GRIFIN

COGNITIVE AND PROGRAMMABLE SECURITY FOR RESILIENT NEXT-GENERATION NETWORKS

Auteurs

Gregory BLANC
SAMOVAR
IMT/Télécom SudParis
Institut Polytechnique de Paris

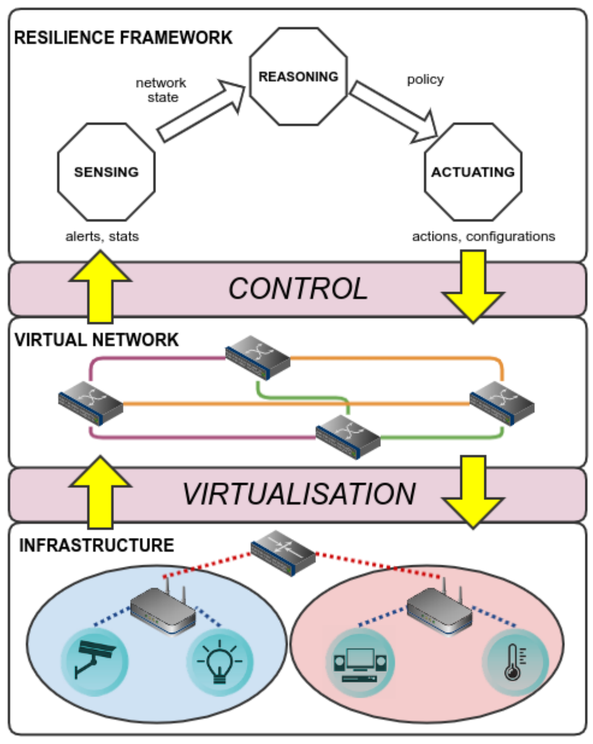
Thomas SILVERSTON
LORIA
Université de Lorraine

Sébastien TIXEUIL
LIP6
Sorbonne Université

Partenaires

CONTEXT
AND RESEARCH OBJECTIVES

- Next-generation networks will rely on **network slicing** and **edge computing**
- Number of interconnected devices keep on growing but security is stalling
- Necessity to provide **continuous** and **ubiquitous** yet **privacy-preserving** monitoring of connected devices
- Ensuring **resilience** instead of complete mitigation requires **refinement** and **adaptation** of security policies
- Machine learning (**ML**) and software-defined networking (**SDN**) as *enablers* for distributed anomaly detection and intent-based network security

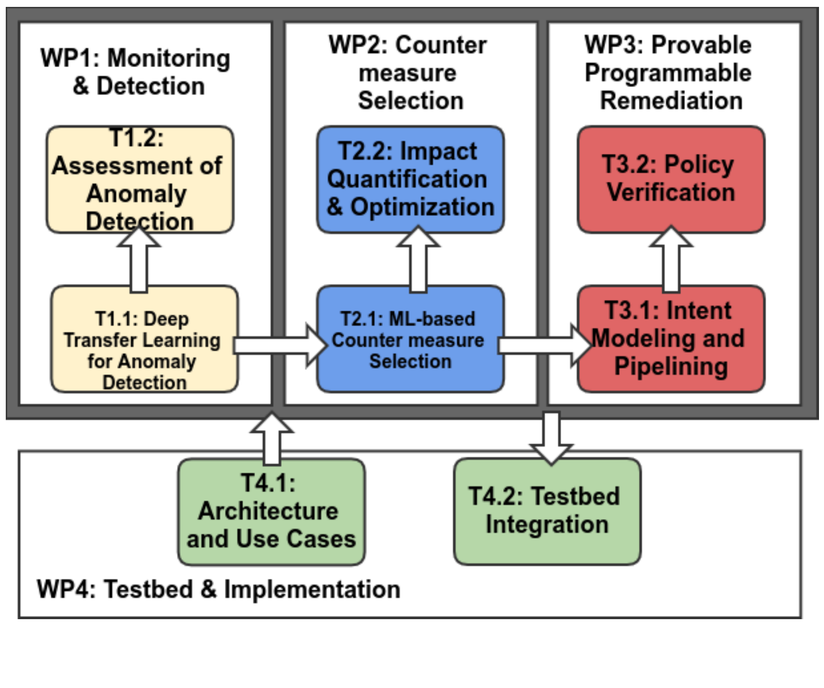


EARLY RESULTS
AND FUTURE WORK

1. A **taxonomy** of the approaches for the **evaluation** of intrusion detectors is ongoing: the state of the art is rich with *methodologies*, *criteria* and *metrics*
2. A doctoral research proposal is *open* to work on the **reasoning** and **actuating** components: **situation-aware** and **adaptive** countermeasure selection, countermeasures **refinement** and data-plane aware **distribution**, **verification** of the deployed countermeasures (see detailed offer on the website)

APPROACH
AND WORK PACKAGES

1. **Perception layer** is spread across **edge nodes** for an **adaptive** monitoring in terms of *sampling* and *scope*: distribution enables the capture of heterogeneous events, partial observation accommodates weak spots (resource-scarcity, low trust) with the ability to transfer learnt models
2. Ability to **assess** intrusion detectors in a *unified way* is key to **certification**
3. Optimal response to attacks involve **selecting countermeasures** able to address the attack vectors while minimizing the possible collateral damages
4. Relying on the possibility to explore and test different response alternatives will help design an **appropriate response**
5. **Intent-based** network adaptation leverages SDN to implement computed policy decisions: **modelling** the high-level intents and distributedly **pipelining** them across the *programmable* data plane
6. **Verification** of the deployed policy improves the overall *security loop*: **efficiency monitoring**, **error detection**



RESSI 2022
May 10-12, 2022

Contact gregory.blanc@telecom-sudparis.eu

anr-grifin.telecom-sudparis.eu