lero THE IRISH SOFTWARE RESEARCH CENTRE
Science Foundation Ireland For what's next
University of Limerick
The Sunday Times Good University Guide 2019 Irish University of the Year

Sharing Knowledge About Security Incidents in Cyber-Physical Systems

Faeq Alrimawi, Liliana Pasquale, Bashar Nuseibeh
faeq.alrimawi@lero.ie

INTRO

- ➢Security incidents exploiting interactions between cyber & physical components are increasing
  - These interactions give more opportunities to attackers to cause harm
- ➢Common aspects between incidents can be observed
  - For example, in both, the Ukrainian grid incident & the German steel-mill incident, spear-phishing was used
- ➢Knowledge and expertise about such incidents is limited

METHODS

Share incident knowledge across Cyber-Physical Systems (CPSs)

1. Represent incident knowledge as incident patterns, which capture common aspects of incident instances
2. Extract incident patterns from specific incidents to:
   - Share incident information
   - Avoid disclosing sensitive information
3. Instantiate incident patterns to assess how they can re-occur in CPSs

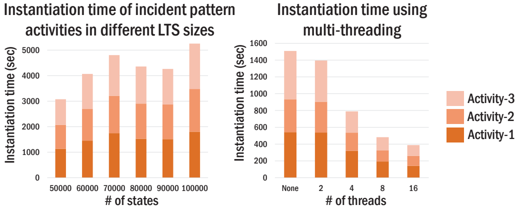
RESULTS

Scalability & Correctness. We can instantiate an incident pattern into different systems (of increasing sizes), obtaining sound results.

A smart building LTSs & Instantiation output

LTS		Instantiation Output	
States	Transitions	Generated traces	Relevant traces
50,000	198,771	14,777	600
60,000	252,897	23,848	704
70,000	295,160	98,720	801
80,000	349,517	143,186	881
90,000	399,319	184,269	942
100,000	445,028	216,561	1,012

Performance. We can instantiate an incident pattern activity in reasonable time, and improve performance by multi-threading.


Instantiation time of incident pattern activities in different LTS sizes
Instantiation time using multi-threading

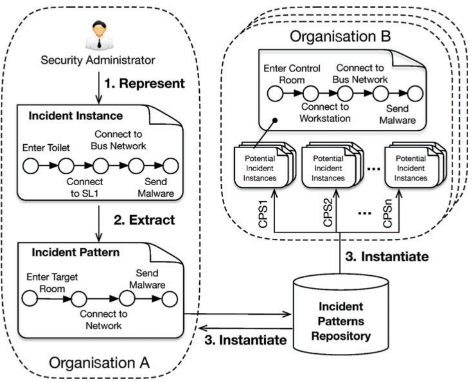
Theory

Incidents Are Meant for Learning, Not Repeating

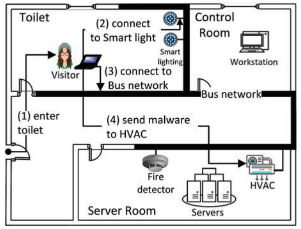
Capturing & sharing **commonalities** between **incidents** in cyber-physical systems can potentially **improve the security** of systems and **readiness** for future **investigations**

Take a picture to download related papers

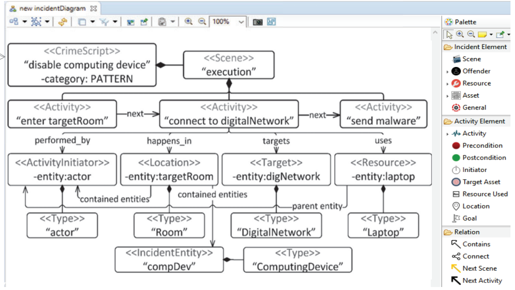
Approach



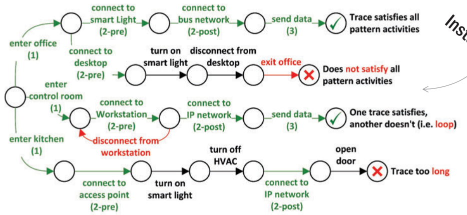
Incident Instance



Incident Pattern



Instantiations


enter office (1)
connect to smart Light (2-pre)
connect to bus network (2-post)
send data (3)
Trace satisfies all pattern activities
connect to desktop (2-pre)
turn on smart light
disconnect from desktop
exit office
Does not satisfy all pattern activities
enter control room (1)
connect to Workstation (2-pre)
connect to IP network (2-post)
send data (3)
One trace satisfies, another doesn't (i.e. loop)
disconnect from workstation
enter kitchen (1)
connect to access point (2-pre)
turn on smart light
turn off HVAC
connect to IP network (2-post)
open door
Trace too long

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union
European Union
European Regional Development Fund
Southern Regional Assembly