CREDC

Robust and Scalable Security Monitoring and Compliance Management for Dynamic EDS

Carlos E. Rubio-Medrano, Ziming Zhao, and Gail-Joon Ahn

GOALS

- Provide means for the efficient, robust, and practical monitoring of security-relevant information originating from *energy delivery system* (EDS) infrastructures and clouds.
- Support the automated *verification, validation, and attestation* (VV&A) of EDS to properly assess whether particular designs and implementations comply with a well-defined set of security requirements.

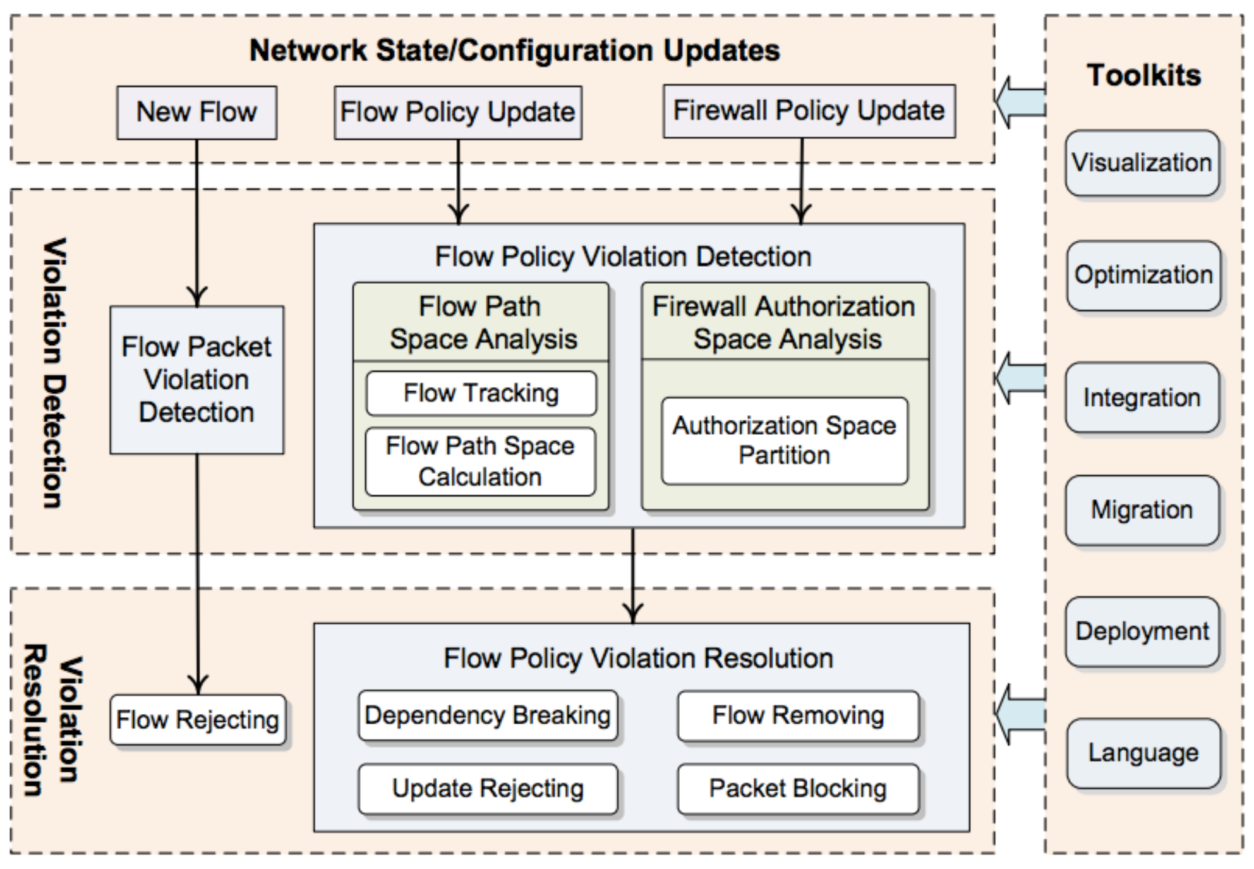
FUNDAMENTAL QUESTIONS/CHALLENGES

- Industrial EDS software control solutions, including SCADA and AMI, will inevitably migrate to clouds so as to gain flexibility and scalability. The highly dynamic cloud enables EDS to respond to on-demand changes and reconfigurations.
- However, such a process may significantly add new threats that may compromise the overall security of EDS. To cope with these challenges, it is imperative 1) to continuously monitor the security of cloud-based EDS by placing collaborative virtual security sensors in the EDS cloud environment, and 2) to automatically perform security compliance checks and management on each individual EDS cloud component and the EDS cloud as a whole.

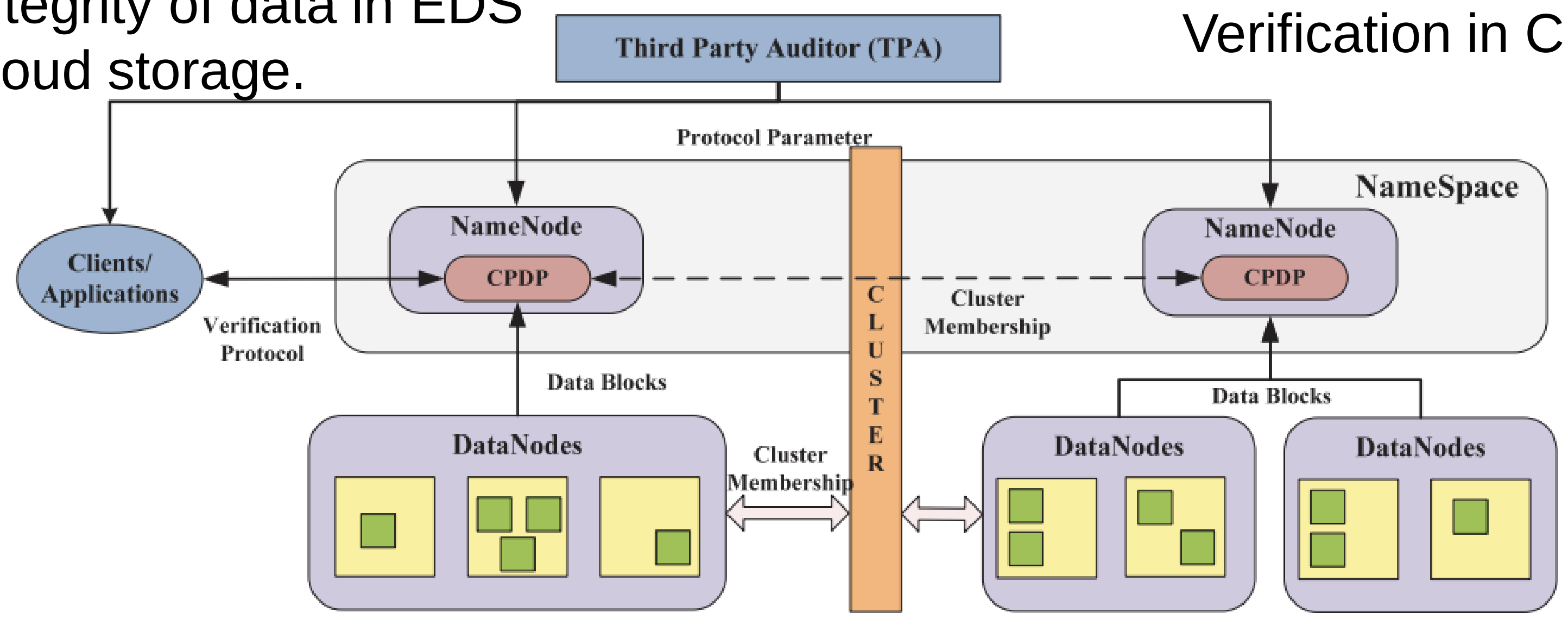
SECURITY MONITORING IN EDS CLOUD

- EDS cloud is dynamic because of the continuous migration of diverse data and information related to energy usage and demand responses. It is difficult to find a fixed location to place security sensors. To solve this, we leverage:
  - Software-defined networks (SDN) to observe and analyze traffic between EDS software modules.
  - Provable data possession (PDP) to ensure the integrity of data in EDS cloud storage.

SDN-based Network Policy Management

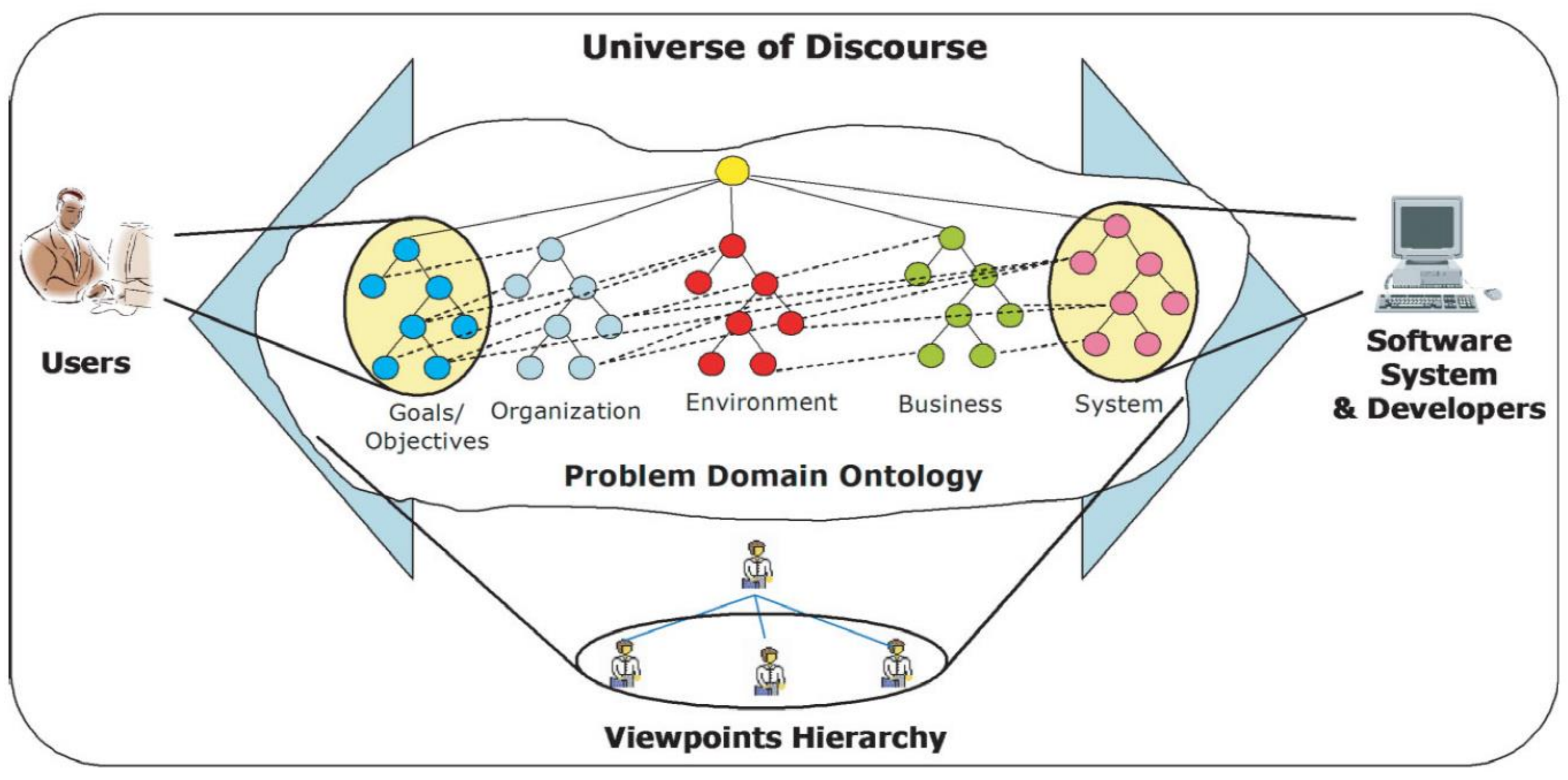


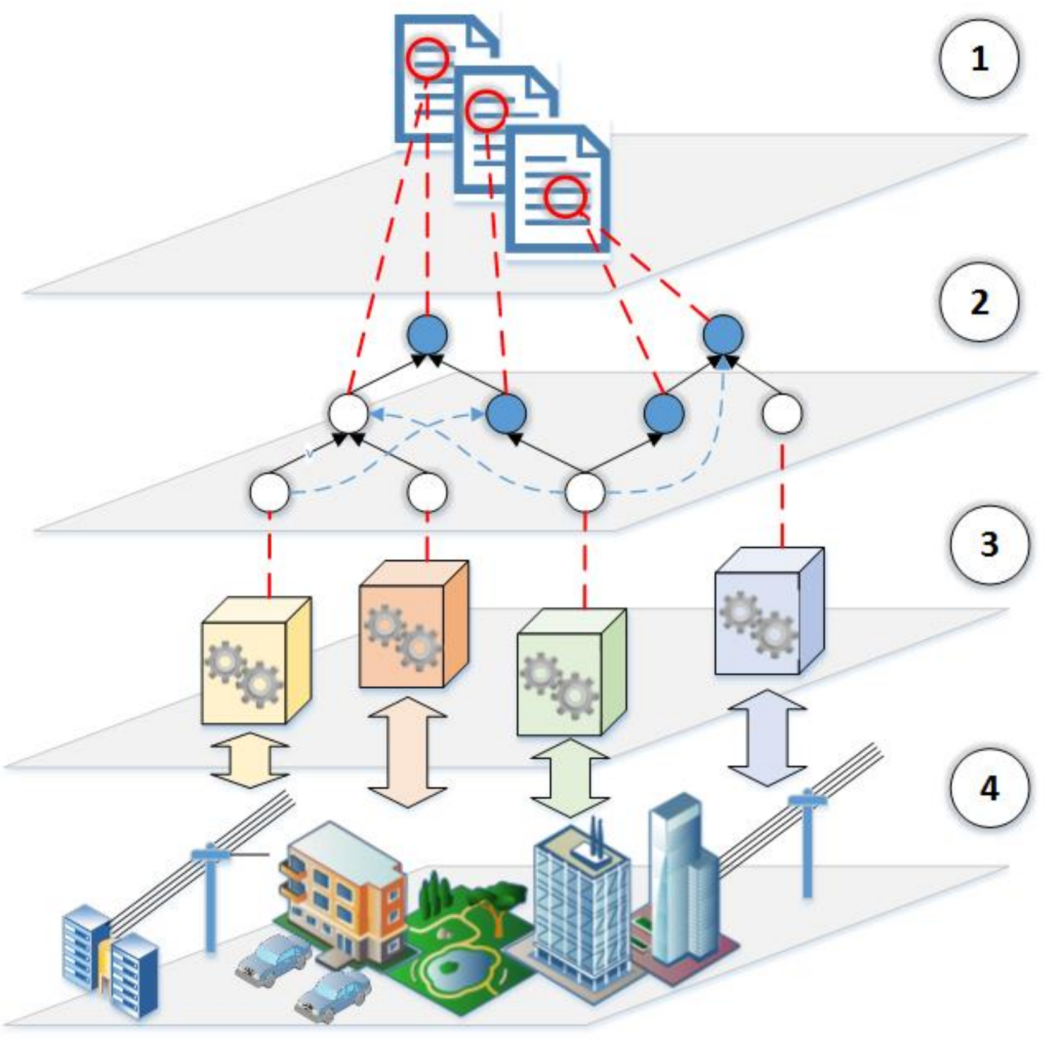
Provable Data Possession for Integrity Verification in Cloud



SECURITY COMPLIANCE MANAGEMENT IN EDS

- It is essential to build an *automated*, *configurable*, *well-defined* (theoretically justifiable), *systematic* (able to validate repeatably) and *practical* (deployable to organizations) multi-layer framework for automated VV&A in EDS.
- For that purpose, we plan to leverage our previous experience on the automation of the *Department of Defense's certification and accreditation process.*





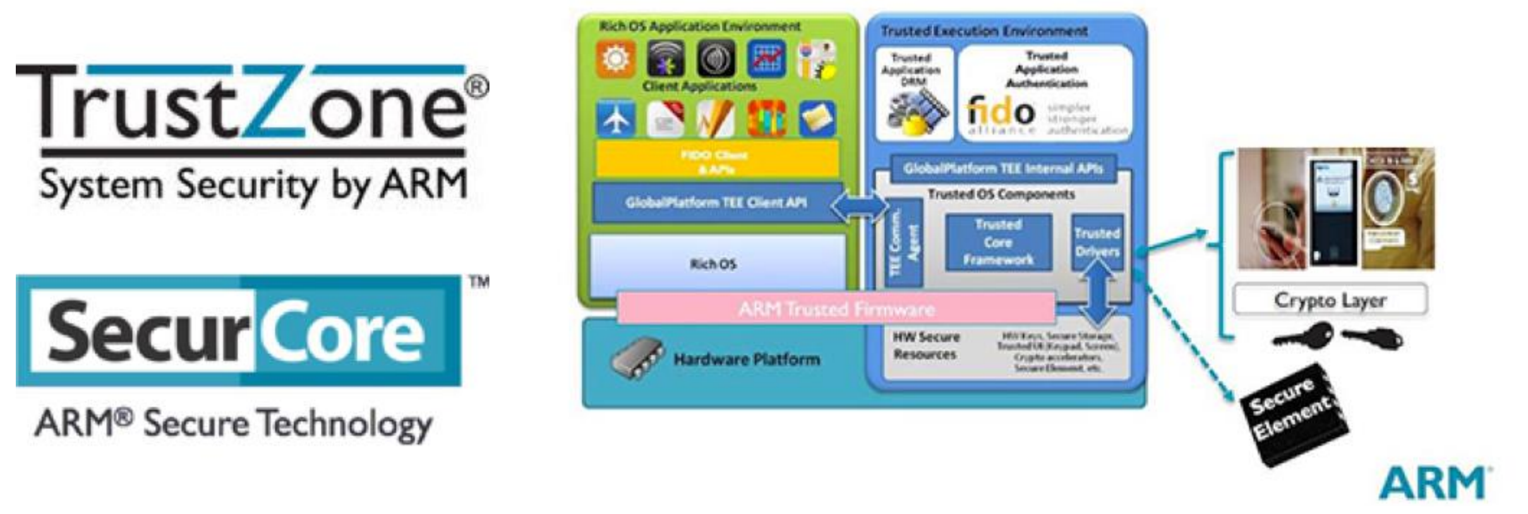
1. Initially, we plan to gather the most relevant documents on best practices for EDS, e.g., the ISECOM Open Source Security Testing Manual and various standards from the NIST Smart Grid Interoperability Panel.
2. We plan to obtain a well-defined description of the best practices and guidelines in the form of ontologies.
3. Based on such ontologies, we plan to develop an extensible framework that supports software modules handling automated monitoring and risk, countermeasure, and compliance analysis.
4. Data from EDS infrastructure, e.g., Smart Grids, will be collected in the field and processed by our supporting software modules.

BROADER IMPACT

- Support for advanced decision-making and correcting actions for secure management of EDS by means of visual user guidance techniques, e.g., rich *graphical user interfaces* (GUIs).
- Support for the rigorous study of security risks and assessments by means of the simulation, prevention, and risk analysis of attacks for mission-critical EDS.
- Improvement of the public's confidence in mission-critical EDS infrastructure (software and hardware).

INTERACTION WITH OTHER PROJECTS

- We plan to collaborate extensively with the research group led by Dr. Anna Scaglione (ASU) in the following research activities:
  - *Trustworthy Sensors, Meters, and IoT Devices for EDS*: We plan to leverage their experience in the use of metering and sensor devices for EDS in order to develop customized software modules for security VV&A.



  - *Security Gaps in Responsible EDS*: We plan to collaborate on the development of attack scenarios based on cyber-physical interactions with existing hardware infrastructure for EDS. Such a process includes vulnerability analysis, attack feasibility, and the development of techniques for risk and countermeasure analysis.

FUTURE EFFORTS

- Provide a comprehensive ontological representation that can serve as a reference for implementing best practices and guidelines for security for Smart Grids and EDS.
- Develop an advanced attack simulator that can effectively assess the resilience of EDS against current and future threats.
- Develop an extensible framework for building and incorporating customized *pluggable* software modules for automated security VV&A.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY