Compositional Security, Verification & Risk Management for Systems-Of-Systems-Enabled Supply Chains

Dr. Sofia-Anna Menesidou

Cybersecurity Researcher Associate @ UBITECH LTD
Digital Security & Trusted Computing Group

PUZZLE INTERNATIONAL CYBERSECURITY CONFERENCE
Master Center, Novi Sad, Serbia
June 21st, 2023

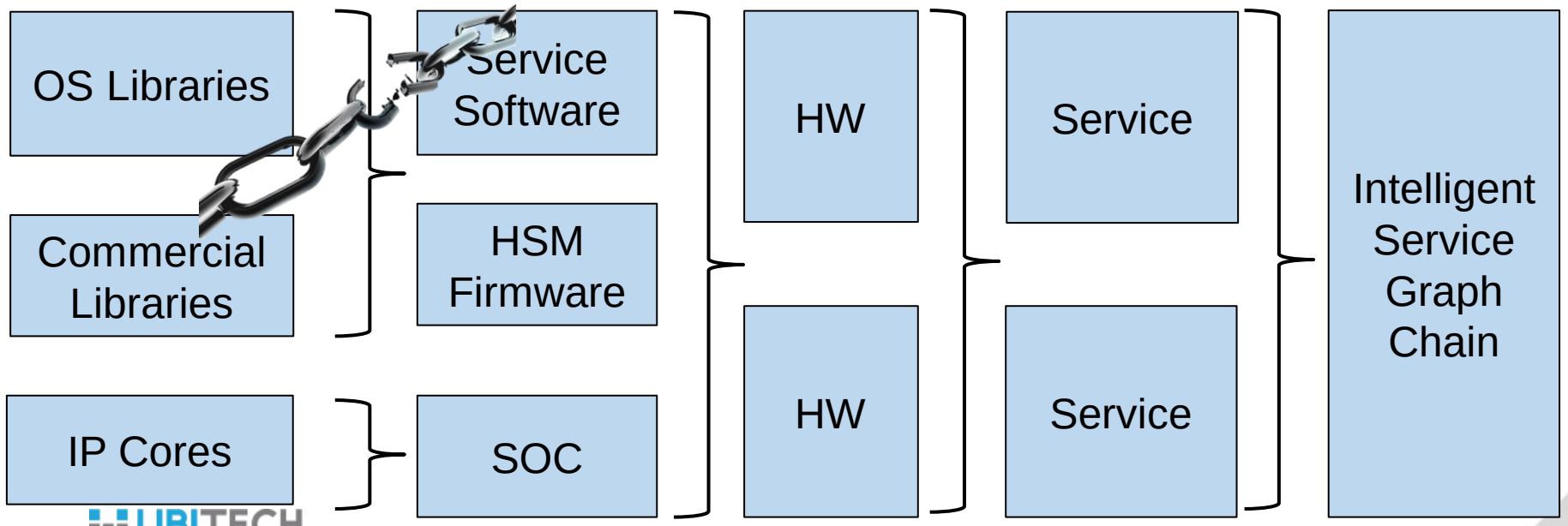
Introduction

- **IoT** have gained significant **attention** and are becoming **increasingly omnipresent**.
- **IoT applications** have **dominated** the agenda of industry leaders in recent years.
- Currently, there are **more than 10 billion active IoT devices**, while this number is estimated to **surpass 25.4 billion in 2030**.
- IoT devices operate **collaboratively** to offer **high-quality services**, creating a **digitalization wave** that turned IoT devices into complete interconnected ICT systems.
- There is a need for **targeted design and development** of **IoT-specific** defensive mechanisms.
  - **Lack of holistic solutions** and **risk management** that **protect the IoT devices** through the entire management **life cycle** including their update and patching.
  - **Absence of formal verification approaches** to drive secure open specifications for IoT software and hardware based on security-by-design principle.
  - **Non-efficient mechanisms** to guarantee IoT devices **operational assurance** and establish **trust**.

UBITECH
ubiquitous solutions

Compositional Security & Verification (1/2)

- SoS refer to a **collaborative** and **interactive** ecosystem that **continually evolving**.
- Today's **service graph chains** are **highly-complex SoS**.
- If security in one **sub-(sub-sub-)system fails**, this can have **consequences for the security of the overall system**.
- Shifting for standalone component security to **compositional security**.



UBITECH
ubiquitous solutions

Compositional Security & Verification (2/2)

- Contemporary systems are built up from **smaller components**, that **may not meet system's security requirements**.

- Attacks using **properties of one component** to **subvert another** have shown up in practice in many different settings, including cryptographic protocols, systems software, application software, web browsers and infrastructure.

- Reasoning about the **behavior of a combination of interacting systems**, however, is notoriously **difficult**.

- **Trust** is the key to security of cooperative Systems-of-Systems.
  - *"A **cooperative system** is defined to be a system of multiple dynamic entities that share information or tasks to accomplish a common, though perhaps not singular, objective."* [from: https://www.springer.com/series/5788]

Trust & Trusted Computing

- **TRUST**: "*assured **reliance** that someone is **good** and **honest** and **will not harm** you, or that something is safe and reliable.*"
- The definition of "***assured***" is "characterized by certainty or security."
- **Certainty** means "*the quality or state of being certain, especially on the basis of **evidence***".
- What's This All About? → Trusted Computing!
- **Base our trust in computing technology on evidence** that the technology is genuine and that it does only what the vendor says it does!
- **The technology has not been modified by any unauthorized entity** to perform any other actions and consistently behaves in expected ways
- **Verifiable evidence** on the **correct configuration** and **execution** of a device comprising **multiple components/assets**

UBITECH
ubiquitous solutions

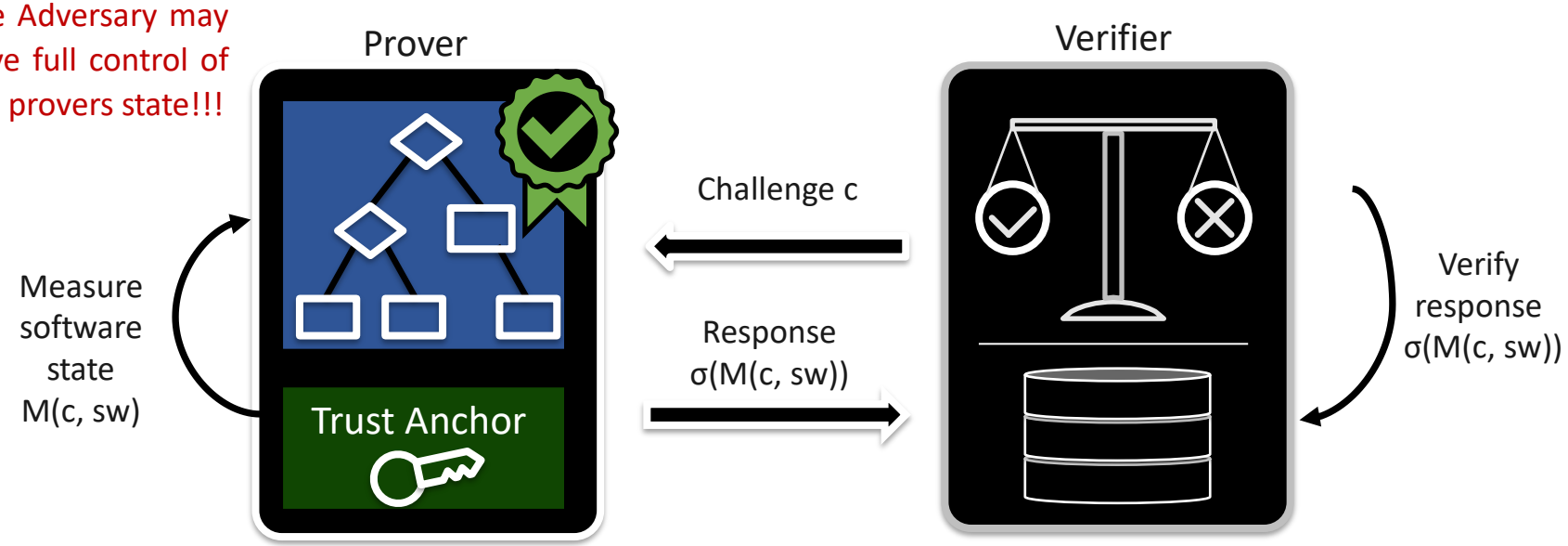
Remote Attestation

- **Remote Attestation (RA)** is a security service (e.g., integrity verification) that measures the software state of a system to infer/detect if it is compromised!

- Two-party interaction between:
  - **Verifier**: Trusted entity
  - **Prover**: Potentially infected and remote IoT device

- **Goal**: To verify the internal state of the prover

The Adversary may have full control of the provers state!!!



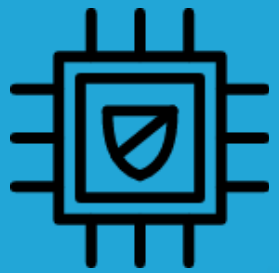
UBITECH
ubiquitous solutions

Challenges (1/3)

- **Hardware-based Remote Attestation**
  - Require a dedicated HW Root of Trust (e.g., TPM, SGX, TrustZone)
  - *Is it really a good fit for low-end IoT devices?*

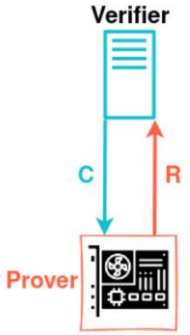
- **Software-based Remote Attestation**
  - A viable approach for devices with no hardware security features
  - *Is it possible to guarantee that the attestation key is not accessed by the adversary?*

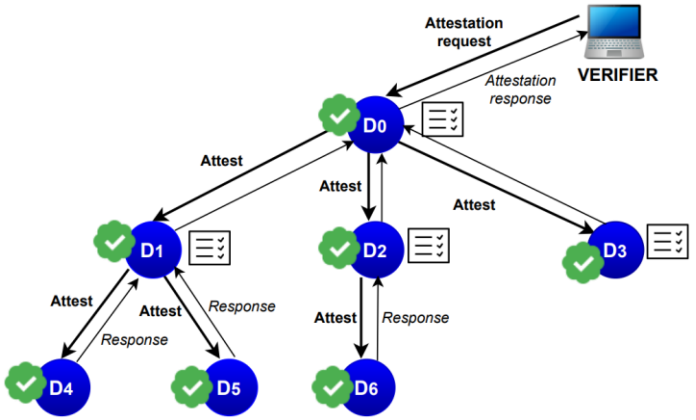
- **Hybrid Remote Attestation solutions**
  - HW/SW co-design with minimal HW support
  - *Is the best fit for constrained devices?*



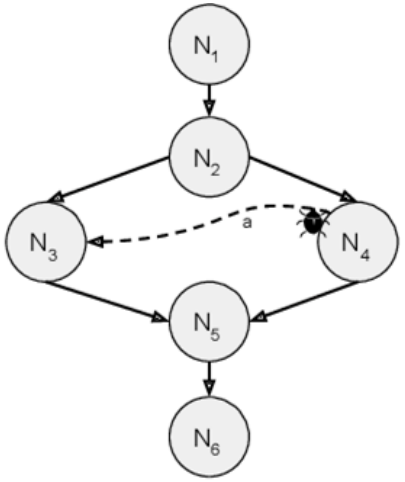
Challenges (2/3)

- **Singular RA - One-to-One**
  - Efficiency issues (e.g., tracing)
  - Scalability issues





- **Swarm/Collective RA - Many-to-many**
  - Recursive aggregation of results
  - Expensive to maintain the dynamic network setting

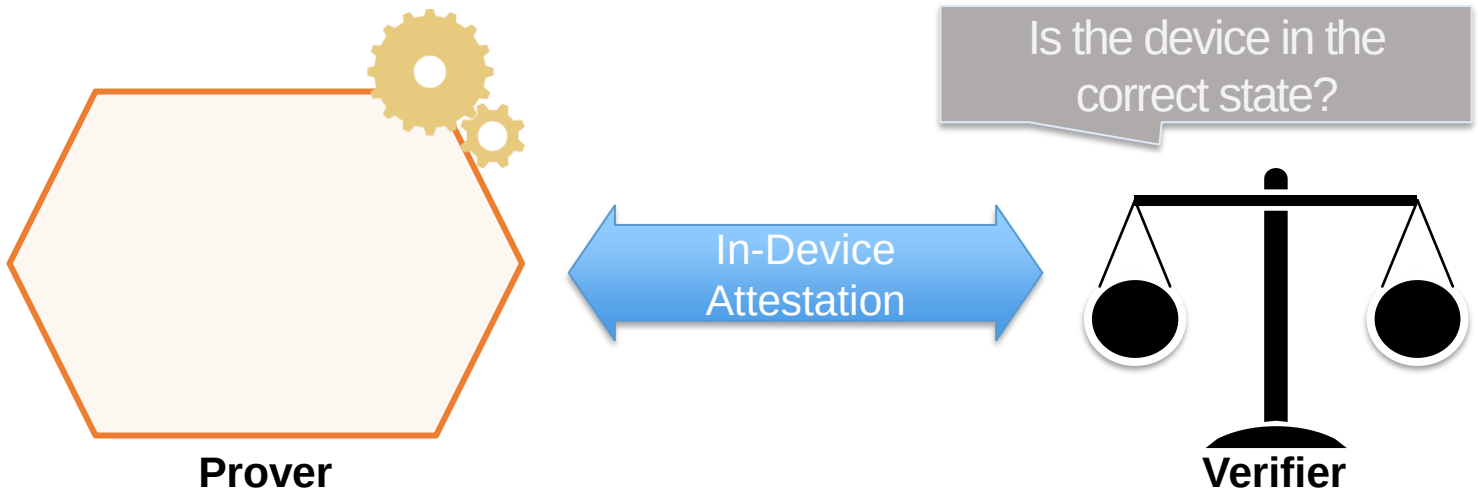


- **Control-flow attestation**
  - Ensure the integrity the execution during run-time
  - Larger computational overhead

UBITECH
ubiquitous solutions

Challenges (3/3)

- *How do we **verify (and quantify) the level of trust** of a device and how can **this statement be transferred between multiple devices** as part of a service graph chain?*



Requirements

- **Efficient**
  - More efficient than attesting each single device
- **Scalable**
  - Supports integrity verification of large swarms
- **Flexible**
  - Independent of integrity measurement mechanism used by devices
- **Applicable to low-end embedded systems**
  - Requirement only inexpensive security extensions for low-cost devices
- **Decentralized**
  - Distributes load and energy consumption over all devices

Efficient and continuous security assessment

- Security assessment should be performed during the **whole lifecycle of a service graph chain** from the **deployment**, **sw/fw updates** to **runtime attestation.**

- Efficiency and scalability issues necessitate **new more efficient approaches for attestation and operational assurance**.
    - built upon of **trusted hw-based models during design time**
    - **limited vector of properties** that need to be attested, as a result of the security-by-design approach (e.g., breach of hw-based models)
    - **perform risk-assessment** to identify the most prominent attack vectors and **calculate the required trust level per device** of the service graph chain

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

REWIRE

UBITECH
ubiquitous solutions

Use Cases

SMART CITIES

"Systems-of-Systems" for empowering Public Safety

- **Secure Device On-Boarding**
  - Automated & scalable process for the dynamic and zero-touch on-boarding of devices
  - Device's Trust level must be measured and verified
- **SW & FW Update for Critical IoT Devices**
  - Scalability is an issue
- **Collaborative Threat & Misbehavior Detection**
  - Leverage the Federate Learning approaches of REWIRE
  - Combination of "testing & learning" both at the edge and at the backend for creating enhanced knowledge

SMART SATELITES

Secure SW Updates for Spacecraft Applications & Services

- **Service or Security Patch Deployment**
  - Secure and Authenticated Communication Channel; Trust-Aware Authentication
  - For the transmission of mission-critical payloads and or patches from the Ground Station
- **Enhanced Isolation**
  - Use of the TEE for offering the required level of isolations and segregation to the running processes

AUTOMOTIVE

Trust Management

- **Automated and Immediate Attack Mitigation**
  - Ongoing attacks need to be analyzed for impact on the target ECU's Trust Level
  - ECU's Trust level must be measured and verified
- **Automatic cyberattack response strategies**
  - Migration of applications or data (incl. crypto keys!) between ECUs with least impact on the vehicle's operation
  - Communication relationships of applications need to be migrated in parallel
- **Modular SW and FW Updates of ECUs**
  - Part of the mitigation process – ECU where actions are offloaded need to download the SW to continue its execution
  - Secure and Authenticated channel for getting the SW update

TARGET APPLICATION DOMAINS

REWIRE

Use of the TEE for:

- ✓ **Decentralized Attribute-based Encryption**
- ✓ **Attribute-based Access Control**
- ✓ **Attestation services bouquet**
- ✓ **Efficient verification of Blockchain status**

UBITECH
ubiquitous solutions

Follow our projects

REWIRE

REWiring the ComposItional Security VeRification and AssurancE of Systems of Systems Lifecycle

- *Provable Secure cryptographic protocols, definition of customized instruction set (ISA) to empower IoT processing units that will realize the custom system on chip for the specified requirements,*
- *Firmware (FW) & software (SW) security updates and patching validation*
- *Runtime attestation for verification of IoT devices' operational assurance using customizable lightweight TEEs, and*
- *Blockchain-assisted AI-based misbehaviour detection in distributed fashion*

https://www.rewire-he.eu/

REWIRE HorizonEU Project

Partners

UBITECH ubiquitous solutions

University of Surrey

UCLouvain

Secura A BUREAU VERITAS COMPANY

Orchestrating a brighter world NEC

TU Delft

Suite5

uni.systems

EIGHTBELLS Independent Research & Consultancy

Libre Space Foundation

KENOTOM EMBEDDED ENGINEERING EXCELLENCE

Odin S

Collins Aerospace APPLIED RESEARCH & TECHNOLOGY

UBITECH ubiquitous solutions

Supply Chain Service Challenges

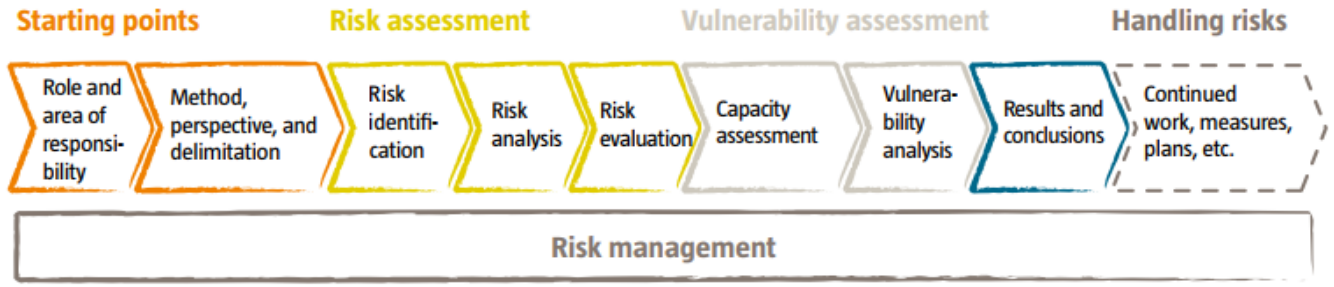
- Global supply chains are becoming more **complex and integrated**.
- The organizations operating within the supply chains are heavily **dependent on ICT** and they are exchanging large amounts of data.
- There is a pressing **need for methodologies and tools for the efficient evaluation and management of security threats and vulnerabilities** throughout the interconnected infrastructures of the stakeholders of the supply chain services.

UBITECH
ubiquitous solutions

Risk Management & Risk Assessment

- ***Risk management (RM)*** *– a process aiming at an efficient balance between realizing opportunities for gains while minimizing vulnerabilities and losses [ENISA]*
  - *continuously re-iterating process*
  - *Goal → is to reach an acceptable level of security at an acceptable cost*

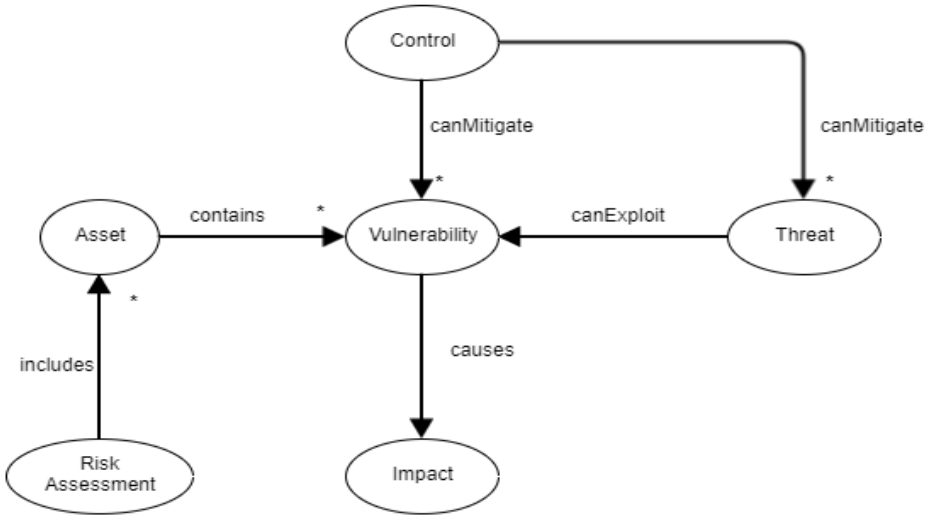
- ***Risk Assessment (RA)*** *– provides relative numerical risk ratings (scores) to each specific vulnerability*
  - *it is not continuous*



UBITECH
ubiquitous solutions

Risk Assessment

- ***Identification of Risks***
  - *it's origin*
  - *a certain activity, event or incident (i.e., threat)*
  - *its consequences, results or impact*
  - *a specific reason for its occurrence*
  - *protective mechanisms and controls (together with their possible l*
    effectiveness)
  - *time and place of occurrence*
- ***Analysis of Impact***
  - ***Qualitative analysis***
    - *rates the magnitude of the potential impact of a threat as hig*
      medium, or low → subjective decision
  - ***Quantitative analysis***
    - *the probability of an event occurring and the losses that may*
      incurred → difficult
- ***Evaluation of Risks***
  - *consequences (e.g., impacts),*
  - *the likelihood of events,*
  - *the cumulative impact of a series of events that could occur*
    simultaneously.



UBITECH
ubiquitous solutions

CYSMET Risk Management Methodology

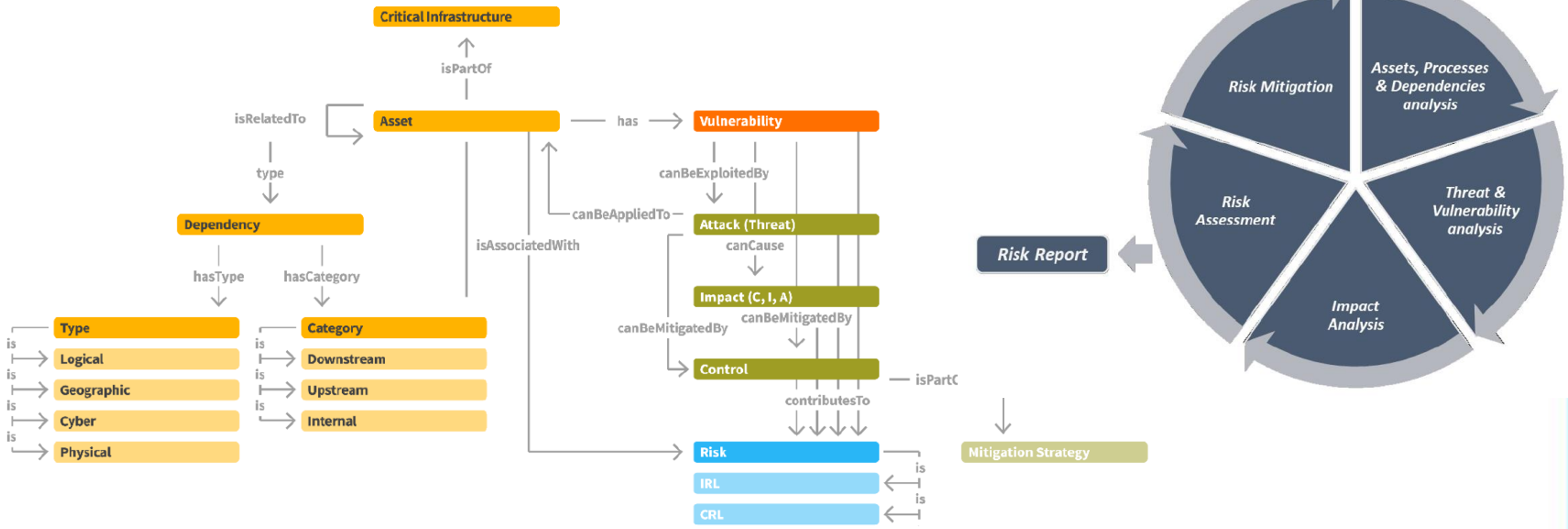
- **Risk Management Methodology** focused to small ports requirements.
- **Complies** with all relevant **standards** and **frameworks**
- **Enhances the existing methodologies** (e.g., CYSM, MEDUSA, eBIOS, MITIGATE) by:
  - including additional to **ICT assets** in the perimeter of the **assessment** (**OT**, **IoT**);
  - using **additional vulnerability DB records** related to OT and IoT;
  - calculating **risk and attack paths** originated by **both cyber and cyber-physical threats**;
  - applying the **updated v3.1 of the CVSS**;
  - utilizing **all CVSS v3.1 metric fields**: Base, Temporal and Environmental Scores to increase accuracy of the measurements;
  - using the **vulnerability and impact assessments as a combined process** (the CVSS v3.1 considers the impact that a vulnerability exploitation could have on the environment under consideration).

CYSMET

UBITECH
ubiquitous solutions

Risk Quantification

- **Cybersecurity Risk Assessment Methodology**
  - **Interdependency** graph model for supply chain digital reflection
  - **CVSSv3.1**
  - **Individual**, **Attack Path** Risk Levels



CYSMET

UBITECH
ubiquitous solutions

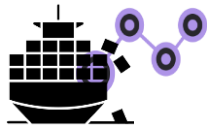
CYSMET Services

- **Risk Management**
  - deals with threats identified in the Supply Chain Services
- **Collaborative Risk Assessment**
  - focuses on assessing the likelihood of various risks and the overall resilience and reliability of Supply Chain Services
- **Attack Simulation**
  - design, execute and analyze simulation experiments and the calculation of the cascading effects
- **Open Threat Intelligence and Information Exchange**
  - integration of data, related to known attacks, threats, vulnerabilities from open information sources

CYSMET

UBITECH
ubiquitous solutions

Use Case



MARITIME SUPPLY CHAIN

Dynamic system of interconnected organizations (e.g., port authorities, customs services, marine insurance companies), critical infrastructure (e.g., energy, transportation, telecommunications), people and other elements aimed at providing a product/service to end users.

- **SCS cybersecurity incidents** – increased by 51% during the second half of 2021 due to the pandemic
- **Maritime SCSs & ports** – significantly increased its reliance on Information and Communications Technology (ICT)
- **Small & Medium Sized Ports (SMP)** – mainstay of a variety of activities in remote areas

CYSMET

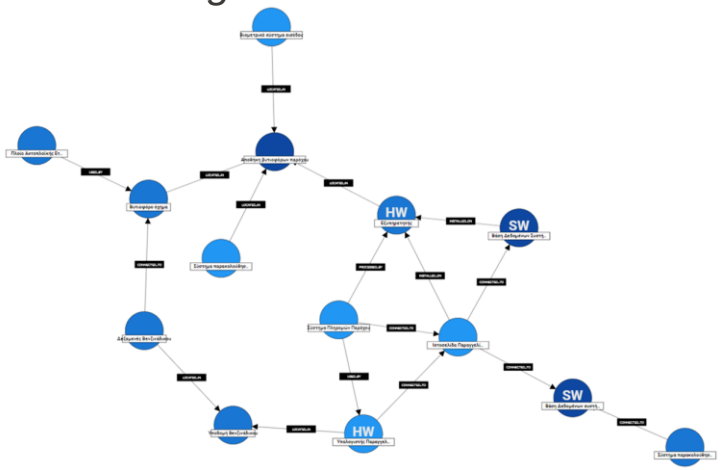
UBITECH
ubiquitous solutions

Follow our projects

CYSMET

Integrated, Dynamic & Collaborative Risk Management System for Maritime Transport & Supply Chains

- *Modelling of asset and service dependencies between comprising stakeholders of Maritime Supply Chains.*
- *Dynamic integration and management of Open Threat & Vulnerability information.*
- *Dynamic and collaborative Risk Assessment & Management methodology.*
- *Platform validation and evaluation through real scenarios.*



UBITECH ubiquitous solutions

https://cysmet.ubitech.eu

CYSMET Project

Partners

UBITECH ubiquitous solutions

GRUPPO Maggioli

ΟΡΓΑΝΙΣΜΟΣ ΛΙΜΕΝΟΣ ΒΟΛΟΥ Α.Ε.

Ευρωπαϊκή Ένωση

ΕΠΑνΕΚ 2014-2020 ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ

ΕΣΠΑ 2014-2020

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Thank you!

Dr. Sofia Anna Menesidou

Cybersecurity Researcher Associate @ UBITECH
Digital Security & Trusted Computing Group