Software for a better world

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

University College Dublin
An Coláiste Ollscoile, Baile Átha Cliath

University of Limerick
Ollscoil Luimnigh

University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

A World Leading SFI Research Centre

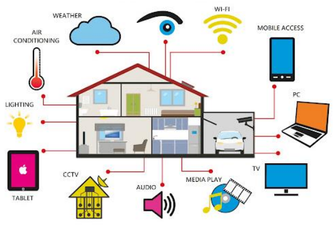
Science Foundation Ireland For what's next

Engineering Sustainably Secure Cyber-Physical Systems

Liliana Pasquale, Kushal Ramkumar, Wanling Cai, Gavin Doherty, John McCarthy, Bashar Nuseibeh

1 ENGINEERING SECURITY BY DESIGN IS DIFFICULT IN MODERN CYBER-PHYSICAL SYSTEMS (CPS)

Smart Home



Smart Factory

Cyber-Physical Systems (CPS) allow security threats to extend over a wider attack surface and cause physical damage [1].

CPS operate in an open world.

Adding/removing system components and device behaviour changes

Evolving Security Goals & Requirements

Unknown Attacks

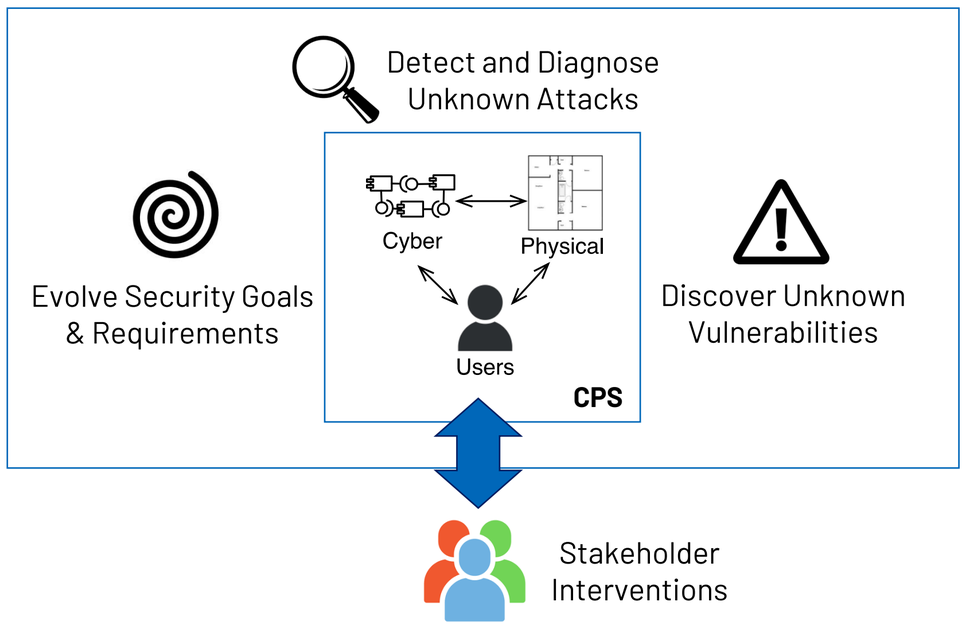
Zero-day or previously known attacks that can manifest differently depending on the CPS configuration.

Unknown Vulnerabilities

Unpatched or zero-day vulnerabilities.

2 SUSTAINABLE SECURITY:

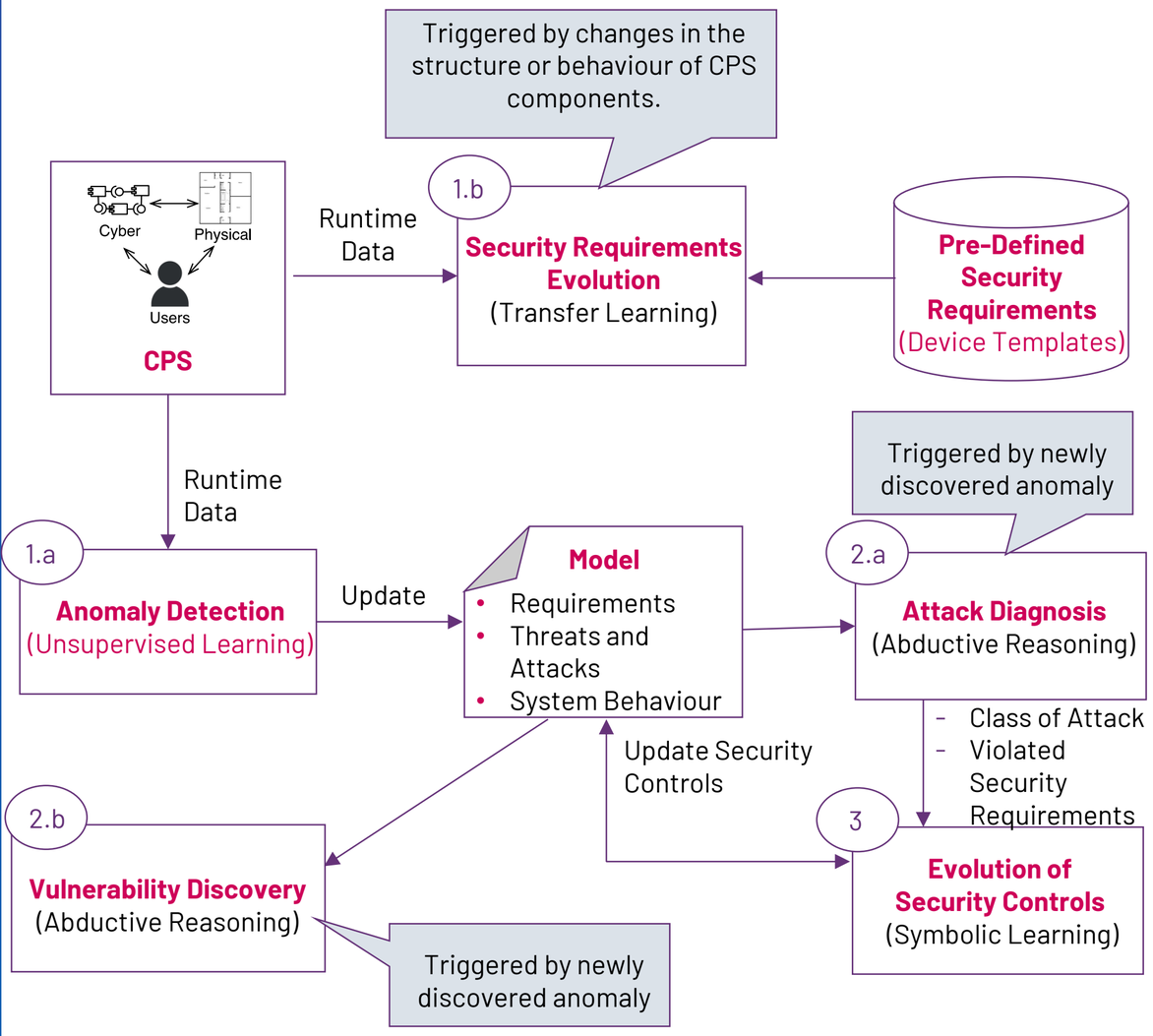
This project aims to engineer sustainably secure CPS [2] that can preserve security goals and requirements.



Objectives:

1) **Engineering Security Evolution:** CPS should evolve their security controls to address attacks, vulnerabilities and security goals & requirements changes.
2) **Engineering Stakeholders Interventions:** stakeholders should be involved in securing the CPS when this cannot be done automatically.

3 ENGINEERING SECURITY EVOLUTION:



4 ENGINEERING STAKEHOLDERS INTERVENTIONS:

Designing interactions with stakeholders to foster their engagement and improve the CPS security posture.

Stakeholders and Tasks

- **Users**: Monitor data, confirm anomalies, execute security controls
- **Engineers:** Diagnose attacks, select or execute security controls
- **Pentesters:** Diagnose attacks and discover unknown vulnerabilities

When?

Reasoning techniques based on projected satisfaction of security goals.

Who?

Reasoning techniques based on models of humans in a cyber-human system (e.g., [3]).

Situational Awareness

Personalised synthetic explanations of the state of the CPS (using LLMs).

Interaction Design

- User-centred design
- Human-machine collaboration
- Automation and human agency

References

[1] Tsigkanos, C., Pasquale, L., Ghezzi, C. and Nuseibeh, B., 2016. "On the interplay between cyber and physical spaces for adaptive security". *IEEE Transactions on Dependable and Secure Computing*, *15*(3), pp.466-480.

[2] Pasquale, Liliana, Kushal Ramkumar, Wanling Cai, John McCarthy, Gavin Doherty, and Bashar Nuseibeh. "Sustainable Adaptive Security." *arXiv preprint arXiv:2306.04481*(2023).

[3] Eskins, D. and Sanders, W.H.. "The multiple-asymmetric-utility system model: A framework for modeling cyber-human systems. In *2011 8th International Conference on Quantitative Evaluation of SysTems*, pp. 233-242, 2011.

HOST INSTITUTION

University of Limerick
Ollscoil Luimnigh

PARTNER INSTITUTIONS

Ollscoil na Gaillimhe University of Galway · Maynooth University National University of Ireland Maynooth · Trinity College Dublin Coláiste na Tríonóide, Baile Átha Cliath The University of Dublin · University College Dublin An Coláiste Ollscoile, Baile Átha Cliath · UCC University College Cork, Ireland Coláiste na hOllscoile Corcaigh · MTU Ollscoil Teicneolaíochta na Mumhan Munster Technological University · DCU · SETU South East Technological University · Dundalk Institute of Technology Dhún Dealgan · TUS · ATU Atlantic Technological University

FUNDED BY:

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

Science Foundation Ireland For what's next