Teserakt

IoT, M2M, V2V:
The needs for and evolution towards end-to-end encryption

Jean-Philippe Aumasson

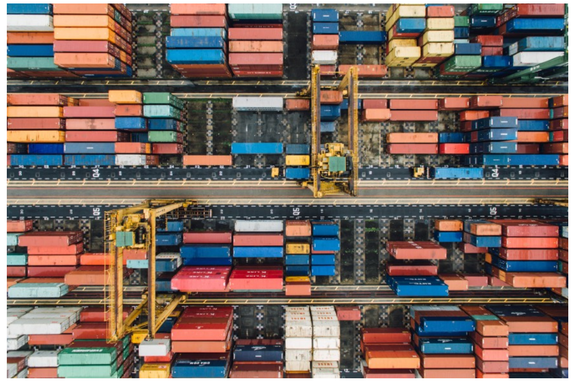
Industrial IoT – a.k.a. “IIoT”

Automotive

Healthcare

Transportation

Oil and Gas



Supply Chain

Energy and Smart grid

Example: automotive

- Vehicle tracking
- Connected cars

Communications

- V2V Vehicle-to-Vehicle
- V2I Vehicle-to-Infrastructure
- V2P Vehicle-to-Pedestrian
- V2N Vehicle-to-Network

Used by most major carmakers

Human-to-human mobile messaging

2012
Nothing encrypted

Competitive advantages
Snowden revelations
Privacy concerns
Progress in crypto

2019
Encryption everywhere

IoT/M2M communication today

2019
Nothing encrypted

Future

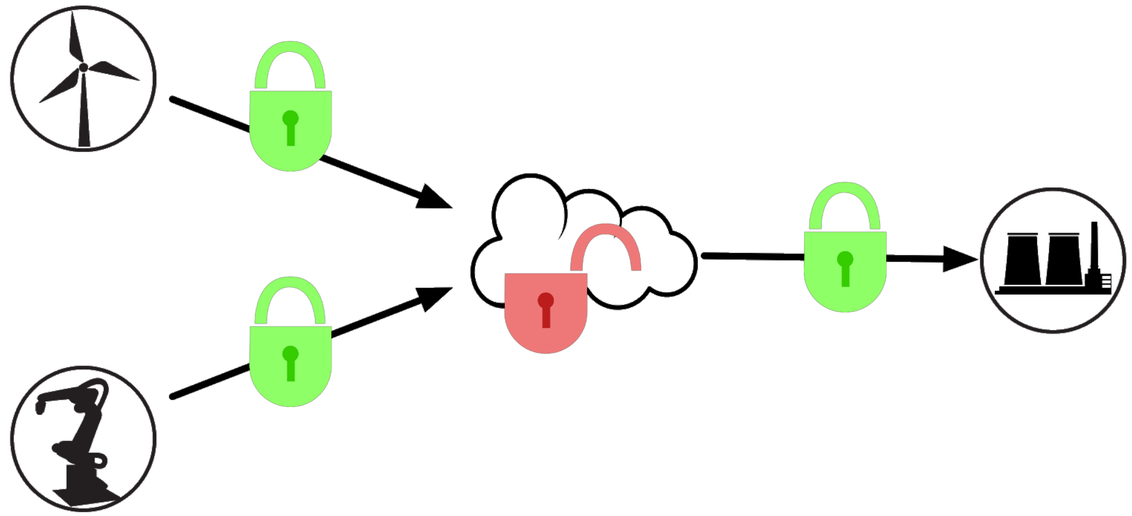
Privacy concerns
Mature technology
Safety-critical systems
Regulatory constraints

Forbes

The Case For End-To-End Encryption

Insecure IoT devices to be prohibited, US Federal purchases restricted

IoT communication security today

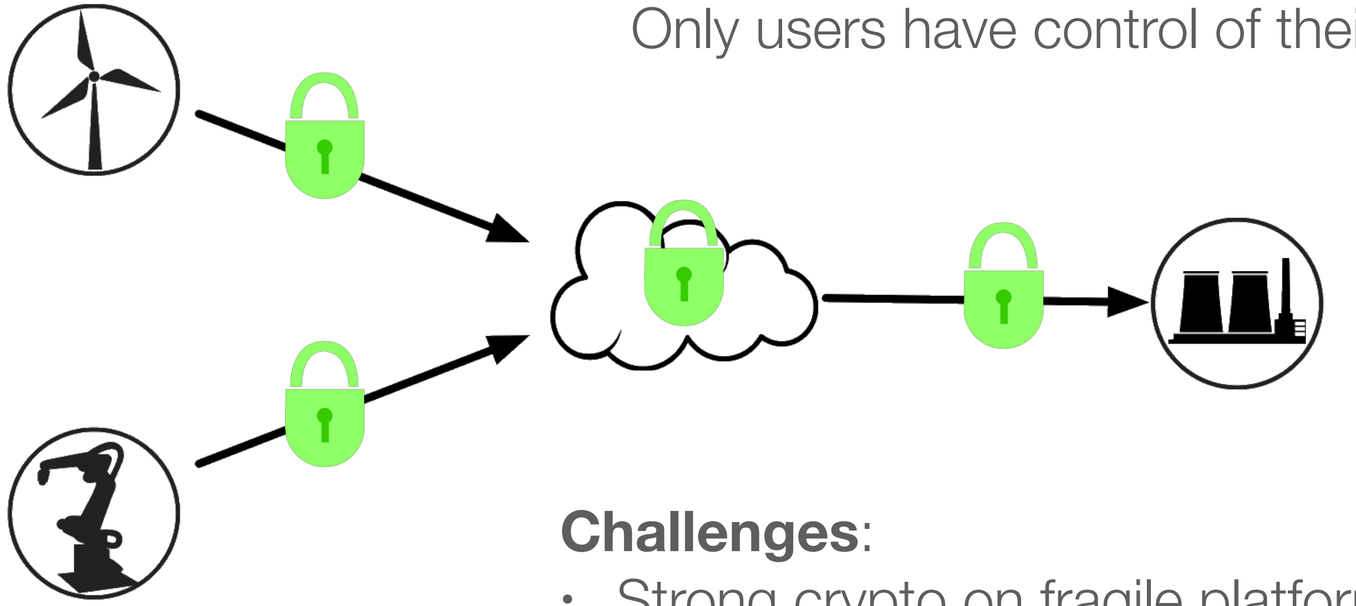


Client-server encryption (typically TLS)

Data is exposed in clear and modifiable without the final recipient noticing

Adversaries: external attackers, insiders, or users

IoT communications security tomorrow



Only users have control of their data

Challenges:

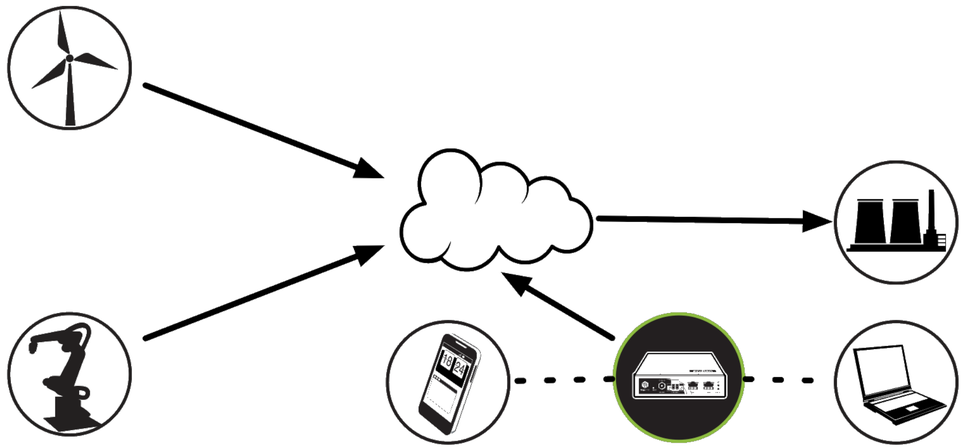
- Strong crypto on fragile platforms
- Performance constraints (CPU, bandwidth)
- Out-of-order / undelivered messages
- Key management / distribution

Example: MQTT

- Main IoT/M2M protocol, established industry standard
- Only IoT protocol supported by leading cloud platforms

- Publish-subscribe pattern: **broker can read all the messages**

Possible approach: server acting as an MQTT client, avoiding changes to the broker



The IoT crypto problem

IIoT platforms are different environments than phones or big computers:

- **Performance constraints**, e.g. latency, code size, RAM
- **System constraints**, e.g. no clock, no PRNG, no filesystem, no storage
- **Network constraints**, e.g. limited bandwidth, fixed message size
- **Crypto constraints**, e.g. fixed set of algorithms available

NIST's ongoing project aims to address performance constraints by standardizing "lightweight" ciphers

The key management problem

THE hardest crypto problem in practice

Most challenging in IoT, when

- Devices are **not always online**
- **Public-key** crypto may be unavailable
- **Message size** is limited, etc.

How to securely provision unique per-device keys?

How to have secure group messaging? (forward/backward secrecy)

How to implement key rotation/distribution securely?

The key management problem

THE hardest crypto problem in practice

Most challenging in IoT, when

- Devices are **not always online**
- **Public-key** crypto may be unavailable
- **Message size** is limited, etc.

“Can't we use the same transparent crypto as in WhatsApp?”

No. The Signal protocol is way too heavy and complex for most IoT systems:

Too heavy for many platforms, large state, difficult to scale, optimized for chat-like messaging rather than IoT topologies, etc.

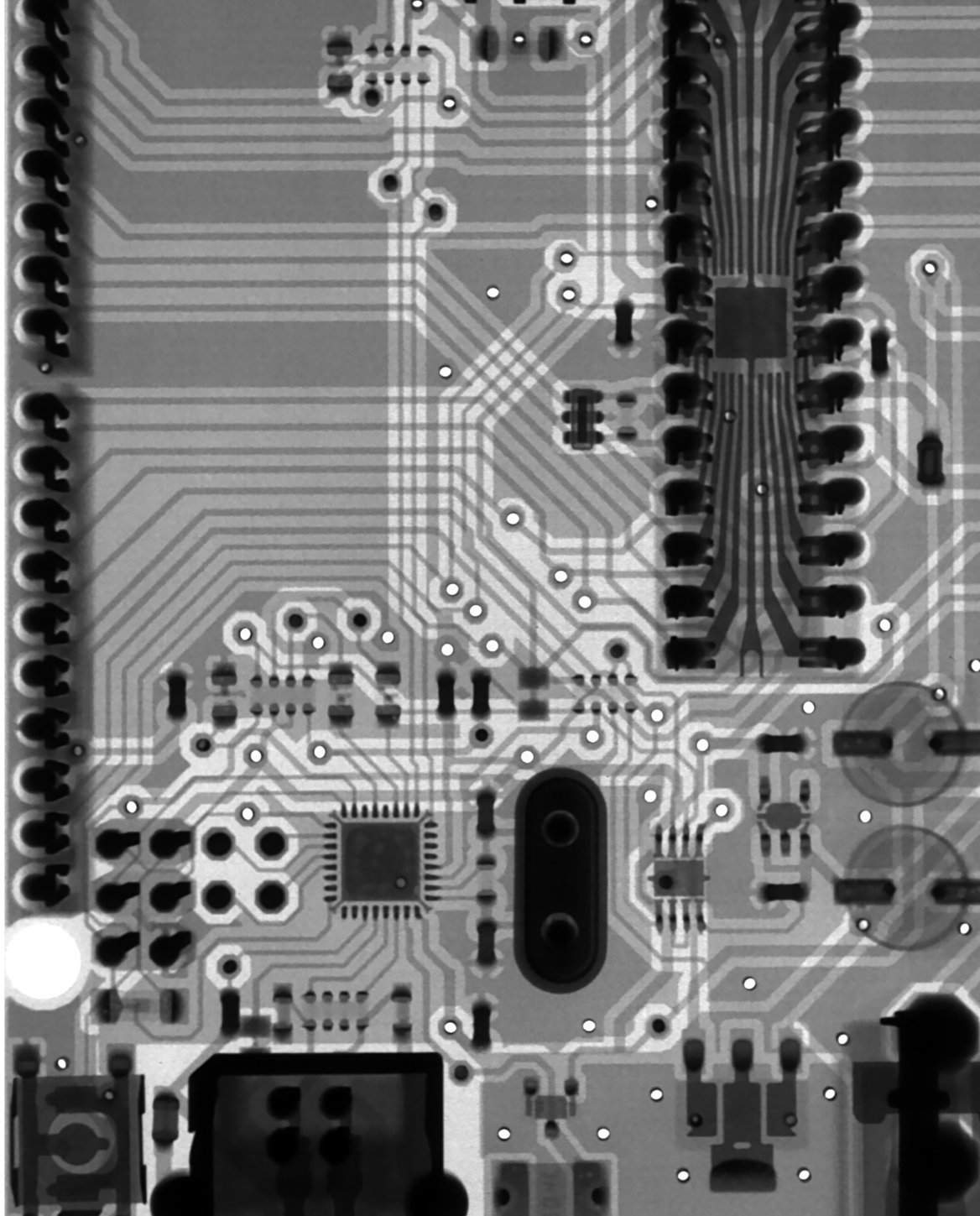
Crypto isn’t enough

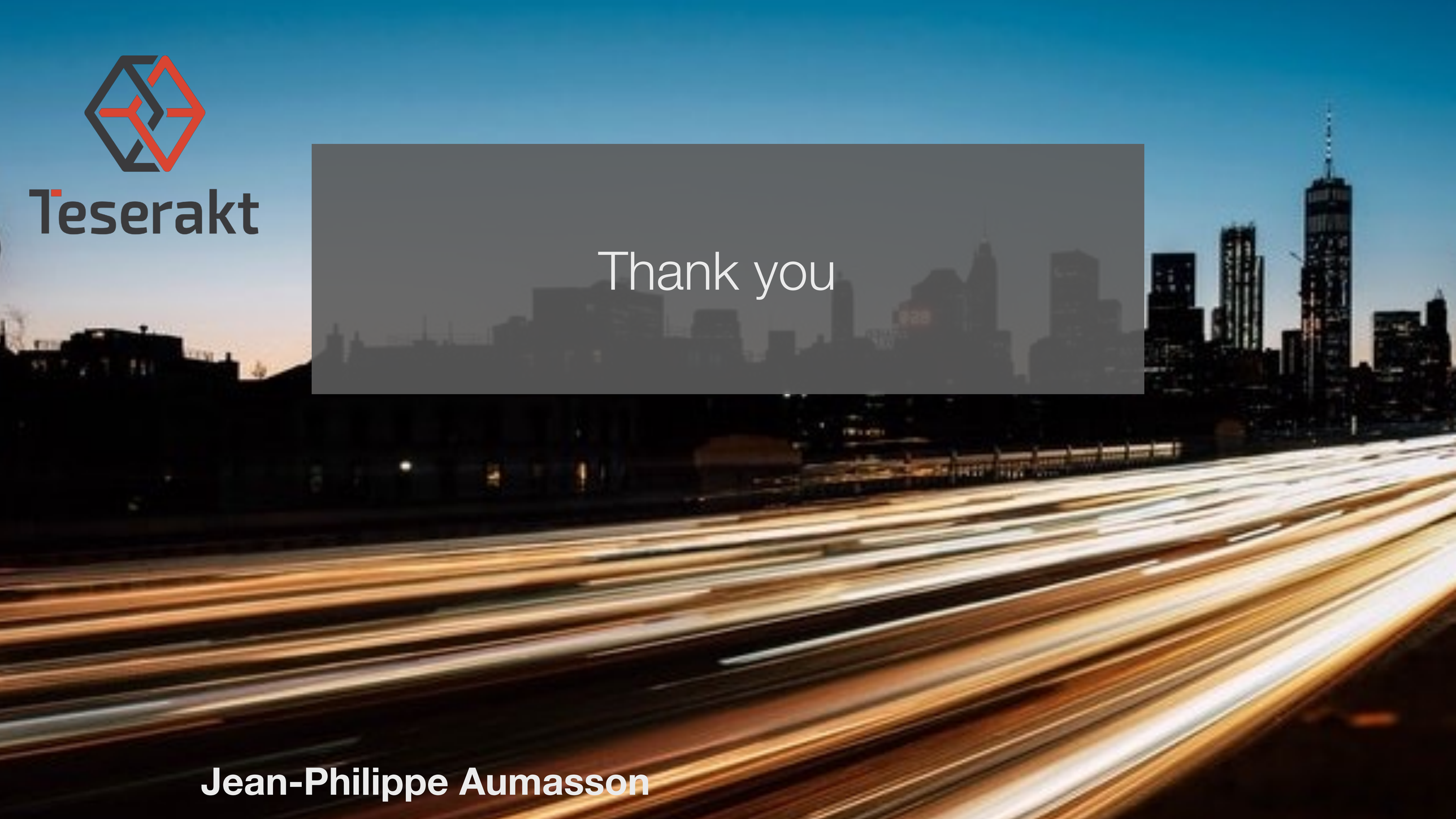
Many notions of security:

- **End-to-end security**
  Confidentiality, integrity & more
- **Endpoint security**
  Firmware security, configuration, secure storage, etc.
- **Transport security**
  Client–server links, authentication..
- **Anonymity / untraceability**

Why end-to-end security in your IoT networks?

- **Better be early than late adopter**
  The evolution is guaranteed to happen when sensitive data is transmitted
- **Enabler of new applications** involving sensitive data; privacy-, safety-, or business-critical
- **Peace of mind:** Use third-party services without having to trust them
- **Regulatory compliance** (GDPR, etc.)




Teserakt
Thank you
Jean-Philippe Aumasson