intel Security

Using the tpm with iot

David Grawrock

Security Architect, Senior Principle Engineer

Agenda

TPM History Lesson

What Does IoT Need

How Does The TPM Fulfill Needs

Usage

History

Worked on the TPM from 1999 through 2007 as TPM Workgroup Chair and Technical Committee Vice-Chair

These pictures are from a workgroup meeting in England, 2003

I was the TCG liaison to ISO SC27 to get the TPM specification as an ISO standard (we were successful)

Basic TPM Functionality

Root of Trust for Reporting (RTR)

- Enabling attestation

Root of Trust for Storage (RTS)

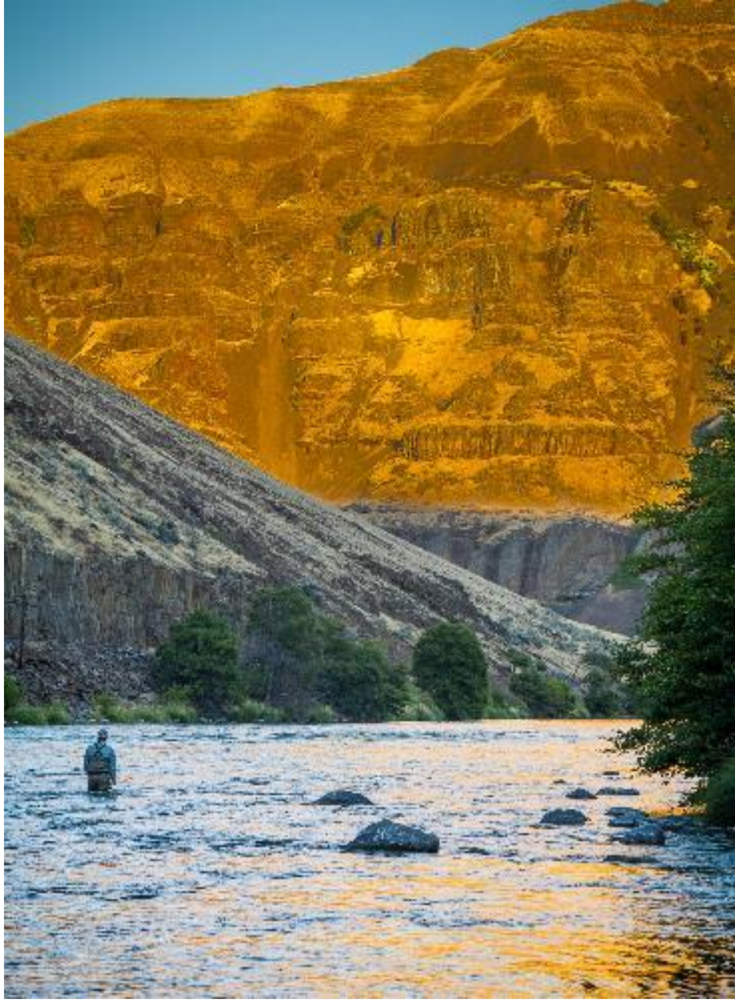
- Enabling protected storage

Platform adds Root of Trust for Measurement (RTM)

- Enabling attestation and protected storage

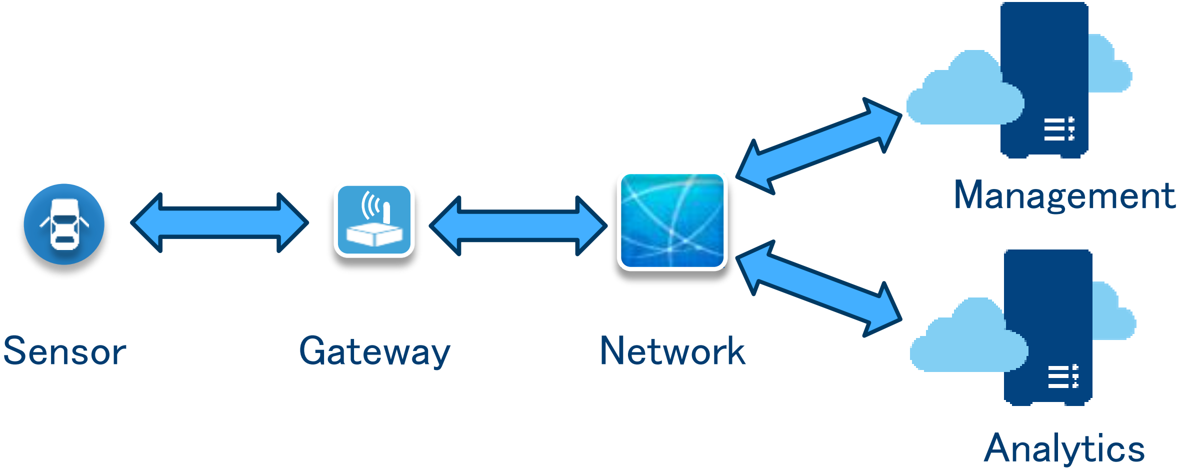
Isolated execution environment

- Mitigate attempts to manipulate keys and operations



What Does IoT Need

Ecosystem

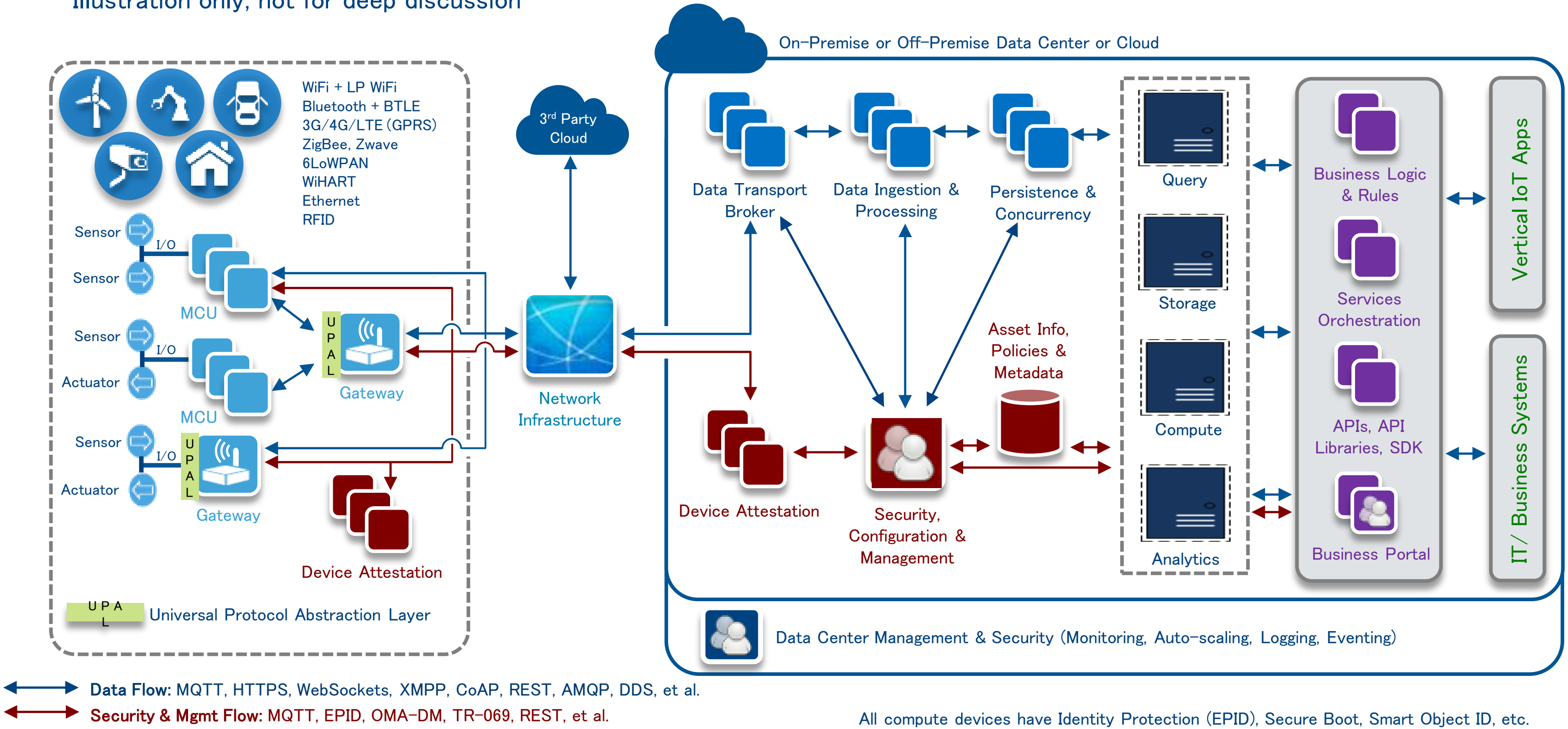


Does the ecosystem enable end to end security?

Simple goal, get data from sensor, send it up to analytics and then do something based on that analysis

Ecosystem Details

Illustration only, not for deep discussion



Data Flow: MQTT, HTTPS, WebSockets, XMPP, CoAP, REST, AMQP, DDS, et al.

Security & Mgmt Flow: MQTT, EPID, OMA-DM, TR-069, REST, et al.

All compute devices have Identity Protection (EPID), Secure Boot, Smart Object ID, etc.

Basic Questions for IoT

What device are you

- Related is what are the device properties

What is the software stack

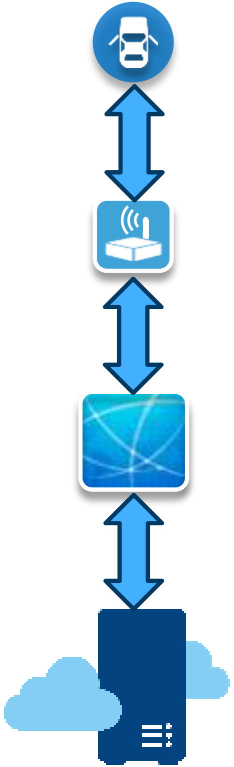
- What is the execution environment

Is there protected storage on the device

- Key material at a minimum

Is there a Trusted Execution Environment

- Mitigate software attacks, hopefully mitigate hardware attacks



Questions apply to any device in the ecosystem

How Does the TPM Fulfill the Needs

What Device Are You

Identifying the device enables analytics, operations, and management

- Can’t rely on data or send commands to unknown device

TPM provides identity

- Can be fixed with Endorsement Key (EK), anonymous with Attestation Identity Key (AIK), or provisioned by application

Identities can be controlled using TPM authorizations

- Richer set of authorizations in 2.0

What is the Software Stack

Identifying the software in use enables management, updates, and finer control

Software identity comes from RTM

TPM provides ability to attest to the software and allow authorizations and decisions based on the software identity

Is There Protected Storage on the Device

Entities want to rely on device properties and one critical property is the ability to provide long-term storage with confidentiality and integrity guarantees

TPM provides storage that has both confidentiality and integrity

Attestation proves the existence of the protected storage

Is There a Trusted Execution Environment

Need assurance that operations can occur without modification

- Especially true in keeping key material confidential

TPM has TEE mitigates both hardware and software attacks

- TPM API only allows specific operations and key material never leaves TPM without being encrypted

Usage

TPM Properties

TPMs come in many shapes and sizes

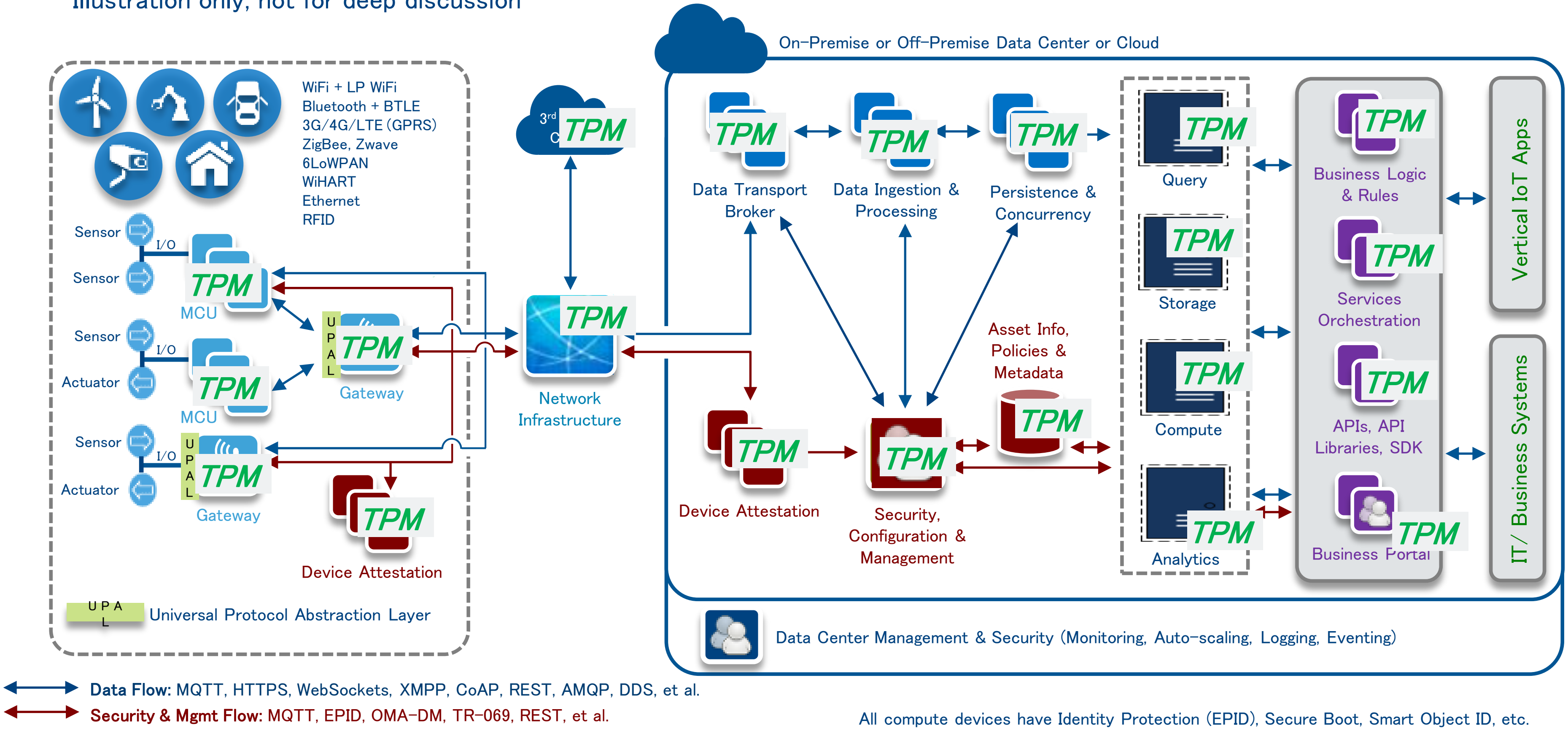
- Discrete hardware devices
- Embedded hardware devices
- Firmware implementations
- Others are possible

Different properties for each

- Need to match the properties to the platform in question
  - Sensor, gateway, network, cloud
- Specific use models matter

Where Are the TPMs?

Illustration only, not for deep discussion



Data Flow: MQTT, HTTPS, WebSockets, XMPP, CoAP, REST, AMQP, DDS, et al.

Security & Mgmt Flow: MQTT, EPID, OMA-DM, TR-069, REST, et al.

All compute devices have Identity Protection (EPID), Secure Boot, Smart Object ID, etc.

Questions Again

What device are you

- TPM provides identity

What is the software stack

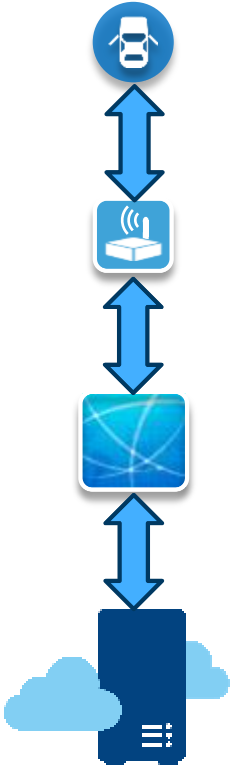
- TPM provides RTM and attestation

Is there protected storage on the device

- TPM provides storage

Is there a Trusted Execution Environment

- TPM operations execute inside of TPM



TPM provides the glue that can tie the stack together

Questions?

Legal Information

Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at www.intel.com

Intel, the Intel logo, are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

intel®

Security