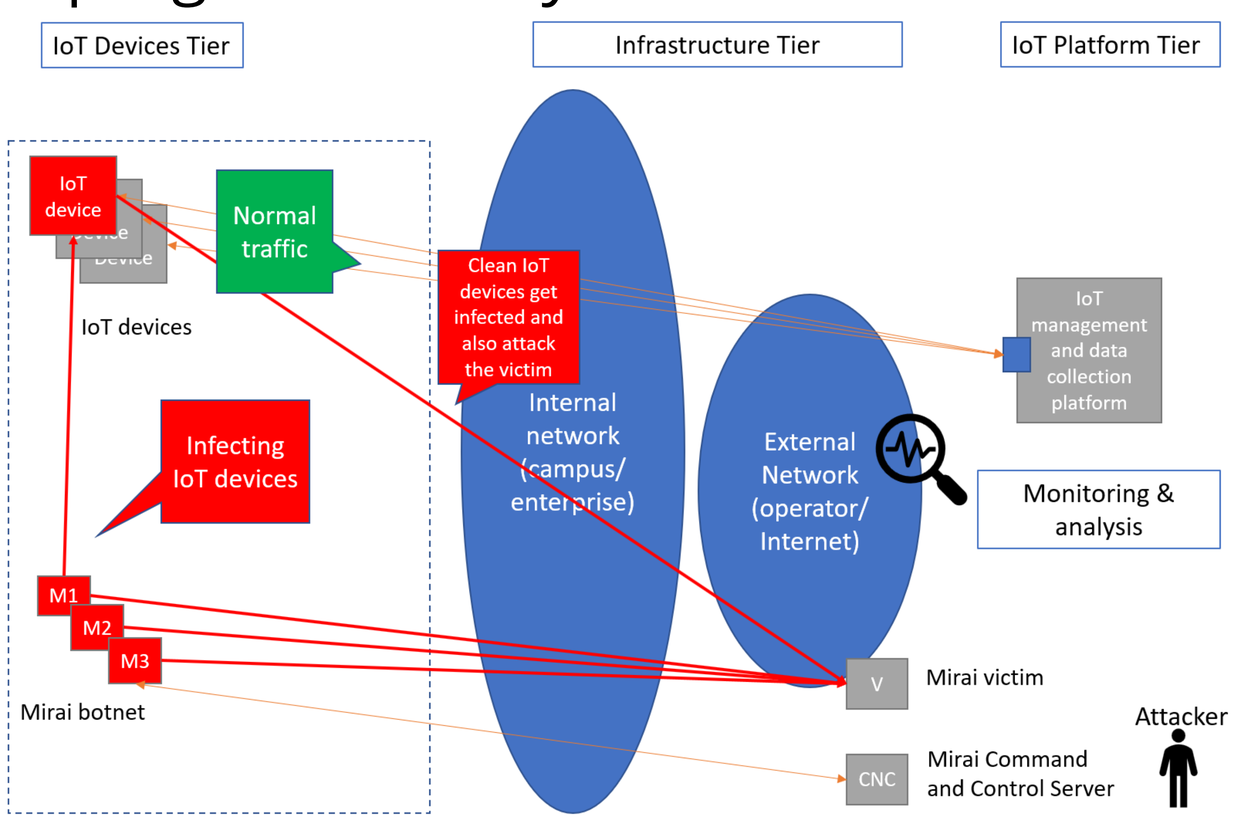
AI-NET-PROTECT

TNO innovation for life

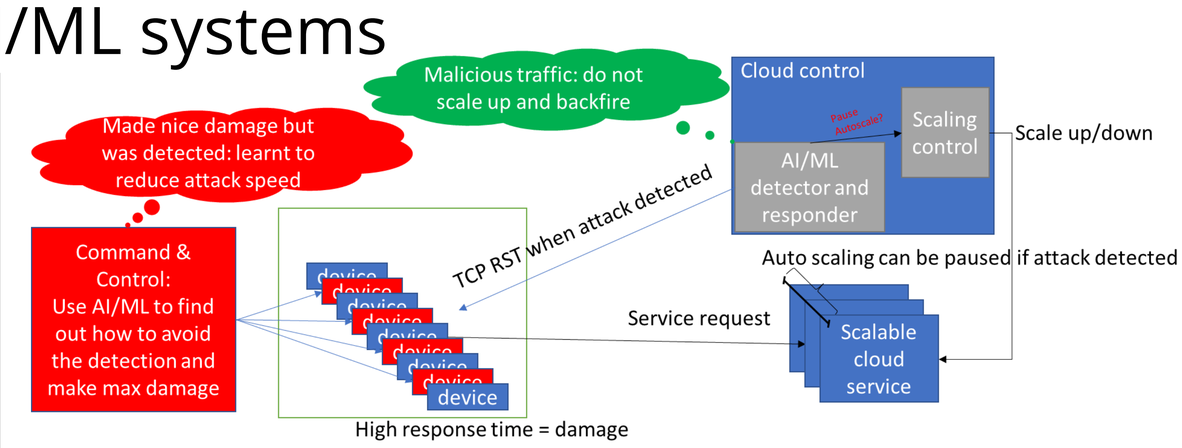
Elevate security of IoT by using cloud programmability and AI/ML

- IoT = Internet of … Troubles !
  - Huge number of devices, old firmware, default passwords, no crypto,…
- Our focus: take perspective of infrastructure you can control (cloud, telco)
  - Do not try to fix IoT devices themselves
- Run/detect/isolate/… using programmable infrastructure functions
  - Programmability: easier design as well as reconfiguration in run-time
  - Exploit AI/ML to help with anomaly detection and/or resource management

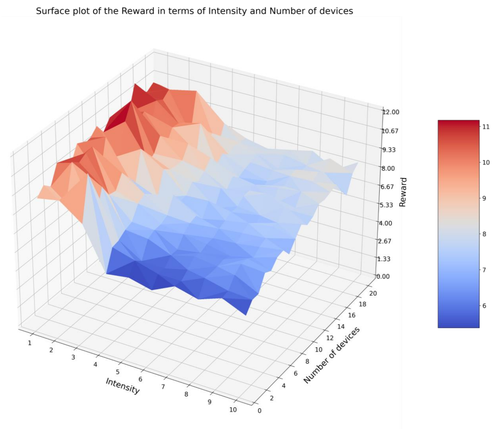


Work in progress: attacks *against* AI/ML systems

- What if AI/ML system becomes target on its own ?
- Example:
  - infected IoT devices send malicious requests
  - …which are detected and blocked by AI/ML-based defense system
  - However, attack pattern can be then tuned to avoid detection (e.g., send less traffic)
  - Moreover, attacker can also employ AI/ML to learn how to by-pass AI/ML-based detectors
- **General problem of AI/ML, not limited to IoT**
- **Interested ? mailto:piotr.zuraniewski@tno.nl**

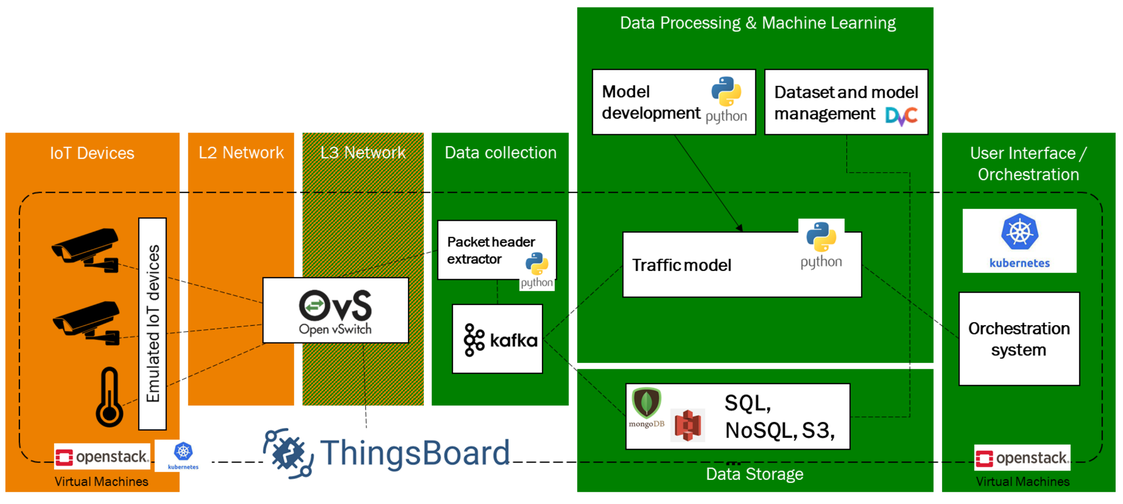


- Reinforced learning to get optimal parameters set for attack



Realization in TNO Research Cloud – malware deployed as cloud service

- Virtual lab in our private cloud, emulating enterprise network, IoT devices, ISP, cloud services, public Internet,…
- Programmability and automation for ease of management, reproducibility and flexibility (e.g., scaling)
- Real but partially disarmed malware (Mirai) and custom software used to infect IoT devices and orchestrate attacks
- AI/ML: data collection and analysis pipelines to monitor, model, detect and ultimately react



SPONSORED BY THE
Federal Ministry of Education and Research
VINNOVA Sweden's Innovation Agency
Ministerie van Economische Zaken en Klimaat
Narodowe Centrum Badań i Rozwoju
eureka