ASSURED Scientific Workshop on Sustainable Security in "Systems-of-Systems"

Dimitris Papamartzivanos

Digital Security & Trusted Computing Group

UBITECH Ltd

ASSURED Scientific Workshop

Darmstadt, Germany | April 25-26, 2023

www.project-assured.eu

AGENDA

Day 1 Workshop Program (all times are in CEST): 9:00am – 18:30pm CEST			
From	**To**	**Topic**	**Speaker**
9:00 – 9:15		**Introduction to ASSURED**	***Dimitris Papamartzivanos*** *(UBITECH)*
WPs Technical RoadMap			
9:15-10:15		**"CASU: Compromise Avoidance via Secure Update for Low-End Embedded Systems"**	***Gene Tsudik*** *(University of California)*
10:15 – 11:00		**"Trusted Environment for Future Consumer Devices"**	***Jan-Erik Ekbrg*** *(Huawei)*
11:00 – 11:15		**Coffee Break**	
11:15 – 12:00		**"System Tracing: From Cloud to IoT"**	***Ahmad Atamli*** *(NVIDIA)*
12:00 – 12:45		**"Efficient and Scalable Fuzzing of Complex Software Stacks"**	***Thorsten Holtz*** *(CISPA Center for Information Security)*
12:45 – 14:00		Lunch Break	
14:00 – 14:45		**"Financial Crime Detection with Privacy"**	***Zeki Erkin*** *(Cyber Security Group, Delft University of Technology)*
14:45 – 15:30		**"Post-Quantum Direct Anonymous Attestation (PQ-DAA)"**	***Nada El Kassem*** *(University of Surrey)*
15:30 – 15:45		**Coffee Break**	
15:45 – 16:30		**Panel Discussion – "Towards Sustainable Security – Converging Software and Adaptable Hardware Security"**	
16:30 – 17:15		**"A software-based approach to secure bare-metal devices"**	***Bruno Crispo*** *(Department of Computer Science and Information Enginering, University of Trento)*
17:15 – 17.45		**"TBD"**	***Matthias Schunter*** *(INTEL)*
17:45 –18:25		**"Are the Trust Frameworks ready? Towards achieving Digital Sovereignty in Decentralized Ecosystems and its role in Credentials Exchange"**	**Bithin Alangot** (Huawei)
18:25 – 18:30		**Closing Remarks**	***Jean-Baptiste Milon*** *(MARTEL)*

AGENDA

Day 2 Workshop Program (all times are in CEST): 9:30am – 18:30pm CEST			
From	**To**	**Topic**	**Speaker**
9:00 – 9:45		**"Securing location and reducing device exposure"**	***Panagiotis Papadimitratos*** *(Networked Systems Security Group, KTH Royal Institute of Technology)*
9:45 – 10:30		**"Asynchronous Remote Key Generation and its Applications"**	***Mark Manulis*** *(Department of Computer Science, Universität der Bundeswehr München)*
10:30 – 10:45		**Coffee Break**	
10:45 – 11:15		**"GNNs-Based Zero-Assumption Control-Flow Attestation"**	***Marco Chilese*** *(Technical University of Darmstadt)*
11:15 – 11:45		***"Are we there Yet? Decentralized Trust Anchors as the Future of Digital Identity Verification"***	***Benjamin Larsen*** *(Technical University of Denmark)*
11:45 – 12:15		**"TBD"**	***Dimitris Papamartzivanos, Stefanos Vasileiadis*** *(UBITECH)*
12:15 – 12:45		**"Searchable Symmetric Encryption and its attacks"**	***Kaitai Liang*** *(Technical University of Delft)*
12:45 – 14:00		*Lunch Break*	
14:00 – 14:45		**"Beyond Physical: Revisiting the Interplay of Side-channel analysis and AI"**	***Lejla Batina*** *(Digital Security Group, Radboud University)*
14:45 – 15:00		**"Edge Computing and Systems-of-Systems: Security through Zero Trust – Overview"**	***Christian D. Jensen*** *(Technical University of Denmark)*
Session – The use of Trusted Computing towards Enhanced Security and Privacy			
15:00 – 15:15		**"Security challenges and trusted computing in the Smart Satellites domain"**	***Manolis Bakiris*** *(SPACE HELLAS)*
15:15 – 15:30		**ASSURED Workshop Closing Remarks**	Dimitris Papamartzivanos, Jean Baptiste Milon, Thanassis Giannetsos

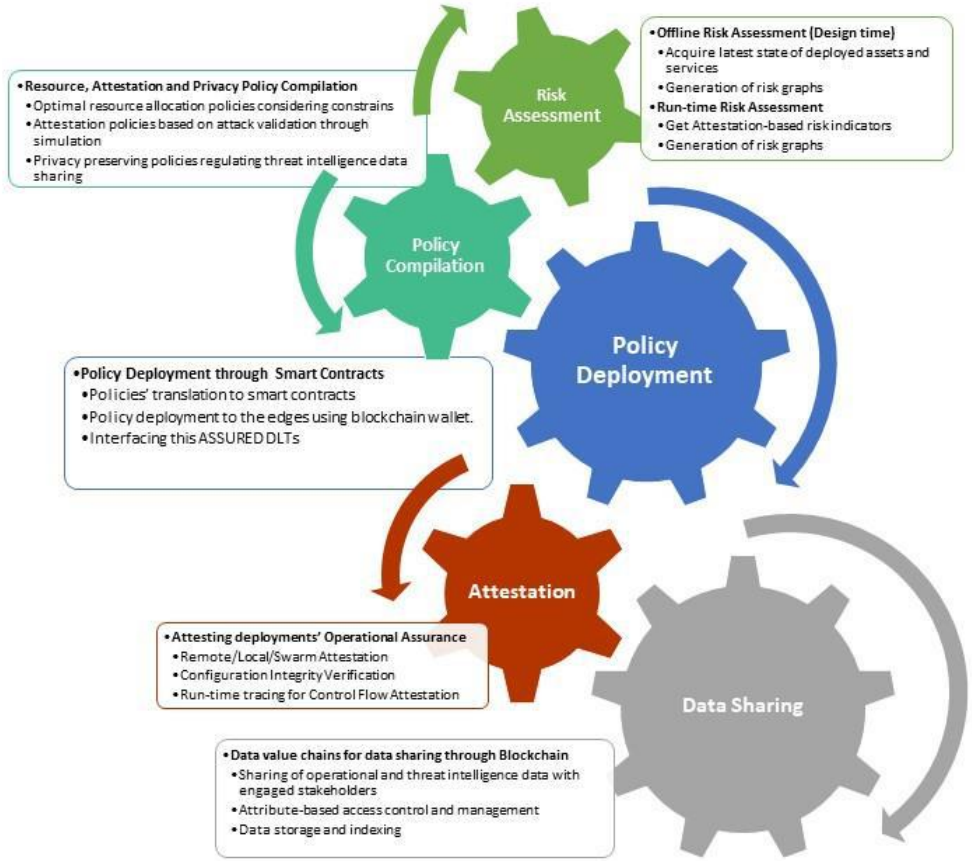
ASSURED Vision

Reference Project and Catalyst for establishing Trusted Service Graph Chains in next-generation “Systems-of-Systems” addressing **Security**, **Safety** and various levels of **Trustworthiness** for mixed-criticality services

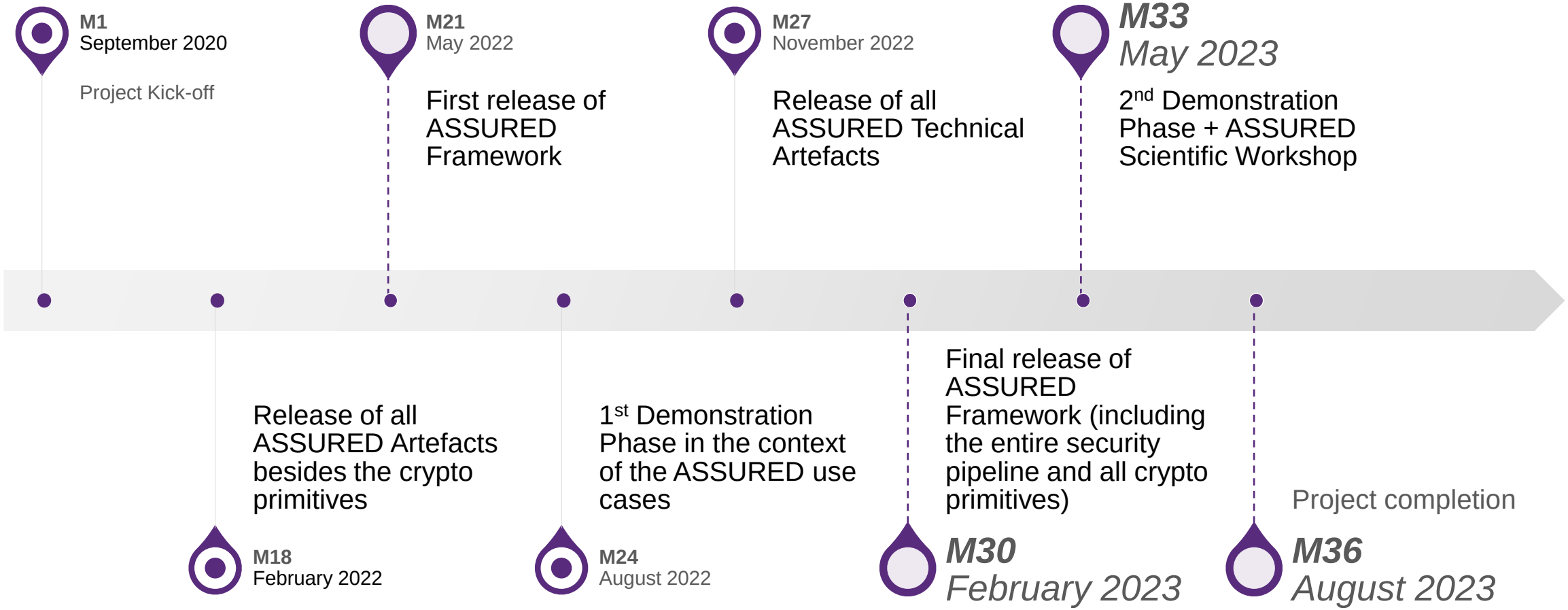
Implement the transition to **Zero Trust** concept with the principle “*Never Trust, Always Verify*” for assuring vertical trust for all devices comprising the supply chain

ASSURED Performs Cuting-Edge Research in Trusted Computing, Blockchain & Lightweight Crypto

Enhanced Operational Assurance	Increase trust to a device output by assessing its configuration & execution state – **Real-time tracing capabilities with reasonable performance overhead**
Risk Assessment	Identity risk interdependencies in a service graph chain that can affect the safety of the system
Threat Intelligence Information Sharing	Secure and auditable sharing of operational and attestation data only to authorized & authenticated devices & users – Useful for **Certification**
Decentralized Identity Management	How to ensure that each entity is the one that it claims to be – TC-based Wallet running at each user/device
Dynamic Policy Enforcement	Optimal Deployment of security (attestation) policies
Vulnerability Analysis	Protection of cyber-physical systems through run-time attack path analysis



Project Milestones and Progress Timeline



Summary of Project Highlights

- **Definition of highly-usable, resilient cyber-security, privacy protection framework (WP1)**
  - ✓ Long-term security, privacy and operational assurance
  - ✓ Safe implementation of mixed-criticality applications in “Systems-of-Systems”
- **Definition of Reactive, Runtime Risk Assessment and Policy Recommendation Capabilities (WP2)**
  - ✓ Linked also to real-time monitoring & analysis of system execution states
- **Orchestration of various Remote Attestation Schemes (WP3)**
  - ✓ Control-flow Attestation (CFA), Configuration Integrity Verification (CIV), Direct Anonymous Attestation (DAA), Swarm Attestation, ML-based Attestation
- **Secure and auditable sharing of (threat intelligence) data (WP4)**
  - ✓ Continuous authentication & authorization and decentralized identity management (TPM-based Wallet)
  - ✓ Attribute-based Access Control (ABAC), Attribute-based Encryption (ABE), Searchable Encryption
- **Definition and implementation of a policy-compliant Blockchain architecture (WP4, WP5)**

TARGET APPLICATION DOMAINS

SMART MANUFACTURING

Safe Human-Robot Collaboration in Automated Assembly Lines

- ✓ Lack of **validation against a malicious user** attempting a system modification
- ✓ Lack of protection against loss of **data integrity and trustworthiness**
  - *Deployed sensors collaboratively calculate the position of a worker*
- ✓ **Continuous monitoring and verification of software integrity**
- ✓ Secure **zero touch onboarding** of new sensors
- ✓ Swarm Attestation

SMART AEROSPACE

To increase the trustworthiness of all internal components

- ✓ Need for **fast and secure SW updates**
  - Configuration Integrity Verification
- ✓ Need for verification in the i**ntegration of new products and system level solutions**
- ✓ **Remote maintenance**
- ✓ **Security Misconfiguration, Vulnerable and outdated components**
  - CFA, CIV as trust enablers
- ✓ **Stong requirements for certification**

PUBLIC SAFETY

“Systems-of-Systems” Collaboration for Public Safety

- ✓ **Anonymity and privacy of users**
  - Direct Anonymous Attestation
- ✓ Strong **authentication and authorizatio**n of various stakeholders when accessing sensitive information
  - Attribute-based Access Control
- ✓ Integration of legacy devices
- ✓ Secure data sharing and Device Attestation

SMART SATELLITES

Secure Communication & Key Refreshment

- ✓ Lightweight **authentication** and **secure communications**
- ✓ **Integrity of mission critical payloads**
- ✓ **Software updates**
- ✓ Key Management

Considerable Dissemination Achievements (Multiple Channels, Different Audiences)

Very Rich Track Record of Publications & Presentations

- ~50 Scientific Publications (Journal, Conference)
- >=25 Events (Workshops, Conferences, Presentations, Collaboration Sessions etc.)
- >=40 News articles published on website
- 8 Newsletters issued
- Standardization collaboration activities

Meet the consortium

ASSURED

UBITECH ubiquitous solutions

MARTEL innovate

Suite5 We Deliver Intelligence

netcompany intrasoft

SPACE

United Technologies Research Center

uni.systems

BIBA Bremer Institut für Produktion und Logistik

CITY OF ATHENS ΔΑΕΜ

TECHNISCHE UNIVERSITÄT DARMSTADT

TU Delft

DTU

UNIVERSITY OF SURREY

NVIDIA

THANKS

PROJECT-ASSURED.EU

@Project_Assured

ASSURED project is funded by the EU's Horizon2020 programme under Grant Agreement number 952697