\Orchestrating a brighter world NEC

Tackling Data Security, Privacy, Trust Challenges in the Internet of Things

Aditya Kumar, Group Technical Specialist
Digital Transformation – IoT, AI, Smart Infrastructure

27.Feb.2019

Table of contents

Global Cyber Security Trends*

Threat present everywhere

Devices	Device Gateways	Network / Cloud	Server – Web / Application

600% increase in attacks **2017→2018 [6k to 50k]**

China 21%, US 11%, **India 5%**, Japan 4%

Top targets - **Router 33.6%, DVR 23.2%**

49% attackers were **Non-Blacklisted**

24,000 avg. malicious app blocked per day in 2018

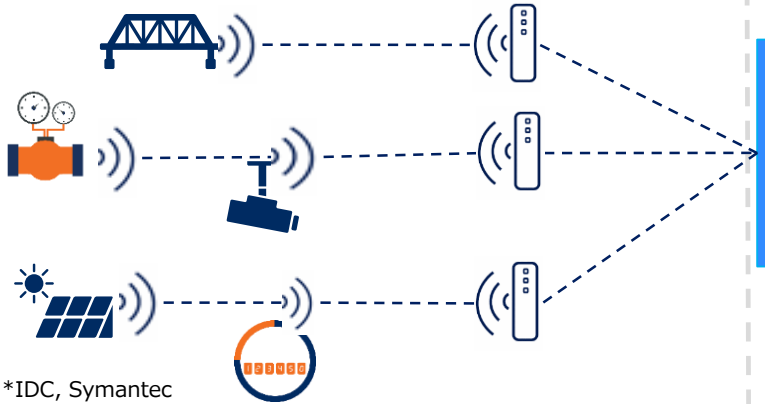
55% increase in spam (email, network)

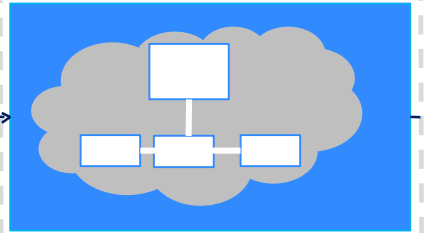
1Billion request analysed per day in 2018

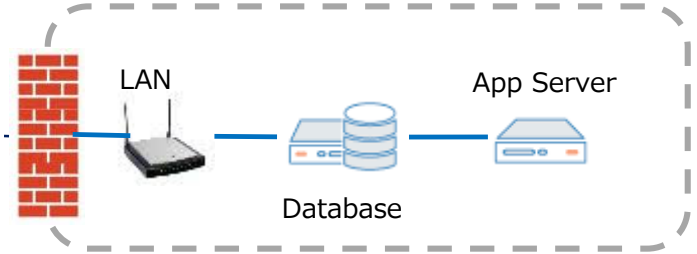
1 in 13 web request lead to malware

92% increase in new download variant

13% increase in vulnerabilities







*IDC, Symantec

Many Solutions Available For End-2-End PC Security…

Gateway Hardware	Network	Server	Server
			
Trusted Platform Module	NMS Firewall	Anti Virus Database Web /App	Firmware Mobility

Gateway Hardware

- **Easy to enter Server via Device** – Boot/Firmware/ Network

Examples Of IoT Hacking And Vulnerabilities In Recorded History*

MIRAI BOTNET

2016: DDOS attack on DYN service provider left internet down including twitter, CNN, Netflix

CARDIAC PACEMAKER

2017: US FDA confirmed that pacemaker can be hacked to reduce battery life / incorrect pairing

JEEP COMPASS

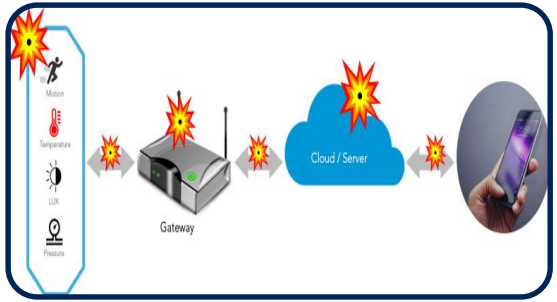
2015: A team of researchers was able to take control of the JEEP SUV via CAN's bus

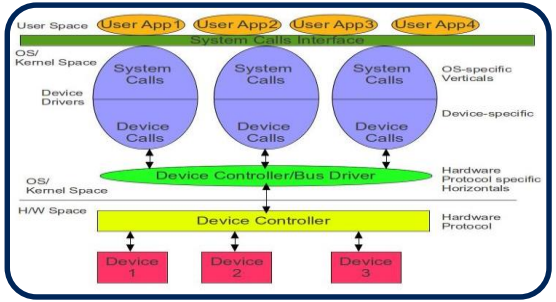
TRENDNET CAM

Baby monitoring cameras + audio were readable by outsider using camera IP address

*Iotforall

IoT Devices Potential Security Concerns <1/2>



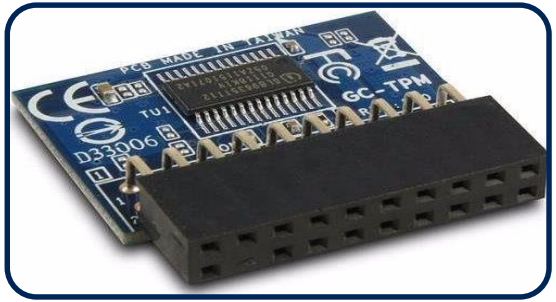


Devices deployed and operated in unmonitored hostile environment

Vulnerable RTOS for malware attack

Can’t review all device drivers, OS and services

IoT Devices Potential Security Concerns <2/2>



Standard PC services model , TPM not exactly applicable to edge devices

Hackers can do actual physical harm

Physical servicing of deployed device may not be possible always

How To Address These Challenges At Device Level ?

1. Implement security at both Hardware (TPM) and Software (FW) level
2. Hardware enabled challengeable device identity (Device ID / UDS)
3. Unchangeable boot up process at start-up (ROM code)
4. Strong isolation of sensitive code execution esp. actuation triggers
5. Capability to remotely evaluate device status
6. Crypto enabled Watch-Dog trigger if device becomes unresponsive

Why Hardware Support Is Required ?

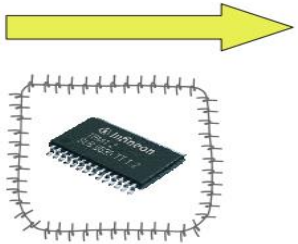
There are problems with software-only solutions

Device Identity	If a bug leads to a Device ID disclosure how do we securely (and remotely) recover a device?
Device State and Attestation	Cannot trust software to report its own health
Roots of Trust for Storage, encryption	How do we securely extend trust chain, store keys, etc.?

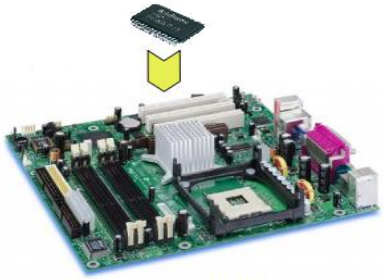
Can We Use Existing Hardware Security Solutions ? <1/2>

Standard Processor System

- Easy to program
- Easy to change
- Easy to attack

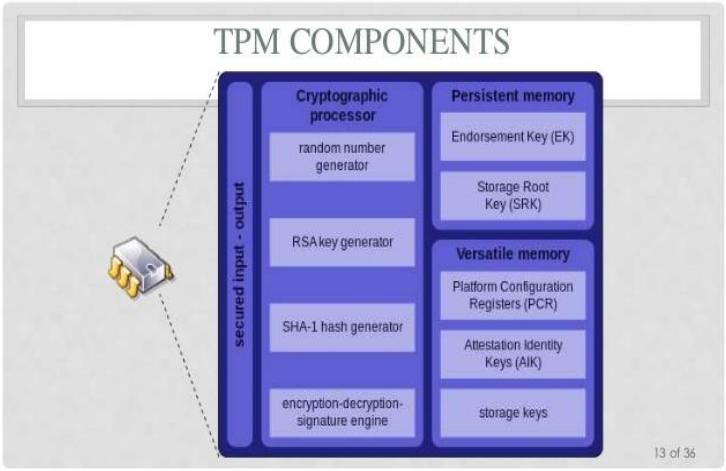


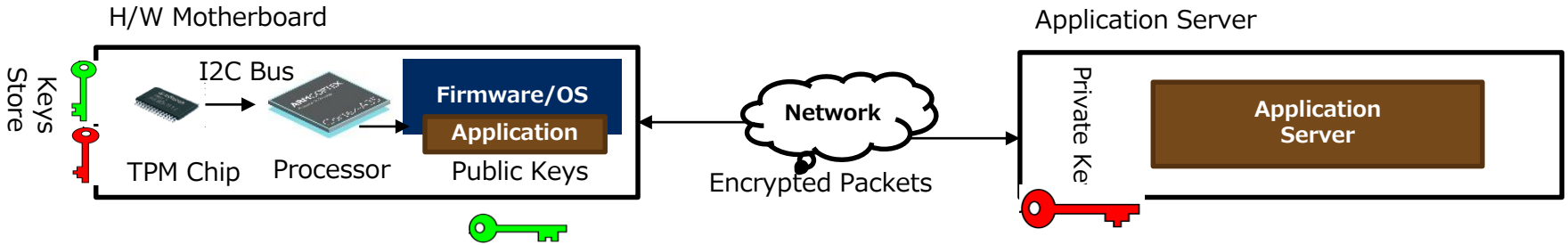
TPM-Security Module



Trusted platform

- Shielded and encapsulated chip
- Controlled interface to external
- Trusted software in a protected hardware





Trusted Platform Module + PKI based authentication

Can We Use Existing Hardware Security Solutions ? <2/2>

1) Why not just store Device ID key in e-fuses?

If malware can read the fused key, you're no better off than with a software-based key

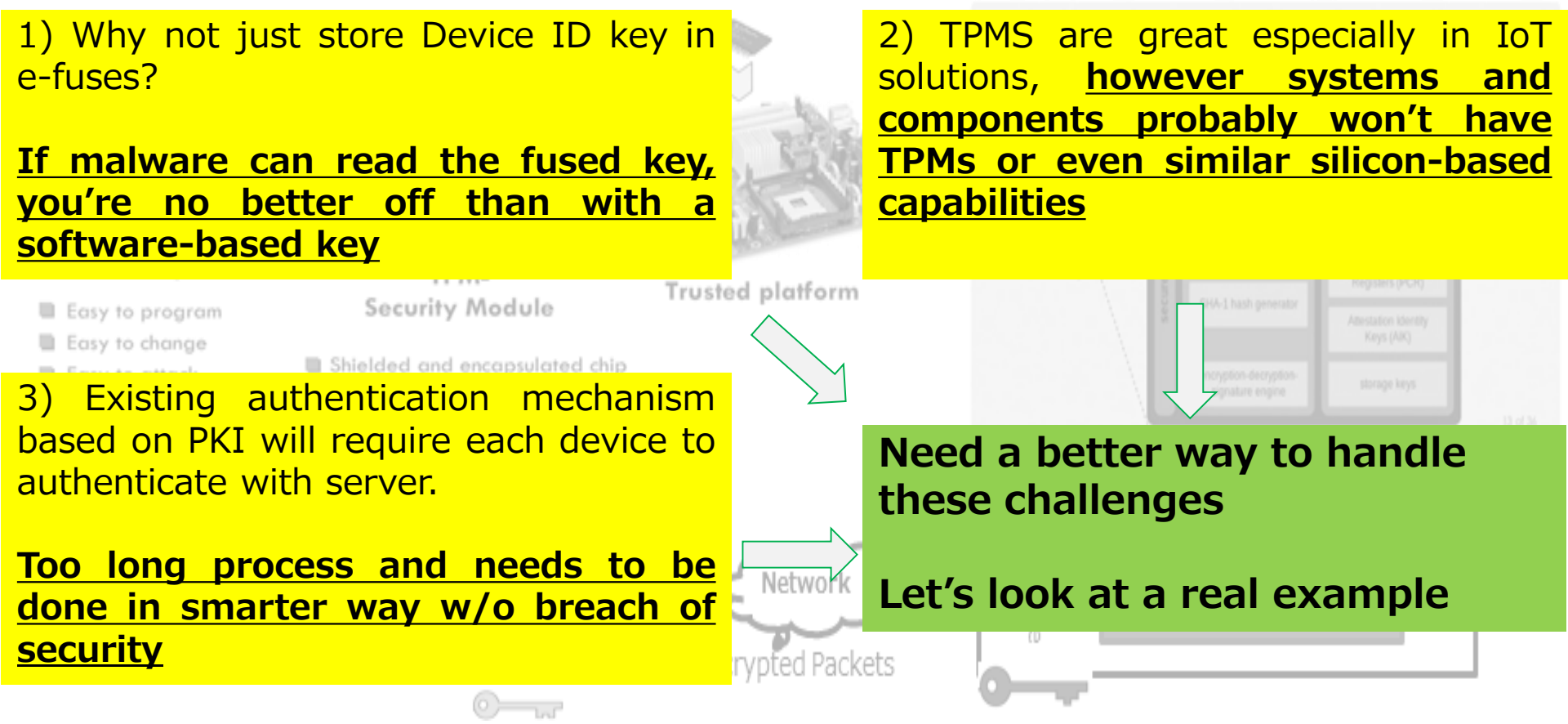
2) TPMS are great especially in IoT solutions, **however systems and components probably won't have TPMs or even similar silicon-based capabilities**

3) Existing authentication mechanism based on PKI will require each device to authenticate with server.

Too long process and needs to be done in smarter way w/o breach of security

Need a better way to handle these challenges

Let's look at a real example



Case Study : Indian Connected Inverter Devices Solution

End-2-end Security

Security on chip | Secured TCP/IP | Secured Cloud | Secured Application

Devices

Residential Inverters

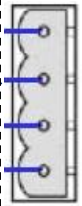
Solar Inverter

Grid Inverter

RS485

Custom IoT Gateway

Modbus



Microchip CEC1702

GPRS 4G/2G Module

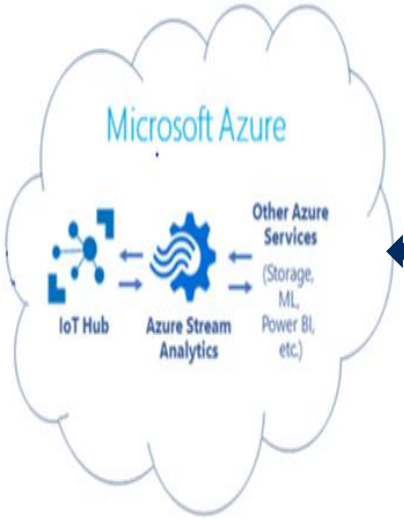
GPIO Pins

Wi-Fi Module

Modbus + GPRS + Wi-Fi + Azure IoT Hub Connector (MQTT)

MQTT

Internet



BI powered by ML / Data Analytics

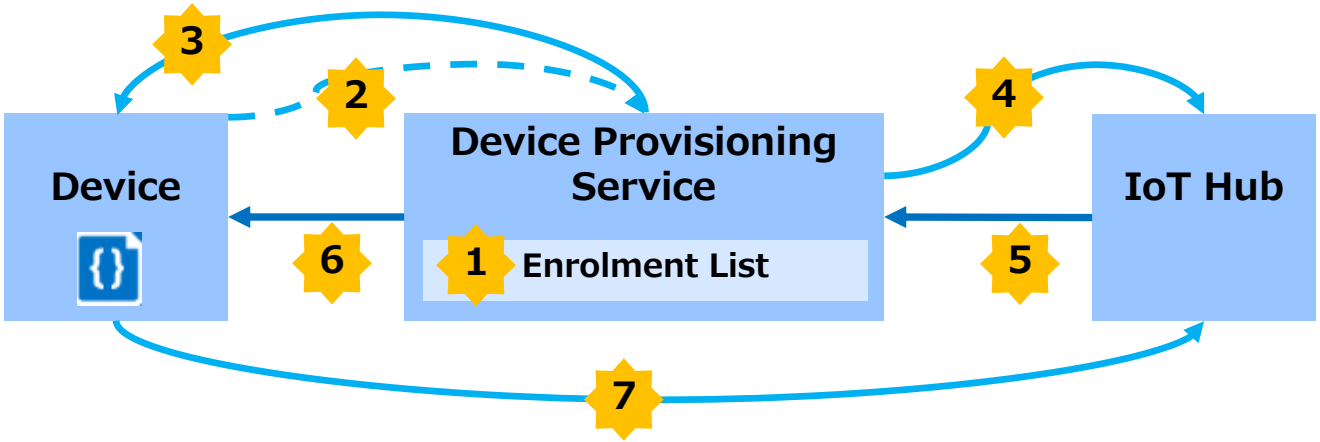
GUI App

Mobile App

CEC1702 Secure boot provides a hardware-based root of trust – Supports MS Azure DICE security framework capability

NEC SoW : Develop, Operate and Managed the software and platform services

Device Provisioning Service



1. Add device registration information to the enrolment list in the Azure portal
2. Device contacts the provisioning service endpoint set at the factory → Passes the identifying information to the provisioning service to prove its identity
3. The provisioning service validates device registration ID and key against the enrolment list entry
4. The provisioning service registers the device with an IoT hub and populates the device's desired twin state
5. The IoT hub returns device ID information to the provisioning service
6. The provisioning service returns the IoT hub connection information to the device. Device can send data directly to the IoT hub
7. The device connects to IoT hub. The device gets the desired state from its device twin in IoT hub

Device Management Snapshot

Admin | Signout

- Dashboard
- Device Management
- Device Group
- Reports
- Map Device
- Add Admin User
- Help

Device Management

Displaying the list of all the device available

OTA, Rule, Enable/Disable

All Group Name | prod

	Device ID	Group Name	Model	Comm Status	Device Status
☐	productiongti	default	gti	Offline	Enabled
☐	produtunit33	default	Unkown	Offline	Enabled
☐	testprod	default	Unkown	Offline	Enabled
☐	productionit	default	gti	Offline	Enabled
☐	productionitfota	default	1234	Offline	Enabled
☐	productionitgti	default	gti	Online	Enabled
☐	productionittest	default	gti	Online	Enabled
☐	productionitpcu	default	pcu	Offline	Enabled

Items per page: 10 | 1 - 8 of 8

productionittest Properties

Property	Value
Rule Created Date	2019-02-19:11:31:15
Last Firmware Update	20121214
Location	12345678
Model	gti

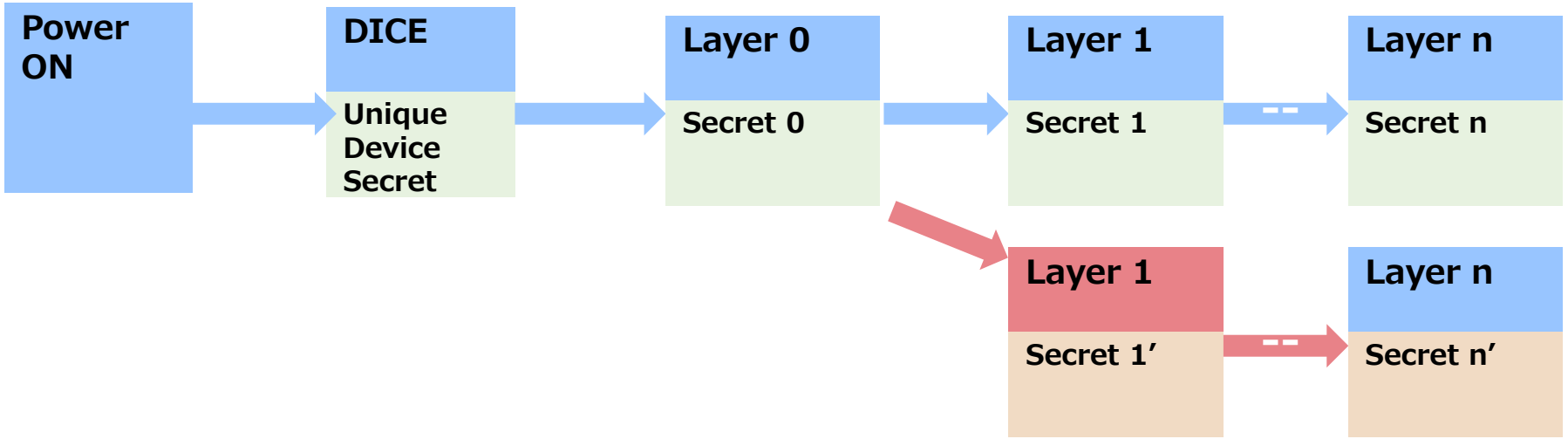
productionittest Data

(Send Date: Feb 24, 2019, 2:16:59 PM)

Data	Value
Product Model	70
DSP Software Version	531
LCD Software Version	35
AC Output Type	Three phase four-wire mode

DICE : Device Identifier Composition Engine

New Root of Trust for Measurement specification from the Trusted Computing Group (TCG)



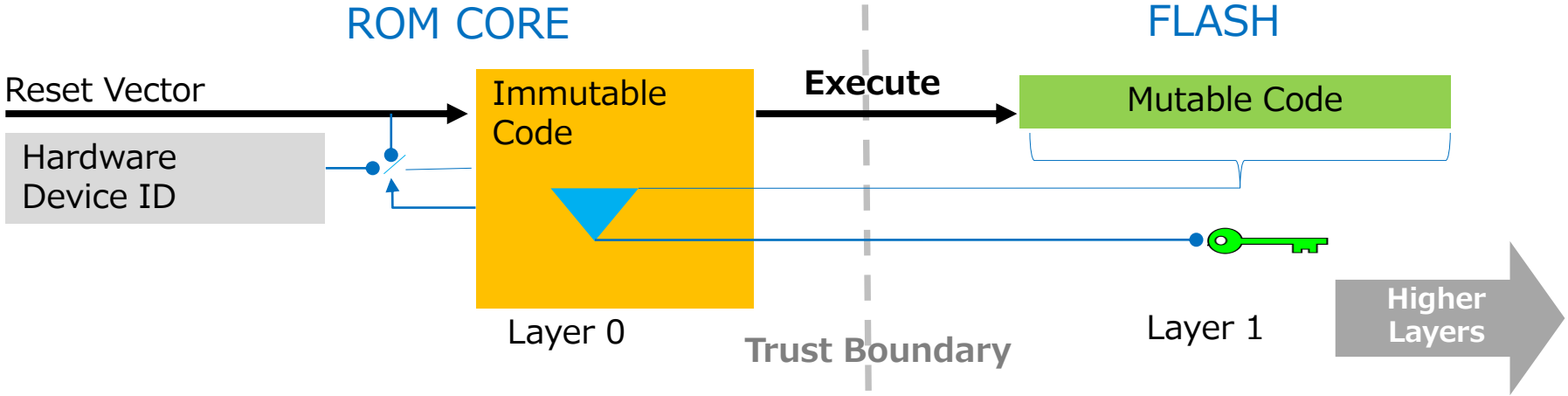
Device start-up (boot) is layered with unconditional access to DICE model

Beginning with a Unique Device Secret (UDS), secrets/keys for device, and each layer/configuration

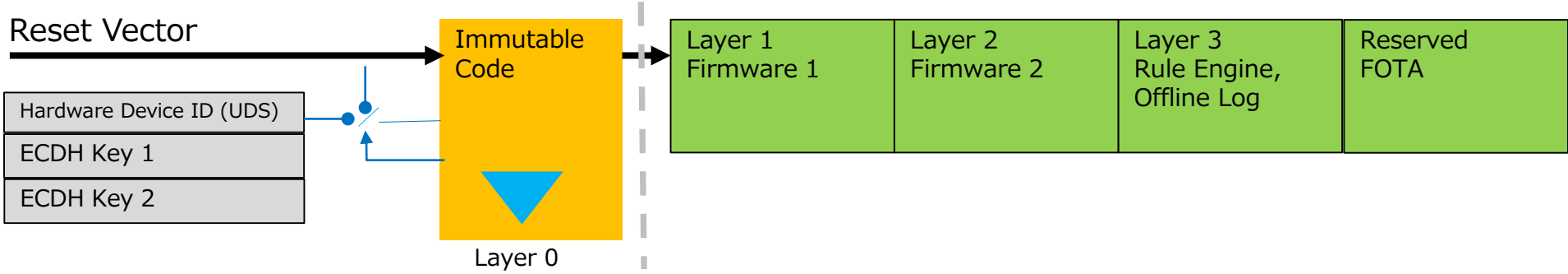
Implies that if different code or configuration is booted, secrets are different

So if a vulnerability exists and a secret is disclosed, patching the code automatically re-keys the device

Simplistic Architecture Of DICE Framework



Our implementation in Connected Inverters



Summary

Don’t let edge devices become new Trojan horse in IoT

Concern related to devices security, privacy and trust needs to be addressed properly

Physical (Hardware) + Logical (Software) based device security is need of the hour

MCU enabled TPMs with DICE framework can be a possible solution for device security

NEC

Aditya.kumar@india.nec.com
Ph : +91-9717741155