SweGRIDS

DPS2: **Integration effort prediction for asset management data collection**

PhD student: Sotirios Katsikeas, sotkat@kth.se

Main Supervisor: Pontus Johnson (KTH)

Project funded by:

Energimyndigheten

Hitachi Energy

SVENSKA KRAFTNÄT

Background & Motivation

- Assessing the cyber security of IT and ICS infrastructures is becoming increasingly important because:
  - We greatly depend on such infrastructures (e.g. Internet and Power Grids)
  - The complexity of such infrastructures is increasing
  - The number of IT security issues and cyber-attacks increases
- Opportunity
  - Many common properties exist among different IT and ICS systems

Objective of the project

SweGRIDS

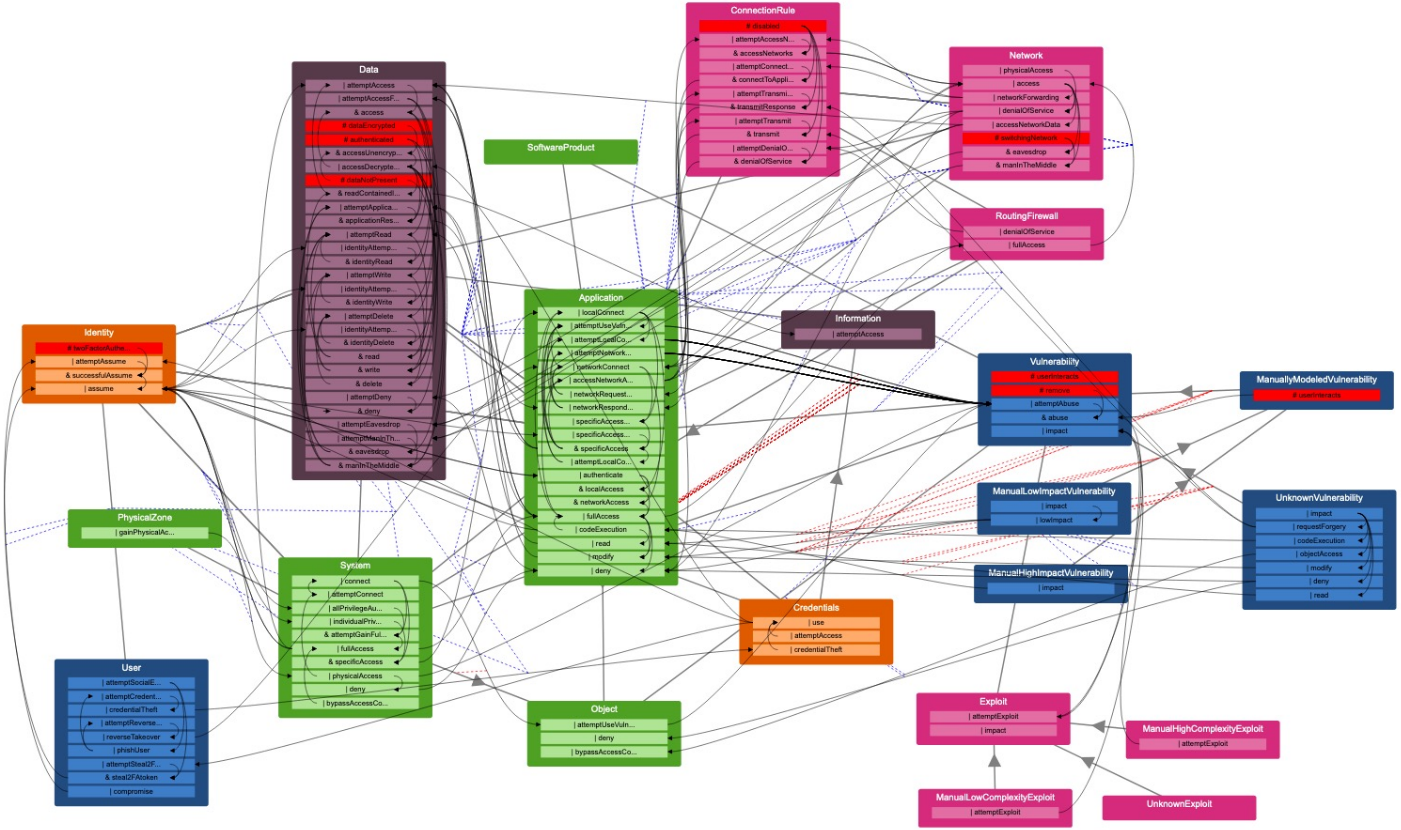
Create Domain Specific Languages (DSLs) for the IT and ICS domains (as well as for subparts of them)

- Using those languages, create models of the real infrastructures
- Simulate cyber attacks and analyse the results
- Facilitate integration efforts and security by design
    - Legitimate operations are also simulated
    - Vulnerabilities will be known at design/testing time

Approach: Using MAL

- MAL (the Meta Attack Language) (https://mal-lang.org)
  - Is a meta-language
    - Is a way to avoid creating new attack graphs for every case
    - Specifies the rules and elements for domain specific languages (DSL)
    - Those are: i) Assets, ii) Attack steps iii) Defenses, iv) Risks
  - Makes modeling of new domains easier & allows reusability of elements
  - Exploits attack graphs and probabilistic simulations

Approach: Using MAL (1/2)



ConnectionRule
# disabled
| attemptAccessN...
& accessNetworks
| attemptConnect...
& connectToAppli...
| attemptTransmi...
& transmitResponse
| attemptTransmit
& transmit
| attemptDenialO...
& denialOfService

Network
| physicalAccess
| access
| networkForwarding
| denialOfService
| accessNetworkData
switchingNetwork
& eavesdrop
& manInTheMiddle

RoutingFirewall
| denialOfService
| fullAccess

Data
| attemptAccess
| attemptAccessF...
& access
# dataEncrypted
# authenticated
& accessUnencryp...
| accessDecrypte...
dataNotPresent
& readContainedI...
| attemptApplica...
& applicationRes...
| attemptRead
| identityAttemp...
& identityRead
| attemptWrite
| identityAttemp...
& identityWrite
| attemptDelete
| identityAttemp...
& identityDelete
& read
& write
& delete
| attemptDeny
& deny
| attemptEavesdrop
| attemptManInTh...
& eavesdrop
& manInTheMiddle

SoftwareProduct

Application
| localConnect
| attemptUseVuln...
| attemptLocalCo...
| attemptNetwork...
| networkConnect
| accessNetworkA...
| networkRequest...
| networkRespond...
| specificAccess...
| specificAccess...
& specificAccess
| attemptLocalCo...
| authenticate
& localAccess
& networkAccess
| fullAccess
| codeExecution
| read
| modify
| deny

Information
| attemptAccess

Identity
# twoFactorAuthe...
| attemptAssume
& successfulAssume
| assume

Vulnerability
# userInteracts
# remove
| attemptAbuse
& abuse
| impact

ManuallyModeledVulnerability
# userInteracts

ManualLowImpactVulnerability
| impact
| lowImpact

UnknownVulnerability
| impact
| requestForgery
| codeExecution
| objectAccess
| modify
| deny
| read

ManualHighImpactVulnerability
| impact

PhysicalZone
| gainPhysicalAc...

System
| connect
| attemptConnect
| allPrivilegeAu...
| individualPriv...
& attemptGainFul...
| fullAccess
& specificAccess
| physicalAccess
| deny
| bypassAccessCo...

Credentials
| use
| attemptAccess
| credentialTheft

User
| attemptSocialE...
| attemptCredent...
| credentialTheft
| attemptReverse...
| reverseTakeover
| phishUser
| attemptSteal2F...
& steal2FAtoken
| compromise

Object
| attemptUseVuln...
| deny
| bypassAccessCo...

Exploit
| attemptExploit
| impact

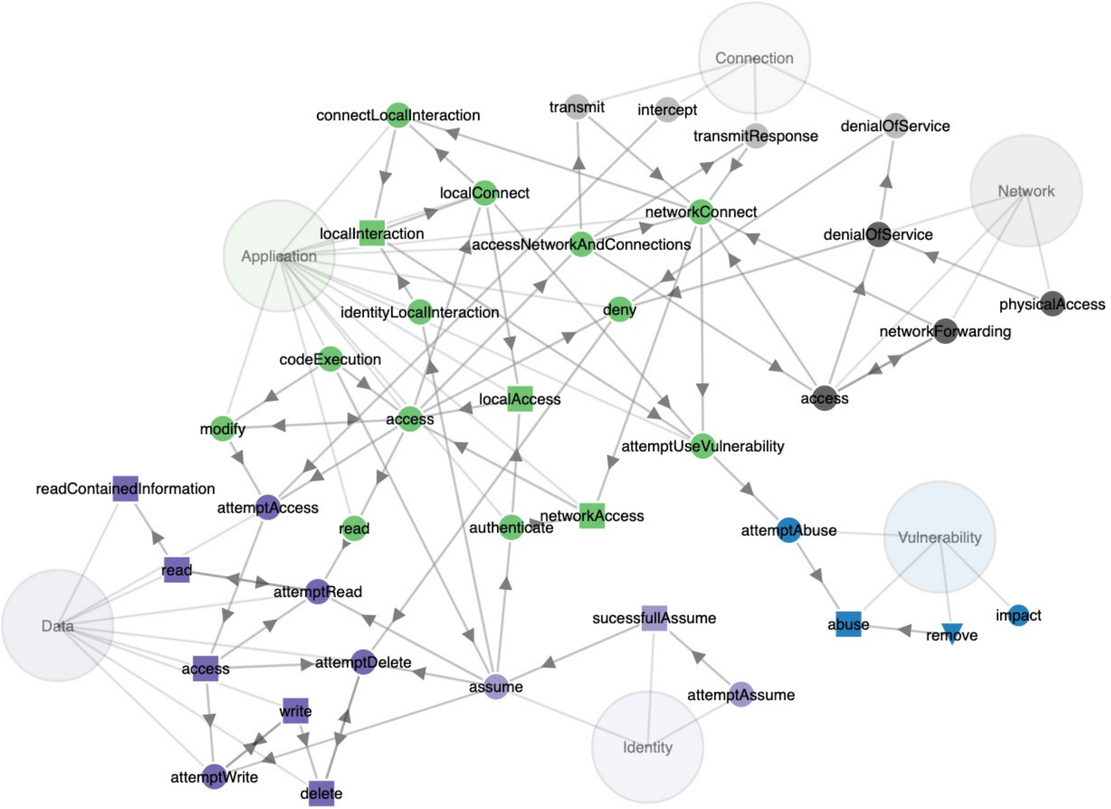
ManualHighComplexityExploit
| attemptExploit

ManualLowComplexityExploit
| attemptExploit

UnknownExploit

SweGRIDS

Approach: Using MAL (2/2)



Results: Work so far

- **Research Communities in Cybersecurity**: A Comprehensive Literature Review
- **archiLang**: A prototype for transforming ArchiMate models to MAL instances
- **coreLang**: A MAL-based DSL for the generic IT domain is already developed
  - Publicly available on GitHub at: https://github.com/mal-lang/coreLang
- **icsLang**: A MAL-based DSL for the ICS domain is under active development
  - Also available on GitHub at: https://github.com/mal-lang/icsLang

Future work:

- Evaluation methodology for MAL-based DSLs and application on coreLang
- "Dynamic MAL": Use of Dynamic Programing on MAL models to optimize the attacker's value from attacking a system
- A MAL-based DSL for smart buildings and cities (Thesis project under supervision)

Thank you for your time!

SweGRIDS

Do you want to find out more about my work?

Drop by my poster!

Visit: https://www.kth.se/profile/sotkat

Or contact me at sotkat@kth.se!