CENTRE FOR CYBER DEFENCE AND INFORMATION SECURITY

Six Years of CDIS Research

Mads Dam

Research coordinator, CDIS

mfd@kth.se

CDIS Research Projects 2020-2026

Some base stat's

~20 projects, 5 completed

Roughly half directly CDIS funded

Other half by affiliated agencies (MSB/MCF, FOI, FHS, KTH)

Large majority single PhD projects

80+ publications of which:

- ~25 in top conference/journals
- 1 best paper award (PQCrypto)

Topics:

- Cyber command and control
- Socio-tech-legal aspects
- Systems and security modelling
- Design and analysis techniques
- System security
- Crypto
- Other

Highlight 1: Post quantum cryptography

Problem:

Quantum computers that break a lot of classical cryptography may soon be available

Lattice-based cryptography recently standardized as quantum safe alternative

Post-quantum cryptography not as efficient nor as well understood as traditional cryptography

Contributions:

- Analysis of security proofs for lattice-based cryptography
- New constructions for lattice-based cryptography
- Variants of quantum attacks against traditional cryptography

Highlight 1: Post quantum cryptography

Publications:

Five main published papers, three related to lattice-based cryptography, two related to quantum algorithms

Further papers as result of collaboration within CDIS developing side channel attacks

Highlights:

Adaptation of standardized lattice-based signature scheme with a new technique

Much more compact than previous comparable schemes

Received best-paper award and best young researcher award at one of the biggest cryptography conferences

J. Gärtner: Compact Lattice Signatures via Iterative Rejection Sampling, in Proc. Crypto'25 (A*, best paper award)

Highlight 2: Attack simulations for defense

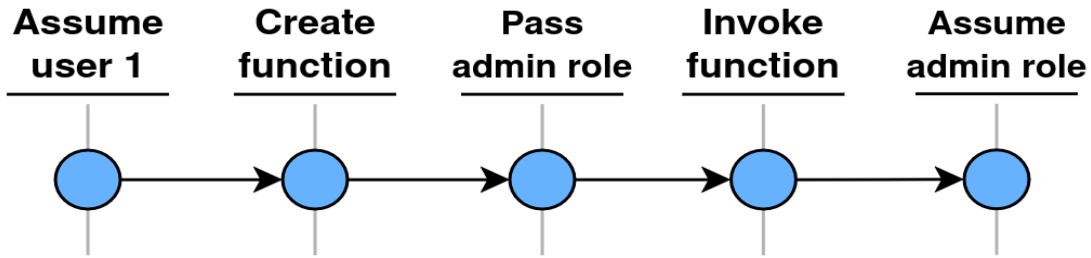
Objective:

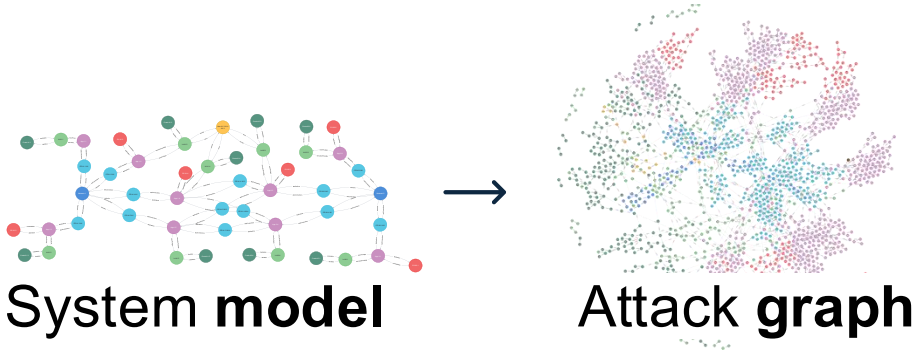
Model and simulate cyberattacks in realistic dynamic environments

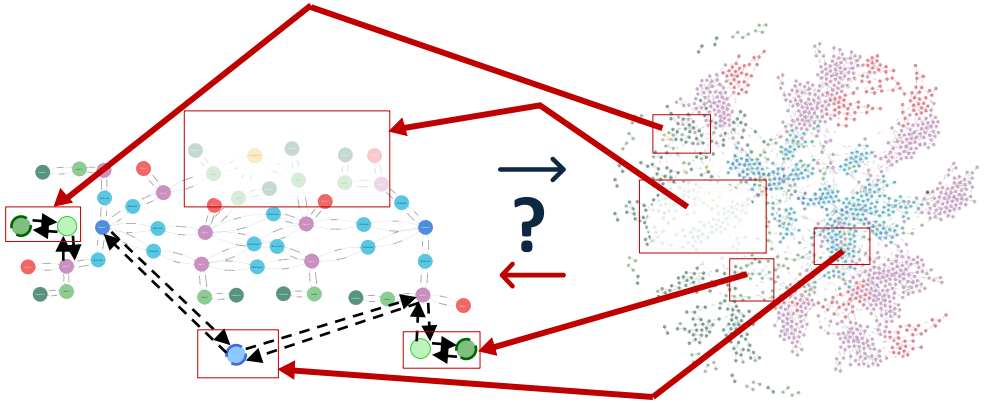
- Adversaries can add, remove, and re-configure resources

Derive attack graphs from system models

- Traverse the graph to simulate attacks
- Functions as automated penetration testing or automated security assessments





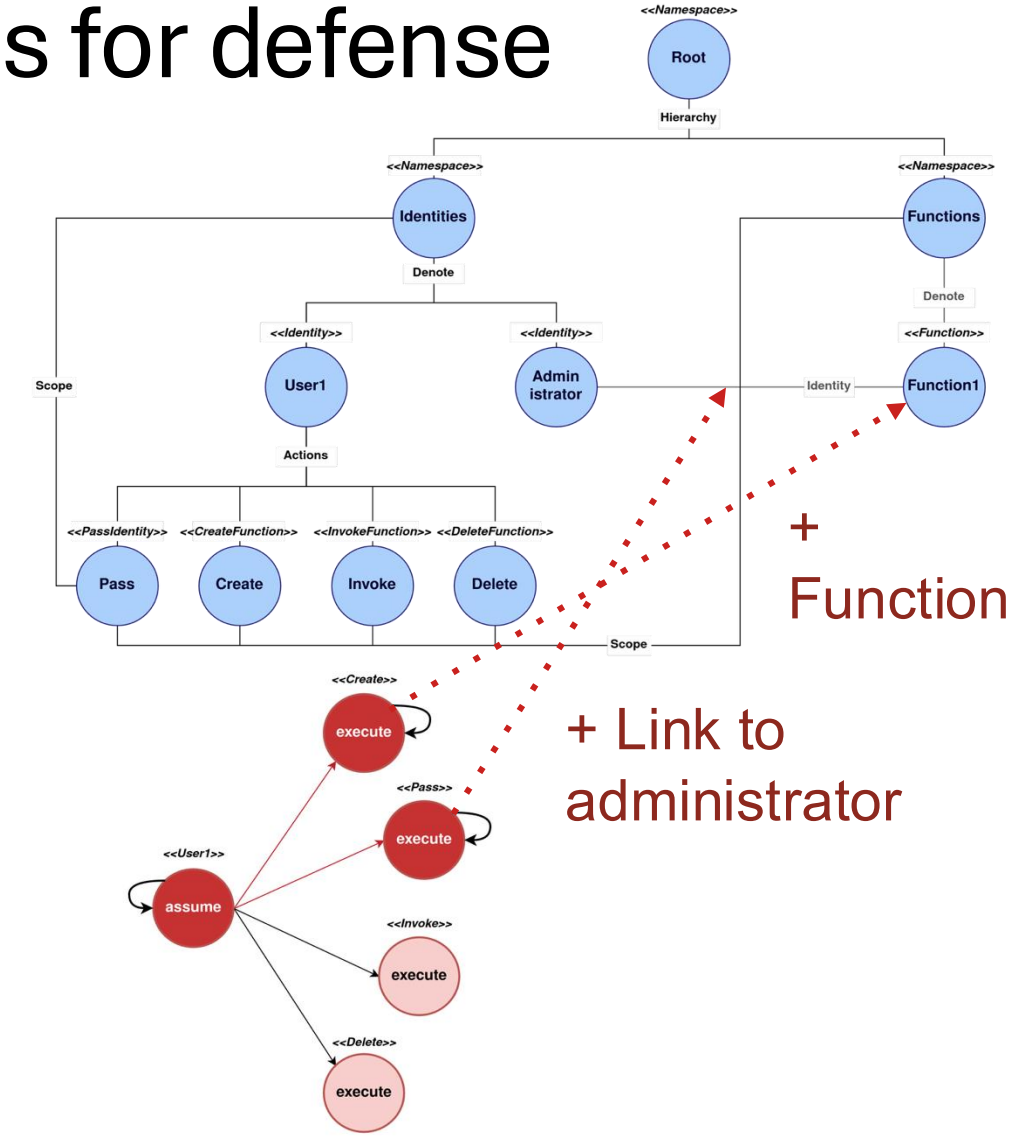


Highlight 2: Attack simulations for defense

Contributions:

Dynamic Meta Attack Language (DynaMAL)

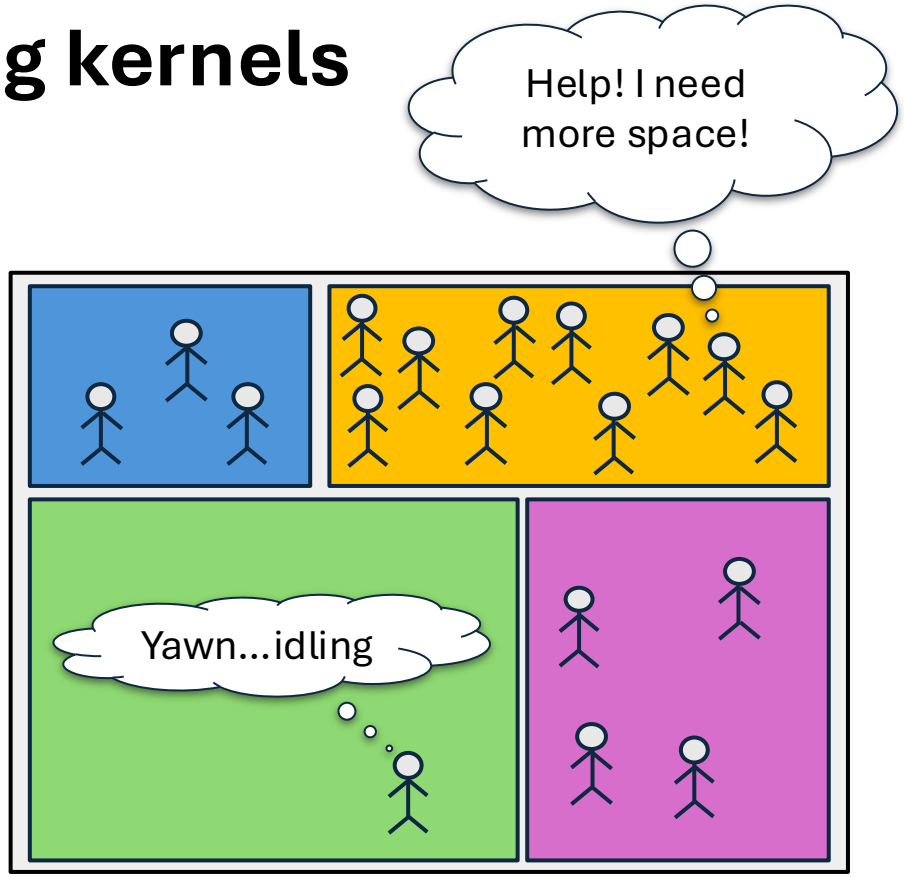
- Attack graph can add/remove system objects
- Implements lazy graph generation
- Solved some off-the-shelf hacking challenges automatically



V. Engström: Modeling and Simulating Cyberattacks with Dynamic Graphs (thesis)

Highlight 3: S3K – A dynamic partitioning kernel

Traditional partitioning kernels



Protection through Isolation

- Security facility, processes are isolated into separate "rooms" to contain faults
- *Required in avionics*.

Problem: Rigid, Fixed Partitions

- Statically sized for worst-case scenarios
- Significant resource waste

Objective

- Dynamic resource transfer
- While preserving safety and security guarantees !!

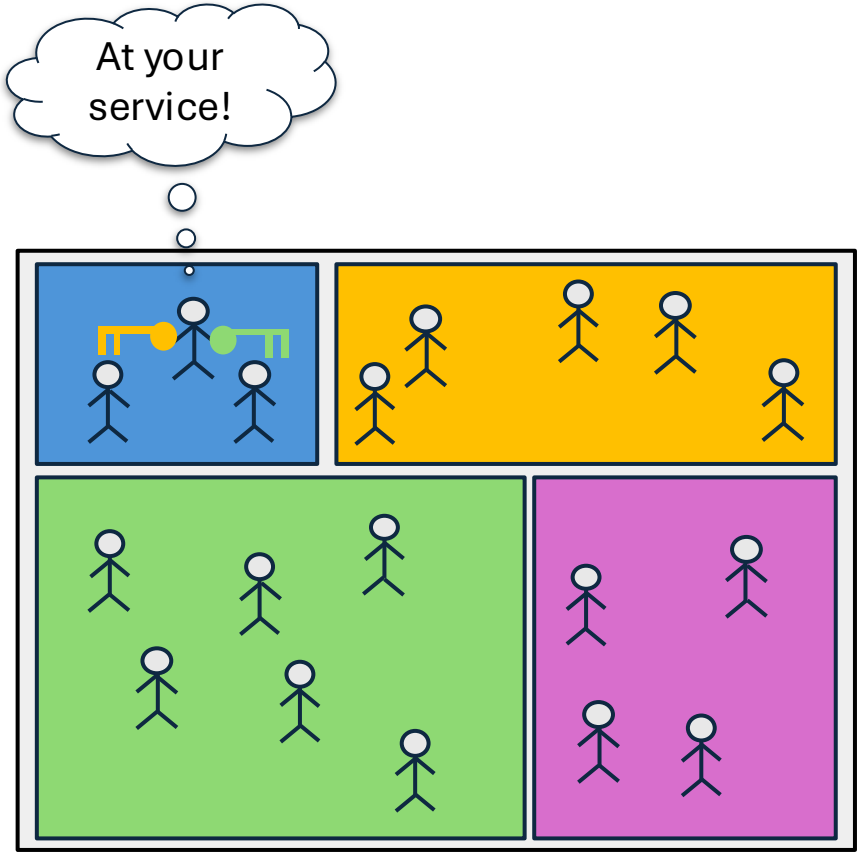
Highlight 3: S3K – A dynamic partitioning kernel

Hard real-time capability system

- Partitions created and managed recursively
- No information leakage – all kernel op's are time bounded
- Capabilities manage time and space
- Ability to manage/monitor determined by capabilities

Defensibility use case

- Maximize defender's lateral movement/observability
- Minimize that of the adversary

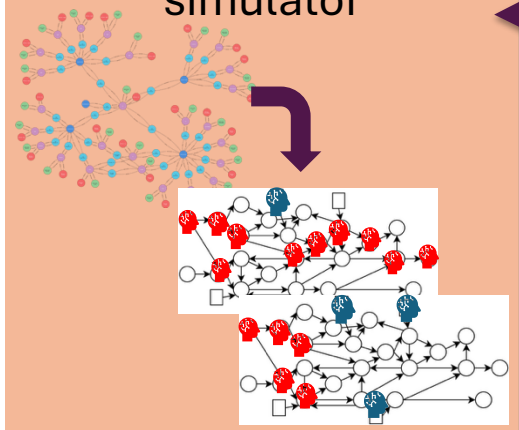


H. Karlsson and R. Guanciale, "Partitioning Kernel With Capability Controlled Temporal and Spatial Partitioning," in *2025 IEEE Real-Time Systems Symposium (RTSS)*, IEEE, 2025 (A*)

Highlight 4: Project Tyr

Semi-autonomous command and control system

Digital twin – attack/defense simulator



- ICT infrastructure models
- Possible attack paths (attack graphs)
- Emulated attack behavior

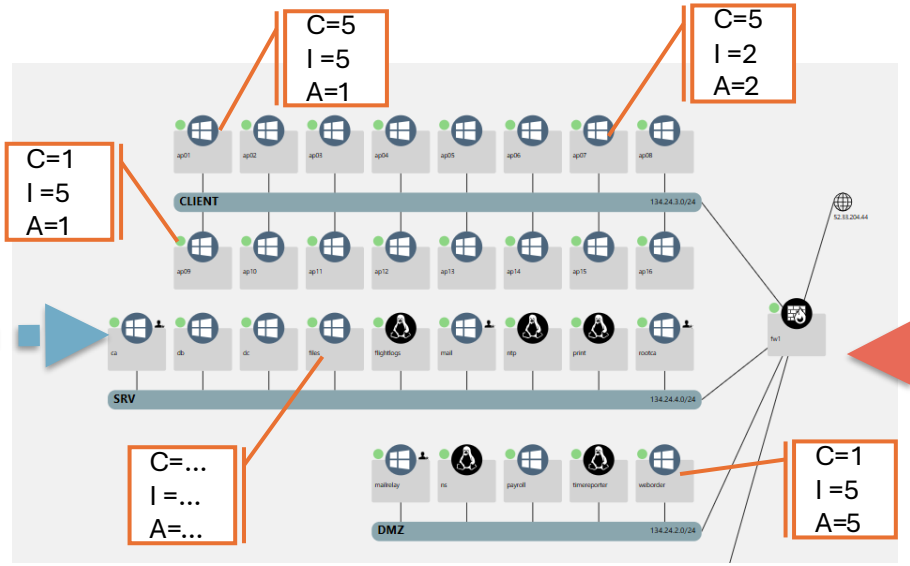
Training

KTH AI defender (SENTIENCE project)

Suggest actions

Execute actions

SOC operators



Scenario hosted in FOI's CRATE:
ICT infrastructure (3 nets, 30 hosts).
CIA business value of hosts.
Attack starting points.

LORE – FOI's attacker agent

Goal:

Prevent / minimize value loss from LORE reaching hosts.

Highlight 4: Project Tyr

The Project

Collaborative project with CDIS and FOI

Funding FMV

Showcase of CDIS project results

- Sentience and DynaMAL

Results

- Simplified scenario
- Defender is able to defend
- Experiments still ongoing

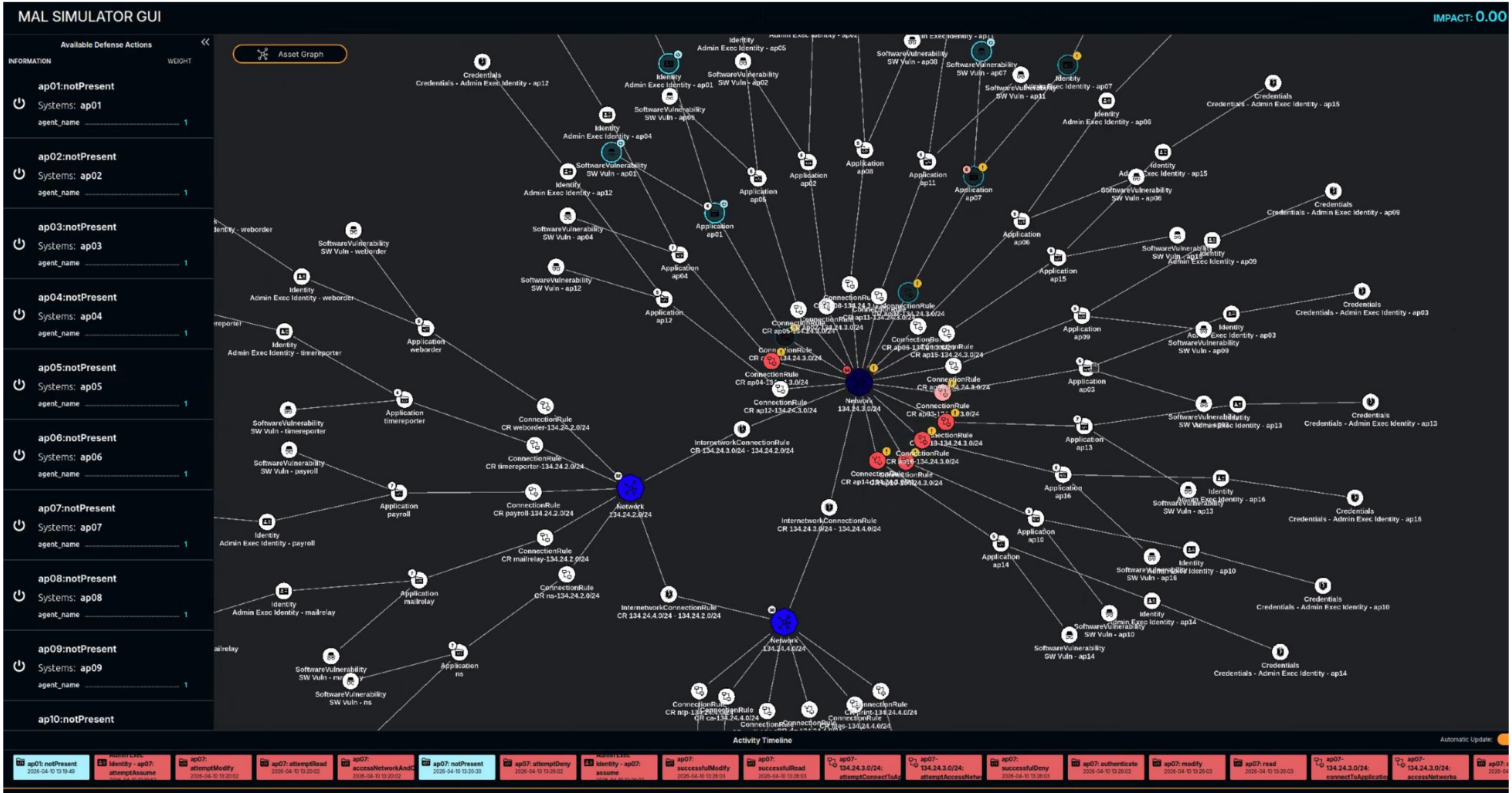
Impact

Majority of work spent on building and connecting reusable infrastructure components

KTH: Threat modelling for attack simulation infrastructure

FOI: LORE profiles, LORE action logs, more vulnerable CRATE configs, log collection configs for CRATE, user and admin emulation, ..

🎮 Come play the Tyr game at the poster exhibition



Challenges and Opportunities – AI AI AI AI …

Destined to deeply affect all aspects of the cyber domain

- Research/practice
- Technology/ways of working
- Defense/offense

through

- speed, time to react
- capabilities, breadth, depth, skill level, trustworthiness

Challenges and opportunities

Already ongoing: Automated…

- coding
- vulnerability detection
- repair
- anomaly detection
- incident response

!

Challenges:

- Zero response time => automation
- Controllable AI
- XAI => PAI (“provable” AI)

?

Challenges and Opportunities – CDIS Impact

Trust, collaboration, active communication

- Researchers – defense - industry
- Broaden involvement
- Keys to success
- Long term project

Scope

- Do we cover the right topics?
- Offensive techniques?

Project formats

- Mainly single PhD projects
- Demonstrators/prototypes
- Multidisciplinarity
- “Flagship” projects?

Recruitment

- PhD level, how to improve
- Master projects
- Internships, postdocs