Uptane Virtual Industry Conference: Securing Software Updates and Supply Chains on Connected Vehicles

A virtual industry conference offered in association with escar Europe '22

Thursday, October 13, 13:00 to 16:45 CEST
(7 to 10:45 a.m. EDT, 20:00 to 23:45 JST)

For the second year, the community that developed Uptane, an open source, secure software update standard that protects software delivered over-the-air to the computerized units of automobiles, is pleased to invite OEMs and suppliers to a free virtual conference. This year's online gathering, a pre-event for escar Europe's 20th anniversary conference, will focus on the past achievements, and present challenges for the Uptane framework. We will also look ahead to how Uptane is currently adapting to future directions within the industry.

This virtual conference is organized into two 90-minute sessions, each addressing three primary topics. At the end of each topical presentation, we will allow 5 to10 minutes for questions, and we're including a 45-minute break in-between sessions. One free registration covers the full workshop, even if you are not attending the escar conference. To register, go to https://nyu.zoom.us/meeting/register/tJwsceuuqjItE9GNyaRCanWq7hNhGu96AXTh

Part 1: "Coming of age: The past and present of the Uptane Standard"

What Uptane is, what it does, and how it works (13:00-13:25)

Justin Cappos is a professor in the Computer Science and Engineering department at New York University. Justin's research philosophy focuses on improving real world systems, often by addressing issues that arise in practical deployments. His dissertation work was on Stork, the first package manager designed for environments that use operating system virtualization, such as cloud computing. Improvements in Stork, particularly relating to security, have been widely adopted and are used on the majority of Linux systems via integrations into Apt, YUM, YaST, and Pacman. His later research advances have been adopted into production use by Microsoft, IBM, VMware, Cloudflare, Docker, RedHat, ControlPlane, Datadog, and git, to name a few, as well as a substantial percentage of automobiles. More information is available at https://ssl.engineering.nyu.edu/personalpages/jcappos/.

How Uptane prevents or deflects specific attacks

Marina Moore is a PhD candidate at NYU's Tandon School of Engineering where she conducts research on secure software updates and supply chain security in the Secure Systems Lab. While at NYU, she has worked primarily on research and development for The Update Framework (TUF), Uptane, and Notary, and has delivered talks at KubeCon + CloudNativeCon and WiCyS 2019. Marina served as lead author on a paper about Uptane's dual-layer specification that was published in an ESCAR USA 2020 Special Issue, and she is a co-author of the Uptane whitepaper “Scudo: A Proposal for Resolving Software Supply Chain Insecurities in Vehicles.”

How the Uptane community is working to explicitly address fundamental security assumptions and to adapt best practices from other industries. (13:55-14:30)

Phil Lapczynski is a Principal Engineer for Automotive Security at Renesas Electronics America, Inc. He formerly led the flash bootloader and OTA team at Vector North America. He is an active member of the Uptane Advisory Group and a contributing member to SAE TEVEES18 – Vehicle Electrical System Security Committee. Additionally, he leads the HPSE API working group within the SAE TEVEES18B - Vehicle Electrical Hardware Security Task Force. Phil also participates in the Auto-ISAC Analyst Working Group and is a member of the Auto-ISAC SBOM working group. He has been a mentor and instructor at the CyberTruck Challenge and CyberAuto Challenge since 2017, and teaches the Software Updates training within the Advanced Engineering Track for Auto-ISAC.

Part 2: “The Road Ahead: How Uptane is Addressing Emerging Challenges”

How Uptane supports conformance with international standards and compliance with national and regional regulations (15:15-15:45)

ISO/SAE 21434 and ISO 24089

Suzanne Lightman is currently a Senior Advisor at the Computer Security Division of the Information Technology Lab at the National Institute of Standards and Technology (NIST). In this position, she serves as the main point person for cybersecurity and transportation systems, as well as for cybersecurity of industrial systems. Lightman has been involved in the development of the NIST Cybersecurity Framework, cybersecurity in cyber-physical systems, identity management, IoT cybersecurity, and cybersecurity and privacy policy. Her standards work includes contributions to automotive cybersecurity engineering (SAE/ISO 21434, ISO 24089) and industrial cybersecurity (IEC 62443). Lightman has two decades of experience in cybersecurity policy and implementation having held positions in the private sector, and also in both the legislative and executive branches of government. In addition, she has worked on ethical hacking teams, and has led in-depth audits and reviews of cybersecurity.

UN ECE 29 R155 and R156

Nick Russell, BSc (Hons), MBCS, is a Director of Standards at BlackBerry with more than 20 years of experience in the area of standardisation. Most recently, he has been involved in the development of ISO 24089, the international standard for software update engineering for road vehicles. Prior to that, he co-chaired the group on continual and post-production aspects for ISO/SAE 21434, the international standard for cybersecurity engineering for road vehicles. Nick also participates in the UNECE WP.29 international regulatory committee, where he is assisting with the international cybersecurity and software update regulations UN R155 and UN R156.

How Uptane is addressing emerging critical issues (15:45-16:20)

AFTERMARKET ECUs

Cameron Mott is Program Manager, R&D with the Southwest Research Institute's Intelligent Systems Division. He has more than 15 years of experience in leading advanced research and development projects for connected and automated vehicles. Through his passion of enabling secure communication in the automotive domain, he strives to improve the capability, safety, and security of modern vehicles. Cameron has served as a principal investigator for a project that created the first compromise-resilient software over-the-air update framework for the automotive industry called Uptane. He has since implemented a secure software update capability into automated vehicles for the US Army.

SUPPLY CHAIN SECURITY

Aditya Sirish A Yelgundhalli is a Ph.D. student at New York University's Secure Systems Lab where he conducts research in software supply chain security. He is a co-maintainer of the in-toto software supply chain framework, and a contributor to The Update Framework. Aditya is one of the contributors to Scudo, a framework that brought in-toto's software supply chain security features to the automotive space, extending the protections of the Uptane standard. Scudo is described in the Uptane whitepaper "Scudo: A Proposal for Resolving Software Supply Chain Insecurities in Vehicles."

How a major OEM has been transitioning from existing systems to Uptane (16:20-16:45)

David Kruger has been a domain architect in the PACCAR Information Technology Division for seven years. Prior to that, he worked as a software engineer for four years. David is responsible for ensuring global systems and applications, such as OTA, are designed properly. He has a security first mindset and constantly pushes his team to use the latest technology and best practices. Outside of his career David enjoys playing French horn, growing extremely hot peppers, and fishing.