Report:
W3C IG on Web-of-Things
Security and Privacy

Oliver Pfaff
(oliver.pfaff@siemens.com)

Coordinates

- **Abbreviation**: SP
- **Mailing list prefix**: [IG-SP]
- **Landing page**: https://www.w3.org/WoT/IG/wiki/Security,_Privacy_and_Resilience (linked on the Wiki page of the W3C WoT IG)

Call For Action

- **Provide a helicopter view** by creating/supplying deliverables in style of analyst reports
  - Note: this holds for the current phase (until ca. EoY)
- Rationale:
  1. (Almost) all IoT/WoT products/projects face SP challenges
     – *need is unquestioned*
  2. Most seem to do some ad-hoc without (yet) having a big picture
     – *directions are needed*
  3. Confusion about new security mechanisms (see below) seems omnipresent
     – *muddying the water*

Main Deliverables

- Landscape of Security&Privacy Means:
  - Objective: survey the landscape of security&privacy means for WoT
  - Status: work-in-progress
    - High-level structure exists, distinguishes design-time and runtime means
    - Initial list of design-time mechanisms exists
    - Drill-down structure for design-time mechanisms exists
    - Initial elaboration exists for: **JOSE**, **OAuth-for-CoAP**, **DTLS**
- Security&Privacy Requirements Catalogue:
  - Objective: service document for the use case authors/owners in the WoT IG
  - Status: work-in-progress
    - Initial list of requirements exists
    - Initial elaboration exists for: **entity authentication**, **SSO**, **things authorization**

Supporting Documents

- Challenges:
  - Objective: complementary view focusing on given constraints such as unattended operations, limitations in I/O, CPU/memory, network connections, “patchability” etc.
  - Status: work-in-progress, initial draft exists
- Advanced Concepts:
  - Objective: complements the (atomic) view of the security privacy requirements and landscape with a composite view. Example: **end-to-end security**
  - Status: work-in-progress, initial draft exists
- Glossary:
  - Status: work-in-progress, initial draft exists
- References:
  - Status: work-in-progress, initial draft exists

Requirements Shopping

(*note: early preview, to-be-discussed/completed*)

		Consumer goods				Capital/investment goods						
		Home automation	Health monitoring	Sports and entertainment	Car connectivity	Building automation	Smart metering	Industrial control systems	Container monitoring	Lightning systems	Public safety	Door lock systems
Provisioning and management												
	Commisioning (of the physical device)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Supply of credentials (by/for the device)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)
	Supply/registration of device metadata	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)
	Management of device metadata	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)	Y (implied)
Authentication and authorization												
	Initial entity authentication (of/at the device)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	SSO	N	N	N	N	N	N	N	N	N	N	N
	Authorization (of/for the device)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Secure communications												
	Data origin authentication and integrity (of messages sent by/to the device)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Confidentiality (of messages sent by/to the device)	(Y)	Y	(Y)	(Y)	(Y)	(Y)	(Y)	(Y)	(Y)	(Y)	(Y)
Misc												
	Throttling/rate limitations	?	?	?	?	?	?	?	?	?	?	?
	Intrusion detection/prevention	?	?	?	?	?	?	?	?	?	?	?
	Pseudonymization and anonymization (of PII)	?	Y	(Y)	?	?	?	?	?	?	?	?

Requirements Fulfillment (1)

Design-Time Mechanism Clustering

- **Classic**:
  - *Synopsis*: invented <2010, native to enterprise/office-IT resp. traditional Web
  - *Shopping list*: Diameter, Kerberos, LDAP, P3P, PKCS, PKI, RADIUS, S/MIME, SAML, SSL/TLS/DTLS, WS-*, X.509, XML Signature/Encryption…
- **New**:
  - *Synopsis*: invented 2010-2015, addressing new Web application styles (apps/APIs)
  - *Shopping list*: FIDO, JOSE, OAuth, OIDC, SCIM, UMA…
- **Future**:
  - *Synopsis*: >2015, native to IoT/WoT
  - *Shopping list (initial)*: ACE (incl. DCAF, TWAI, OAuth/UMA…), COSE, DICE…

Requirements Fulfillment (2)

(*note: early preview, to-be-discussed/completed*)

		Classical				New			Future	
		Kerberos	LDAP	SAML	SSL/TLS	JOSE	Oauth	OIDC	COSE	DCAF
Provisioning and management										
	Commisioning (of the physical device)	N	N	N	N	N	N	N	N	N
	Supply of credentials (by/for the device)	N	N	N	N	N	N	N	N	N
	Supply/registration of device metadata	(Y)	(Y)	N	N	N	(Y)	(Y)	N	N
	Management of device metadata	N	(Y)	N	N	N	(Y)	(Y)	N	N
Authentication and authorization										
	Initial entity authentication (of/at the device)	(Y)	((Y))	N	Y	N	(Y)	(Y)	N	Y
	Transfer of initial authn/SSO	(Y)	N	(Y)	((Y))	N	(Y)	(Y)	N	Y
	Authorization (of/for the device)	(Y)	N	N	N	N	(Y)	N	N	Y
Secure communications										
	Data origin authentication and integrity (of messages sent by/to the device)	(Y)	N	N	Y	Y	N	N	Y	N
	Confidentiality (of messages sent by/to the device)	Y	N	N	Y	Y	N	N	Y	N
Misc										
	Throttling/rate limitations	N	N	N	N	N	N	N	N	N
	Intrusion detection/prevention	N	N	N	N	N	N	N	N	N
	Pseudonymization and anonymization (of PII)	N	N	(Y)	N	N	N	(Y)	N	N

Resulting Recipe

(for W3C WoT IG Participants ;-)

1. Look up your use case in the requirements shopping table
2. Get your resulting SP requirements list
3. Per item on the SP requirements list, look up the SP mechanism candidates table
   - Beware: the set of future mechanisms evolves right now
4. Make your selection and create your cocktail of (design-time) SP mechanisms

Small-print:

- We can not preemptively do the architectural work (with respect to SP) of your IoT/WoT <superDuper> project
- We will (hopefully) help this work by providing a big picture

Action Items (@all)

1. Make sure your use cases are reflected in SP
2. Make sure to use SP deliverables when describing (SP for) your use cases
3. Make sure the SP mechanism candidates list contains all your favorites
4. Make sure the SP drill-down provides information that compiles for you