Uptane: Virtual Workshop
“A Conversation on End-to-End Secure Automotive Software Updates”

https://uptane.github.io
2023-03-31
Uptane Development Timeline

- **2015**: US DHS issue grant
  - NYU, UoFM UMTI, and SwRI receive grants from DHS and decide to combine efforts

- **2016**: First Workshop
  - Uptane held first industry workshop

- **2017**: Uptane Alliance
  - Uptane Alliance organized under IEEE-ISTO

- **2018**: Uptane joins Linux Foundation
  - Uptane Alliance formally joins the Linux Foundation as a Joint Development Foundation project

- **2019**: Uptane 1.0.0
  - Uptane Standard 1.0.0 released under IEEE-ISTO

- **2020**: Uptane 1.0.1 & 1.2.0
  - Uptane Standard 1.0.1 errata release under Linux foundation.

- **2021**: Uptane 1.1.0 & 1.2.0
  - Uptane Alliance organized under IEEE-ISTO

- **2022**: Uptane 2.0.0
  - Uptane Standard 2.0.0 released. First major revision change to the standard.

- **2023**: Uptane 2.1.0 & 2.2.0
  - Releases planned for 2023 Q2 and Q4
## Alignment with Standards and Regulations

### Standards

<table>
<thead>
<tr>
<th>ISO/SAE 21434</th>
<th>Road vehicles — Cybersecurity engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 24089</td>
<td>Road Vehicles – Software Update Engineering</td>
</tr>
<tr>
<td></td>
<td>Base requirements for SUMS</td>
</tr>
</tbody>
</table>

### Regulations

<table>
<thead>
<tr>
<th>UN R155</th>
<th>Cybersecurity and cybersecurity management system (CSMS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>UN R156</td>
<td>Uniform provisions concerning the approval of vehicles with regards to software update and software update management systems (SUMS)</td>
</tr>
</tbody>
</table>
Threat Categories

**Read** the contents of updates to discover confidential information, reverse-engineer firmware, or identify security fixes to determine the fixed security vulnerability.

**Deny** installation of updates to prevent vehicles from fixing software problems.

**Disrupt** ECUs in the vehicle, denying use of the vehicle or of certain functions.

**Control** ECUs within the vehicle, and possibly the vehicle itself.
Uptane Goals

- Prevent known attacks on software update systems
- Provide compromise resilience and security by design
- Minimize damage from a compromised signing key or repository
Offline and Online Key Benefits

The OEM needs to tell ECUs which software is authentic and should be installed.

<table>
<thead>
<tr>
<th>Online Keys</th>
<th>Offline Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interactive signing</td>
<td>One-time signing</td>
</tr>
<tr>
<td>Addresses real-time</td>
<td>Strong compromise resistance</td>
</tr>
<tr>
<td>security requirements</td>
<td></td>
</tr>
</tbody>
</table>


Offline and Online Keys

Uptane uses two repositories to provide OEMs with both **security** and **flexibility**!
Image Repository

Repository of validated and released software images
1) Human managed
2) Offline keys
3) Infrequent updates
4) Provides flexible delegation for image signing
Director Repository

Allows OEM to control which software should be installed in which vehicle

1) Automated
2) Online keys
3) Frequent requests
4) Generates signed vehicle specific manifest
5) Works in coordination with a Vehicle Configuration Database
Uptane Ecosystem

- Image Repository
- Secure Time Source
- Director Repository

Primary ECU:
- Download and verify Image and Director Repo Metadata
- Send Metadata and Images to Secondaries

Secondary ECU with Full Verification:
- Receive Metadata and Images from Primary ECU
- Verify and install

Secondary ECU with Partial Verification:
- Receive Metadata and Images from Primary ECU
- Verify partially

Uptane is the “Last Mile” in the Software Supply Chain
Threat Targets in the Software Supply Chain

Verifiably protect steps in software supply chain that could be vulnerable to compromise

- Code
- Build
- Package
- Test
in-toto

- Verifiably define the steps of the software supply chain
- Verifiably define the authorized actors
- Guarantee everything happens according to definition and nothing else
in-toto Layout -- Signed by Project Owner

```json
{
    "_type": "layout",
    "expires": "2017-08-31T12:44:15Z",
    "keys": {
        "0c6c50": {...}
    },
    "signatures": [...],
    "steps": [{
        "_type": "step",
        "name": "checkout-code",
        "expected_command": ["git", "clone", "..."],
        "expected_materials": [],
        "expected_products": {
            "CREATE": ["demo-project/foo.py"], ...
        },
        "pubkeys": ["0c6c50..."],
        "threshold": 1
    }, ...],
    "inspections": [...]
}
```
in-toto Links -- Signed Evidence for each Step

$ in-toto-run -- ./do-the-supply-chain-step
in-toto Verification

$ in-toto-verify --layout <layout> --key <pub key>
in-toto Protects Complex Supply Chains
Scudo = in-toto + Uptane

- Delivers metadata for all images securely before installation
- Enforce policies about the flow of artifacts through the supply chain
- Identifies responsibilities for in-toto verification on vehicle ECUs
- Protects complex vendor supply chains
PURE 3 Extends Uptane with Scudo

- Adopted as a formal enhancement to the Uptane Standard in March 2023
- Integrates in-toto into the automotive supply chain
- Provides protection for vehicles with constrained ECUs
## Uptane Timeline 2023

<table>
<thead>
<tr>
<th>1st quarter 2023</th>
<th>2nd quarter 2023</th>
<th>3rd quarter 2023</th>
<th>4th quarter 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>This workshop</td>
<td>Release V.2.1.0 of Standard and Deployment Best Practices</td>
<td>Hold virtual workshop in connection with escar Europe)</td>
<td>Release V.2.2.0 of Standard and Deployment Best Practices</td>
</tr>
<tr>
<td>Launch “Uptane Experience”</td>
<td>Hold in-person (or hybrid) workshop in the Detroit area in connection with escar USA (June 23, 2023)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>stories by posting the first video and soliciting other contribution</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Complete first batch of Uptane website revisions, including adding capability to incorporate wikis</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Guest Speakers
Matt MacKay

Software Supply Chain

Matt leads a diverse team that focuses on governance, risk, compliance and monitoring and response activities for GM’s Product Cybersecurity team. Specific responsibilities include incident response, coordinated vulnerability disclosure, cyber compliance, cyber threat intelligence analysis, OSS compliance, supply chain security, training, and process refinement.
Charlie is a researcher on product security and supply chain integrity at Hitachi America Ltd. He is the Chair of the Automotive ISAC SBOM Working Group and is a longtime contributor to the US Department of Commerce NTIA and DHS CISA SBOM projects. Prior to his current role, Mr. Hart held several positions as a software engineer, manager, and executive.
Open Discussion
Discussion Topic Starters

Software supply chain challenges
- Software supply chain integrity
- Software supply chain tools
- Software supply chain interface agreements
- Software supply chain development chain escrow
- Reproducible builds
- Software lifecycle (end of support and decommissioning)
Next Steps
Looking Forward

Adoption → Adaptation → Deployment

Please contact us if you are interested to join, contribute and/or learn more:
https://uptane.github.io/participate.html
Thank you.

More info at
https://uptane.github.io
Appendix
Supplemental: Scudo = in-toto + Uptane

Successful integrations of in-toto and TUF in use in production:

Integrated in-toto with Uptane considers the nuances of the auto industry:

More advanced specification of Scudo available as an upcoming Uptane PURE:
https://github.com/uptane/pures/pull/9
Supplemental: Scudo = in-toto + Uptane
Uptane POUFs (Protocols, Operations, Usage, and Formats)

- A profile layer on top of the Uptane Standard
- Allows for interoperable Uptane implementations
- Describes an implementation
  - Choices made from the Uptane Standard and Deployment Considerations
  - Networking information, file storage and data definitions
PUREs

- Modeled on TAPs from The Update Framework
- A formal method for the community to propose additions or modifications of the Uptane Standard
- Two PUREs approved to date
Education

- Whitepapers, Videos, Tutorials, etc.
- Communicating emerging issues in automotive cybersecurity
- Promoting awareness of cybersecurity issues to the automotive community
- Addressing software supply chain issues
- Topics for upcoming whitepapers: Compliance with regulations and standards, Security issues in the use of aftermarket materials, Transitioning to Uptane