

RSA® Conference 2017

Singapore | 26–28 July | Marina Bay Sands

POWER OF
OPPORTUNITY

SESSION ID: CMI-R08

How APAC IOT Leaders are Handling Security—Next Secure ‘Things’ Roadmap



Suhas Desai

Vice President – Digital Security

Aujas

@desai_suhas

Agenda

- IOT Landscape in APAC
- 6 IOT Security Worries
- IOT Leaders Security Strategy
- Roadmap to secure Next “Things”

One week without IOT Enabled Devices

- Dominican Republic Travel
- Opted to not use Smart Phone, No E-Metering, No Smart Parking , No Smart Banking , No Wearable Devices

The **Parque Colon** is a monumental tribute to Christopher Columbus



Image Source: Google Search

APAC Banks Adaption for Robots



Image Source: Google Search

Smart Cities Initiatives



Image Source: Smart City India

Telematics Insurance

Telematics Car Insurance

Image Source: Google Search

API Banking & IOT Enabled Payment Devices

The screenshot shows the Open Bank Project website. At the top left is the logo 'OPENBANKPROJECT'. To the right are navigation links: 'About', 'Apps', 'FAQ', and 'Contact'. Further right are social media icons for Facebook, Twitter, and LinkedIn. The main content area features the headline 'Bank as a platform. Transparency as an asset.' followed by a paragraph: 'The Open Bank Project is an open source API and App store for banks that empowers financial institutions to securely and rapidly enhance their digital offerings using an ecosystem of 3rd party applications and services.' Below this is a form with an input field containing 'email@example.com' and a 'Keep me informed' button. On the right side, there is a diagram with gears. At the top of the diagram are icons for a person with a hat and a person in a suit. Below these are icons for a laptop, a mobile phone, and a desktop monitor. In the center is the 'OPENBANKPROJECT' logo. At the bottom is a 'BANK' label with a money bag icon containing a dollar sign.

Image Source: Open Bank Project

Aadhaar Payments through Connected Devices



Image Source: UIDAI

Intelligent Devices in Customer Services

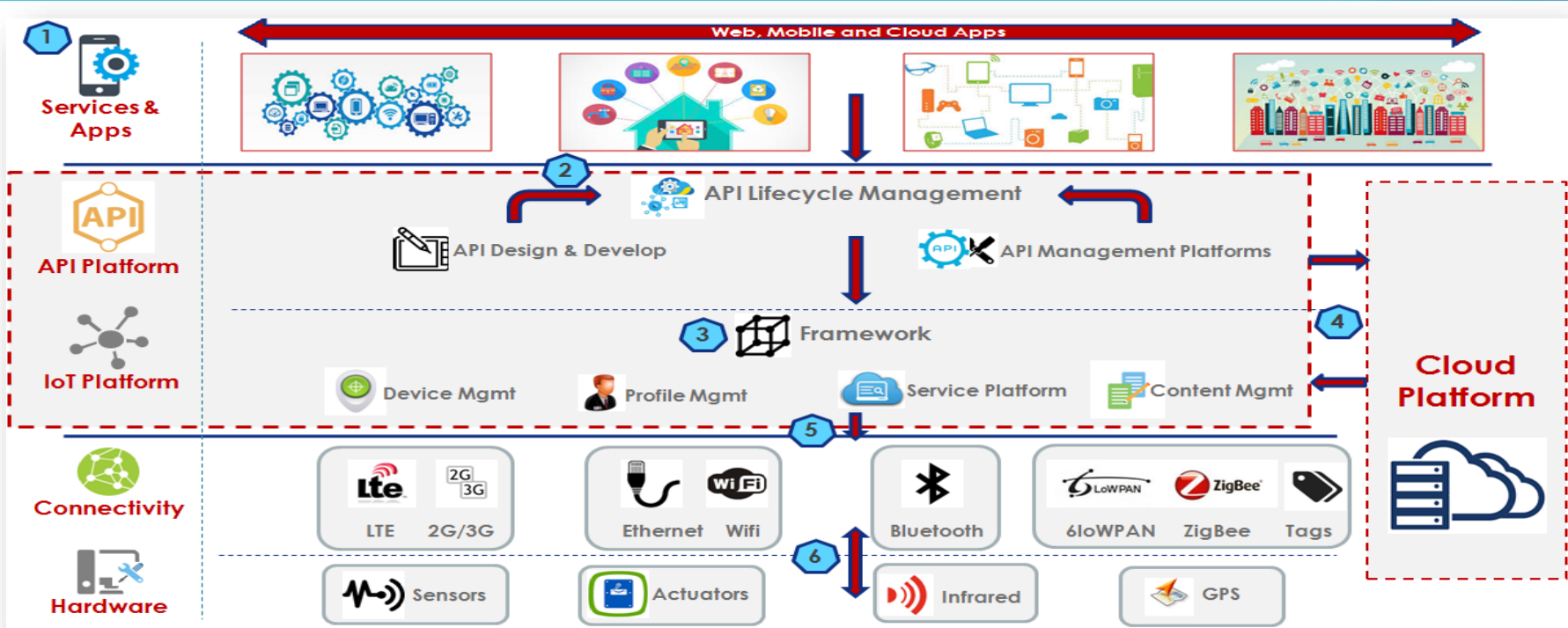


Image Source: Google Search

Source Code Quiz

```
main()
{
int i = 7;
printf(“%d”,i++*i++);
return 0;
}
```

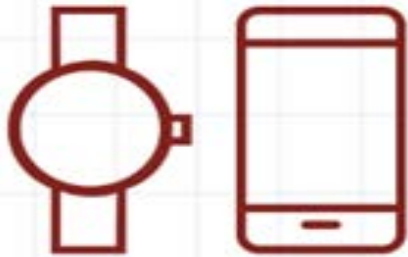
Internet of Things Architecture



Communications Security – Key Concern

How to establish security in communication channels from IOT Devices to Platforms?

6 IOT Security Worries



1 Insecure Devices

Attacks on IoT devices and their network interfaces are becoming very common. Attackers can eavesdrop and steal data. With the exponential growth predicted for IoT - It is only going to get worse.

Security Worries

2 Insecure Communication

Insecure message transmission over various communication channels might lead to privacy issues and may also lead to fraudulent transactions.



Security Worries

3 Insecure Cloud

Cloud interfaces between IoT devices and platforms can be a target for data breach. Pay attention to cloud APIs, cloud platform, security configurations and data security controls.



Security Worries

4 Insecure Applications

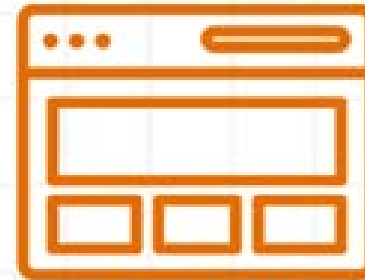


Mobile and IoT device applications can be a target for data breaches. There can also be issues related to device theft/loss and local data storage.

Security Worries

5 Insecure Web

IoT platform's web interface could be a target for attacks like SQL injection, XSS, CSRF and other web security attacks. Pay attention to implementation and configuration.



Security Worries

6 Insecure APIs



APIs are a critical component of any digital platform. Not only is it important to have in-built security measures, but attention needs to be paid during integration with the IoT platform, cloud systems, etc.

Source Code Quiz

```
main()
{
printf(“%d”, printf(“RSAC”));
return 0;
}
```

More Smart Devices = More (Sensitive) Data = Higher Risk



APAC IOT Leaders Security Strategies

- Central Banks Security Guidelines and Security Governance Framework Compliance for the **IOT Enabled Payment Devices**
- APAC Specific **Smart City Guidelines** like NYC Smart , Equitable City
- Mandate to use **secure** IOT Devices OS , Firmware's and communication Protocols

Security Strategies

- IOT Platform and API Management Platforms Integrations Policies and Security Governance Framework
- SIEM Integrations and Policies Adaption to have proper Security Incidence Management
- Strategies to adapt IOT and Cloud Security Guidelines from **NIST**, **OWASP**, **GSMA** and **IIC Security Framework** [WIP]

Roadmap – PPTA, Frameworks and Standardization

- **People, Process, Technology & Assurance (PPTA) Program**
- **Security Framework** Adaption
- **Standardization** of IOT Devices, Communications and Platforms Security

Apply

- Ensure to have secure communication Channels from IOT devices
- Implement secure IOT devices in payment industry
- Practice Smart Cities Guidelines to secure metering devices
- Monitor your IOT devices data logs

RSA[®]
Conference
2017

Singapore

**Lets secure next Things for better
future!**

[E: suhas.desai@aujas.com](mailto:suhas.desai@aujas.com)