SCIPIO

SECURE CHIPS FOR CYBER-INTELLIGENT PHYSICALLY INTERCONNECTED OBJECTS

PROJECT PROPOSAL

Contact: Fethulah Smailbegovic (f.smailbegovic@tudelft.nl)

TU Delft Delft University of Technology

CognitiveIC
Feel. Think. Act.

1 – Motivation 

- Only **4%** of organizations **are confident** they have fully considered the cybersecurity implications of their current strategy and incorporated all relevant risks and threats. **[EY Global Information Survey 2018]**
- Cybercrime damages will cost the world **$6 trillion** annually by 2021, up from $3 trillion in 2015. **[Cybersecurity Ventures 2018]**
- There is a hacker attack **every 39 seconds**. **[University of Maryland 2017]**
- **Most compromises** took minutes or less (87%), only 3% are discovered quickly (minutes) **68% went undiscovered for months or more**. **[Verizon 2018]**
- It becomes worse with each new Internet connected device. **Almost 27billion** of IoT connected devices expected in 2019. **[www.statista.com]**
- **Hence, complete and efficient solutions to provide defence against cyberattacks are urgently needed!**

2 – State of the Art

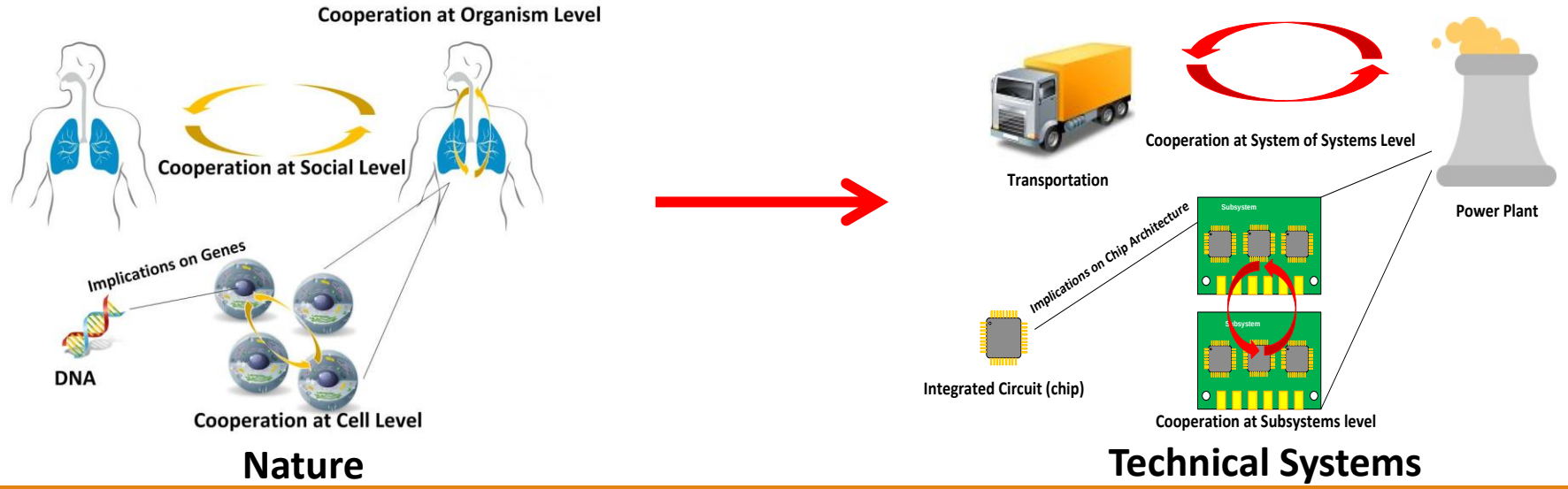
State-of-the art security solutions.

- All existing solutions are mainly **software related assuming HW is trustworthy.**
- **No complete, adaptive and efficient self-learning approach to** protection, incident response and recovery of the system.
- The **response to unknown attacks** involves significant **software and hardware re-design**.
- **The existing security solutions** and **system complexity overwhelm the human user** what **significantly contribute to** growth and spread of **cyberattacks**.

Therefore, there is urgent need for new HW driven, smart and agile security solution to protect and defend digital assets.

3 – Concept

- Nature provides inspiration for the concept of HW driven and smart cooperation in ICT. Concept is based on these fundamentals:
  - **Just as DNA enables cooperation in nature, chip enables cooperation in electronic systems.**
  - Each chip **feels** the environment, **thinks** about actions and **acts** alone or in conjunction with other components.



4 – Objectives 🎯

- Reduce the success rate of the existing attack patterns and any of their combination by 95% assuming timely detection and response.
- Reduce system response and recovery time to minutes and less rather than days, weeks or months.
- Guarantee 95% protection of all data on the chip at all times.
- Guarantee recovery of at least 50% of data and functionality in case of successful attack.

5 - Consortium

- Consortium (at the moment):
  - Technical University in Delft (Computer Engineering)
    - TU Delft has many years of experience in participation and coordination of EU and nationally funded projects.
  - CognitiveIC (SME, spin off from TU Delft)
  - CNRS - Centre national de la recherche scientifique
- We still need in consortium:
  - Security Analysis and Penetration Testing
  - HW (digital, analog) and SW design skills
  - System Integrators (e.g. PCB Designers, Testers)
  - Use Case Providers (e.g. Industry, Manufacturing, Health, Automotive, …)