Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

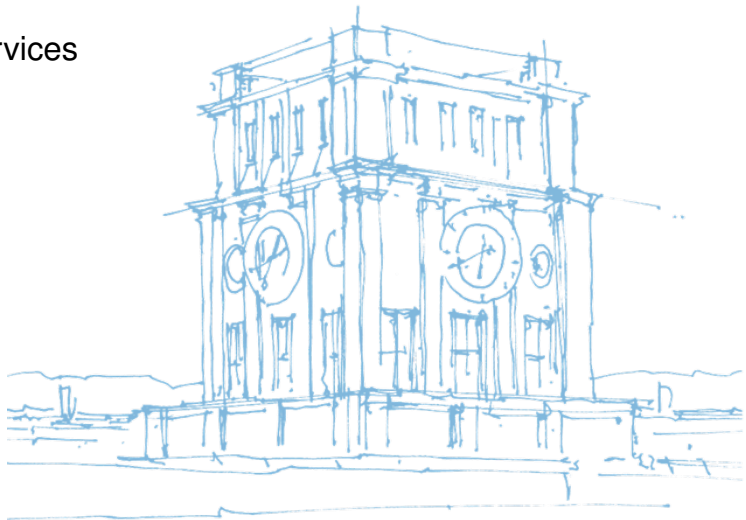
Exposing Insecure Configurations of Network Session and Permission Graphs

Final talk for the Master's Thesis by

Thomas Maier
advised by Simon Bauer, Dr. Holger Kinkelin
and Thomas Penteker (Siemens AG)

Monday 17th June, 2019

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich



Introduction

Problem:
Lateral Movement in Windows networks

Goal:
Prevention of Identity Snowball Attacks

Contribution:
Solution based on graph-theoretic metrics

Agenda

Problem and Motivation

Problem Analysis

Exposing Insecure Configurations

Design and Implementation

Evaluation

Related Work

Problem and Motivation

Identity Snowball Attack

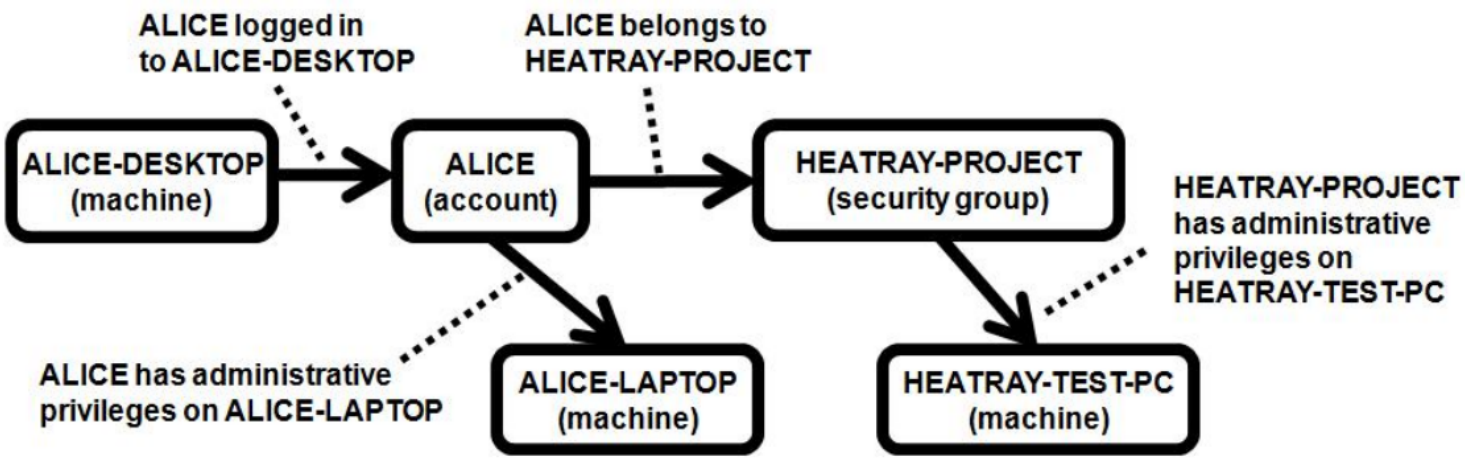


Figure 1: Identity Snowball Attack [1]

How to find Undesired Configurations
in Network Session and Permission Graphs?

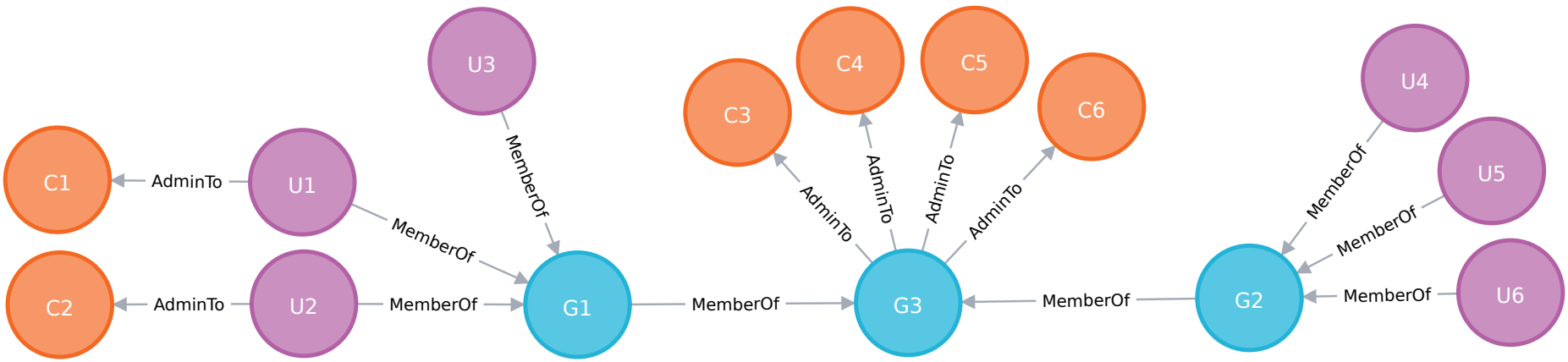


Figure 2: Minimalist sample graph

Problem Analysis

Scope of the Thesis

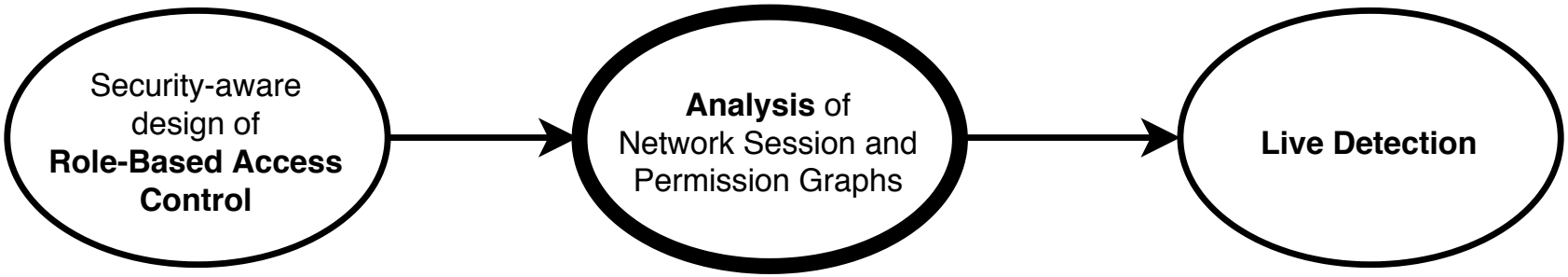


Figure 3: Possible points in time

$\Rightarrow$ Analysis before the actual attack

Problem Analysis

Problem Statement

Analysis of Network Session and Permission Graphs

$\Rightarrow$ We want to ...

- ... **define undesired graph configurations**, deduced from real-world issues.
- ... **detect undesired configurations** within the graph.
- ... be able to **scale** the solution even **for large graphs**.
- ... apply the solutions for network session and permission graphs, not only Active Directory.

Exposing Insecure Configurations

Users, **G**roups, **C**omputers

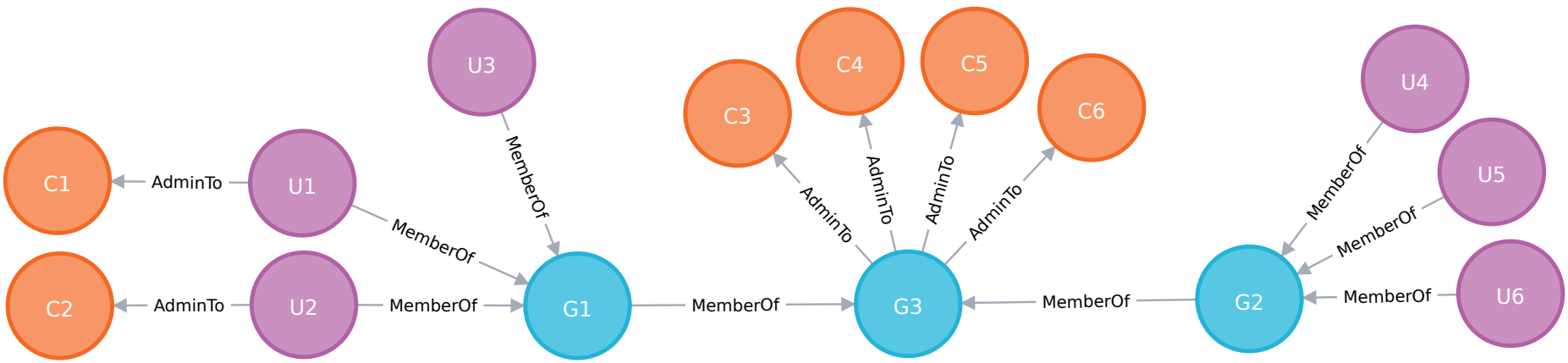


Figure 4: Minimalist sample graph

Exposing Insecure Configurations

Degree Centrality

"Direct neighbors of the attacker"

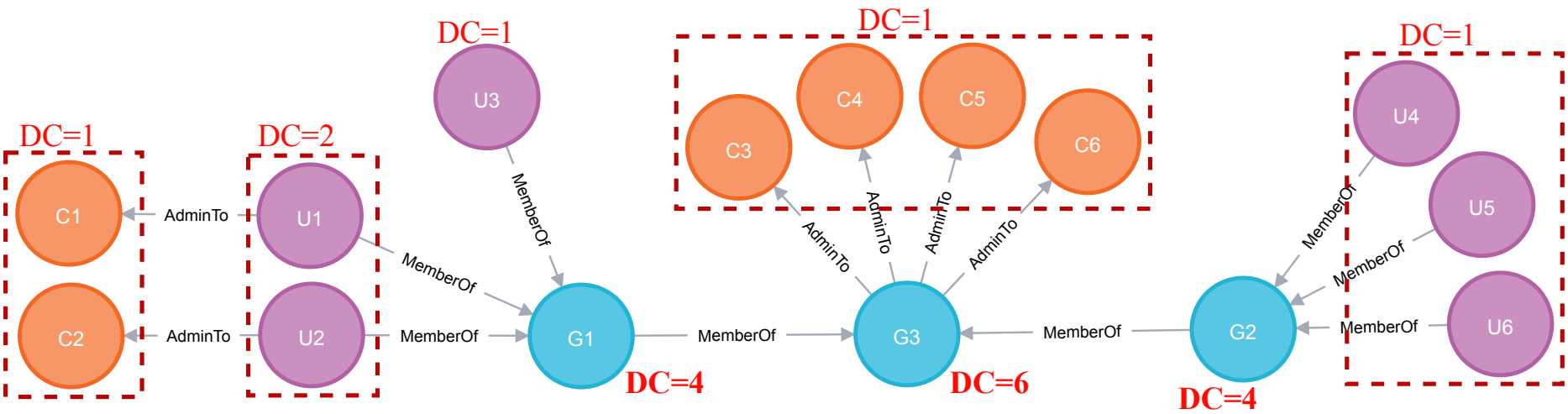


Figure 5: Sample graph with Degree Centrality (DC)

Exposing Insecure Configurations

Betweenness Centrality

"Nodes on the attacker's path"

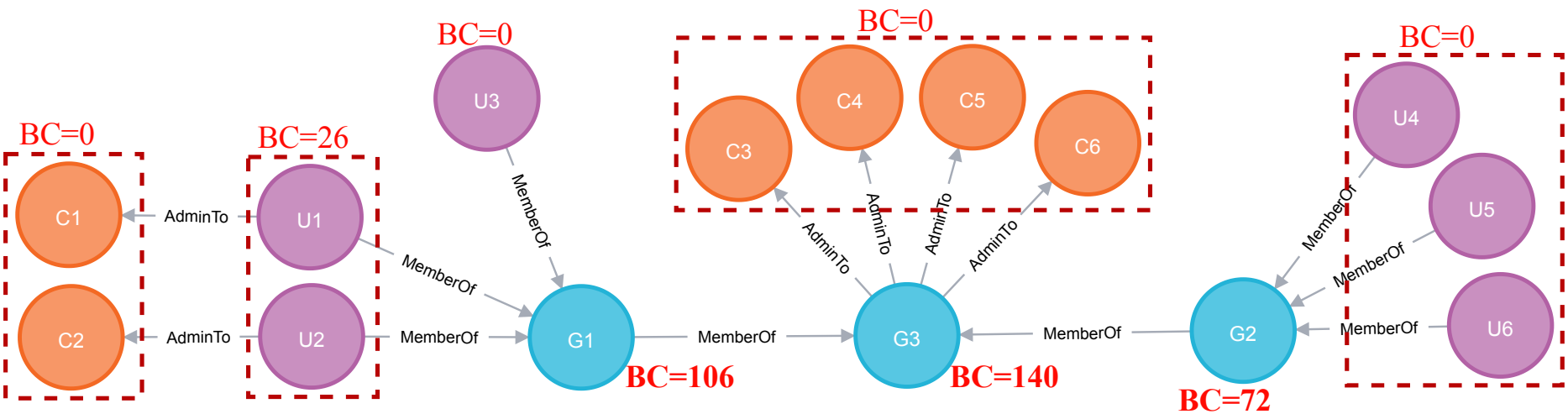


Figure 6: Sample graph with Betweenness Centrality (BC)

Exposing Insecure Configurations

Closeness Centrality

"Closeness to the attacker"

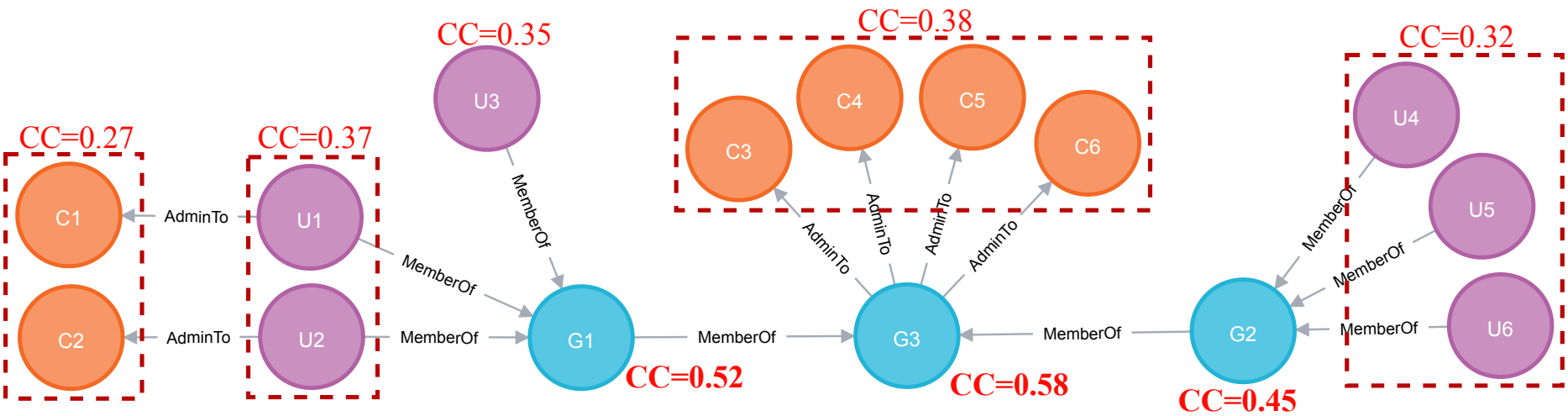


Figure 7: Sample graph with Close Centrality (CC)

Design and Implementation

Investigation Process

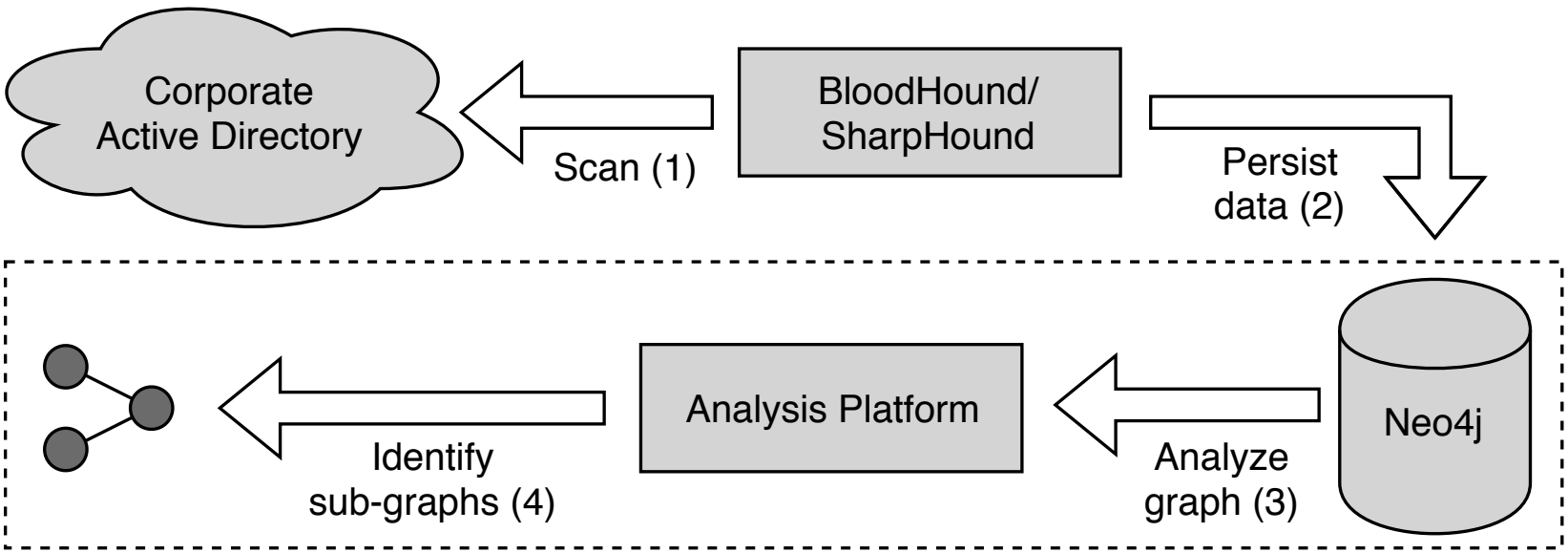


Figure 8: Technical perspective of the investigation process

Design and Implementation

Environments

- Simulated environment
  1. Randomly generate graphs
  2. Inject undesired configurations
  3. Find undesired configurations

- Real-world environment
  1. Collect network session and permission graph
  2. Find undesired configurations
  3. Discussion about meaningfulness of findings

Design and Implementation

Architecture Overview

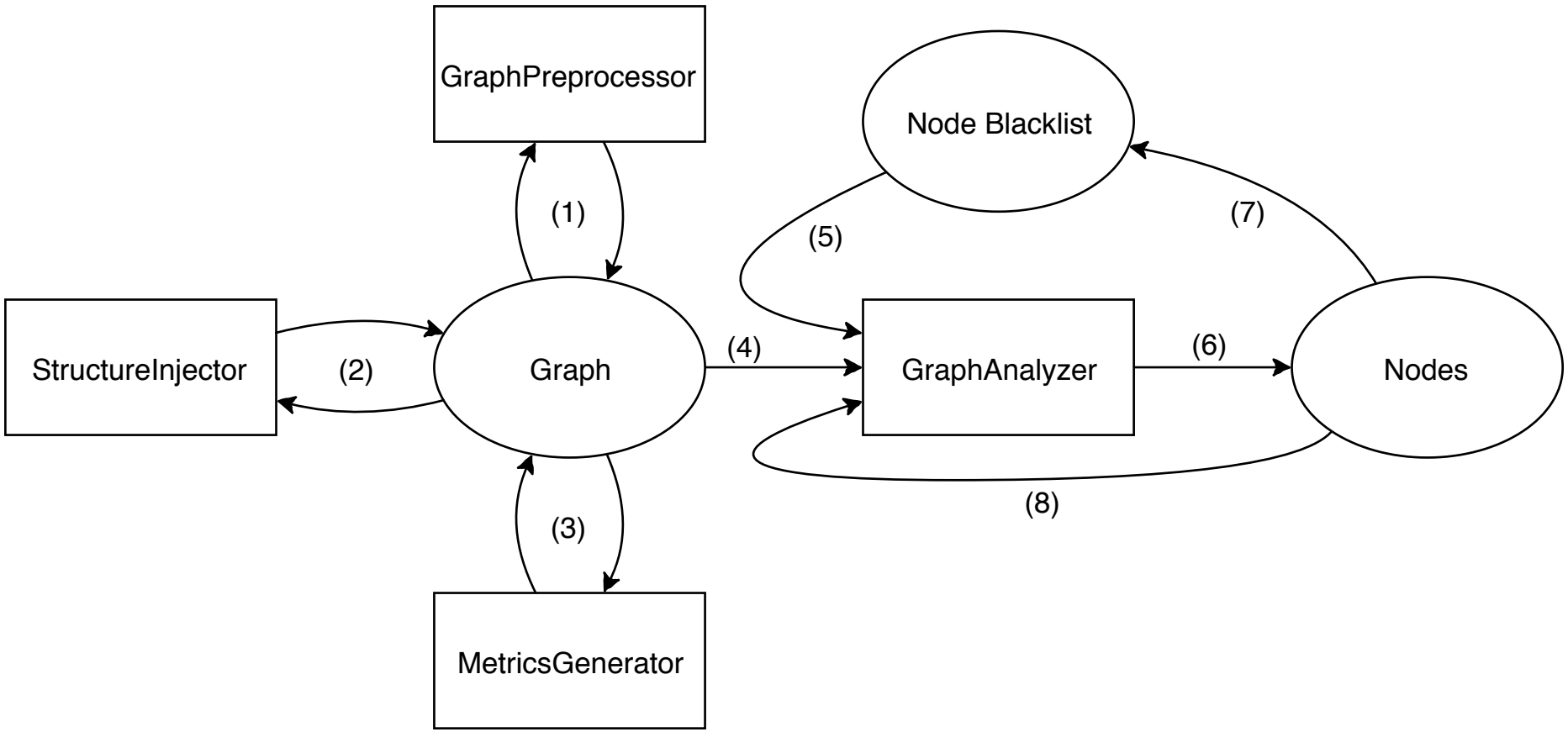


Figure 9: Analysis platform

Evaluation

Injection of Undesired Configuration

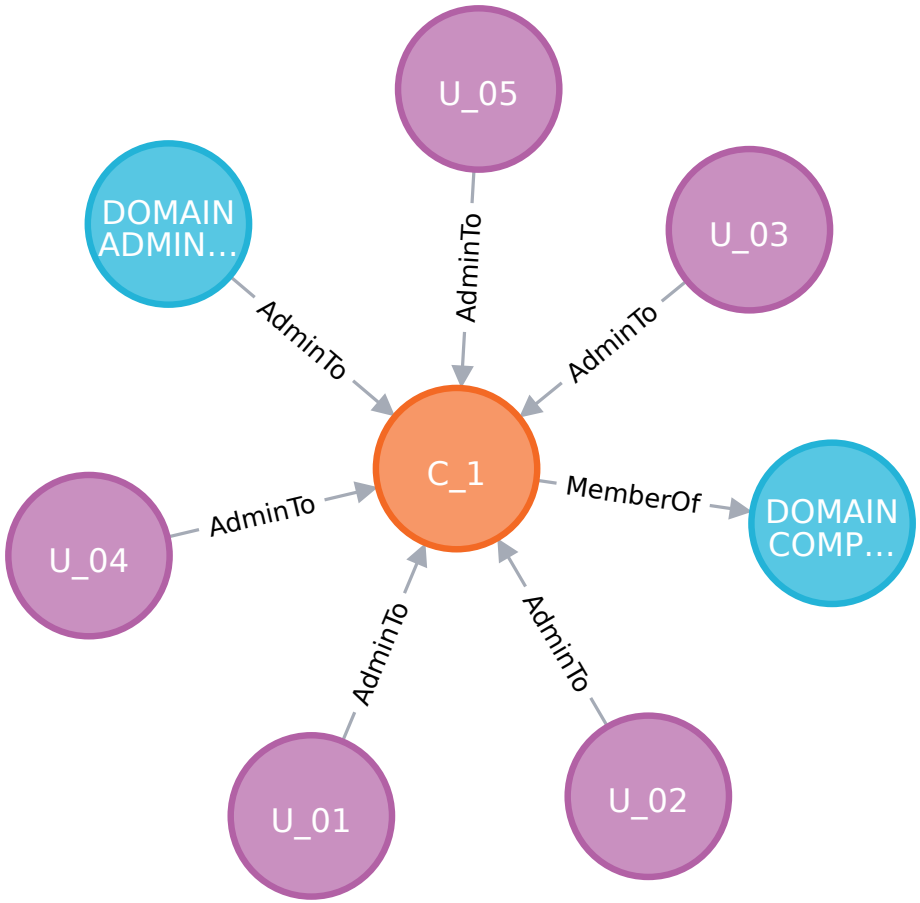


Figure 10: Undesired configuration: One computer with five admin users

Evaluation

Node with Betweenness Centrality *BC* = 7660

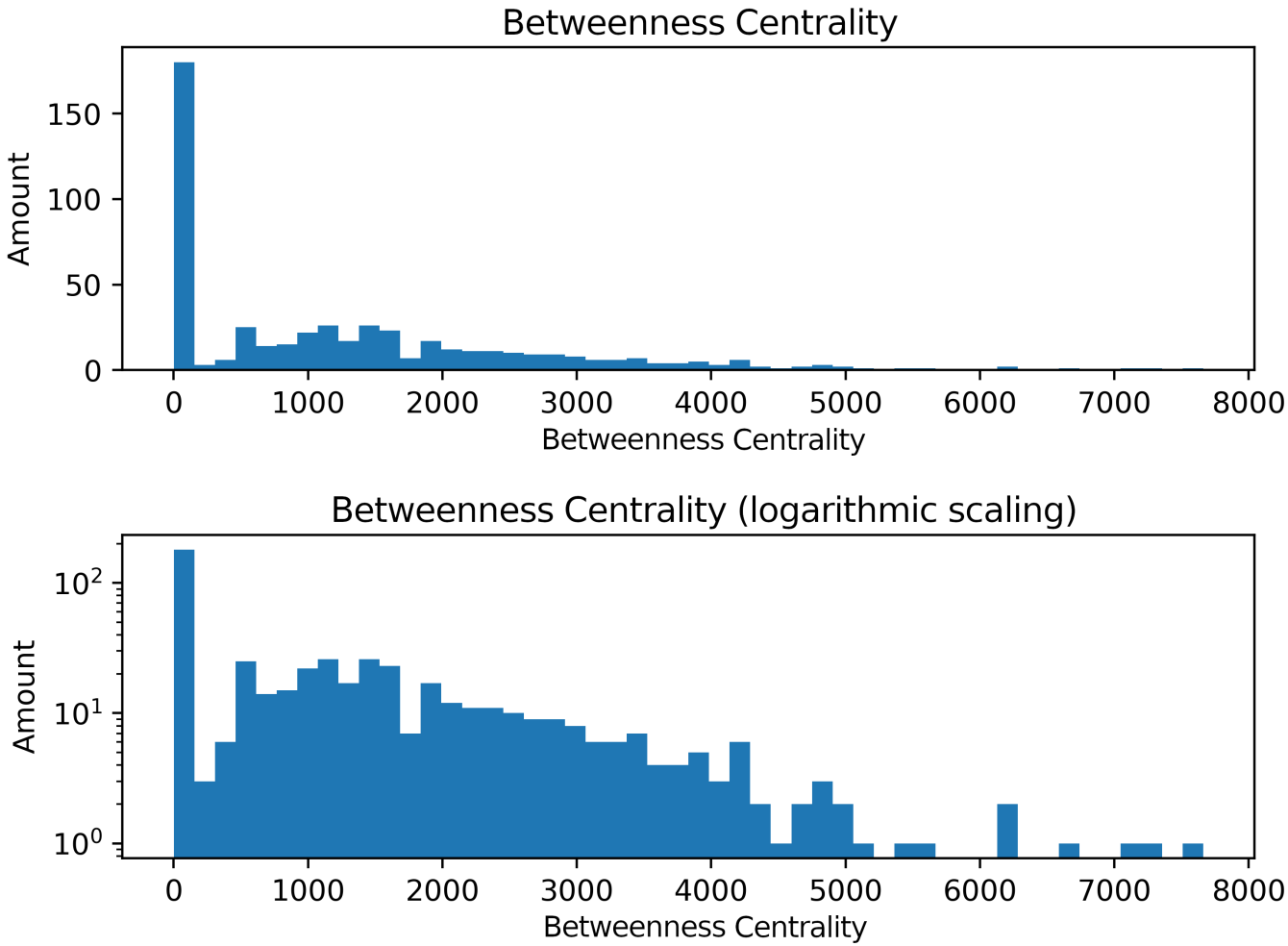


Figure 11: Betweenness Centrality of a graph (injected one computer with ten admin users)

Evaluation

Real Environment

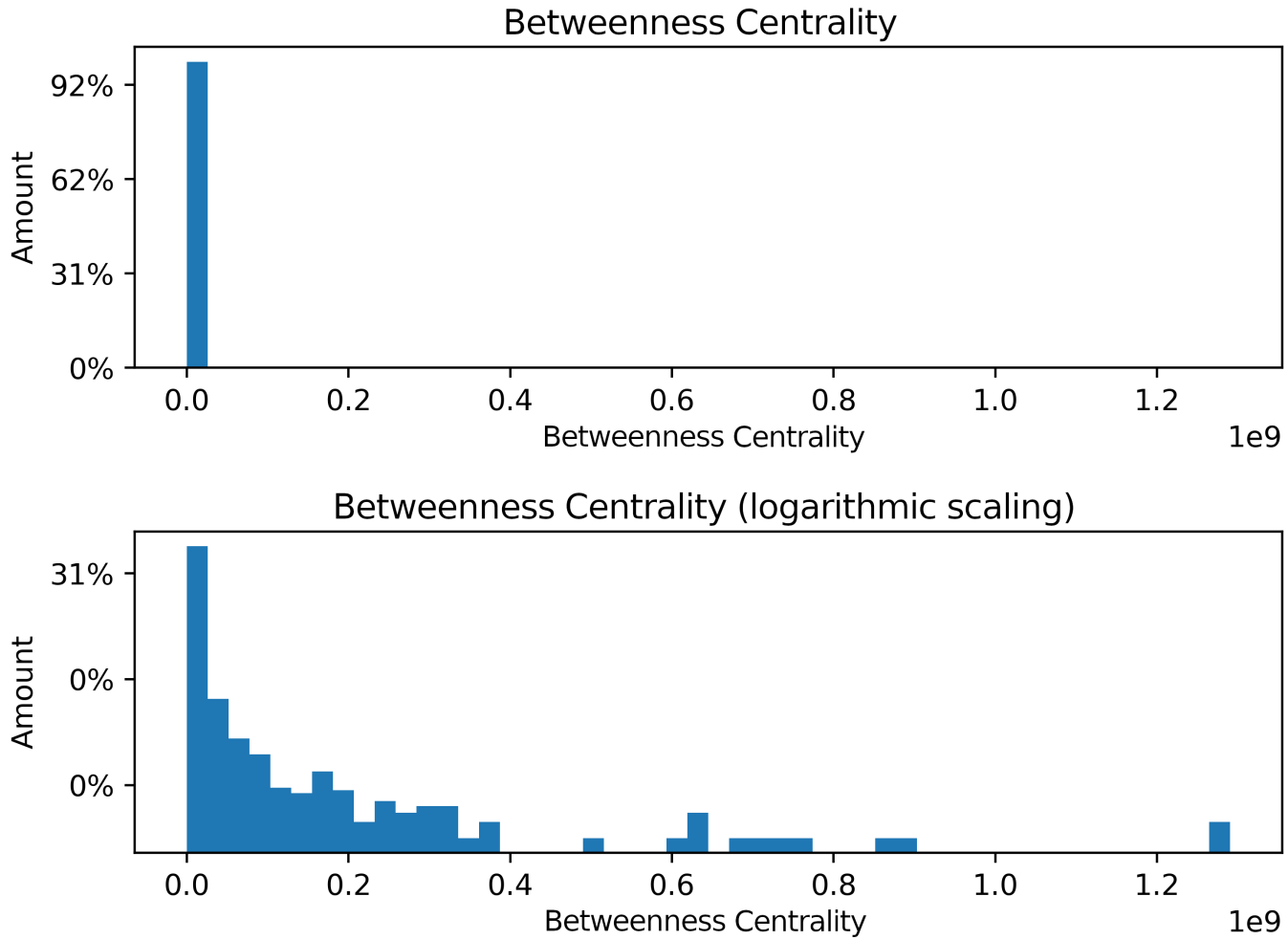


Figure 12: Betweenness Centrality of a real AD network

Evaluation

Results

- Found common AD groups
  e.g. `DOMAIN USERS`, `DOMAIN ADMINS`
  $\Rightarrow$ Intentionally blacklisted
- Found undesired sub-structures (intentionally injected)
  e.g. users with many administrative permissions
- Found odd configurations
  e.g. users in many groups
- PageRank may be a comprehensive metric

Related Work

Comparison to Other Approaches

- **Automated Analysis**: Heat-ray by Microsoft [1]
  $\Rightarrow$ Limited usage of graph metrics (only one variation of Betweenness Centrality)

- **Manual Analysis**: BloodHound AD [3]
  $\Rightarrow$ Manual investigation per path, user, group or machine is necessary

Summary

- **Problems** with existing solutions to prevent Identity Snowball Attacks
- **Analysis** of Network Session and Permission Graphs
- **Novel centralized approach** for detection with centrality metrics
- **Evaluation** in a real-world and a simulated environment

Bibliography

[1] John Dunagan, Alice X. Zheng, and Daniel R. Simon.
Heat-ray: Combating identity snowball attacks using machine learning, combinatorial optimization and attack graphs.
In *Proceedings of the ACM SIGOPS 22Nd Symposium on Operating Systems Principles*, SOSP '09, pages 305–320. ACM.

[2] Didier Stevens.
Windows Credential Guard & Mimikatz.
https://blog.nviso.be/2018/01/09/windows-credential-guard-mimikatz/.

[3] Andrew Robbins, Rohan Vazarkar, and Will Schroeder.
BloodHound: Six Degrees of Domain Admin.
https://github.com/BloodHoundAD/BloodHound.

Additional Ideas (Backup Slide)

Page Rank

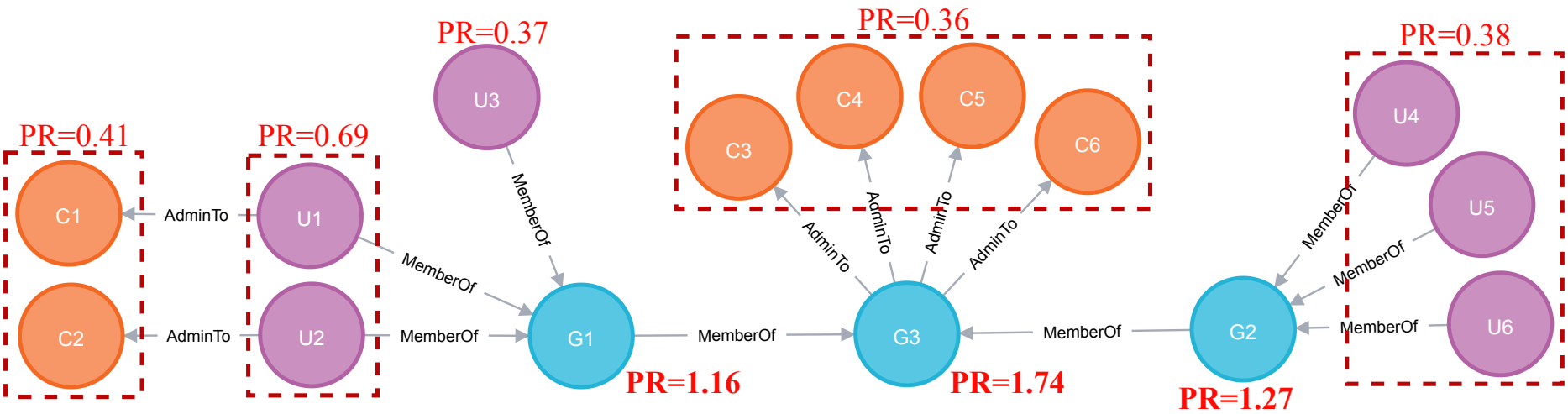


Figure 13: Example graph with Page Rank (PR)