Modelling and analysing network security policies in a given vulnerability setting

Roland Rieke

Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstrasse 75, D-64295 Darmstadt, Germany
E-Mail: rieke@sit.fraunhofer.de
http://private.sit.fraunhofer.de/~rol

CRITIS'06

Challenge: Protect Critical Information Infrastructures

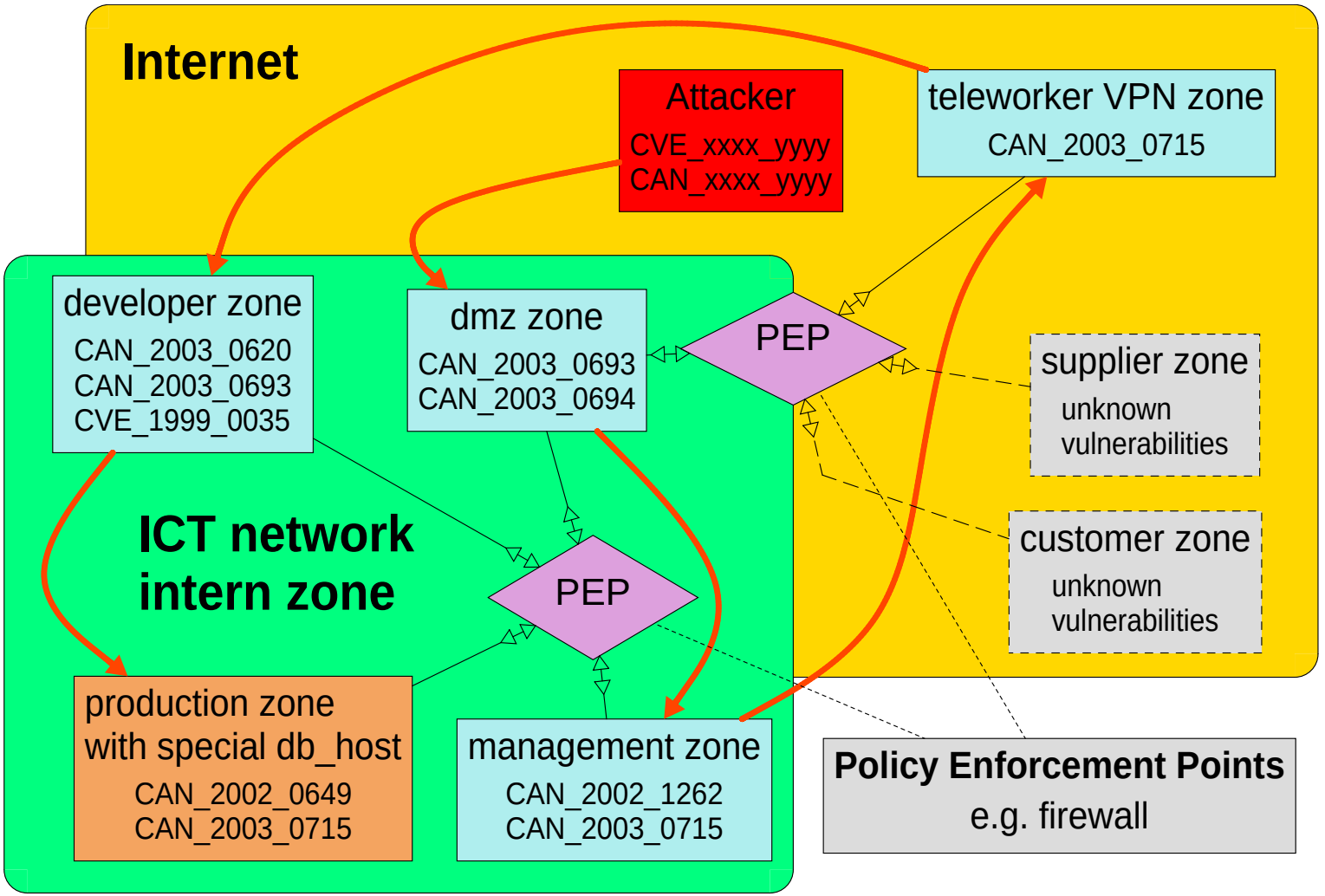
Process to guide the systematic protection (U.S. Fire Admin.)

- identify critical infrastructures essential for mission accomplishment
- determine the threats against those infrastructures
- analyse the vulnerabilities of threatened infrastructures
- assess the risks of degradation/loss of a critical infrastructure
- apply countermeasures where risk is unacceptable

Approach: Support this analytical Process

- supply a formal framework to specify critical (ICT) network infrastructures and threats against them
- provide tool based methods for a systematic evaluation
- assist with finally determining exactly what really needs protection & which strategy and means to apply

Example Scenario



Modelling critical (ICT) network infrastructures

Asset Inventory

hosts products, services, vulnerabilites

trust relation between hosts

topology of network

IDS intrusion detection info

Asset Prioritisation

criticality/worth of component

used for cost/benefit evaluations

Policy Definition

Organisation Based Access Control (Or-BAC) model

roles represent subjects (hosts)

activities represent actions (service, e.g. ssh)

views represent objects (target)

permissions:

role $\times$ activity $\times$ view

Modelling Vulnerabilities and Exploits

Modelling Vulnerabilities

- identifier (cf. Common Vulnerabilities and Exposures (CVE/CAN), MITRE Corporation)
- preconditions (credentials, ...)
- range and impact type (cf. National Institute of Standards and Technology (NIST))
- severity (reflects the probability of exploitation) (cf. Common Vulnerability Scoring System (CVSS) or US-CERT)

Modelling Exploits

- vulnerability
- cost
- impact
- stealth

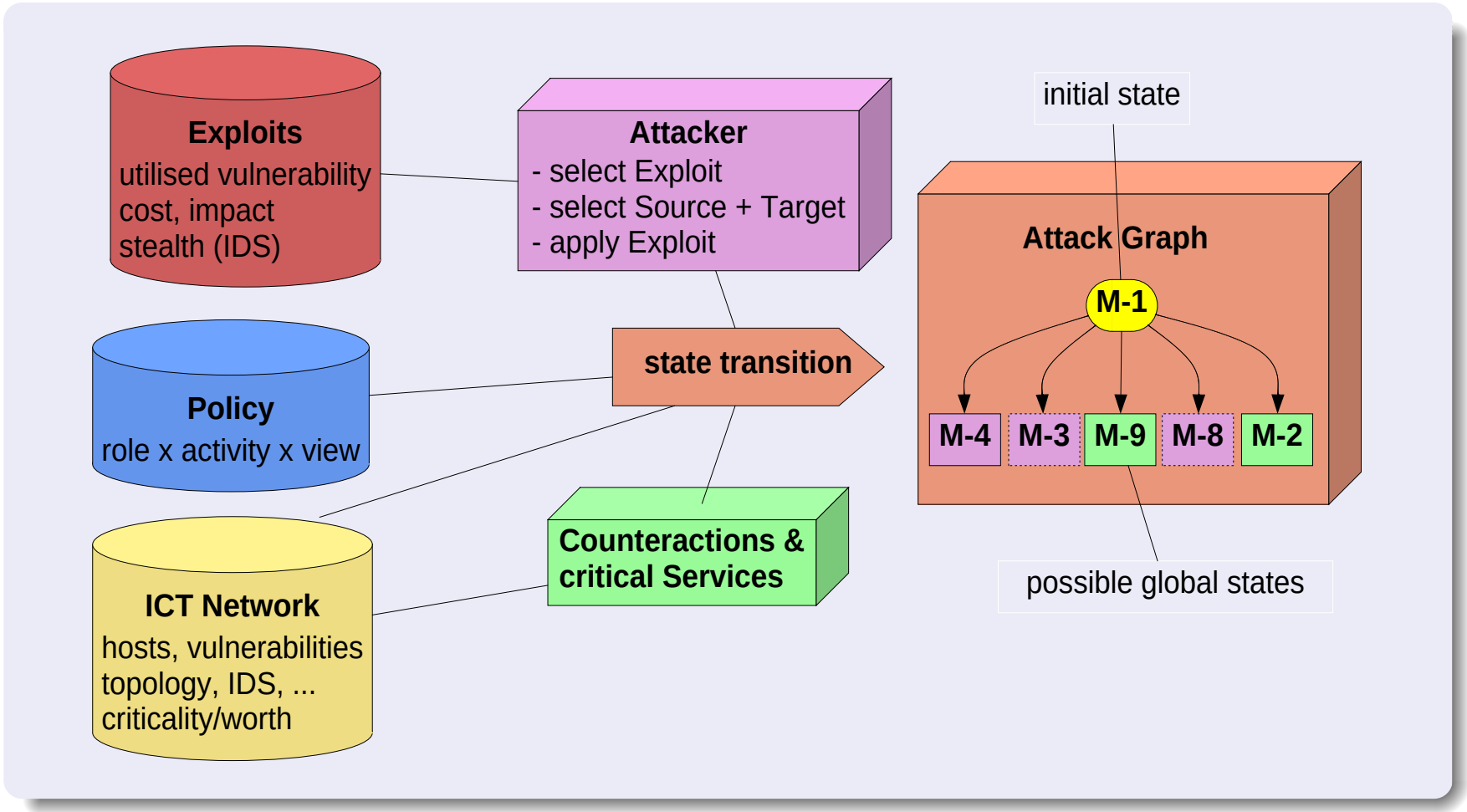
Modelling Attackers

Attacker strategy

- preprocessing of attacker profile (known exploits, hosts, credentials)
  e.g. assume the attacker uses only exploits for vulnerabilities with a severity above a given threshold
- select known exploit
- select source and target
- apply exploit

Note: The model allows multiple attackers (role based)

Attack Graph Computation



Exploit Template

CAN_2003_0693_ssh_exploit

Bind: attack from host S to host T $(S, T, plvl_S, plvl_T)$

E1: intruder knows exploit
$'CAN\_2003\_0693\_ssh\_exploit' \in Attacker\_known\_exploits\_state$,

E2: selection of source and target host
$(S, plvl_S) \in Attacker\_plvl\_state$, $rank(plvl_S) \geq rank('user')$,
$(T, plvl_T) \in Attacker\_plvl\_state$,

E3: is target vulnerable from source
$CAN\_2003\_0693(S, T, plvl_T) =' true'$,

E4: attacker gets all knowledge of host T
$get\_knowledge(T) =' true'$,

E5: intrusion detection check
$ids\_check('CAN\_2003\_0693\_ssh\_exploit', S, T) =' true'$,

E6: assign cost benefit values
$cost\_benefit('CAN\_2003\_0693\_ssh\_exploit', T,' root') =' true'$

E7: no additional impact in this example

Vulnerability Template

E3: is target T vulnerable from source S by CAN_2003_0693 ?

V1: is target configured vulnerable ?
$(T, 'CAN\_2003\_0693') \in host\_vulnerability\_state$,

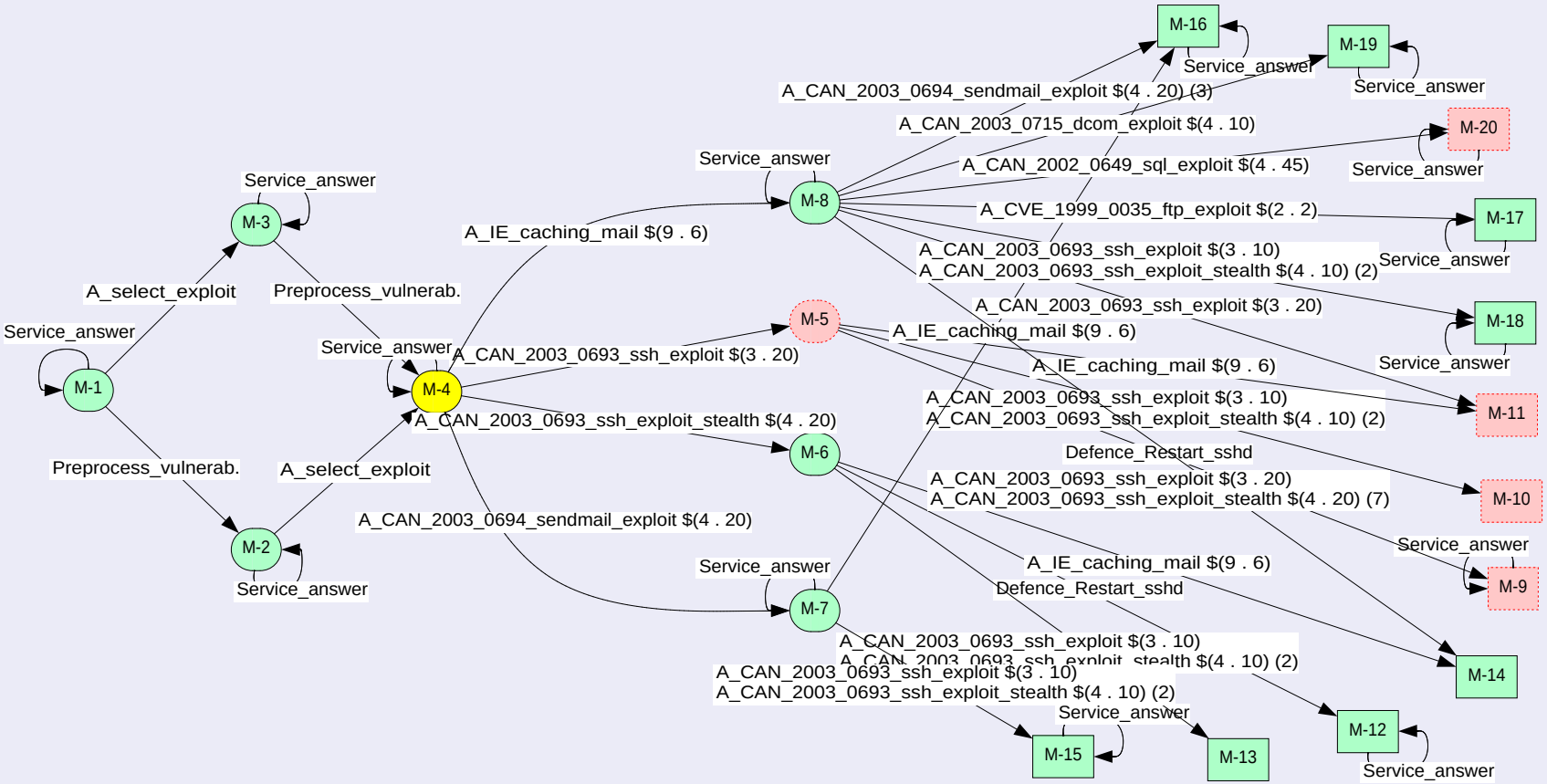
V2: is target currently running sshd ?
$(T, (('sshd', port), plvl\_service)) \in host\_service\_state$,

V3: is target reachable from source on port ssh (policy permission) ?
$Pol :=$
$reachable((S, T, port), role\_view\_activity\_seq(), role\_def\_seq())$,
$Pol \ =::$,

V4: effects for attacker (get sshd privileges on target)
$(T, plvl_T) \hookleftarrow Attacker\_plvl\_state$,
$(T, max\_access(plvl\_service, plvl_T)) \hookrightarrow Attacker\_plvl\_state$,

V5: direct impact (target is no longer running sshd)
$(T, (('sshd', port), plvl\_service)) \hookleftarrow host\_service\_state$

Attack graph of example scenario (small section)



500 nodes and 4136 edges (assuming the attacker knows all exploits), red nodes mark detected attacks

Attack Graph Analysis

Check Security Properties

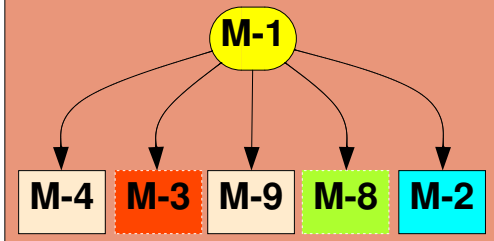
What security goals can be broken by a combination of exploits ?

Quick check "am I affected" by a newly found vulnerability ?

Survivability

Can a client get answers from a DB-server when the network is under attack ?

Attack Graph



Intrusion Detection

What attacks are detected ?

What effects have changes intrusion detection systems ?

Cost/Benefit Analysis

Find least cost attack breaking a given security property !

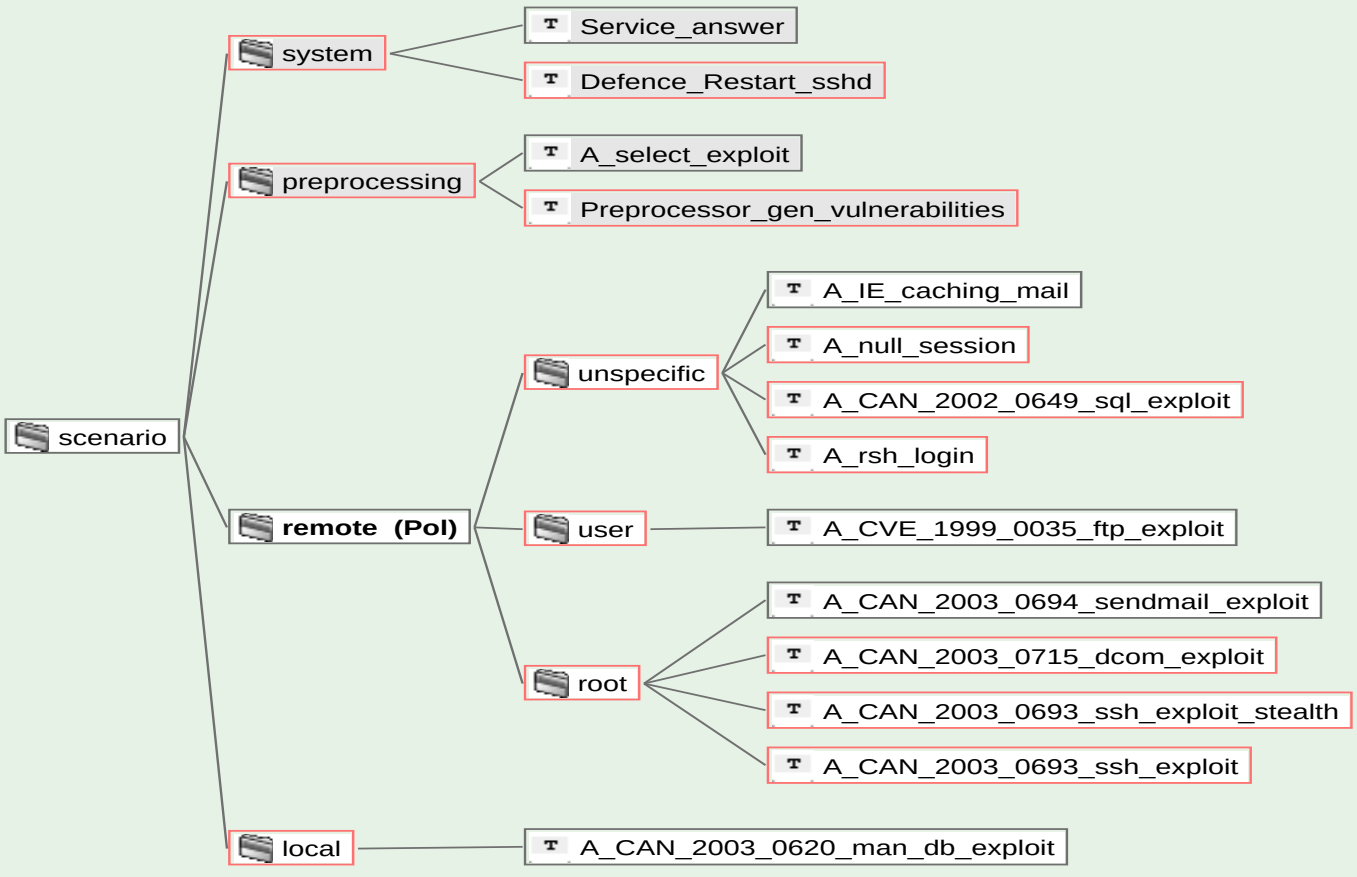
Find maximal attacker impact for a given set of exploits !

Abstraction

How does the attack graph look like when only attacks that affect mission critical resources are shown ?

Abstract Representations

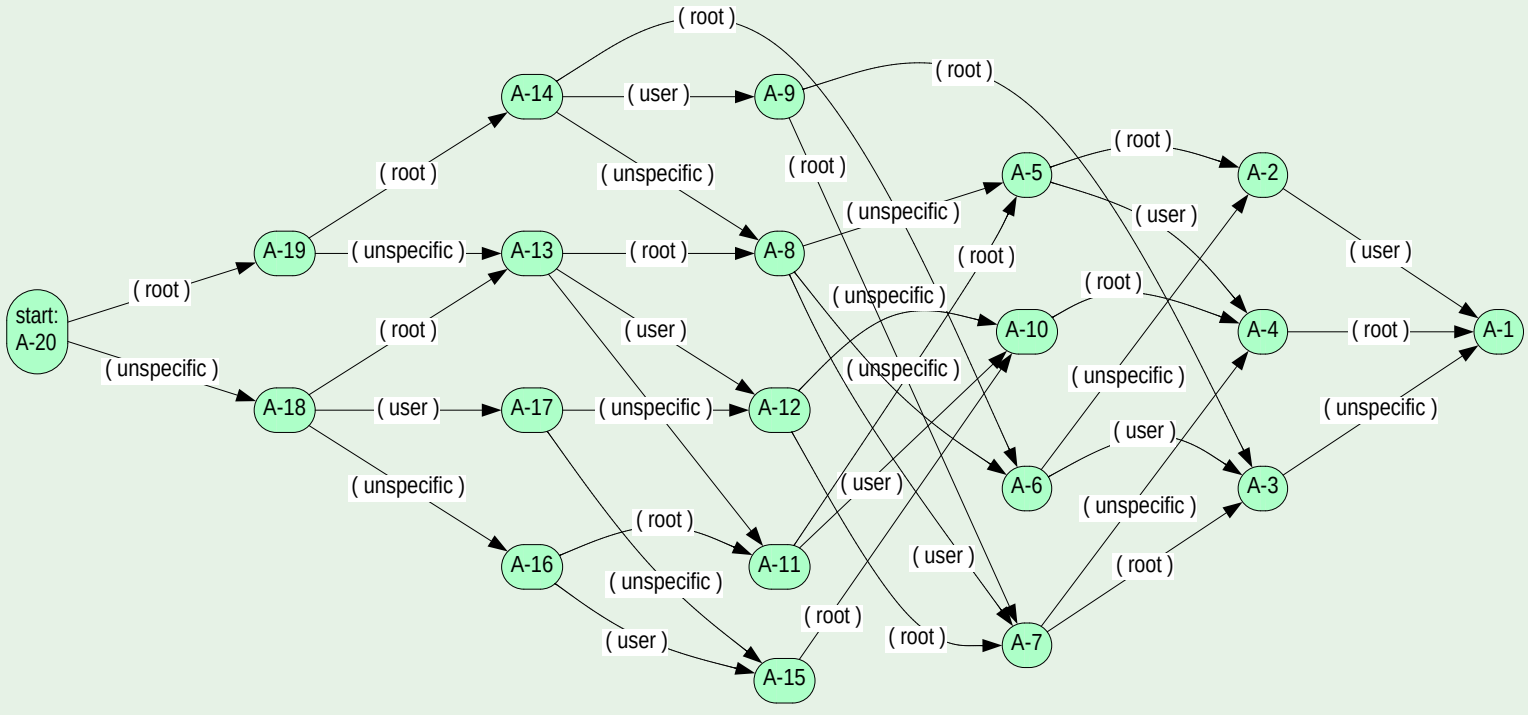
Step 1 - Define a Mapping (alphabetic language hom.)



$$\text{transition} \longrightarrow \text{range} + \text{impact}$$

Abstract Representations

Step 2 - Compute the Abstract Representation

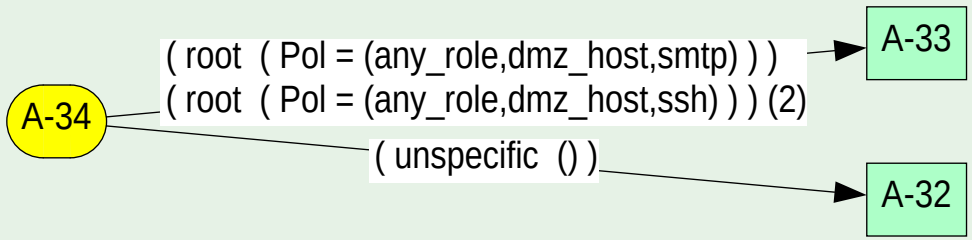


178 states and 1309 edges $\longrightarrow$ 20 states and 37 edges

Abstract Representations

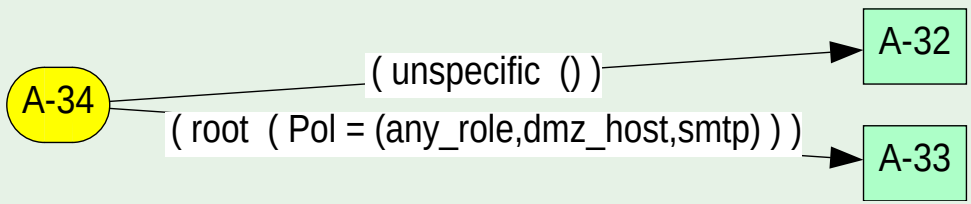
Step 3 - Optionally Refine the Mapping

now details about related policies are visible



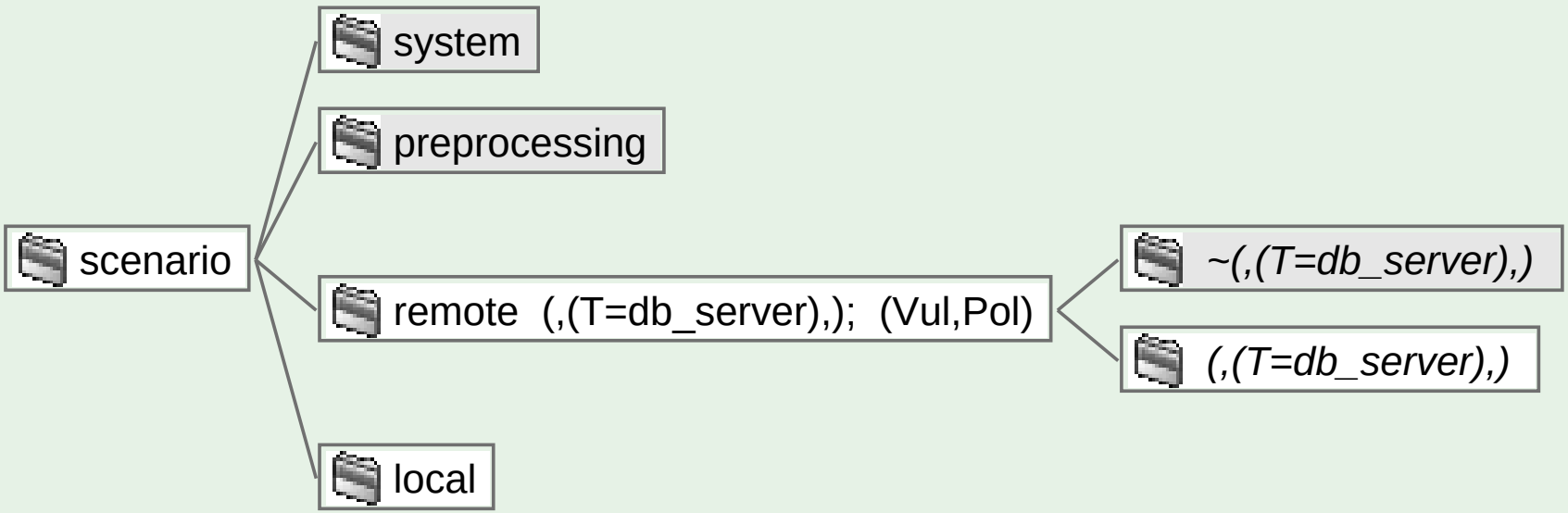
Step 4 - Adapt/Optimise the System Configuration

visualise impact of policy changes in the abstract representation



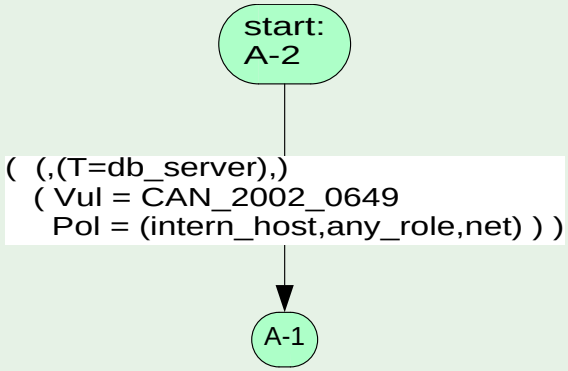
Using Predicates to define Abstractions

Step 1 - The mapping ($T = db\_server$) matches only those transitions that model direct attacks to the target host *db_server*



Using Predicates to define Abstractions

Step 2 - The abstract Representation proves that:



- in the current policy configuration attacks to the *db_server* are possible,
- those attacks are based on exploits of the vulnerability *CAN_2002_0649*, and,
- they are utilising the policy rule (*intern_hosts*, *any_role*, *net*).

Step 4 - Adapt/Optimise the System Configuration

To prevent this attack,

- uninstall the product that is hurt by this vulnerability, or,
- restrict the internal hosts in their possible actions by replacing the above policy with a more restrictive one.

Apply Approach to Networked Infrastructures

Support Critical Networked Infrastructure Protection

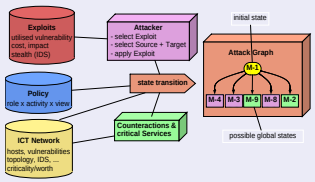
model a networked infrastructure system & threats including specifications of mutual dependencies

analyse interplay of component vulnerabilities & threats

reveal complex threat combinations (malfunctions, accidents, attacks) & raise risk awareness

support systematic evaluation of possible solutions

aim at optimising security & protection with given resources



Adaptation to changing Context

- Monitoring system behaviour and intrusion attempts
- Complex event processing
- Situated risk evaluation
- Policy-based automated threat response
- Impact minimisation