ASSURED CYBERSECURITY AND INSIDER THREATS: DEMO WEBINARS ON ATTESTATION PRIMITIVES, TRACING CAPABILITIES, AND BLOCKCHAIN SECURE DATA SHARING

ASSURED, with the whole consortium, is glad to invite you to the ASSURED Demo webinars entitled "**ASSURED Cybersecurity and Insider Threats**" on Attestation Primitives, Tracing Capabilities, and Blockchain Secure Data Sharing.

The webinar will be held by UBITECH with the help of TU Darmstadt, NVIDIA and TU Delft. More details are available here below.

ASSURED CYBERSECURITY AND INSIDER THREATS: TOWARDS PRACTICAL SOLUTIONS FOR EFFICIENT AND SCALABLE ATTESTATION CAPABILITIES

MAY 31 @ 10:30 AM - 12:30 PM CEST

Seeking to design successful supply chain service management and various IoT applications comprising millions of autonomous cyber-physical systems, one has to cater to the **security, trust and privacy requirements** of all involved actors (i.e., smart connected edge and cloud devices). One key challenge in such complex systems is **how to establish and manage trust**, starting from bi-lateral interactions between two single system components and continuing as such systems get connected to ever larger entities.

But how can we make sound statements on the security properties of single systems and transfer this to statements on the security properties of hierarchical compositions of systems ("Systems-of-Systems" (SoS))?

The webinar will be held remotely on Wednesday, May 31 between 10:00 – 12:30 CEST with the help of Ubitech and the Computer Science department of TU Darmstadt.

Event webpage: https://www.project-assured.eu/event/demo-webinar-on-attestation-primitives/

ASSURED CYBERSECURITY AND INSIDER THREATS: NON-INTRUSIVE CODE COVERAGE: HOW TO USE ASSURED FOR TRACE-BASED DEBUGGING AND RUNTIME ANALYSIS

JUNE 20 @ 10:30 AM - 12:30 PM CEST

The complexity of today's applications presents many new challenges for developers and security engineers, especially with regards to efficient mechanisms to verify software and device integrity for detecting runtime modifications. Recall the latest trend in the attack vectors, as documented by the Open Web Application Security Project (OWASP), where an updated ranking list of Common Vulnerabilities and Exposures (CVEs) was put forth: *It is apparent that memory-related vulnerabilities are becoming more prevalent and lucrative targets to be exploited by adversaries for launching software-based attacks against deployed devices*. Such attacks can range from the exploitation of loopholes due to security misconfiguration and insecure system design to vulnerable & outdated components and cryptographic failures. The common denominator in all such cases is the lack of appropriate security hardening across any part of the application stack: from the secure boot of a system (based on secure, certified, and tested software) to the run-time detection of software and data integrity failures through efficient and effective trustworthiness control design.

The webinar will be held remotely on Tuesday, June 20 between 10:30 – 12:30 CEST with the help of Ubitech and NVIDIA.

Event webpage: https://www.project-assured.eu/event/demo-webinar-on-tracing-capabilities/

Funded by the Horizon 2020
Framework Programme of the European Union

ASSURED CYBERSECURITY AND INSIDER THREATS: BLOCKCHAIN-EMPOWERED MOBILE EDGE INTELLIGENCE FOR SECURE AND SUSTAINABLE COMPUTING

JULY 11 @ 10:30 AM - 12:30 PM CEST

The notion of trust refers to *the degree of confidence that the users and stakeholders can have that the system operates as expected with regards to the entire spectrum of the entire application stack of the device, including both configuration behavior and operational behavior, as defined by the administrators*. In other words, user trust on the behavior of a system is a measure of confidence, and the degree to which the system fulfils the **requirements of the users and stakeholders** with regards to **security** and **privacy** can be seen as a **measure of their confidence level** in the entire system. Since this is a core requirement and a major building block in modern supply chains and service graph chains, a level of confidence in the system translates by default to the **measure of confidence of the user in the outcome of the system**, therefore increasing **end user adoption**, and increasing the **adoption and the trust of the user in all the services and technological advancements that exist in a cyber society**. This is a core vision of the EU, which also lies within the heart of ASSURED.

The webinar will be held remotely on Tuesday, July 11 between 10:30 – 12:30 CEST with the help of Ubitech and TU Delft.

Event webpage: https://www.project-assured.eu/event/demo-webinar-on-blockchain-secure-data-sharing/

Funded by the Horizon 2020
Framework Programme of the European Union

ABOUT ASSURED

ASSURED is a three-year Research & Innovation project funded by the European Union's Horizon 2020 programme under Grant agreement number 952697. ASSURED project is powered by a strong consortium with partners who were carefully selected to provide complementary skills and competencies, which cover all project objectives and activities, starting from the generation of ideas to analysis of requirements, to specification and design, low-cost implementation, system integration, up to demonstration, validation and beyond.

The partners of ASSURED consortium are Technical University of Denmark, Martel Innovate, Eindhoven University of Technology, Technical University of Darmstadt, University of Surrey, Mellanox Technologies, Intrasoft International, Unisystems Luxembourg, UBITECH, Data Intelligence Solutions, United Technologies Research Center, Space Hellas, Bremer Institut für Produktion und Logistik, Dimos Athinaion Epicheirisi Michanografisis.

CONTACTS

Twitter: https://twitter.com/Project_Assured

LinkedIn: https://www.linkedin.com/company/assured-project/

Email: info@project-assured.eu

Contact for press

Valentin Popescu, Martel Communication and Dissemination Specialist
valentin.popescu@martel-innovate.com

Funded by the Horizon 2020
Framework Programme of the European Union