Executive Summary - Uptane Workshop 6/14/19

Lois A DeLong <lad278@nyu.edu>  
To: Uptane Standards <uptane-standards@googlegroups.com>  

I am recirculating these minutes to correct an incomplete reference to the “G32” group in the “Outreach” section. Note the correction in the text below.

Executive Summary
Uptane Industry Workshop
June 14, 2019
Lear Corporation
Southfield, MI

The second Uptane Industry Workshop of 2019 was held on June 14, 2019 at Lear’s facilities in Southfield, MI. The workshop drew 24 attendees who provided important industry perspectives on the Uptane Standardization initiative, and its follow-up activities (test methods, deployment pages, supply chain).

Lightning Review of Uptane

A brief slide presentation was screened as an introduction to the project for those who might be new to it. The slides can be accessed at https://docs.google.com/presentation/d/1IBu1fx4d_nlVF-ASRLBS8LqCXnBcuJwDOilR2LSns4Q/edit?ts=5d03d89c

Uptane After IEEE/ISTO

The Uptane Alliance agreement with IEEE/ISTO comes to an end in July, which is why all work on the Standard must be completed now in order to be issued under the ISTO mantle. After July, the work will continue, but a new legal home for it will be needed. Discussions are currently underway with the Linux Foundation (https://www.linuxfoundation.org/) and this is likely where Uptane will be housed. One advantage of this affiliation is that, in addition to providing a neutral home for the project--an umbrella organization that can extend to it all the privileges of a non-profit--but it also offers a future path to ISO standardization in the near future.

Like the IEEE/ISTO arrangement, the Linux Foundation places no restrictions on what Uptane can do, allows us to offer memberships to companies and organizations at no cost., and does not involve a transfer of copyright. Unlike the previous arrangement, there will be no charge, either for Linux services or for the path to ISO standardization.

Developing and Implementing an Uptane Test Plan

The Uptane Standard requires an accompanying test plan, a method to verify that implementers are in
compliance with its stipulations. This brings up the question of who will do the testing, and how.

SWRI has prepared a plan for submission to the Department of Homeland Security that includes 15 separate tests that could be run to show potential vulnerabilities in Uptane. Each test would go through a detailed series of steps to evaluate components, systems, version control and security. Verification would require that all of the MUSTs in the Standard be performed.

The question before attendees was, did we want to utilize the Uptane community to collectively run the tests and develop any needed tools? Or did we want to hire a test lab to which those seeking to prove they are in compliance would be sent?

There was some discussion about the merits of both options, but eventually, the consensus was to take the initial draft SWRI had prepared for DHS and use this to build a V 1.0 test plan. The community will build this plan and, around it, build a consortium that can also share development of any needed test tools. In this way, the plan is not being built from zero.

The plan will not be ready to be part of IEEE/ISTO version 1, but will be incorporated into a later version of the Standard. Once a basic test plan has been built and used, future work can focus on developing interoperability testing. Down the road, the consortium of Uptane community members that built the test process might consider certifying a few labs to perform the testing.

Building the Deployment Vehicle
The 1.0 standard will also not be accompanied by a deployment considerations document. The materials from the existing Google document have been moved into markdown files on the Uptane website. In the short term, these files will be posted to the Uptane website. As companies implement Uptane, write POUFs, and share their experiences with the community, a working group from the community will identify “best practices,” which will then be compiled into a versioned document.

There was agreement that the deployment materials should include no “MUSTs” in terms of specification implementation instructions, as all MUSTs should be designated in the Standard. What the deployment pages can do is stipulate that a particular step must be done (“must” here being lower case) and then, if there are options for completing the step, they can be presented in the deployment document as choices the implementer can make.

POUFs (Protocols, Operations, Usage, and Formats) and the Dual Layer Standards Framework
A POUF, an acronym for Protocols, Operations, Usage, and Formats, is the top layer of a dual-layer standard framework that has been introduced to the Uptane framework. It contains all of the information needed to meet the interoperability (i.e. backwards compatibility and deployment) goals of an implementation, while the bottom layer of the standard contains only the information needed for basic functionality and security.

The dual layer format and the POUF layout were introduced in a brief slide presentation (https://docs.google.com/presentation/d/1_WMX9cKdGSxD-hM1Wv9AUxwGUWN6glJ8Eq1ttv_ZHrs/edit?usp=sharing) to workshop attendees. Attendees raised several questions about the management of POUFs.

The Uptane Standards group is seeking to minimize its efforts when it comes to POUFs. It was
emphasized that no arm of Uptane will be testing or auditing POUFS.

Participants raised several questions, such as how will enumeration/versioning be handled. There was some concern that the creation of a POUF could potentially be the source of information leaks, and so protection against such an eventuality should be investigated.

The issue was raised if POUFs from OEMs could be listed anonymously to avoid proprietary leaks. Most participants seemed to think that a style guide or template might help address the issue of leaks, which also encouraging their use. An easy to complete “fill in the blanks” form would not only simplify things for the user preparing it, but certain sections could be marked “Confidential: contact __________ for more information” to keep from sharing sensitive information.

**Supply Chain: Uptane and in-toto**

An emerging issue, particularly in the deployment of Uptane, is securing the “supply chain.” By this term, we refer to the various distinct steps that an image or piece of metadata might go through before it is delivered to an ECU.

One possible tool to address this problem is in-toto, a framework for securing the start to finish integrity of the software supply chain. Workshop attendees were shown a slide presentation about the framework and then discussed its possible application to in-toto. (Slide presentation can be accessed at https://docs.google.com/presentation/d/1W47Q-4igRnQQkfwcZaxAWBWzH9Rvz4qDy75xdvgxr2k/edit?ts=5d03d807#slide=id.g24498bea51_0_38.)

There was some discussion of positives and negatives of adapting a solution like in-toto to Uptane. One person pointed out that such a framework can help catch human mistakes and, at the very least identify how and when the mistake happened. It can also help protect software delivered over an untrusted network. Layouts could be created to address configuration management

One possible downside raised was, if in-toto was applied to Uptane, how would you handle the metadata, which could explode in size. It was noted that in-toto can be adopted incrementally (that is it can be used to cover only selected segments of the supply chain.)

It was also noted that the in-toto framework was up for vote for adoption by CnCF in July.

No final resolution was adopted on this issue.

**Last Changes to the Uptane Standard**

At the time of the workshop meeting, there were only two pull requests on the repo to be resolved. One presented a set of small incremental changes, but discussion zeroed in on section 5.4.3.4 dealing with verification of images. The question was what to do with a secondary that does NOT have secondary storage and therefore can not restore a previous image. The consensus was that “recovery options” such as this were operations issues rather than security issues, and that handling this type of situation should be moved to the deployment pages.

The remaining issue dealt with how we defined the purpose of a primary ECU. After some discussion, the revisions proposed online were adopted.

With these actions, the group voted to approve the existing text as IEEE/ISTO Version 1.0 of the Uptane
Standards.

Some brief discussion followed over whether we were going to submit the Reference Implementation POUF for timestamping by IEEE/ISTO. The consensus was that this would be feasible. (Note: A draft of the reference POUF was shared on the Standards mailing list on 6/26).

Outreach and Future workshops

The last portion of the workshop was focused on what groups we might want to reach out to for future collaboration or support. The groups named were:

- CCC--Car Connectivity Consortium (https://carconnectivity.org/)
- NTIA--National Telecommunications and Information Administration
- Trusted Computing Group (https://trustedcomputinggroup.org/)
- World Automotive Working Group (https://www.w3.org/auto/wg/)
- Open Web Application Security Project (OWASP) (https://www.owasp.org/index.php/Main_Page)
- SAE G-32 Cyber Physical Systems Security Committee --a cross-sector initiative that addresses security in multiple industries, including aerospace, automotive, industrial control systems, banking and medicine (https://www.sae.org/works/committeeHome.do?comtID=TEAG32)
- Heavy equipment--outreach to both manufacturers and regulators, both in the U.S. and overseas.

The question was also raised if the group could attract more academics to serve as “evangelists,” that is individuals who would talk up Uptane within academic research communities. It was suggested we create posts on both the Standards and Forum mailing lists asking for names of university-based researchers, both U.S. and International, who should be approached about taking on this role.

The group tentatively agreed to hold a workshop in November some time around the time of escar Europe, which will be held in Stuttgart from November 19 to 20. A workshop may be held in Stuttgart or, if held in the Detroit area, we will look into doing a remote link-up between Germany and the US so European OEMs and suppliers can participate.