Multi-Level Vulnerability Modeling of Cyber-Physical Systems

Yuning Jiang, Yacine Atif, Jianguo Ding
School of Informatics, Univeristy of Skövde,
Skövde 541 28, Sweden
(firstname.lastname@his.se)

The 23rd Nordic Conference on Secure IT Systems - November 28 to 30, 2018 - University of Oslo, Norway

EUROPEAN UNION
Internal Security Fund ISF

Motivation

- Complex cyber-physical systems (CPSs) aggregate multiple components with varied degrees of vulnerability that could be exposed to cyberthreats.
- Threat agents use exploit vectors induced by vulnerability degrees to impact individual CPS assets.
- Risk is a function of vulnerability and threat impact, and needs to be assessed at both asset- and system-level.
- Asset-level vulnerability assessment uses published repositories such as CVE (Common Vulnerabilities and Exposures). System-level vulnerability uses a tree-structure to propagate component vulnerabilities.
- The vast repository of published vulnerabilities requires filtering techniques to prioritise them. E.g. CVE contains 103,786 vulnerabilities, out of which 5,898 (5.7%) were exploited during Q2 2018 (Fortinet Threat Landscape report).

Background

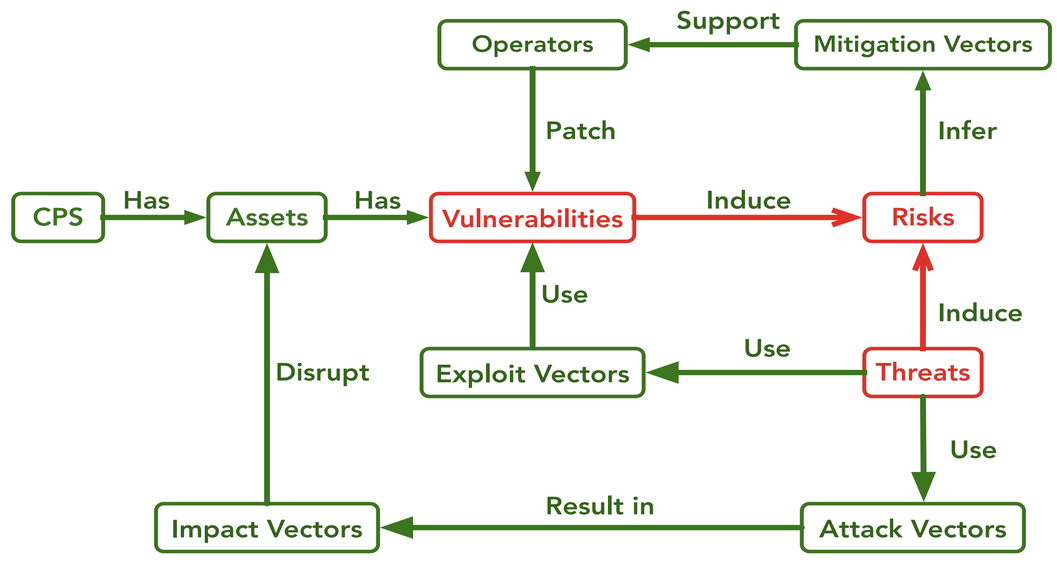

Fig-1 Conceptual Framework

Research Question

- How to model asset-level vulnerability?
- How to model system-level vulnerability?

Methodology

Asset-level Cyber-Vulnerability

- CPS component vulnerabilities are analysed against Web-based repositories (e.g. CVE) using mining techniques.
- Qualitative vulnerability indices are quantified using fuzzy-logic based techniques to alleviate subjective inconsistencies by expert analysts.

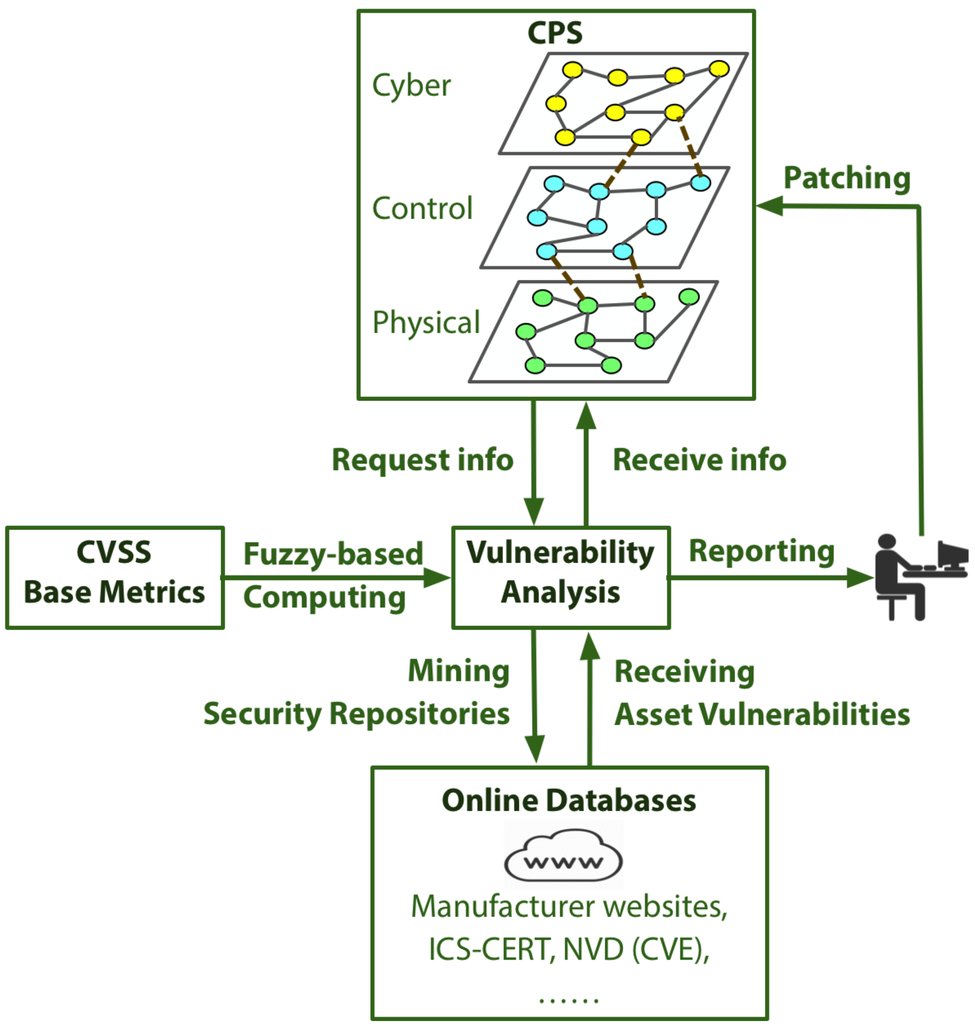

Fig-2 Streamlined Asset-Vulnerability Assessment

System-level Cyber-Vulnerability

Step 1: Compute asset-level vulnerabilites.

Step 2: Construct vulnerability tree.

Step 3: Compute threat impacts.

Step 4: Compute system-level vulnerability.

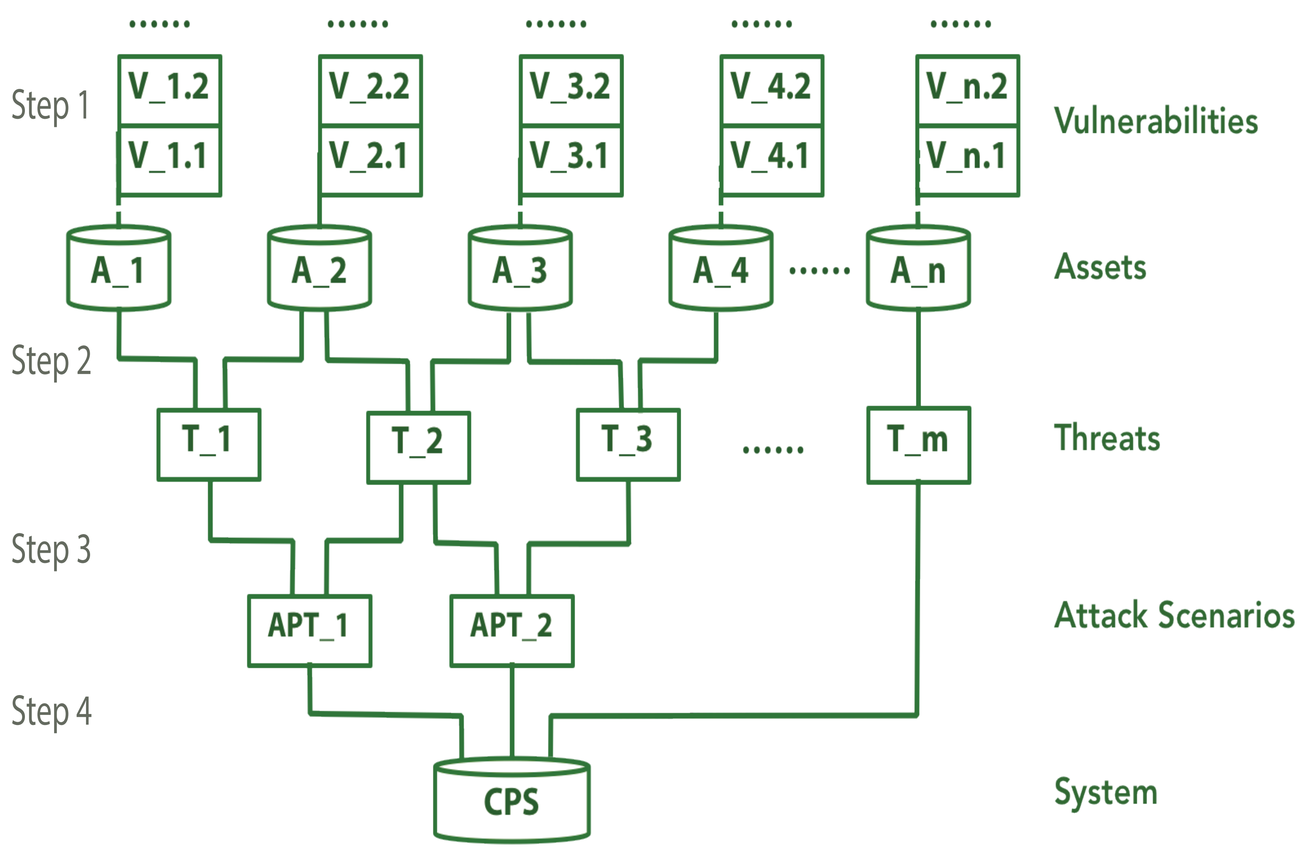

Fig-3 Vulnerability-Aggregation Analysis in CPS

Conclusion

- We suggest a streamlined approach for vulnerability evaluation at both asset- and system-level of CPSs.
- Further implementation and evaluation are being undertaken on a SCADA-based smart power-grid system testbed as a case study.

*This research is supported by EU ISF(Internal Security Fund) Project A431.678/2016 ELVIRA (Threat modeling and resilience of critical infrastructures).