Do not trust your neighbors!
A small IoT platform illustrating a man-in-the-middle attack

Renzo Navas, Hélène Le Bouder, Nora Cuppens, Frédéric Cuppens, Georgios Z. Papadopoulos

contact: prenom.nom@imt-atlantique.fr

Figure – The IoT-driven robot arm bartender

Heterogeneity, Connectivity and Interoperability

- Heterogeneous devices and networks are the norm.
- IPv6 connects billions of devices end-to-end.
- IoT mesh-networks: nodes relay messages to each other.
- The Constrained Application Protocol (CoAP) facilitates application-layer interoperability (the HTTP of IoT).

A Man-in-the-Middle attack

- Insider IoT-node is compromised.
- IoT malicious-mode activation (A)
- In-transit message modification: The compromised node does not relay some legitimate messages for the target (B), but transmits modified messages to disrupt the normal behavior of the platform (B’).
- The target can not detect the attack (lack of end-to-end security).

Security solution proposals

- CoAP, CBOR, COSE... are building blocks to define security services.
- Example of services: authenticated encryption, key establishment, resource access authorization...
- Hardware secure-elements should be present too (e.g. to store keys).

Conclusion

- Security services must be guaranteed end-to-end.
- Principle of least privilege: do not trust your neighbors! trust them only with what they need to be trusted.