SecuriTAS
A Tool for Engineering Adaptive Security

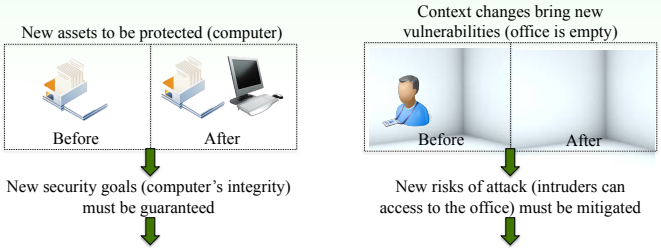
Liliana Pasquale[1], Claudio Menghi[1], Mazeiar Salehie[1], Luca Cavallaro[1], Ina Omoronyia[1], Bashar Nuseibeh[1,2]
[1]Lero – the Irish Software Engineering Research Centre, University of Limerick, Ireland
[2]Department of Computing, The Open University, Milton Keynes, UK
liliana.pasquale@lero.ie

Motivation

- **Security is concerned with the protection of valuable assets from harm.**

Assets can be: Physical objects; Sensitive Information; Intangible properties (Like)

- **Assets and context can change at runtime**, and this may affect related security concerns (threats, attacks, vulnerabilities, risk, security goals, and controls).



The security controls applied in the system **may no longer be effective.**

Adaptive Security

Adaptive Security aims to continue to protect valuable assets from harm, even when security concerns change dynamically.

To prevent potential attacks, security controls are adjusted depending on the (varying) risk of harm.

Application Domain

Access Control Systems

Access control policies (security controls) are not explicitly linked to *what* should be protected (assets) and *why* (security goals and requirements).

It is difficult to re-configure access control policies when assets or context change.

Engineering Adaptive Security with SecuriTAS

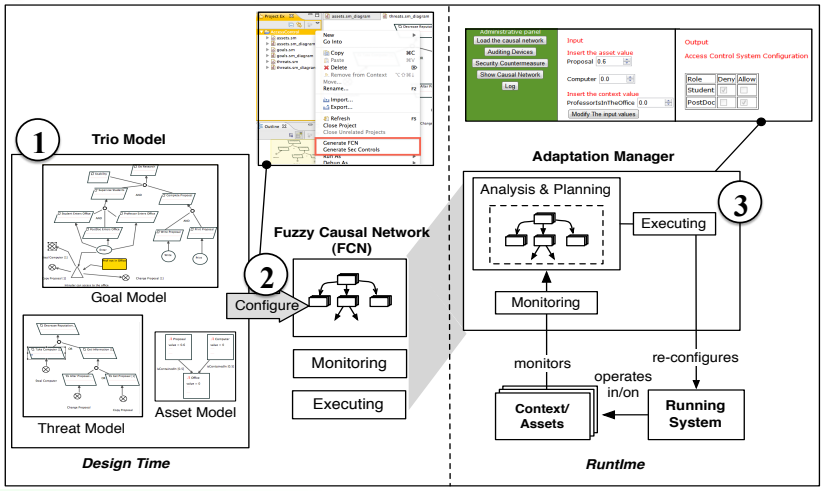
1 Modeling the security concerns together with the system requirements (Trio Model).

- The **Asset Model** represents assets and their relationships.
- The **Threat Model** represents threats and attacks.
- The **Goal Model** represents functional and non-functional requirements, including related vulnerabilities and security requirements.
- Context is explicitly represented and can activate/ deactivate parts of the Asset, Threat and Goal Model.

2 Configuring Adaptive Security

The trio model is used to configure the activities necessary to support adaptive security.

- A **Fuzzy Causal Network (FCN)** is generated from the asset, threat, and goal models. Each node of the FCN is associated with a specific security concern while the links identify influence relationships among security concerns.
- Assets and context are associated with the probes provided by the system to monitor them.
- Security controls are mapped to the security functions implemented in the system.



3 Applying Adaptive Security at Runtime

The Adaptation Manager implements the activities of the MAPE loop (Monitoring, Analysis, Planning and Executing).

- **Monitoring:** Detects changes in assets and context.
- **Analysis:** Updates the values of the nodes of the FCN, and re-estimates the risk and the utility of all possible configurations of security controls.
- **Planning:** Selects the security controls with the best utility.
- **Executing:** Applies the best configuration of security controls on the system.

Demonstration Scenarios