

IFIP 77th Meeting Session 2

Session Chair: Karthik Pattabiraman, UBC

Presenters:

Gabriel Giunta, Industry and Security Technology

Luis Garcia, UCLA

Gabriel's Presentation - 1

- CIP reference architecture - has many layers- Cyber, Physical, Human
- Integrate data from many different source (cyber, physical, human, web/social media etc.)
- Provide a detailed model of the events to mine correlations among them
- Complex event can be comprised of multiple simple events - applying CEP techniques

Gabriel's Presentation - 2

- Need domain expert to define rules to combine simple event into complex events (formal language for describing the rules)
- Binary classification of yes/no decisions with rules
 - No probabilities attached to the rules.
- Event information sent in JSON format. Different processes at different levels of Critical Infrastructure Protection.

Gabriel's Presentation - 3

The screenshot displays the STORM website interface. At the top, a red header contains the STORM logo and the name 'Emilia Gugliandolo'. Below this, a navigation bar includes 'Collaborative Services', 'Network & Sites', 'Process Mining', 'Document Library', and 'Update News'. The main content area features the STORM logo and the tagline 'Safeguarding Cultural Heritage through Technical and Organisational Resources Management'. Five network sites are listed, each with a representative image, a national flag icon, and a red 'NETWORK SITE' button:

- Diocletian Baths**: Rome, Italy.
- Mellor Heritage Project**: Greater Manchester, UK.
- Roman Ruins of Tróia**: Portugal.
- Rethymno historical centre**: Crete, Greece.
- Ephesus**: Anatolia, Turkey.

At the bottom of the site list, a note reads: '(select a Network Site to view available resources)'. A vertical sidebar on the left contains several icons for navigation.

Luis's Presentation- 1

- Distinction between safety and security
 - Safety applies to physical world, security to cyber world
- Attackers: Maximize physical impact while being stealthy
- TSV (Trusted Safety Verifier): Given a set of infrastructure safety requirements, does the PLC program satisfy them ?
- Physics-aware attacks and defences: LTL constraints and verifier
- PLC architecture and adversary model

Luis's Presentation - 2

- 2-way data manipulation via Harvey: Firmware malware that lies about system state
- Find the points in the firmware at which to perform the replacement and insert the malicious code there (engineering decision)
- Demonstrated this on a real power system testbed - drove the voltages to unrealistically high levels
- Challenge: no trusted hardware on legacy devices - need attestation solutions
- Physics-based Attestation: Based on timing requirements of the attacker - perturb the sensors slightly and observe the effects on the system

Luis's Presentation - 3

- Domain specific solution: 3D printing attestation (when you have malicious firmware)
- Control-Behaviour Integrity: Associate control-flow states with Physical states (ScadMan)
- Hybrid-Systems Modeling of CPS: Discrete state transitions + continuous variables (Dynamic Differential Logic)
- Formal rules for macro-programming IoT devices – If-this-then-that type of rules (remediation of the conflict)
- Robust multi-modal inferencing in heterogeneous IoT environments

Take-aways (in my opinion)

- Protecting CPS systems is challenging
 - Many different layers of abstraction, need to correlate among the events
 - Lack of trusted attestation mechanisms; attacker can cover their tracks
- Situational knowledge can come from many different sources
 - Domain experts composing complex rules (Gabriel)
 - Physics of the environment and deployment (Luis)
 - Knowledge of the program's code and behavior (Luis)
- Need for easy-to-use mechanisms to extract situational knowledge at scale