Science Hackathons for Cyberphysical System Security Research

Putting CPS testbed platforms to good use

Simon Foley

IMT Atlantique, Rennes, France

Joint work with **Hackers**: Edwin Bourget, Thomas Cledel, Stephane Grunenwald, Jose Rubio Hernan, Alexandre Kabil, Raphaël Larsen, Kristen Vanhulst; **Research Engineer** Fabien Autrel, and **Applied Psychologist** Vivien Rooney.

ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC@CCS), 2018

Overview

- Context and motivation
- A science hackathon for CPS security research
- Reflection

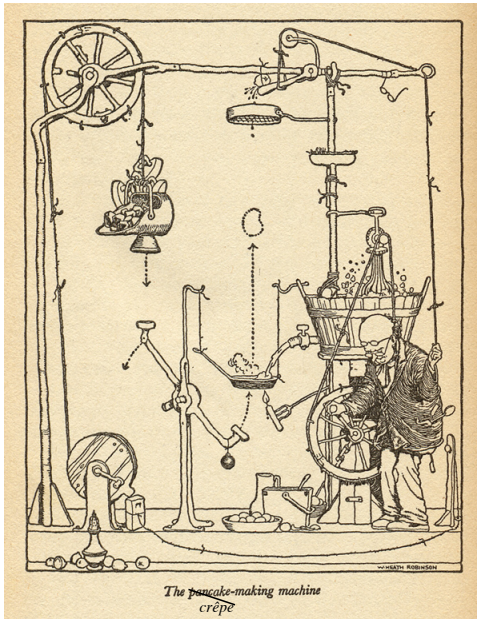
IMT Chair
Cybersecurity of critial infrastructures

- Institute Mines Télécom industry Chair.
  - Held by IMT Atlantique, with Télécom ParisTech and Télécom SudParis.

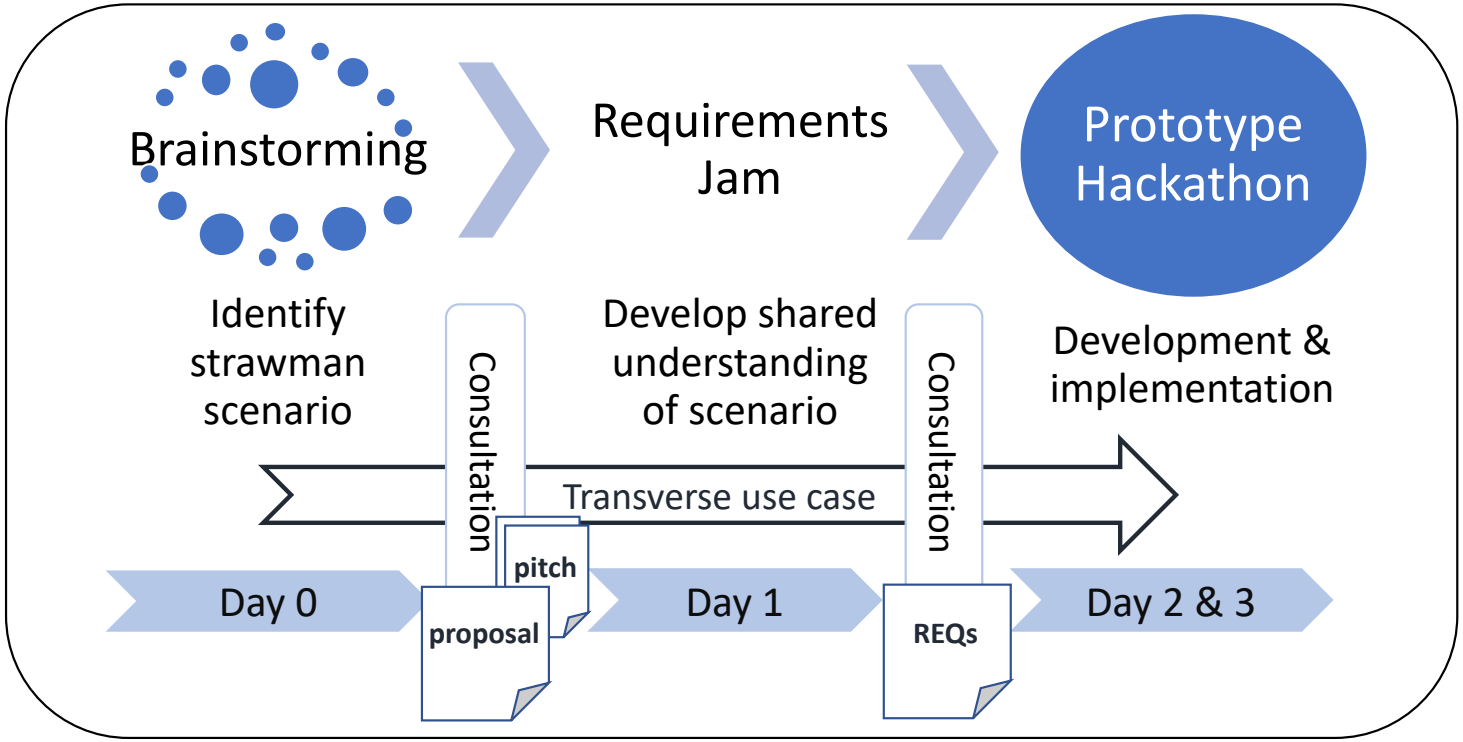
- About 30 academic staff/students, plus
- 8 industry partners, collaborating on
- 12 separate industry-targeted research projects,
- mostly related to security of cyber-physical systems.

Transverse Use Cases

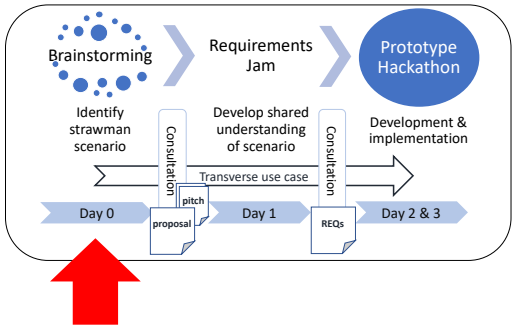
- Targeted industry use-cases
  - How to share project foreground IP within Chaire when background IP may be constrained?
  - 12 projects, risk of research silos emerging
- Transverse use cases
  - Share and demonstrate research results in Chaire, unencumbered by background or sensitive IP.
  - Not a significant development effort: fail fast
- Develop via a *scientific* hackathon
  - Researchers get together, collaborate and develop a research idea.
  - Get exposed to new research questions, learn about some technology and explore how work might fit into a larger research landscape.
  - Like a hackathon, but not competitive



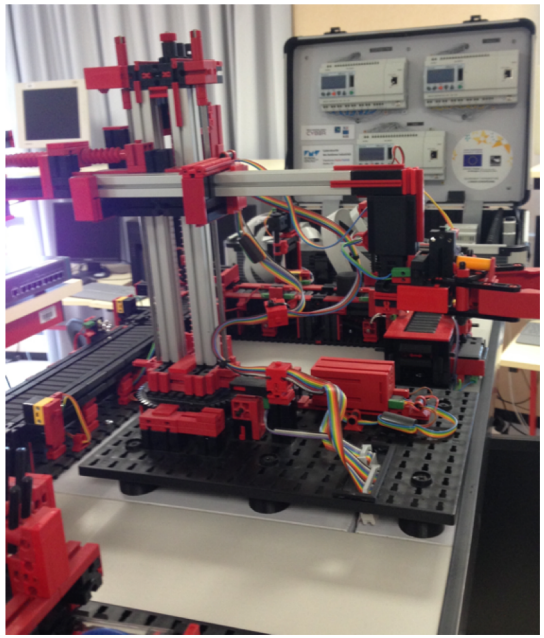
Our science hackathon steps



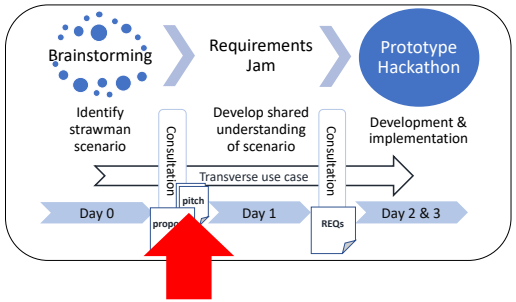
Stage 0: Brainstorming



- **Step 0.** Fabien. Introduction to fischertechnik platform
- **Step 1.** (20 mins) How might your work be interpreted on this platform?
  - Group A: Kristen, Alexandre, Vivien, Thomas
  - Group B: Raphael, Jose, Edwin, Stéphane
  - Each group generate 1-2 slides describing their scenario(s), challenges and what is needed to achieve it.
- **Step 2**: (40 mins) Groups presentations, discuss, look for synergies, refinements.
- **Step 3**: (30 mins) Presentation of an overall view of the use-case (to all), discuss and plan next steps.

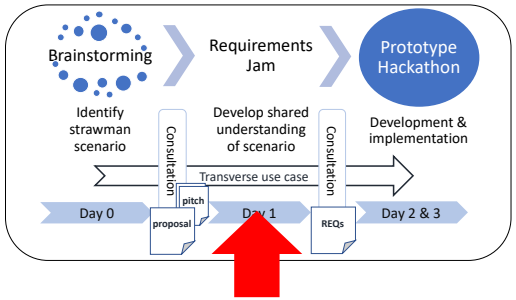


[Title] your *pitch in one slide*

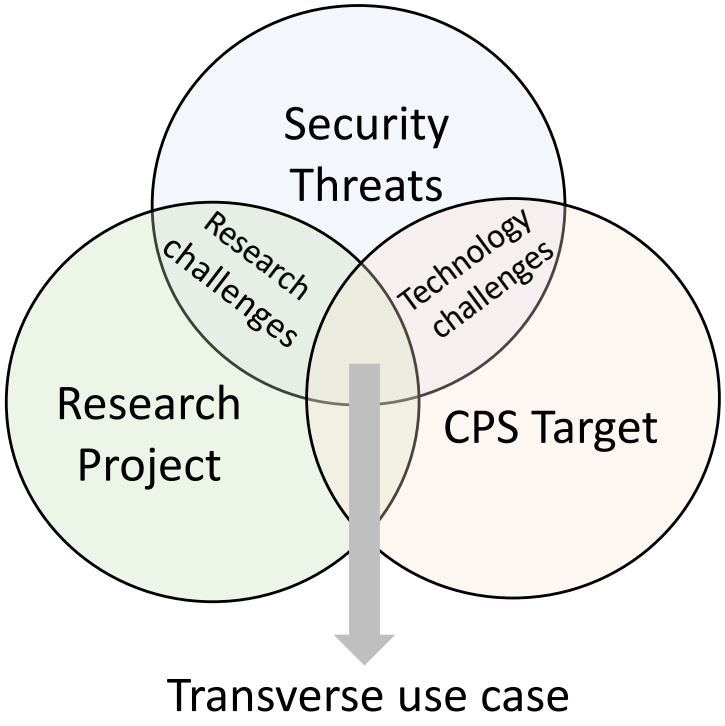


- Threat scenario *What is the threat (related to your research project) that you are focusing on, how do you plan on supporting it in the CPS testbed, and is your approach innovative?*
- Technology challenges *What technical development will be needed on the CPS testbed to implement the scenario? Are there potential obstacles? Can your scenario be implemented with minimal (re-)coding of the target (preferable)?.*
- Research challenge *How does this relate to the research questions on your own project? Will platform development leverage/enable your research work (preferable)?*

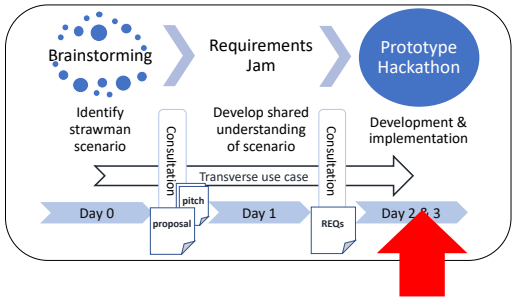
Stage 1: Requirements Jam



- **Objectives:** identify & specify transverse use-case that can be used to illustrate your research.
- **Step 0**. 10h00 Kick-off/planning
- **Step 1**. 10h15 Requirements development
- *lunch and checkpoint somtime here*
- **Step 2**. 15h00 Online presentation & discussion.
- **Step 3**. 16h00 Use case specification
- 17h00 Finish



Stage 2: Hackathon

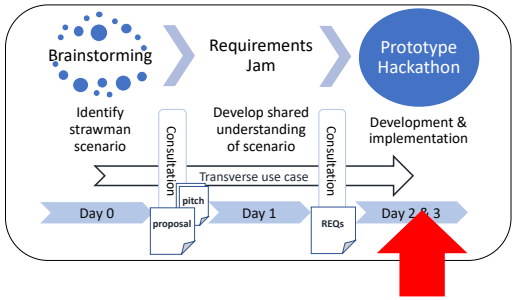


Threat scenario

- stop conveyor-belt & release clamp to halt production line, or
- change milling/drilling times & reduce finished product quality.

- Attacker takes control at the OT administration workstation:
  - exploit a vulnerability of the workstation or obtain administrator credentials, and
  - disable (physically or remotely) the workstation, forcing administrators to use a less secure secondary rescue workstation.
- Attacker sends Modbus packets to PLC.

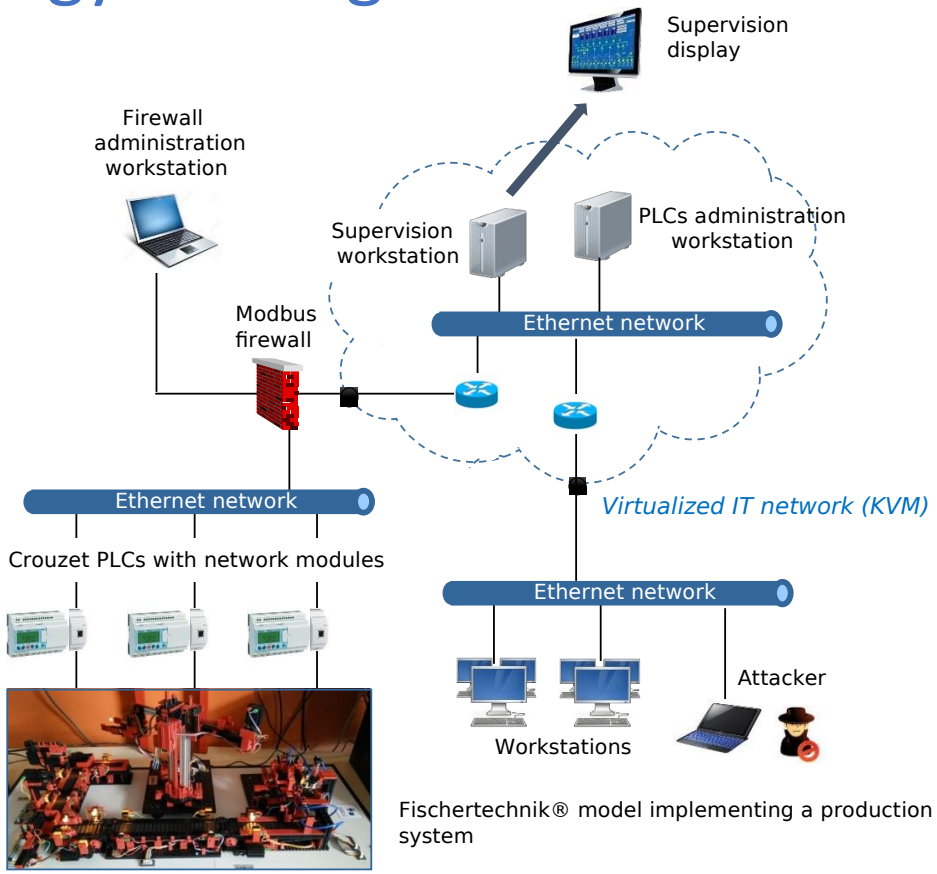
Stage 2: Hackathon



Threat scenario

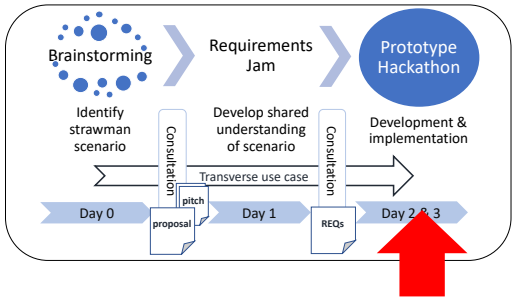
- A
  a
- A

Technology hacking



Fischertechnik® model implementing a production system

Stage 2: Hackathon



Threat scenario

- A
  a
- A

Technology hacking

Research challenges

- Threat model analysis (T4).
- Real-time security & safety diagnosis of anomaly alerts (T3)
- Reasoning about resilience in the deployed configuration (T5).
- Provenance of sensor data (T7).
- Immersive visualization (T2)

Determing whether it was a success

How might it be improved?

- Was something implemented?
  - Yes, although not `end-to-end' and its ongoing work.
- Was something published?
  - In progress, appearing in use-case/example snippets.
- Was something learnt?
  - Yes, its a flipped classroom
- Was ..... ?
- This is just my opinion and tells only half the story
- What was the hackers' experience?

Investigating the hackers experience

via a qualitative study

Method

- Semi-structured interviews with students by Applied Psychologist
- Thematic Analysis applied to interview data
  - 8 interviews, 141 minutes of audio material

The hacker experience

Some of the themes from the study

> *"If someone told us, do that, it wouldn't be a hackathon."* [Interview extract]

- Benefits
  - Clarifying individual research goals: practically and conceptually
  - Understanding broader context of research in the Chaire
  - Transverse use case enriches communication with industry partners
  - Fostering esprit de corps
- Tensions
  - Understanding the form & substance of the hackathon
  - Expectations from me, their supervisors and industry
  - Tension between prescription versus true `hacking'

Reflections

- Hackathon encouraged collaboration and discouraged research silos
- Found a good use for a CPS test bed
- Uncovered tensions around expectations for the science hackathon in form and substance