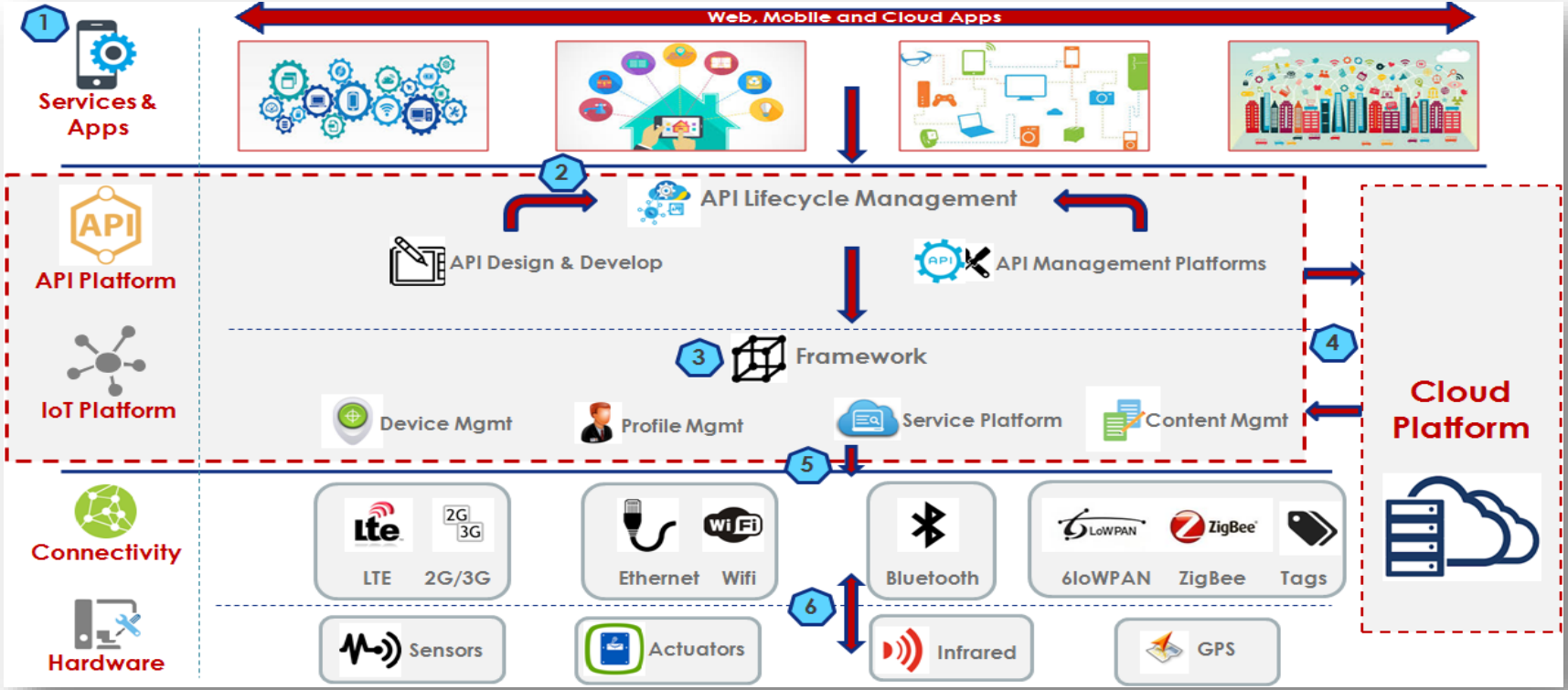


Figure 2: IoT Eco-System

Protocol Suite & Change in Attack Vector

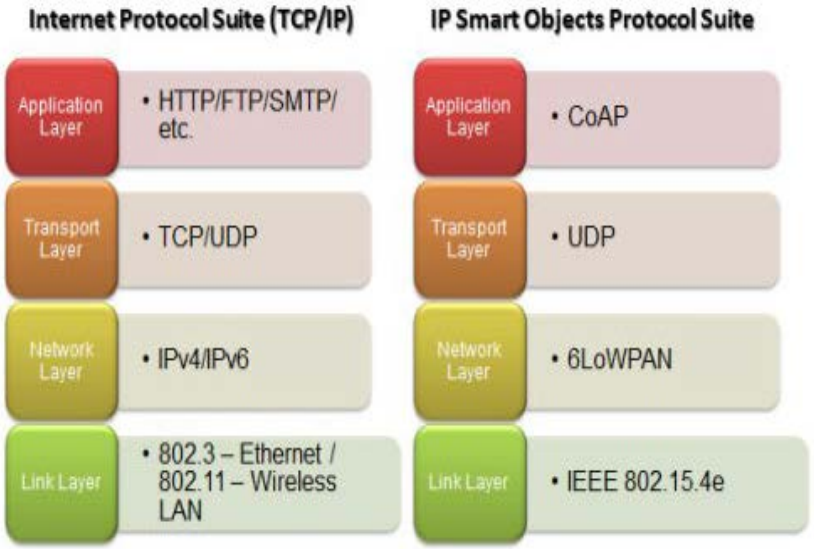


Figure 3 TCP/IP Stack and IP Smart Objects Protocol Stack
Credit: Ronak Sutaria and Raghunath Govindachari from Mindtree Labs

CoAP (Constrained Application Protocol)
An application layer protocol
- Intended for use in resource-constrained internet devices.
- The CoRE group has proposed below features
  - RESTful protocol design minimizing the complexity of mapping with HTTP,
  - Low header overhead and parsing complexity,
  - URI and content-type support,
  - Support for the discovery of resources

6LoWPAN
- acronym of IPv6 over Low power Wireless Personal Area Networks
- operates only in the 2.4 GHz frequency range with 250 kbps transfer rate."

IEEE 802.15.4
- physical layer and media access control for low-rate wireless personal area networks (LR-WPANs).
- Basis for the ZigBee,ISA100.11a, WirelessHART, and MiWi specifications

Security Considerations for Protocols

Single Device Compromise

- Single device compromise should not lead in compromise of the entire collection of devices
- Compromise of a large number of devices can enable additional attacks such as a distributed denial of service.

Hardware based Random number

- Security protocols uses random numbers
- Offering randomness in embedded devices is challenging.
- Recommended to use hardware-based random number generators

Reference : RFC 7452 IETF

Recent Hacks

Hacking into homes: 'Smart home' security flaws ound in popular system

ay 02, 2016 Contact Nicole Casal Moore

Español

ANN ARBOR—Cybersecurity researchers at the University of Michigan were able to hack into the leading "smart home" automation system and essentially get the PIN code to a home's front door.

Their "lock-pick malware app" was one of four attacks that the cybersecurity researchers leveled at an experimental set-up of Samsung's SmartThings, a top-selling Internet of Things platform for consumers. The work is believed to be the first platform-wide study of a real-world connected home system. The

Nissan Disables LEAF's Remote Telematics System After 'Profoundly Trivial' Hack

All that is needed to gain access to any LEAF's telematics system i the car's VIN, researcher says.

roofpoint Uncovers Internet of Things (IoT) Cyberattack

ORE THAN 750,000 PHISHING AND SPAM EMAILS LAUNCHED FROM "THINGBOTS" INCLUDING TELEVISIONS, FRIDGE

NNYVALE, CA – (Marketwired) – 01/16/14 – Proofpoint, Inc., (NASDAQ: PFPT), a leading security-as-a-service provider, has uncovered what may be the first proven ternet of Things (IoT)-based cyberattack involving conventional household "smart" appliances. The global attack campaign involved more than 750,000 malicious email mmunications coming from more than 100,000 everyday consumer gadgets such as home-networking routers, connected multi-media centers, televisions and at leas e refrigerator that had been compromised and used as a platform to launch attacks. As the number of such connected devices is expected to grow to more than four nes the number of connected computers in the next few years according to media reports, proof of an IoT-based attack has significant security implications for device iners and Enterprise targets.

$13 Million Stolen From Japan ATMs Via Stolen S. African Bank Data

Coordinated fraudsters hit ATMs at 1,400 Japanese 7-Eleven stores -- before lunch.

n less than three hours, a coordinated group of fraudsters stole 1.4 billion en (about $12.8 million), by simply strolling into 7-Eleven and withdrawing hose stacks of cash from the ATM.

The fraudsters reportedly used fake credit cards that were created using tolen data on roughly 1,600 account holders from Standard Bank in South

Source : Google Search

Identity & Integrations Issues

IoT Service Provider and its 1 million aggregators.
What are the security considerations?

IoT - Attack Surfaces

Multiple surfaces are involved in the IoT eco-system.
Broadly it involves – **IoT device, Cloud, Mobile Application, Network Interfaces and the Software.**

IoT – Data Security Vulnerabilities

- Insecure web interfaces for IoT Platforms
- Insecure IoT devices & network interfaces
- Communication Channels Security
- Insecure cloud eco-system
- Insecure Cloud , Mobile and IoT applications
- Insecure API management

Compliance Issues

Cloud Service Provider and its 5000 IoT integrations .
What are the security considerations?

Cloud – Attack Surfaces

Cloud comes in private, public and hybrid models.
It has **SaaS, PaaS & IaaS components integrated to IoT**.

Cloud – Data Security Vulnerabilities

- Insecure cloud and **third party APIs** connected through IoT
- Cloud data security **non-compliance**
- **Shared technology** components security Vulnerabilities
- Cloud platform , **Connected APIs** and its **Application Security** Vulnerabilities
- **Abuse** of cloud services

Identity , Compliance & API Management Issues

API Management Platform Provider and its 5 million merchants planned **API monetisation module integrations**.
What are the security considerations?

API – Attack Surfaces

API Management Platform has **Application** and **API Developer portal, API Gateway, API analytics** and **API monetization modules**

API – Data Security Vulnerabilities

- Authentication Module **Integrations (ID&M)** Vulnerabilities
- API **Abuse**, **Malwares** & **Bots**
- API Integrations with **Gateway & Aggregators** Vulnerabilities
- API Message **Weak Cryptography** Issues
- API Integrations with **IoT platforms** Issues

Source Code - Quiz

```
main()
{

int i = 7;

printf(“%d”,i++*i++);

}
```

Securing Internet of Things Eco-system

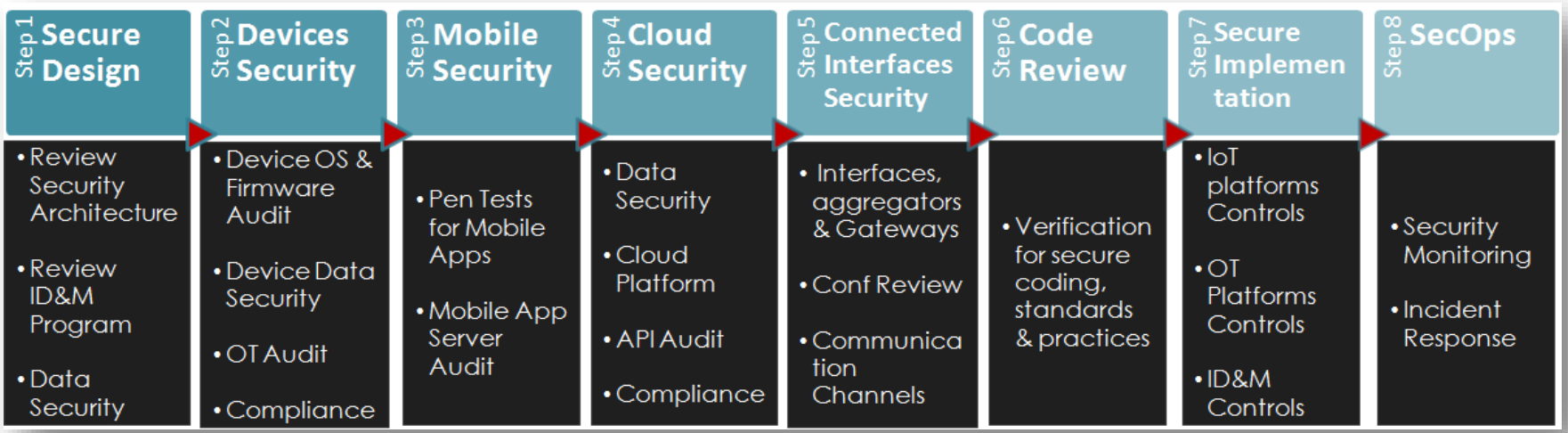


Figure 3: Security Approach – IoT Eco-system

Integration Quiz

- Social networking website – WWW.YOUARETHEGOD.COM - A
- Your IoT business portal – WWW.CUSTOMERISTHEGOD.COM – B
- API Monetisation Module from Social Platform – User Data Sharing API
- Integration Strategy?
  I. Who owns and transfers data? Any data definitions?
  II. What about its communications channels?
  III. How B will receive the data? Where to store and how to use in transit?
  IV. Till what time B can have this data?
  V. What's and how monetisation module will work?

Securing API Management Platform Integrations

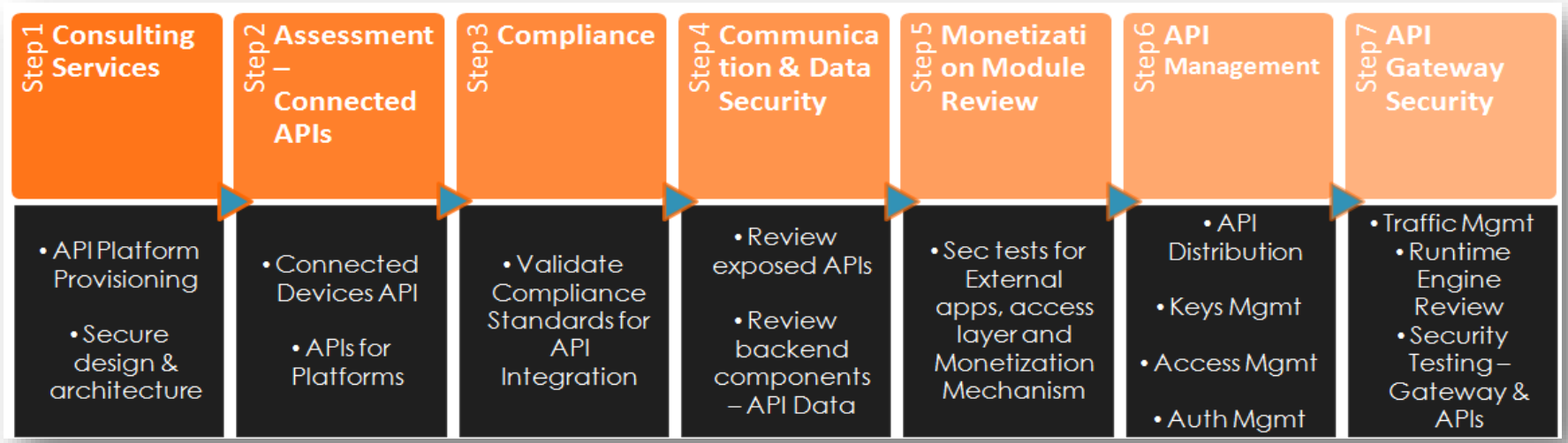


Figure 4: Security Approach – API Management Platforms

Apply – Best practices to secure IoT & API

- Secure implementation of IoT, Mobile & Cloud Apps
- Secure SSO and Identity Management Programs
- Compliance audit for data security at each layer
- Secure API management – distribution, keys and access control
- Secure Gateways & Aggregators integration with platforms
- Secure IoT devices and OT devices

Apply – IoT home appliances integrations

openHAB for any IoT home appliances automation and apply security integrations principals

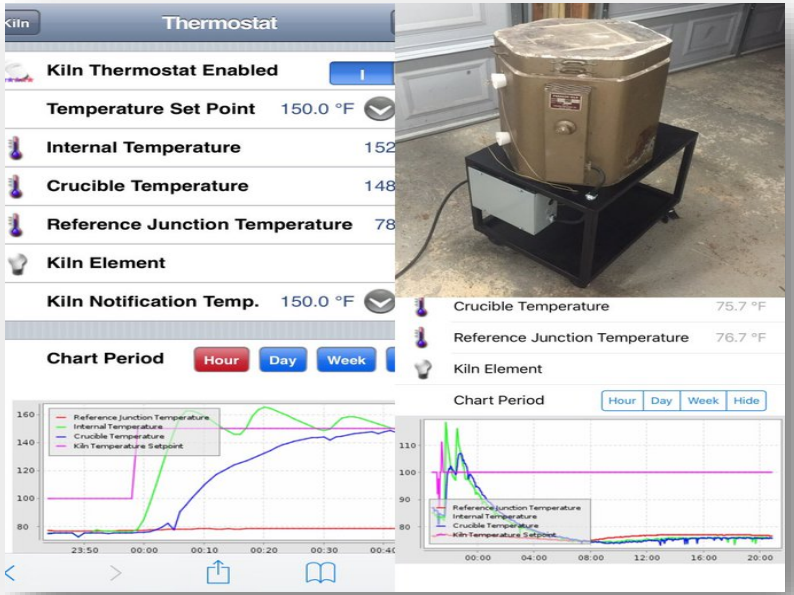


Figure 5 : openHAB with raspberryPi & IoT

openHAB

- Open Source , openHAB is a software to integrate different home automation systems and technologies
- Vendor-neutral - hardware/protocol-agnostic ,Supports JVM (Linux, Mac, Windows)
- Easily extensible to integrate with new systems and devices
- Provides APIs for being integrated in other systems
- openHAB, all USER data (like sensor data or actuator commands) can be controlled and maintain data privacy

Credit: http://www.openhab.org

Summary

- Digital involves IoT/OT, Social, Cloud, Mobile, Analytics and API
- Security risks in Digital & its business impact
- Secure API and IoT integrations is must
- Data security at each layer of IoT is no more option!
- Standardisation for protocols and integrations in IoT

Thank You!

Suhas Desai
suhas.desai@aujas.com

AUJAS
MANAGING INFORMATION RISK