W3C Workshop on the Web-of-Things | Berlin | June 25-26, 2014

Authentication for the Web-of-Things

Oliver Pfaff
Why Am I Here?

- Buy a Siemens product → get a **distributed IT-system** or part thereof
  - *Today*: true for the majority of products
  - *Tomorrow*: growing share
- Siemens products handle **valuable resp. sensitive resources**
  - Corporate or private property
  - Critical infrastructure
  - Health information,…
- Old school solutions in “*We Don’t Check Individual Objects—Because We Control Premises*”-style approach end-of-life → need to **assess individual requests and messages**
  - Authentication (*who sent this information, is it unaltered?*) presents a vital part of such assessments
Does a Best Practice Exist?

1. Authn user
2. Get VINs/vehicle metadata
3. Select car
4. Do things remotely…

Public-facing Web applications

5. Backend operation with VIN

Car connect infrastructure

6. Instruction msg to IMSI
7. Get details

Connected car

Embedded communication endpoint

Mobile app

Vin

User store

User<X>:
User id, Password, VINs…

Vehicle store

Vehicle<Y>:
VIN, IMSI…

CRM store

External networks

Ext. perimeter
(arbitrary clients)

Internal network

Ext. perimeter
(dedicated devices)

Virtual private network

Page 3  June 2014  Corporate Technology

© Siemens AG 2014. All rights reserved
Does It Provide an Overall Solution?

- The *connected car* use case is already **real**. The solutions use some **tricks**:
  - **Layered architecture**: user agents call public-facing Web applications, not the car connect infrastructure or a connected car
    - Certain CRM information is not revealed to public facing Web applications and mobile apps – for instance IMSI numbers
    - The fact that the service is public-facing does not imply that devices are public-facing
  - **Flipping roles**: cars serve user requests but act in HTTP client role, not HTTP server role
    - Infrastructure is identified by URLs and authenticated through SSL/TLS server authentication – the traditional approach in the Web
    - Car is identified by IMSI and authenticated by knowledge of random values (pushed with instruction message to IMSI) – resembling current approaches in e.g. electronic banking (buzzwords: mobile OTP/TAN)
- But it does **not** provide an overall solution for authentication in the Web-of-Things
  - The required **device connectivity** will not always be supplied in form of virtual private networks or by mobile network operators
  - Embedding mobile network endpoints incl. SIM cards and managing their contracts is feasible for things of a certain **object size** (say >1m³) and **value** (say >10.000$)
How Will It Look Like?

**Direct:**

- Claimant → Authentication protocol → Verifier and relying party

Examples: WLAN authentication (shared secret key)
Occurrence: ubiquitous (network access), rare (Web applications)

**Inline third-party, trusted:**

- Claimant → Authentication protocol → Verifier and intermediary → Authentication event information → Relying party

Examples: HTTP Basic
Occurrence: ubiquitous (multi-tiered Web applications, e.g. Java EE)

**Inline third-party, untrusted:**

- Claimant → Authentication protocol → Verifier and intermediary → (No authentication event information) → Verifier and relying party

Examples: OAuth (authz code)
Occurrence: increasing (composite applications, mash-ups)

**Online third-party, trusted:**

- Claimant → Authentication protocol (here: initial credentials) → Verifier and relying party

Examples: Kerberos, SAML, OID, OIDC
Occurrence: ubiquitous (Windows domains, Web SSO systems, social login)

Reverse proxies externalizing initial user authn to login applications

OAuth authz endpoints externalizing initial user authn to login applications
So, Why Am I Here?

- **Mantra:**
  - Security is a key concern of distributed IT-systems
  - Authentication is a key discipline in IT-security
  - There are prerequisites for authentication as well as aftermaths
    - Prerequisites: management of entity identities and credentials
    - Aftermaths: SSO (preserving authentication), authorization and personalization (consuming it)

- In the past 30 years the main focus was on authenticating human users to Internet and Intranet applications esp. Web applications (and vice versa):
  - A set of mechanisms, solutions and practices was established which enable the Web that we know
    - Modulo some tweaks e.g.
      - What’s beyond static passwords?
      - Do people really comprehend SSL/TLS server authentication?
    - Some of that innovation is recent e.g. context-based, adaptive user authentication or OAuth

- This helps but also leaves a bulk of challenges for the Web-of-Things—we’ll have an exciting decade:
  - Authenticating users to devices (and vice versa): accommodate intermediaries, support non-HTTP protocols, establish user-managed authorization…
  - Authenticating devices to applications as well as other devices: define and manage device identity and credentials, protect their bindings to devices, implement authentication protocols and infrastructure, establish user-managed authorization…
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation (Abb)</th>
<th>Description</th>
<th>Abbreviation (Abb)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authn</td>
<td>Authentication</td>
<td>TAN</td>
<td>TransAction Number</td>
</tr>
<tr>
<td>Authz</td>
<td>Authorization</td>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>CAN</td>
<td>Controller Area Network</td>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>CRM</td>
<td>Customer Relationship Management</td>
<td>VIN</td>
<td>Vehicle Identification Number</td>
</tr>
<tr>
<td>HTTP</td>
<td>HyperText Transfer Protocol</td>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>IAM</td>
<td>Identity and Access Management</td>
<td>WoT</td>
<td>Web-of-Things</td>
</tr>
<tr>
<td>Id</td>
<td>Identifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IoT</td>
<td>Internet-of-Things</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Java EE</td>
<td>Java Enterprise Edition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OAuth</td>
<td>Open Authorization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OID</td>
<td>OpenID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OIDC</td>
<td>OpenID Connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OTP</td>
<td>One-Time Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSO</td>
<td>Single-Sign-On</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TAN</td>
<td>TransAction Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VIN</td>
<td>Vehicle Identification Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WoT</td>
<td>Web-of-Things</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Abbreviations</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How Does the Web Evolve?

1995

- **Database-backed applications**, desktop browsers, read-only

2000

- **Browser-based apps**
  - Mobile browser
  - Web browser
  - **AJAX**
  - Mobile apps

2005

- **Composite applications**
  - XML, JSON

2010

- **Things-backed applications**
  - Mobile browsers/apps, **Composite** applications

**Web application**

- **Web container**
  - HTML, XML, JSON

- **User**

**The Web we are familiar with**

- **Web**
  - Mobile browsers/apps, **Web 2.0**, AJAX clients

- **Database** (or directory…)
  - SQL (or…)

**How Does the Web Evolve?**