SIEMENS

Siemens Corporate Technology | July 2016

OAuth for Operational Technology?

OAuth Security Workshop 2016 - July 14/15, 2016 - Trier

© Siemens AG 2016. All rights reserved

What Is Operational Technology?

- Operational Technology (short: OT) comprises "*hardware and software that detects or causes a change through the direct monitoring and/or control of* ***physical devices****,* ***processes*** *and* ***events*** *in the enterprise*" (source: Gartner)
- Examples: building/traffic management, manufacturing, utilities (energy/water supply…), transportation…
- Common ground: IT, IoT and OT utilize software and communication technologies to implement **distributed systems**

© Siemens AG 2016. All rights reserved

How Does OT Differ? *Vs. IoT*

- OT:
  - **Traditional**
  - **Brown-field** i.e. existing components/metadata objects/products…
  - Focus on **capital goods** owned by legal entities
- IoT:
  - **Emerging**
  - **Green-field** i.e. new components/metadata objects/products…
  - Inclusion of **consumer goods** owned by individuals

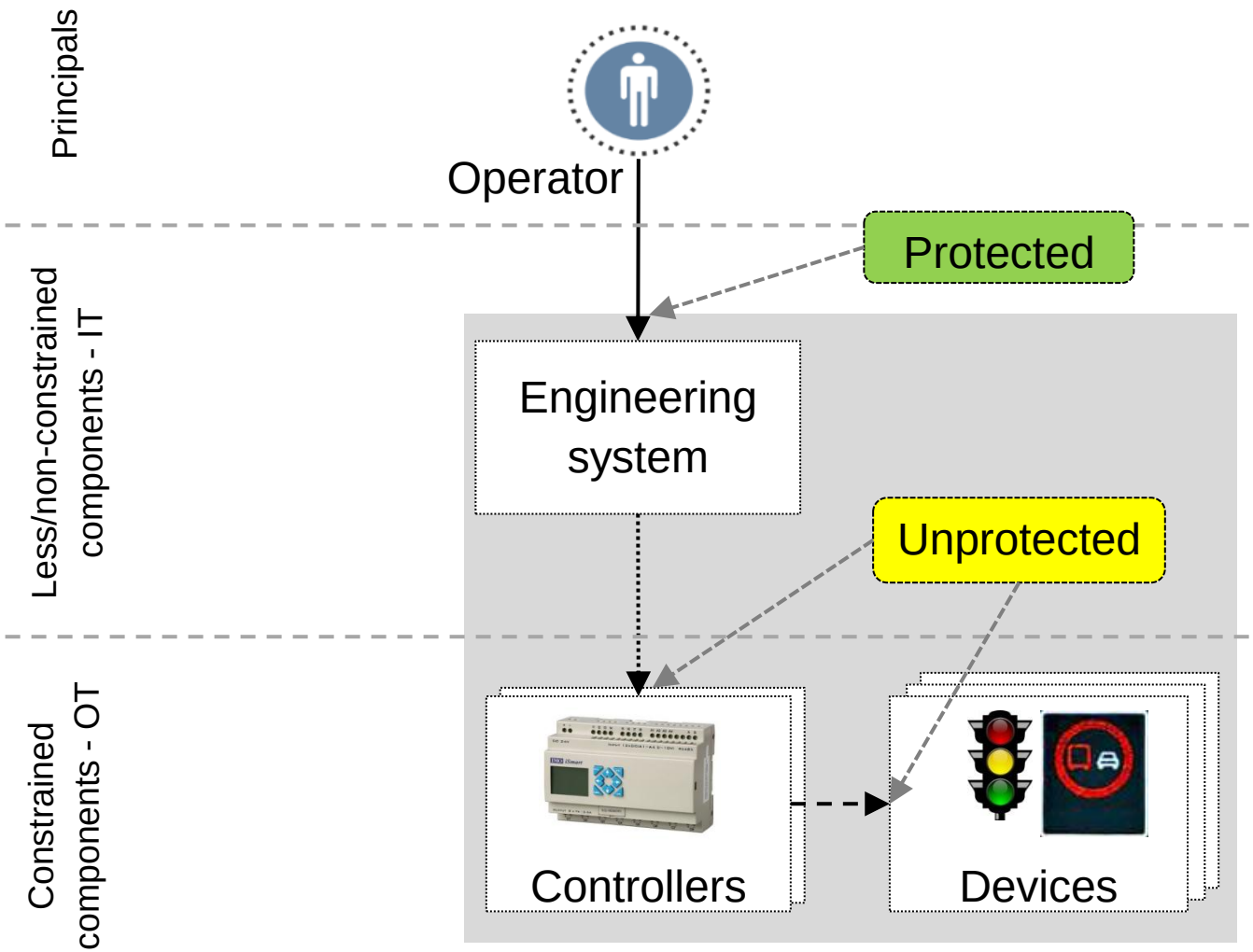
© Siemens AG 2016. All rights reserved

How Does OT Differ? *Vs. IT*

- OT:
  - **Physical objects** - *"things"*
  - **Constrained** computing devices
  - **Domain-specific protocol stacks** e.g. BACnet, CAN bus, Modbus
- IT:
  - **Digital objects** - *"information"*
  - **Less/unconstrained** computing devices
  - **Internet stack** i.e. TCP/IP and esp. HTTP

© Siemens AG 2016. All rights reserved

How About Security?



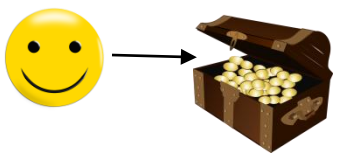
© Siemens AG 2016. All rights reserved

Why Worry?

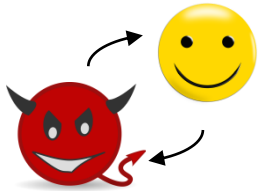
- *Loss of the old perimeter*
  - Legacy mindset: ***every production is an island***
  - Next generation: ***no production is an island***
    - Aka I4.0, IIoT, Industrial Internet…

© Siemens AG 2016. All rights reserved

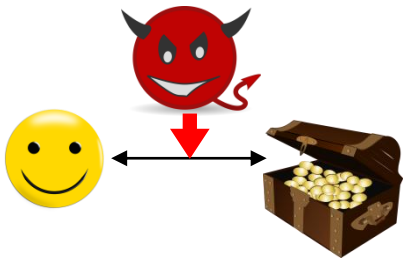
What Must Be Achieved?



- **Authorization:** *determine if attempted resource access is okay*
  - Concerns instructions received over the network
  - Protects against illegal/unwanted resource accesses



- **Entity authentication**: *check properties claimed by an actor*
  - Concerns identifiers, attributes, affiliations, assignments… claimed by remote actors (callers, callees)
  - Protects against identity spoofing/masquerading



- **Message authentication**: *verify contents of received messages*
  - Concerns message contents received over the network
  - Protects against manipulations

© Siemens AG 2016. All rights reserved

How To Do The Trick?

- The **same security requirements** hold for mail/bank accounts and other private resources on the Internet.
- In Internet security they are addressed as follows (with GMail as an example):
  - Authorization: the authenticated identifier of the **requestor is checked** against the identifier of the mail account **owner**.
  - Entity authentication: callee authentication relies on **SSL/TLS server authentication** utilizing X.509 certificates. Callers authentication uses **username/password** or **one-time-password** credentials.
  - Message authentication: done on **transport-level** by means of **SSL/TLS**.
- But the well-known Internet security tools don't do it, at least not by copy&paste:
  - Authorization: solutions that assume to interact with the resource owner as an attentive/responsive individual **don't help** – *ownership is different*
  - Entity authentication: solutions that authenticate Web users and Web servers **don't do it**– *protocol stacks and form-factors are different*
  - Message authentication: SSL/TLS resp. DTLS are often **unavailable,** possibly **out-of-reach**

© Siemens AG 2016. All rights reserved

How to Deal With That? What Might Be Borrowed?

SIEMENS

- Options for establishing OT security mechanisms:
  - Create security mechanisms for from scratch building upon primitives e.g. cryptographic algorithms ➔ *tedious, expensive*
  - Borrow and transform security mechanisms from other domains ➔ *let's look again at the Web and its security*
- Traditional Web security technologies - since 1990: *not promising*
  - Security for **presentation-oriented Web applications**
  - Proprietary approaches for user authentication and authorization
  - **SSL/TLS** for server authentication as well as message authentication and confidentiality on transport-level
- New Web security technologies – since 2010: *promising*
  - Security for **service-oriented Web applications** (Web APIs/REST)
  - **OAuth, OIDC, JOSE** for user/client authentication and authorization as well as application-level message authentication and confidentiality
  - Re-using SSL/TLS for server authentication as well as message authentication and confidentiality on transport-level

© Siemens AG 2016. All rights reserved

Why Is OAuth Appealing?

- ***Feature match***: cares about authorization, entity authentication and (with PoP) message authentication on application-level – *aliens would not help*
- ***Software availability***: production-grade and extensible software components are available - *facilitating re-use*
- ***Production use***: OAuth already is in large-scale production use in the IT domain and protects mission-critical assets - *providing re-assurance*
- ***Divide-and-conquer***: built on the principle of offloading complex security processing tasks from resource servers – *needed for structuring complex systems*
- ***Uneven distribution of complexity***: on side of clients and resource servers OAuth is lightweight/in-complex – *helping constrained components*
- ***Variety of security models***: protected/unprotected registrations, bearer/PoP tokens, revocation etc. – *facilitating diversity*
- ***Versatile security tokens***: supports application or domain-specific token contents – *one-size-fits-all tokens would not help*
- ***Extensibility***: supports additional endpoints, grants, parameters and values – *allowing adaptations*

© Siemens AG 2016. All rights reserved

Which Gymnastics Are Needed?

- ***Protocol bindings***: OT does not rely on HTTP ➔ adapt the supply of added objects to other request/response protocols or even beyond that
- ***Response signing***: SSL/TLS resp. DTLS are often unavailable ➔ use PoP, add response signing
- ***Stateful engines/protocols***: protocols often are stateful ➔ optimize the contents of added objects and exchanges
- ***On-behalf-of***: constrained components may be unable to acquire tokens or register by themselves ➔ accommodate less constrained (helper) components
- ***Legal entity-owned resources***: assets are usually owned by legal entities ➔ don't rely on the resource owner as an attentive/responsive individual actor in authorization decision making
- ***Metadata integration****:* rich component metadata does already exist and is managed elsewhere ➔ re-use and complement that; change only on invitation
- ***Relationship management integration***: relationship information does also exist and is managed ➔ don't start authorization strategies from scratch
- ***Profiling***: components might have unusual properties e.g. perception of time ➔ profile added objects and exchanges accordinly

© Siemens AG 2016. All rights reserved

Conclusion

- OAuth already is in large-scale **production use**. It also is **still evolving** as a building block for Web security
- OT security-enabling is in its **incubation**
- An adoption of OAuth (and related technologies e.g. ACE, JOSE) appears to present a **shortcut** solution towards OT security
- This will depend on some **modifications** and **extensions**:
  - OAuth specifications address extensibility
  - Best-in-class OAuth software components allow implementing them

© Siemens AG 2016. All rights reserved

Abbreviations

ACE	Authentication and authorization for Constrained Environments
API	Application Programming Interface
BACnet	Building Automation and Control networks
CAN	Controller Area Network
DTLS	Datagram Transport Layer Security
I4.0	Industry 4.0
IIC	Industrial Internet Consortium
IIoT	Industrial IoT
IoT	Internet-of-Things
IT	Information Technology
JOSE	JSON Object Signature and Encryption
JSON	JavaScript Object Notation
OAuth	Open Authorization
OIDC	OpenID Connect
OT	Operational Technology
PoP	Proof-of-Possession
REST	REpresentational State Transfer
SSL	Secure Sockets Layer
TLS	Transport Layer Security

© Siemens AG 2016. All rights reserved

Author

Oliver Pfaff, Siemens AG, CT RDA ITS

© Siemens AG 2016. All rights reserved