Fraunhofer AISEC

SMART GRID PROTECTION AGAINST CYBER ATTACKS

SPARKS threat analysis using Attack Trees and Semantic Threat Graphs

Martin Hutle

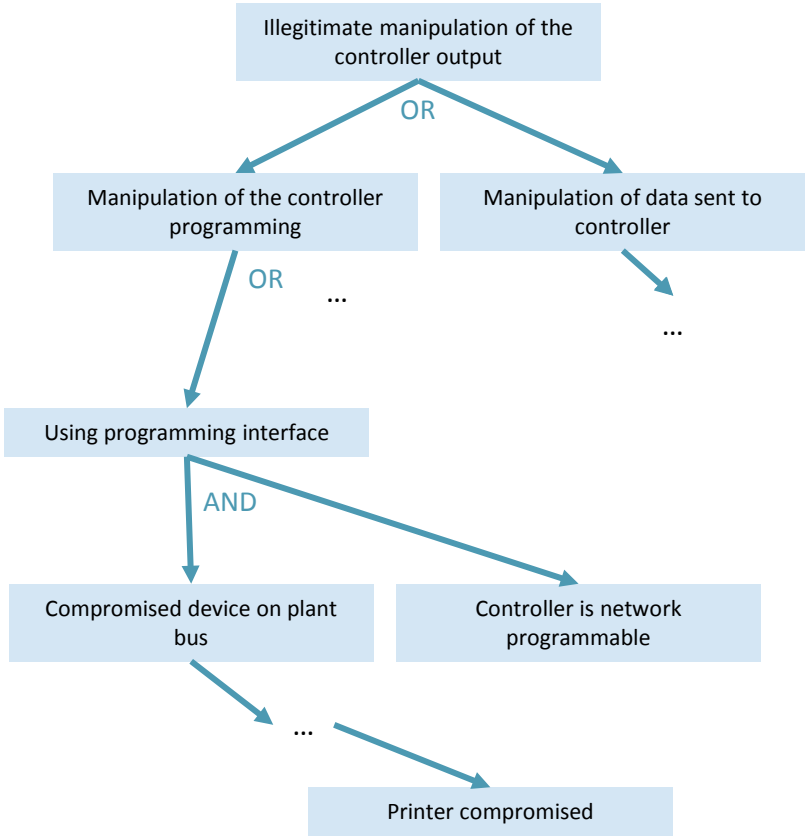
HyRiM workshop, 4. November 2015, Vienna

Joint work with Will Fitzgerald, Ewa Piatkowska, Norbert Wiedermann, Gerhard Hansch

EU FP7 Programme Contract No. 608224

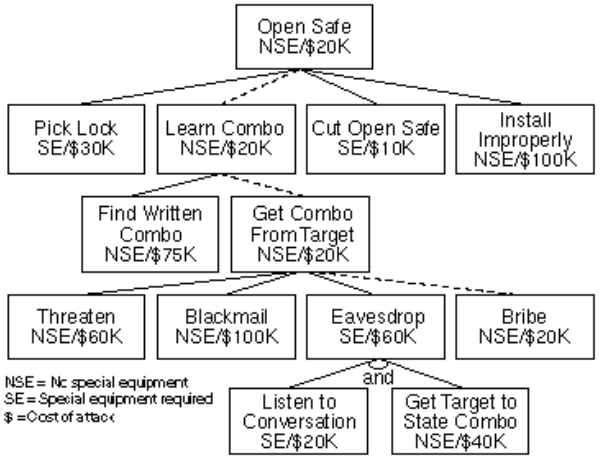
Attack Trees [Schneier 1999]

- Structured analysis of attack vectors from attacker's perspectives
  1. Identification of attack goals (violation of CIA of assets)
  2. Decomposition into sub-goals until sufficient fine granularity is reached (AND, OR)
  3. Evaluation of leaf trees with respect to likelihood
  4. Propagation of values to the root of the tree
     - AND: minimum of children
     - OR: maximum of children
  5. Identification of major attack paths (subgraph)



Attack Trees – State of the Art

- Attack Trees:
  - Introduced 1999 by Bruce Schneier to identify attack vectors [1]
  - Different Tree-Perspectives: Attack, Operation, System, Vulnerability, Fault/Failure, etc.
  - Attack Defense Trees (ADT) [2], Attack Countermeasure Tree (ACT) [3]
  - Sequential and ordered Attack Trees (EAT [4],OAT [5])
- Graphs
  - Directed acyclic graphs (DAG)
  - Vulnerability cause graphs (VCG) [6]
  - Security activity graphs (SAG) [6]
  - Semantic Threat Graphs (STG) [7]
- Applications:
  - Assessment of vulnerabilities in SCADA Systems [8]
  - Vulnerability analysis of digital instrumentation and control systems [9]



[1] Schneier, B., “Attack Trees: Modeling Security Threats,” *Dr. Dobb's Journal of Software Tools*, vol. 24, no. 12, 1999.

[2] Kordy, B. et al., “Attack-defense trees”, 2014

[3] Roy, A., Kim, D. S., and Trivedi, K. S., “Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees”, 2012

[4] Jhawar, R et al., “Attack Trees with Sequential Conjunction” 2015.

[5] Camtepe, S. A. and Yener, B., “Modeling and detection of complex attacks,” In *2007 3rd International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007*, 234–43.

[6] Ardi, S., Byers, D., and Shahmehri, N., “Towards a structured unified process for software security”, 2006

[7] Foley, S. N. and Fitzgerald, W. M., “Management of security policy configuration using a Semantic Threat Graph approach”, 2011

[8] Eric J. Byres, Matthew Franz, and Darrin Miller, “The use of attack trees in assessing vulnerabilities in scada systems”, 2004

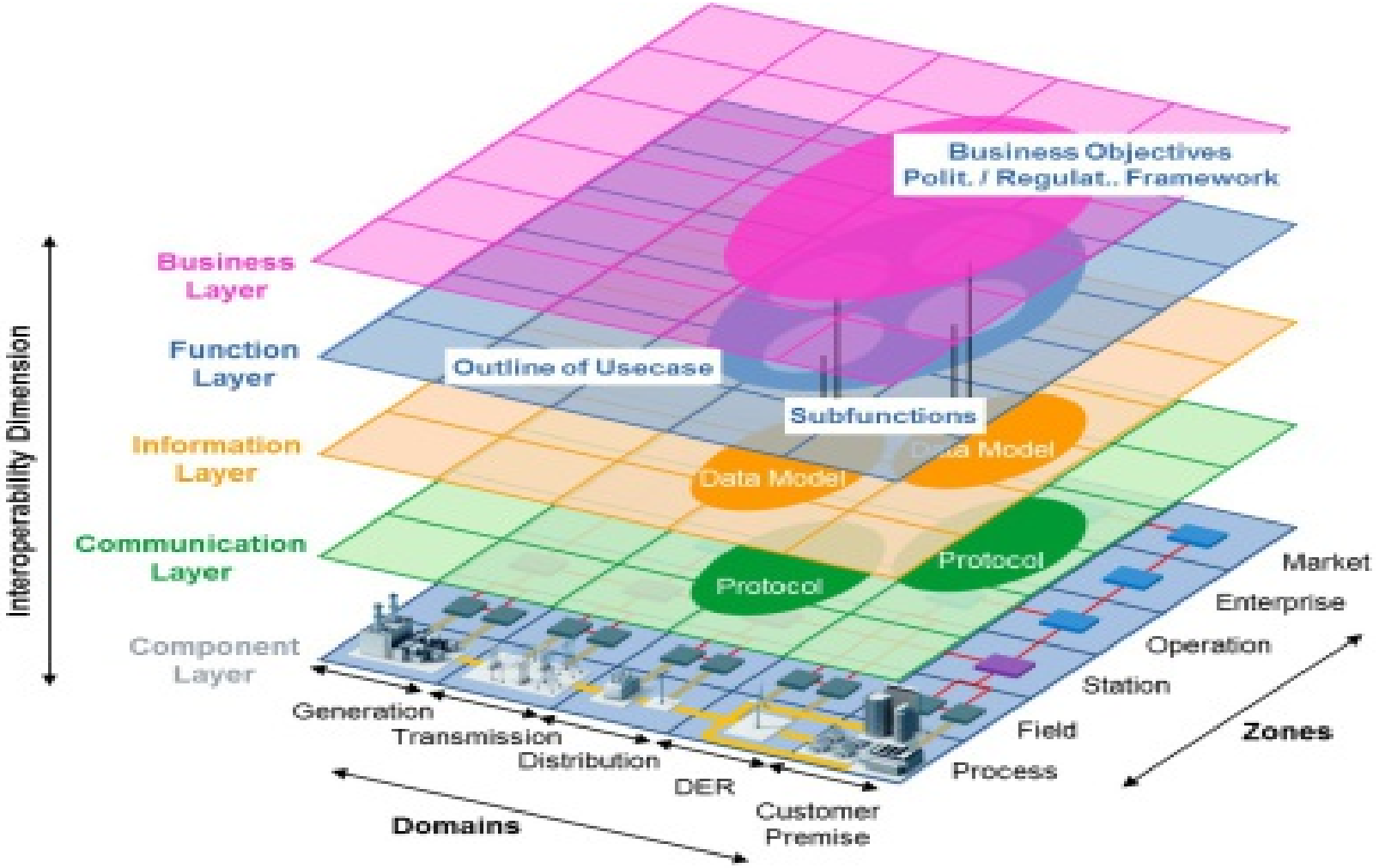
[9] Hutle, M. and Seidel, F., “Vulnerability analysis of digital instrumentation and control systems important to safety – a methodical approach,” 2015.

Objective:
Refining the attack tree approach to fit in the SPARKS risk assessment

- There is a lot of freedom when designing attack trees
- Strategy for tree decomposition
  - mapping SGAM model (components on layers) to attack trees
  - good coverage
  - develop best practices, catalogues (library of sub-trees)
- Attack trees tend to become intractable large and redundant
  - library of already created trees
  - modularity
  - combination with network analysis
    - attacker paths
    - attack trees for details
  - tool support

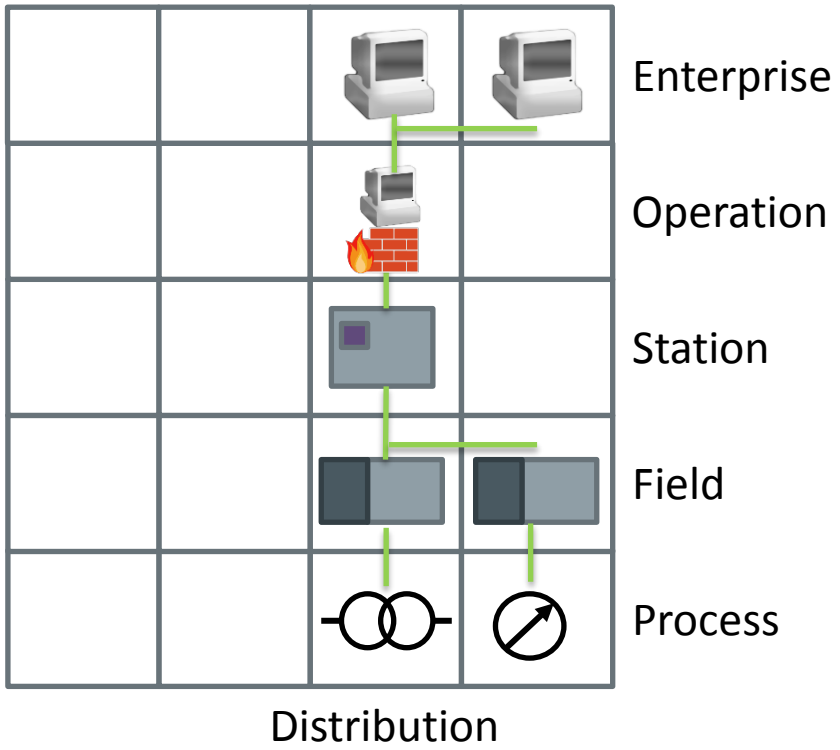
EU FP7 Programme Contract No. 608224

The Smart Grid Architecture Model (SGAM)



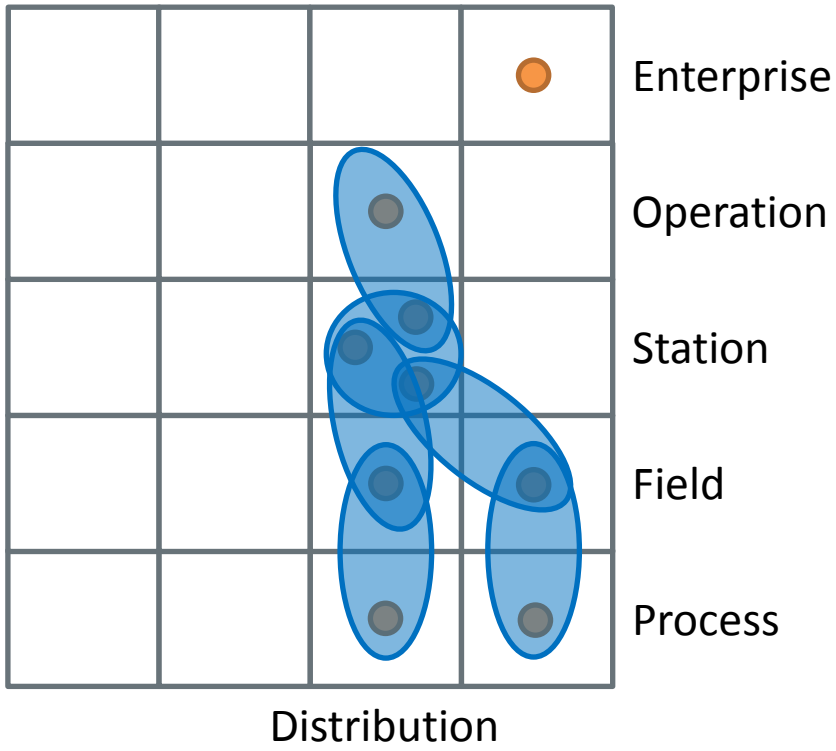
EU FP7 Programme Contract No. 608224

SGAM:
Component and communication layer



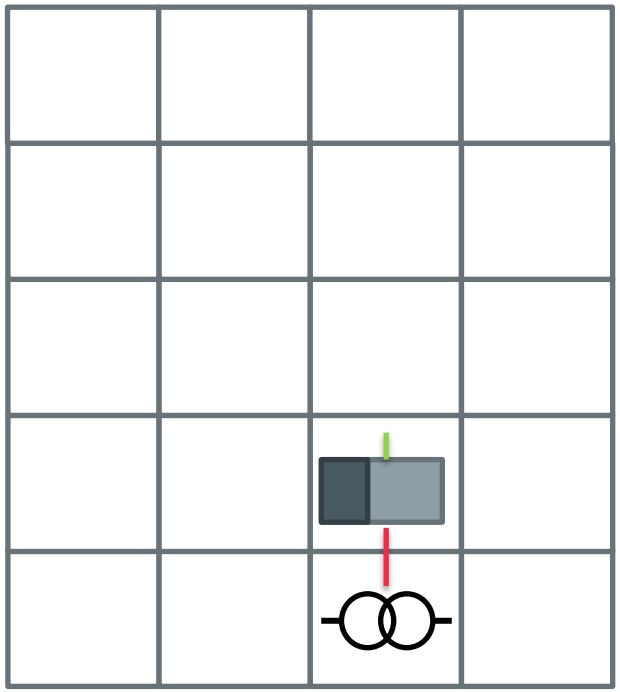
- Components
  - individual steps of an attacker in a multi-stage attack
- Protocols / Connections
  - propagation paths

SGAM:
Information and function layer



- Information elements
  - potential assets for our analysis
- Functions
  - influence on primary assets by function

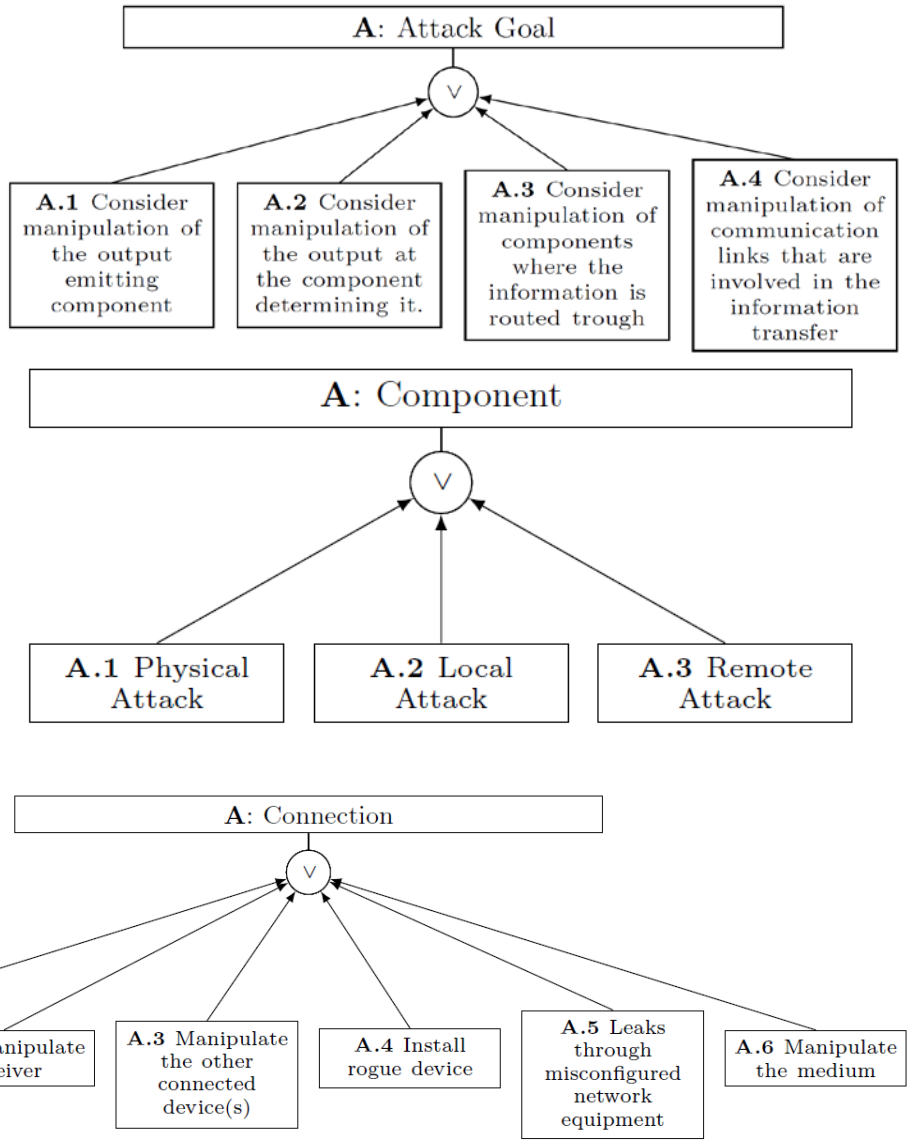
Threat analysis



- Start with primary asset
  - output to process
  - output to HMI
  - output to external system
- Identify attack goal:
  - violation of security objective (CIA) of a primary asset

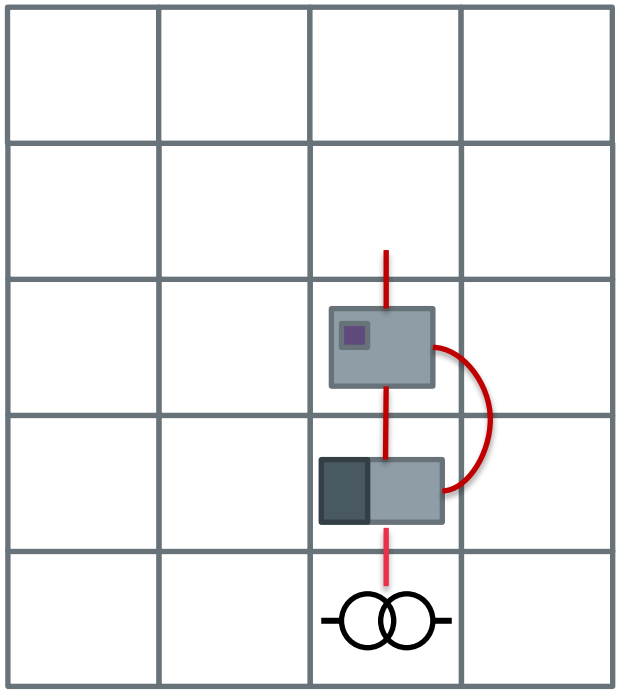
Patterns

- set of typical attack graph patterns that occur in networked CPS
  - root (attack goal)
  - component
  - connection
  - functional dependency
- can be extended when needed
- stop when a new component is reached



EU FP7 Programme Contract No. 608224

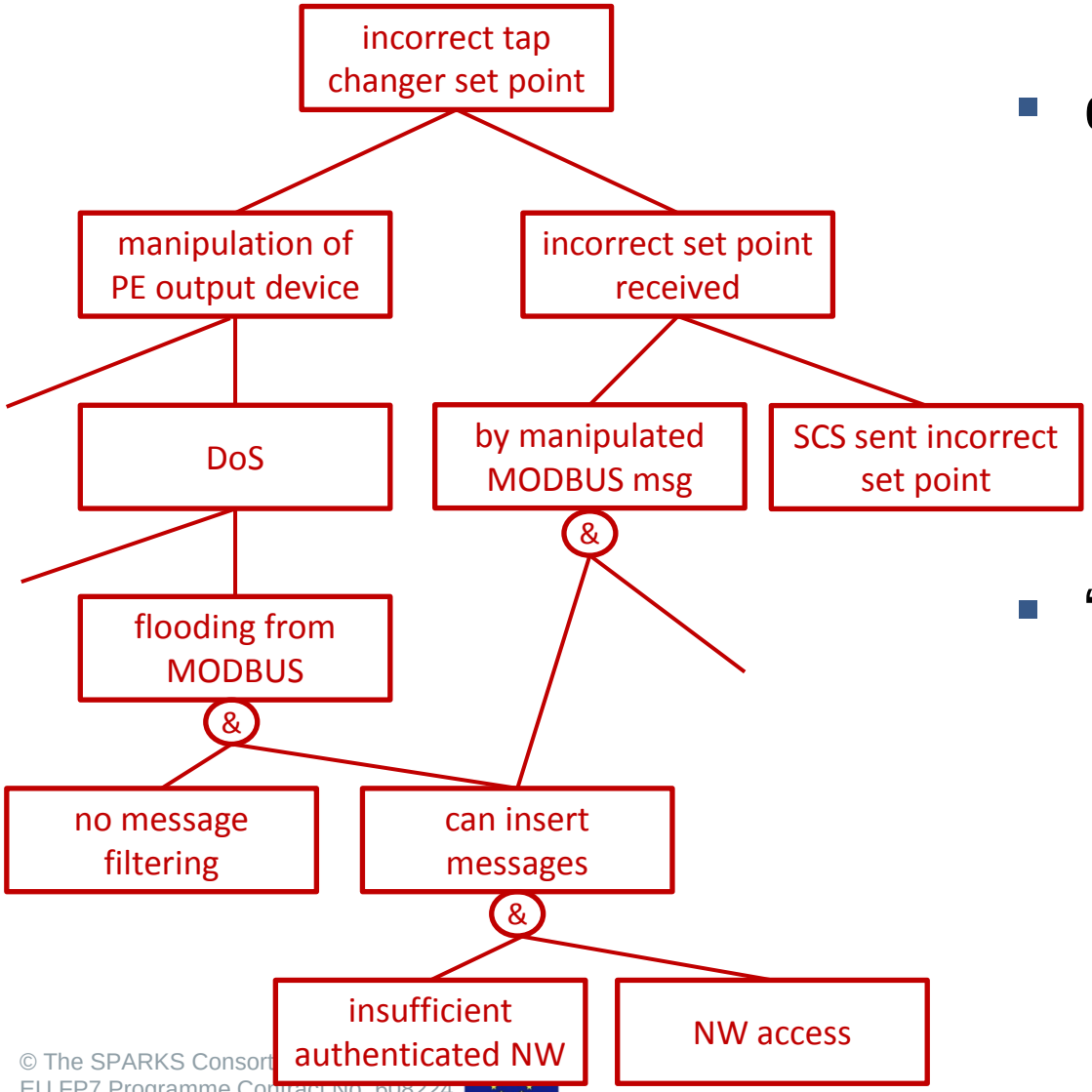
Continue with next component



- evaluated attack graph for each component
- can be combined by the “has access to” nodes
- results (theoretically) in a large overall threat graph
- evaluating the external interfaces
  - Internet
  - mobile networks
  - local (Wi-Fi)
  - physical

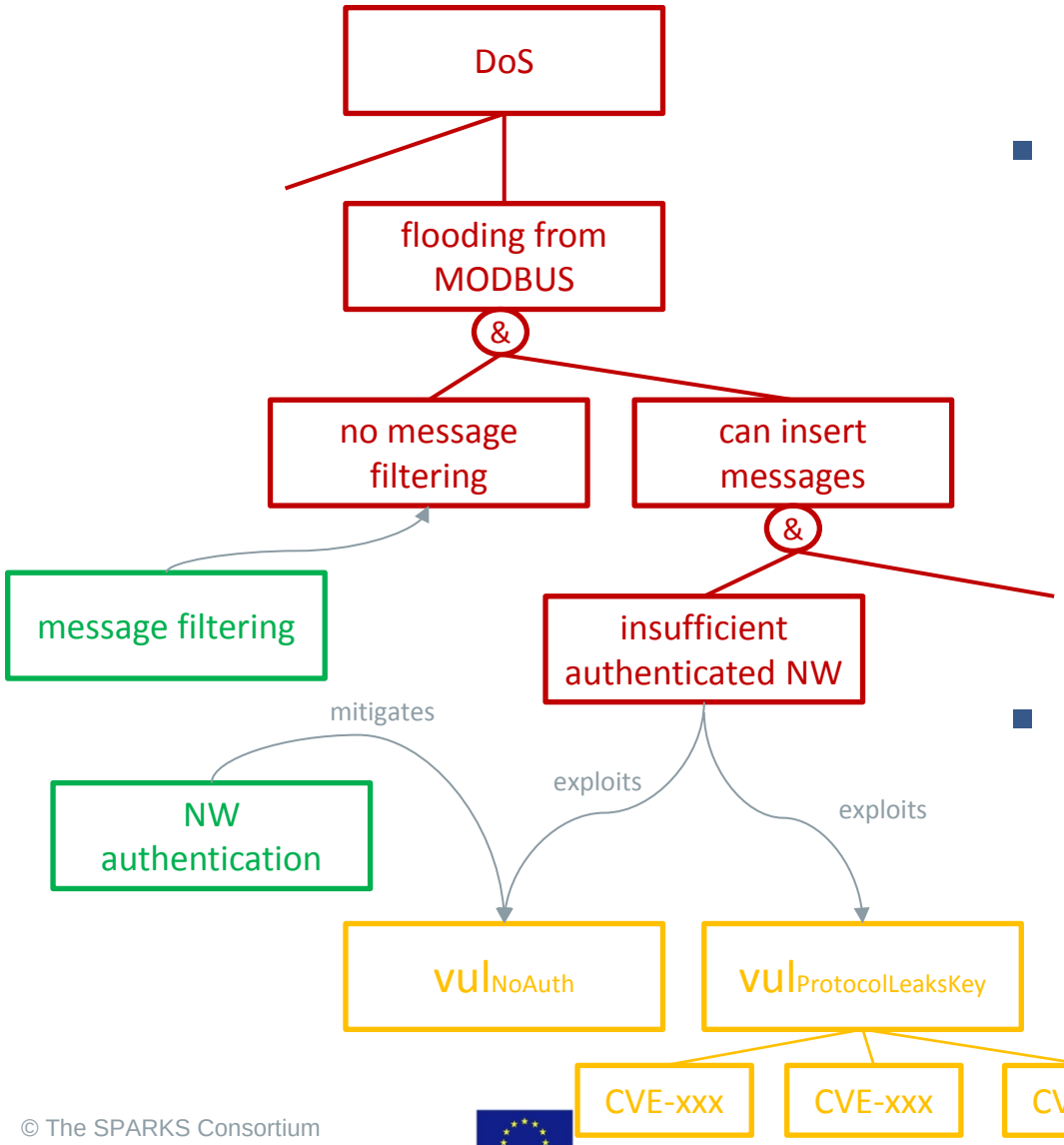
EU FP7 Programme Contract No. 608224

Attack graphs



- decomposing threats
  - by patterns as described before
  - library information (standard threat catalogues)
- "likelihood" evaluation
  - determine threat level for each source node
  - propagate to root
    - overall threat level
    - dominant attack trajectories

Adding semantic threat graphs



- construct STG around leaf nodes
  - threats
  - countermeasures
  - assets
  - vulnerabilities
- allows us to derive countermeasures by machine-based reasoning

EU FP7 Programme Contract No. 608224

Conclusion

- Threat analysis method for SPARKS
- Based on attack trees and STG
- Not another AT extension, but guidance for establishing good attack graphs
  - completeness
  - complexity
- Uses SGAM as input and uses patterns on this input
- Combination with semantic threat graphs
  - deeper understanding of the specific attack
  - machine-based reasoning (ontologies)
  - catalog-based derivation of countermeasures

EU FP7 Programme Contract No. 608224

Thank you for your attention!

Dr. Martin Hutle
Deputy Head of Department
Product Protection and Industrial Security

Fraunhofer AISEC
Parkring 4
85748 Garching bei München, Germany

Phone: +49 89 3229986-135
Fax: +49 89 3229986-222
E-Mail: martin.hutle@aisec.fraunhofer.de
Internet: www.aisec.fraunhofer.de

EU FP7 Programme Contract No. 608224