IoT Security & Privacy Considerations

2016 Taiwan IGF

Kenny Huang, Ph.D. 黃勝雄博士

Executive Council Member, APNIC

huangksh@gmail.com

2016.06.17

“Every step you take will be the threat to privacy”The Economist

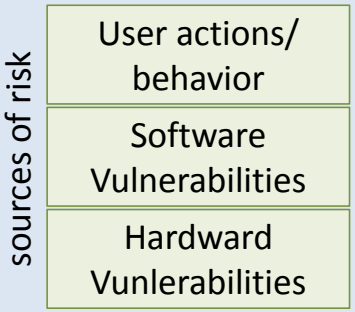
source : The Economist

source : BBC

What Are The Risks

"Personal data is the new oil of the Internet and the new currency of the digital world"

Meglena Kuneva, European Consumer Commissioner

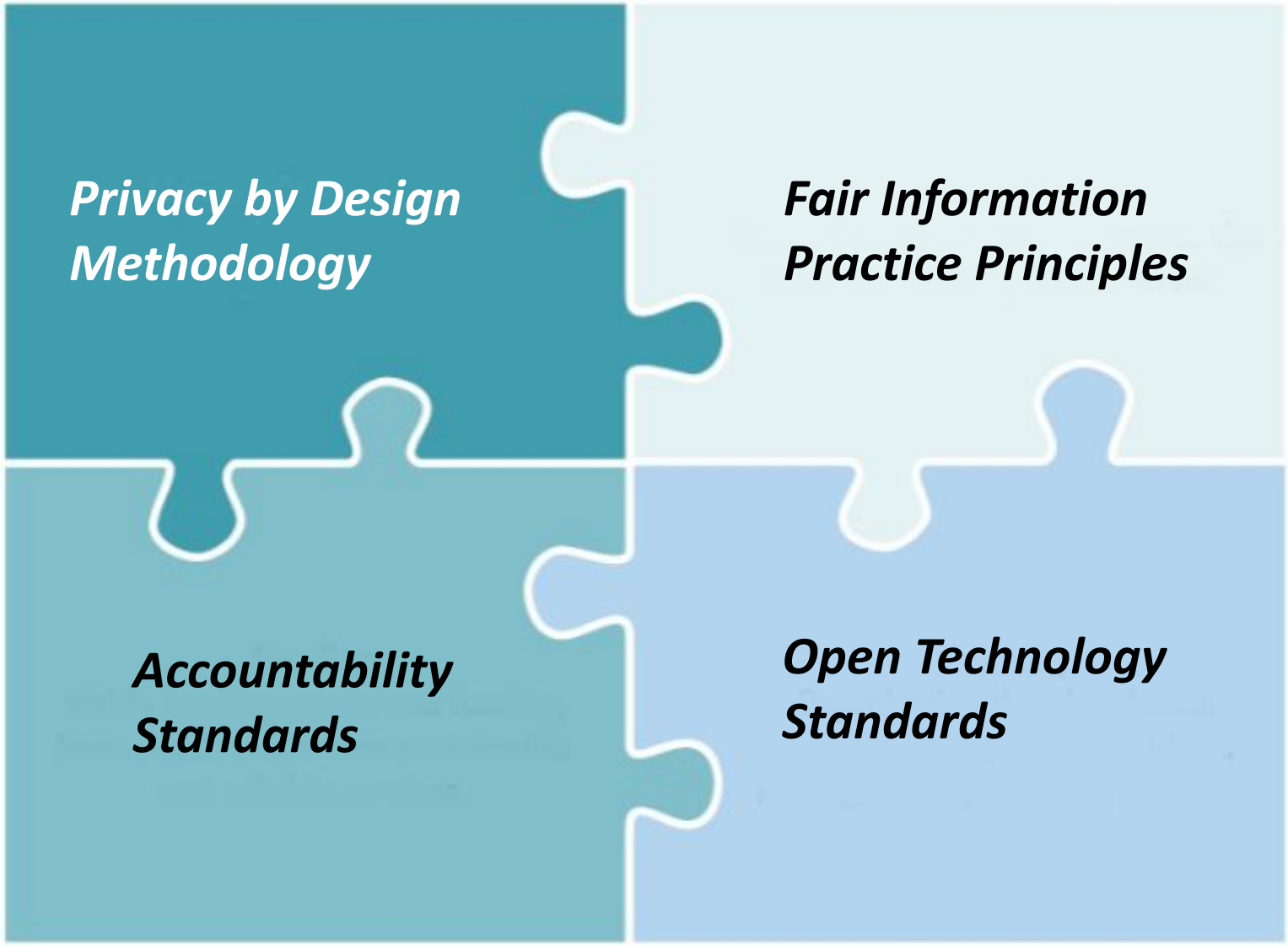


Privacy and Security

"Target CEO out as Data Breach"
- USA Today May 2014

"Hackers' Next Target : Your Health Insurance Company"
- FOXBusiness, May 2014

Policy and Process



Privacy By Design

- Taking privacy into account throughout the whole engineering process
- 7 principles
  - Proactive not reactive
  - Privacy as the default
    - purpose specification; collection limitation; data minimization; use, retention and disclosure limitation
  - Privacy embeded into design
  - Full functionality
  - End-to-end security - full lifecycle protection
    - ensure confidentiality; integrity and availabiliity
  - Visibility and transparency - keep it open
    - accountability; openness; compliance
  - Respect for user privacy - user centric
    - consent; accuracy; access; compliance

Fair Information Practice Principles

- Notice/awareness
  - Consumers should be given notice of an entity's information practices before any personal information is collected from them
- Choice/consent
  - giving consumers options to control how their data is used
- Access/participation
  - consumer's ability to view the data collected, and to verify and contest its accuracy
- Integrity/Security
  - ensure that the data they collect is accurate and secure
- Enforcement/Redress
  - enforcement measures : by the information collectors; to sue violators; criminal penalties

Accountability Standards

- Accountability standards serve as a framework for building trusting, productive relationships among stakeholders
- Accountability standards create benchmarks and a common ground for stakeholders
- For digital data operator collected, operator need to tell people how they use it

Open Technology Standards

- Need a large community that is interested in developing open technology standards. People can identify weakness before it become an issue
- Making sure we have public scrutiny on the things we going to use and to keep our data private

IoT Security is Critical

- Security is the top issue for IoT
  - Deployments will not scale without trust
- With large deployments
  - must limit attack surface of each device
- Applies to even simple sensors
  - Even if there is no secure data issues
- Security must be architected from the beginning and must not be made an option

Bring Security to Traditional Embeded Systems

- Traditional closed systems

- Very few developers have strong experience in creating secure systems
- Need a platform with built-in security and strong guidance on best practices

Security Design Challenges

- Too easy to declare developers of compromised products as incompetent
  - as product security can't be reliably measured, security suffers first on tight product schedules
  - massively parallelized security researchers vs. limited product development budgets and time frames
- The security of a system is dynamic over its lifttime
  - the likehood of an attack often wrongly assessed or undervalued in the chain
- New Denial-of-Service power attacks a problem for battery/scavenging devices
  - structural sensors often inaccessible and battery replacement is expensive
- If your product is successful, it will be hacked.
  - often the deployment costs of firmware udpates surpass the costs of a new device
  - as a result even know-broken systems are kept in use
  - this is not the PC world, no reset, no reinstall
- The assumption of being hacked at some point requires solid mitigation strategy
  - developers must ensure secure, reliable and affortable firmware updates

System Architecture - Security Perspective

Lifecycle Security

Communication Security

IoT Device Security

Directory & Subscription

Security Admin & Multi-tenancy

Data Flow Management - RESTful and Publish/Subscribe

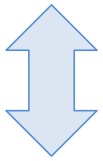
Device Management - Lightweight M2M

Interface - Open Web Standards

Application Protocols - CoAP, HTTP

IoT Server

Open Standards ?



WiFi Bluetooth 3G/4G

IPv6, 6LoWPAN

IPv4

Device Management - Lightweight M2M

Cryptography ?

IoT Device OS

Open Source

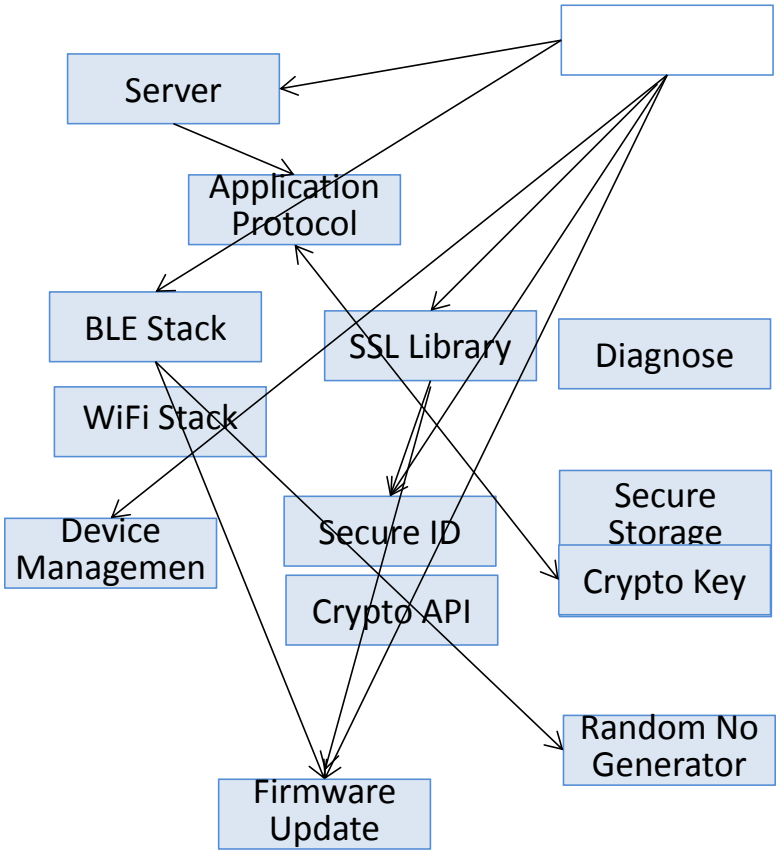
IoT Interoperability

The Interoperability of Things: IoT Semantic Interoperability (IOTSI) Workshop 2016

Participants : IETF, W3C, OMA, AllSeen Alliance, OCF, NIST, CableLabs, ZigBee, and ETSI, etc.

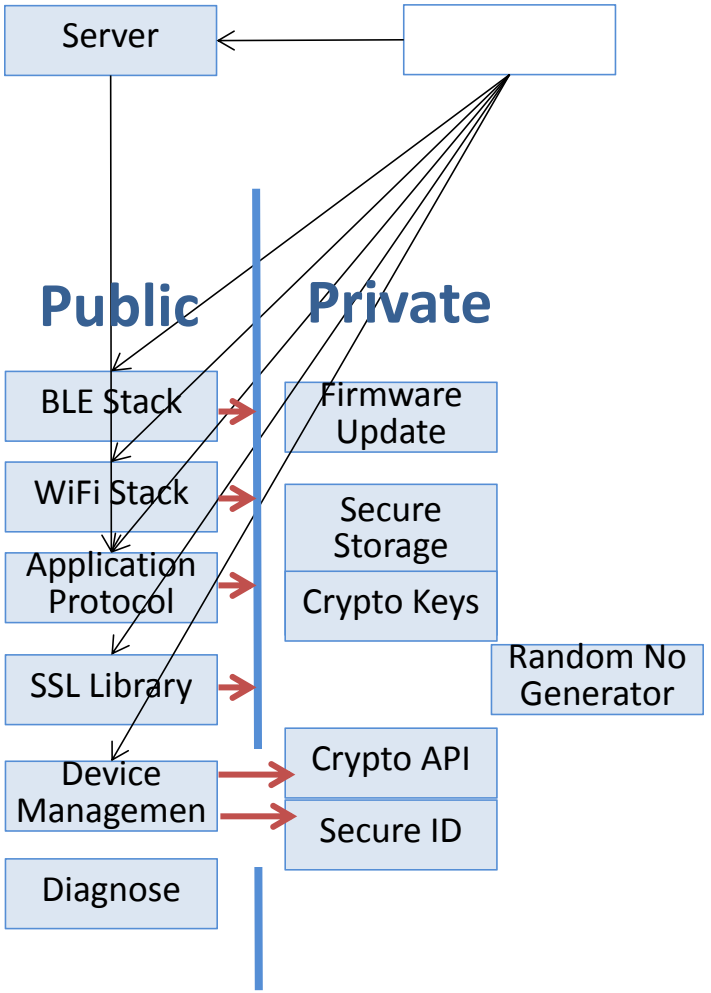
Traditional MCU Flat Security Model

- IoT devices include significant software complexity
  - Secure and privacy enabled server communication
  - Unclonable device identity
  - Cryptography and random number generation
  - Protection of keys/certificates and server API tokens
  - Secure firmware update over the air
- Flat security all code/data lives in a shared address space
- Large attack surface makes hard to verify devide security
- Bugs in any code can lead to a security flaw
- Code based is too large for exhaustive validation
- If malicious code updates Flash it may become impossible to remotely recover a device



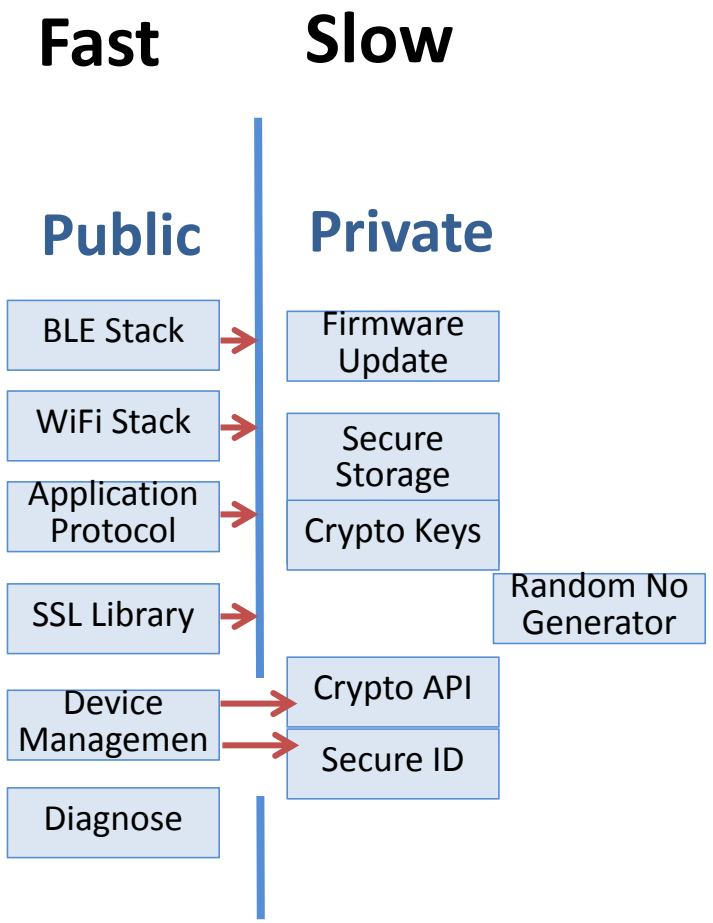
Device Security : Secure Partitioning for MCUs

- Split memory into private critical and public uncritical
- Small private footprint enables exhausive verification
- Public code operates on cryptographic secrets using defined API's but never allow access to raw keys
- Vulnerabilities on public side can't affect private side
- public code can't wirte code directly to Flash
- Private side can reliably recover device to clean state
- private side can verify integrity of the public side image

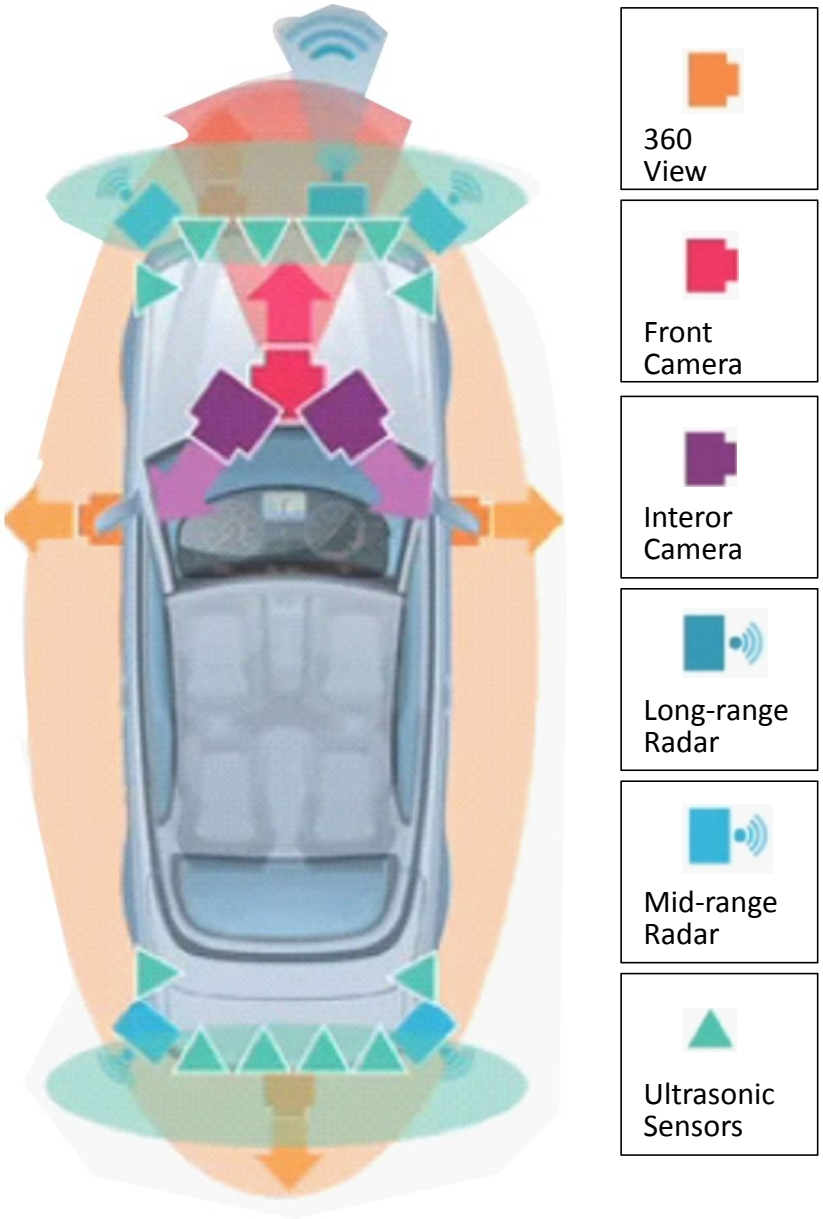


Enable Fast Innovation

- Private modules build with strong security and rarely change
- software is never finished
  - new features, bug fixes, patching vulnerabilities and tracking standards
- Code in the public state is developed rapidly
  - fast time to market
  - quick innovation cycles for public side
  - still a secure product
- When bugs are discovered after deployment a firmware update can be reliably enforced



Driverless Car : Secure But is it Safe



Automative Today, IoT Tomorrow

ASIL B or **ASIL D** support

IEC 61508
ISO 26262

Development process
Fault detection and control features
Failure node and effects analysis FMEA
Compiler qualification & Maintenance

Levels of Vehicle Automation

Level 1 - Function-specific automation
one or more control functions such as breaking and lane keeping are automated but driver has control

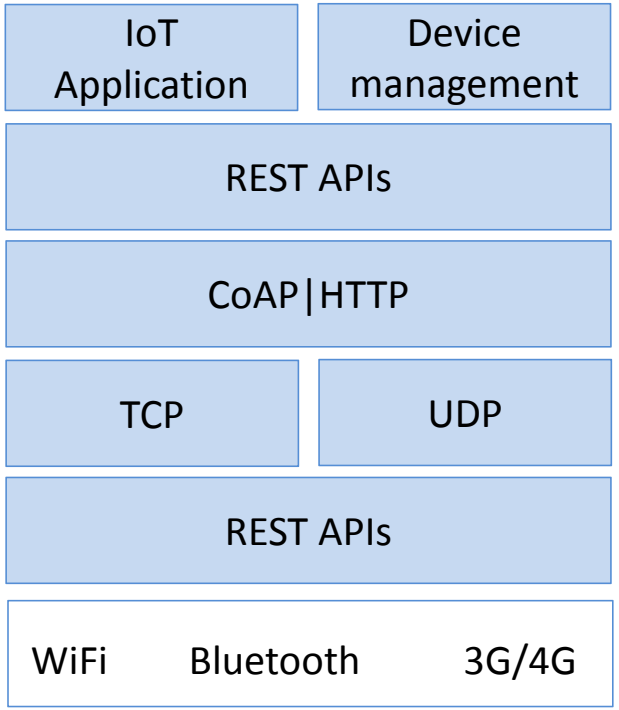
Level 2 - Combined function automation
Two or more control functions automated. eg. ACC with lane centering. Hand off the steering wheel and foot pedal but still responsible to monitoring and expected to control the vehicle

Level 3 - Limited self-driving automation
Vehicle takes control of all safety critical functions mostly. Driver is expected to be available for occasional control without constant monitoring

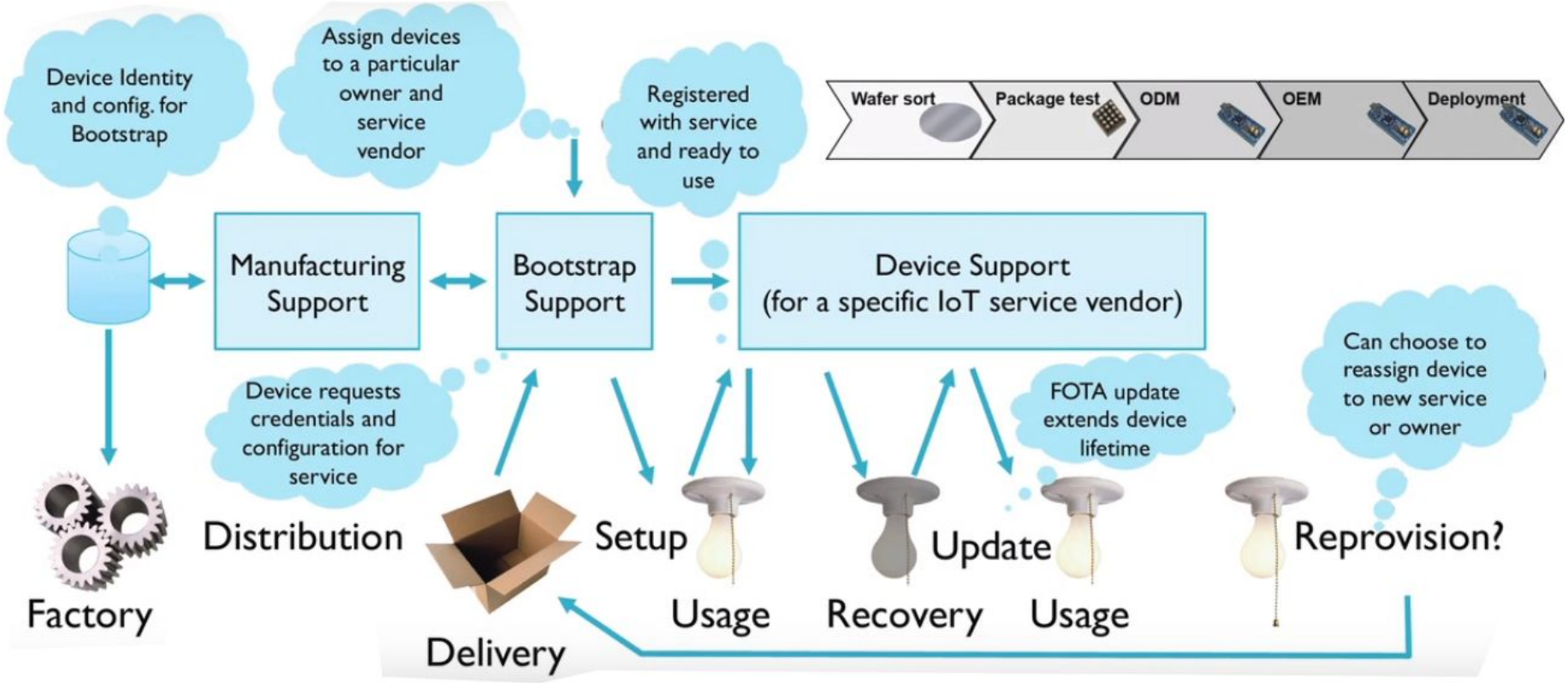
Level 4 - Full self-driving automation
Vehicles takes control all safety critical driving function and monitor roadway all the time. Driver is not expected to be available for control it any time

Internet Protocol to The Edge

- Non-standard approaches are a risk
  - Don't repeat past mistakes
- Use Internet security
  - widely deplyed and proven
  - firewalls and local routers
- 32-bit MCUs can handle IP stacks
  - < $1 trust Moore's law



Lifecycle Security and LWM2M



Common Problems We Need to Solve

- IoT deployments will not scale without trust
  - very few developers have strong security experience
- Flat security model
  - remote code execution allows full access and key extraction
- Compromised communications protocols
  - Man in the moddle attacks and compromised devices
  - Flawed proprietary algorithms
- Insecure firmware updates
  - updates become the malware infection issue
  - compromised through ineffective or no use of cryptograph
- Poor random number generation
  - Negates strong cryptograph

Lifecycle Security

Communication Security

IoT Device Security

Thank You
Question?