Research report at the 72nd IFIP WG 10.4 meeting

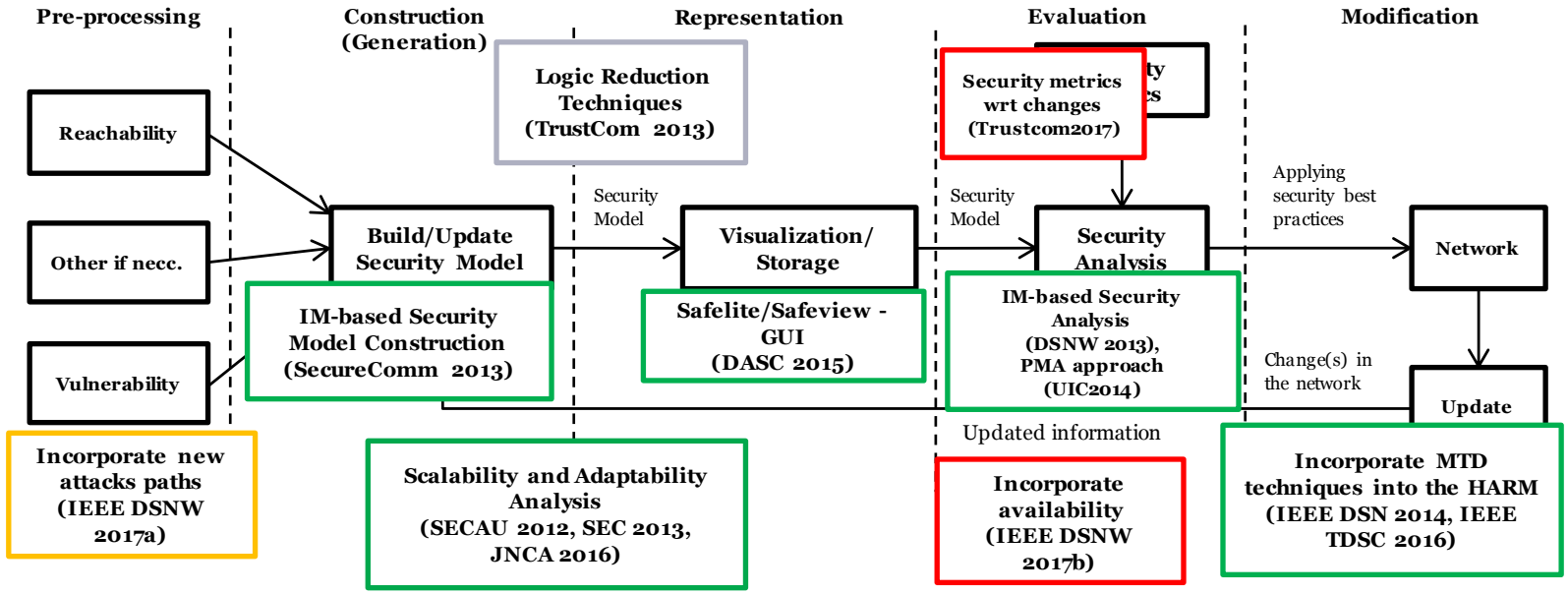
Dong-Seong Kim

Dept. of Computer Science and Software Engineering,
University of Canterbury, Christchurch, New Zealand
dongseong.kim@canterbury.ac.nz

Recent results

- Evaluating Security and Availability of Multiple Redundancy Designs, DSNW 2017
- Evaluating the Effectiveness of Security Metrics for Dynamic Networks, IEEE Trustcom 2017
- Discovering and Mitigating New Attack Paths, DSNW 2017

Graphical Security Models: our selected research contributions



SECAU 2012: "HARMs: Hierarchical Attack Representation Models for Network Security Analysis"
IFIP SEC 2013: "Performance analysis of scalable attack representation models"
IEEE TrustCom 2013: "Scalable Attack Representation Model Using Logic Reduction Techniques"
IEEE DSNW 2013: "Scalable Security Analysis in Hierarchical Attack Representation Model using Centrality Measures"
SecureComm 2013: "Scalable Security Model Generation and Analysis using k-importance Measure"
IEEE DSN 2014: "Scalable Security Models for Assessing Effectiveness of Moving Target Defenses"
IEEE DSNW 2014: "What Vulnerability Do We Need To Patch First?"
IEEE UIC 2014: "Scalable Security Analysis using Partition and Merge Approach in an Infrastructure as a Service Cloud"
IEEE DASC2015: "Towards Automated Generation and Visualization of Hierarchical Attack Representation Models"
IEEE TDSC 2016: "Assessing the Effectiveness of Moving Target Defense using Security Models"
Elsevier JNCA 2016: "Towards scalable security analysis using multi-layered security models"

IEEE DSNW2017a: "Discovering and Mitigating New Attack Paths using Graphical Security Models"
IEEE DSNW2017b: "Evaluating Security and Availability of Multiple Redundancy Designs"
IEEE Trustcom 2017: "Evaluating the Effectiveness of Security Metrics for Dynamic Networks"

Evaluating Security and Availability of Multiple Redundancy Designs when Applying Security Patches

Mengmeng Ge[1], Huy Kang Kim[2], Dong Seong Kim[1]

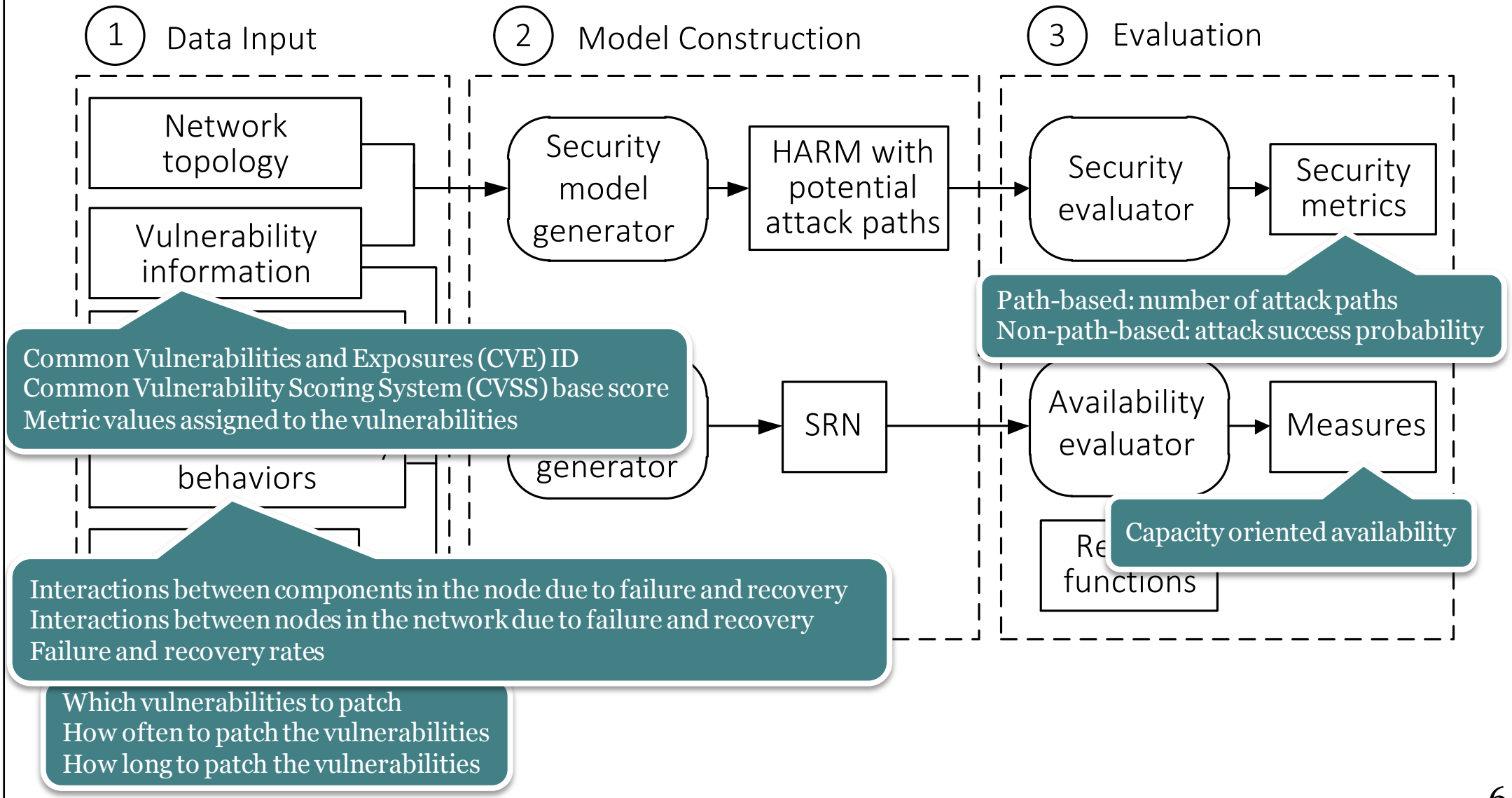
[1]University of Canterbury, New Zealand
[2]Korea University, South Korea

Introduction

- Centralized patch management
  - Enhance security
- Some security patches require system reboot
  - Introduce downtime
- Redundant servers
  - Improve availability
  - Increase attack surface
- Balance between security and availability affected by the security patch

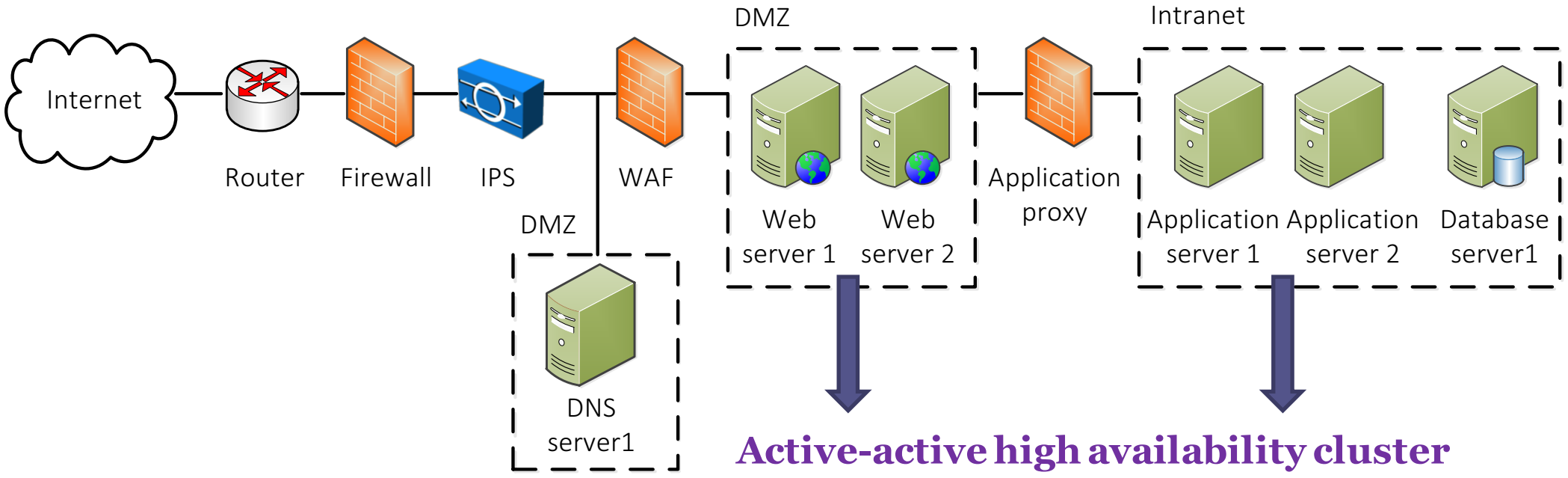
Proposed Approach

Hierarchical Attack Representation Model (HARM)
Stochastic Reward Net (SRN)



Example Enterprise Network

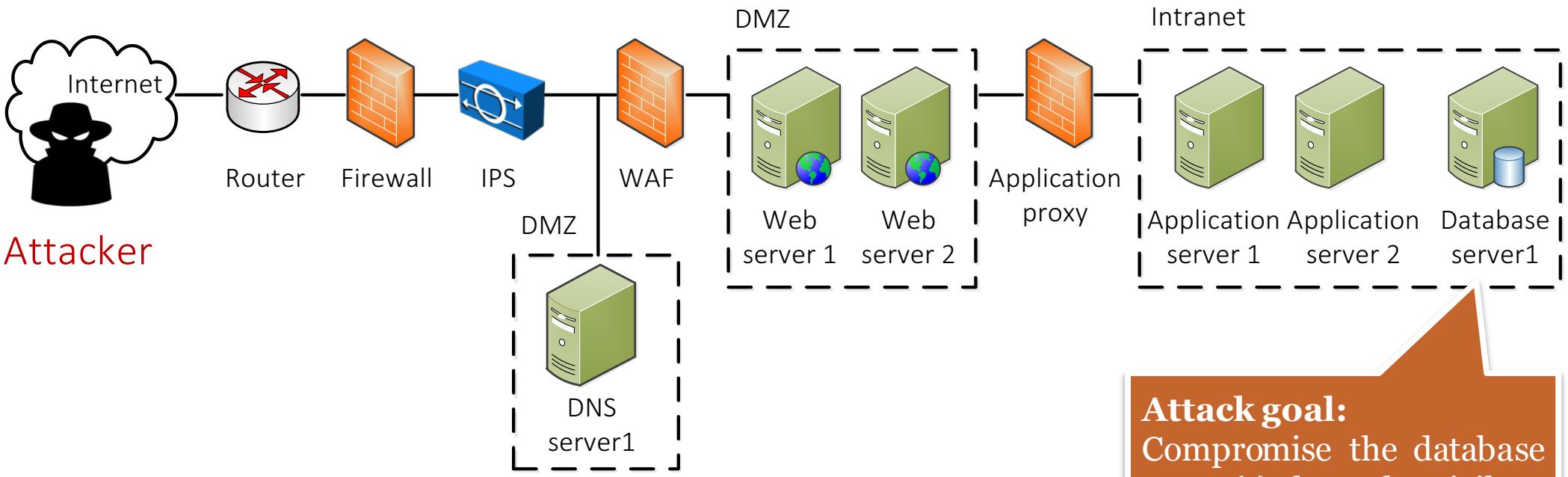
- 3-tier client-server architecture



Active-active high availability cluster
Redundant servers are identical

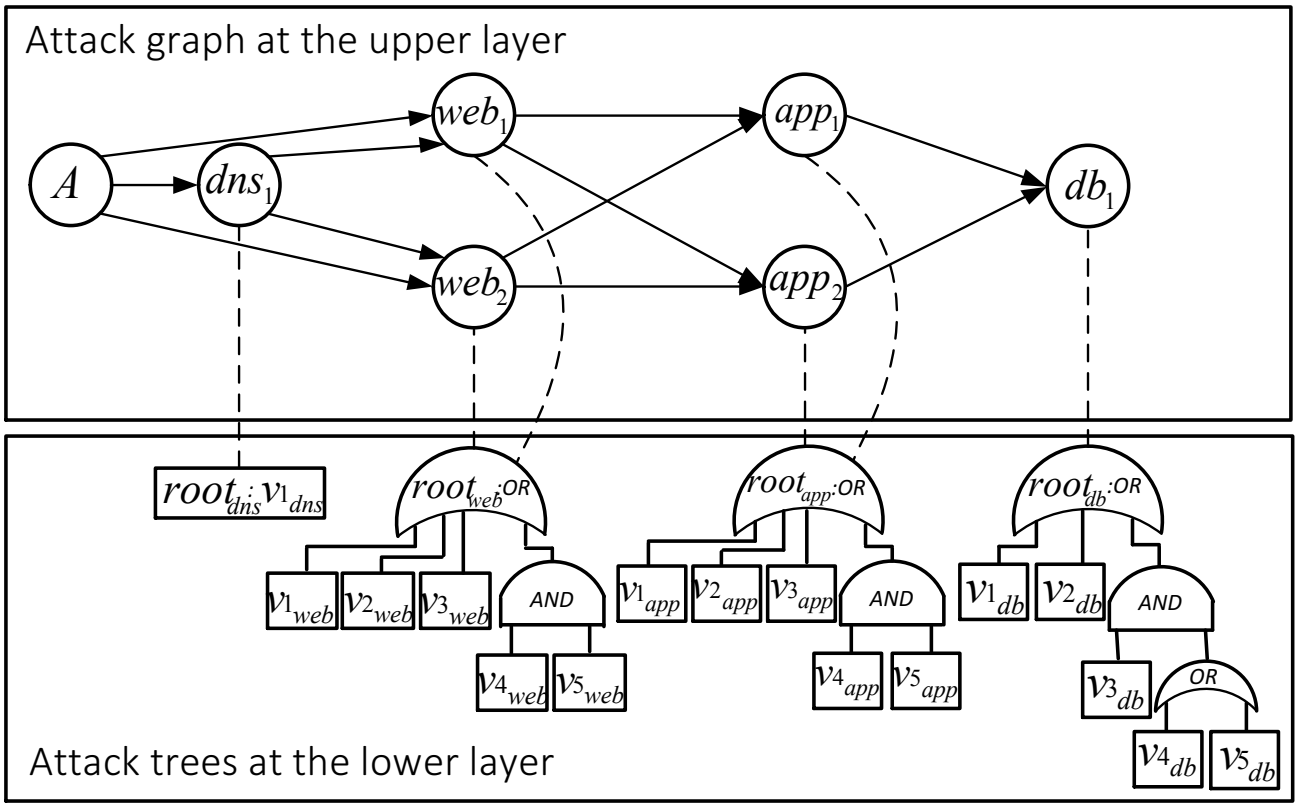
An Attacker Model - Remote Attacker

- Laptop-class device with attack tools

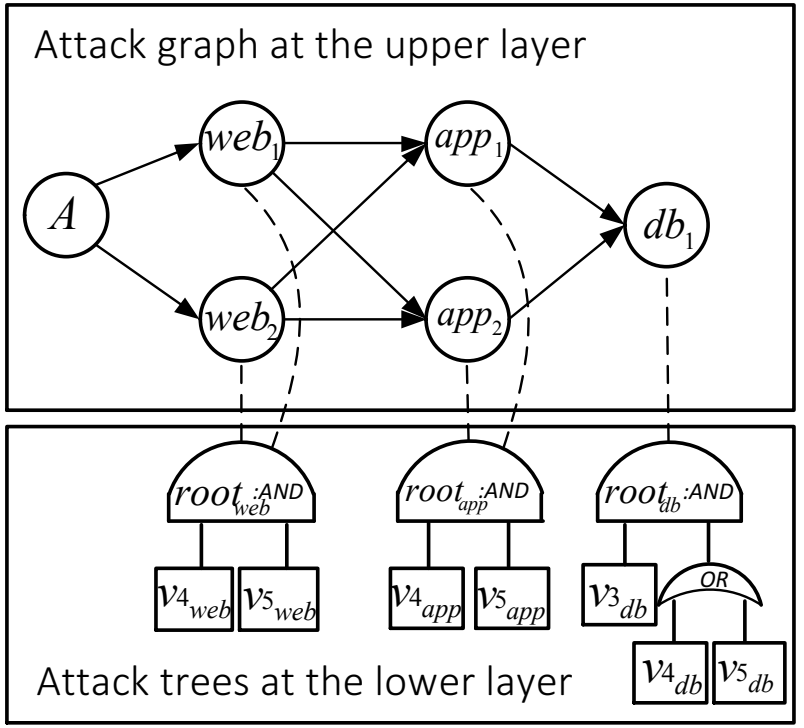


Construction of HARMs

Before patch

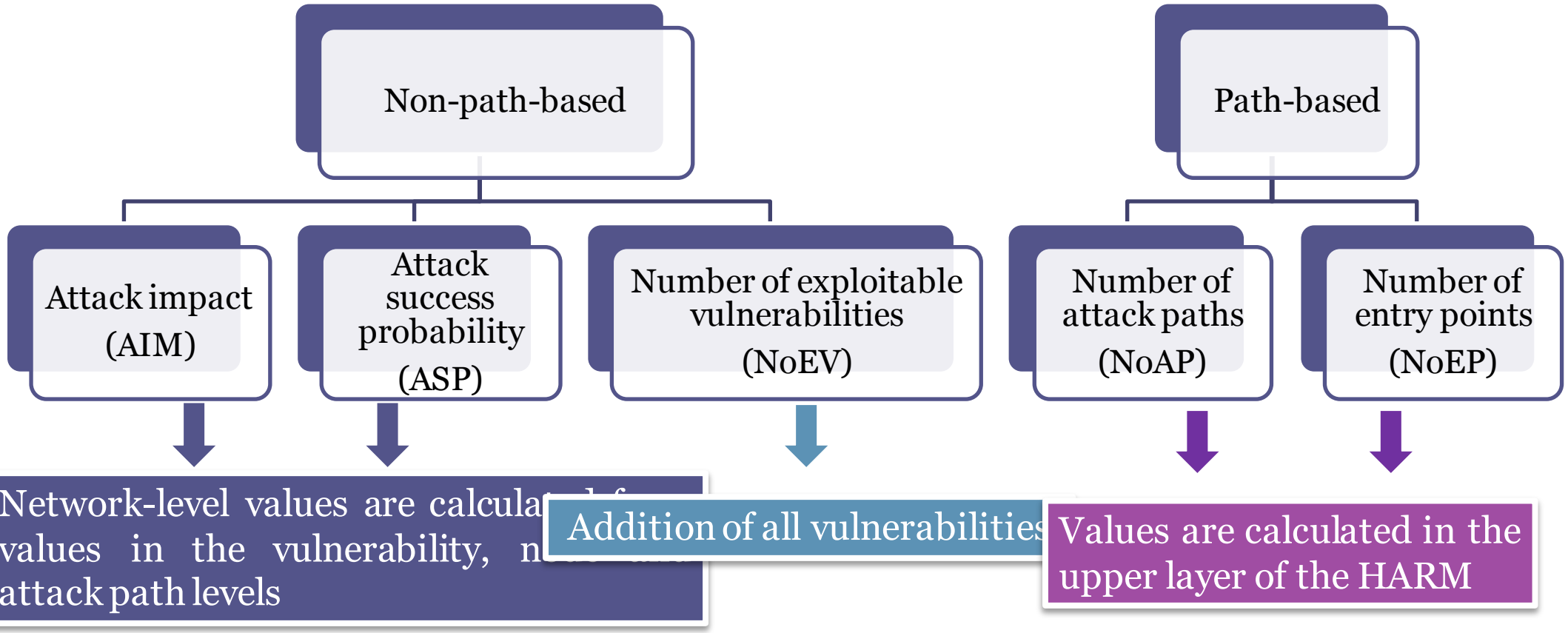


After patch

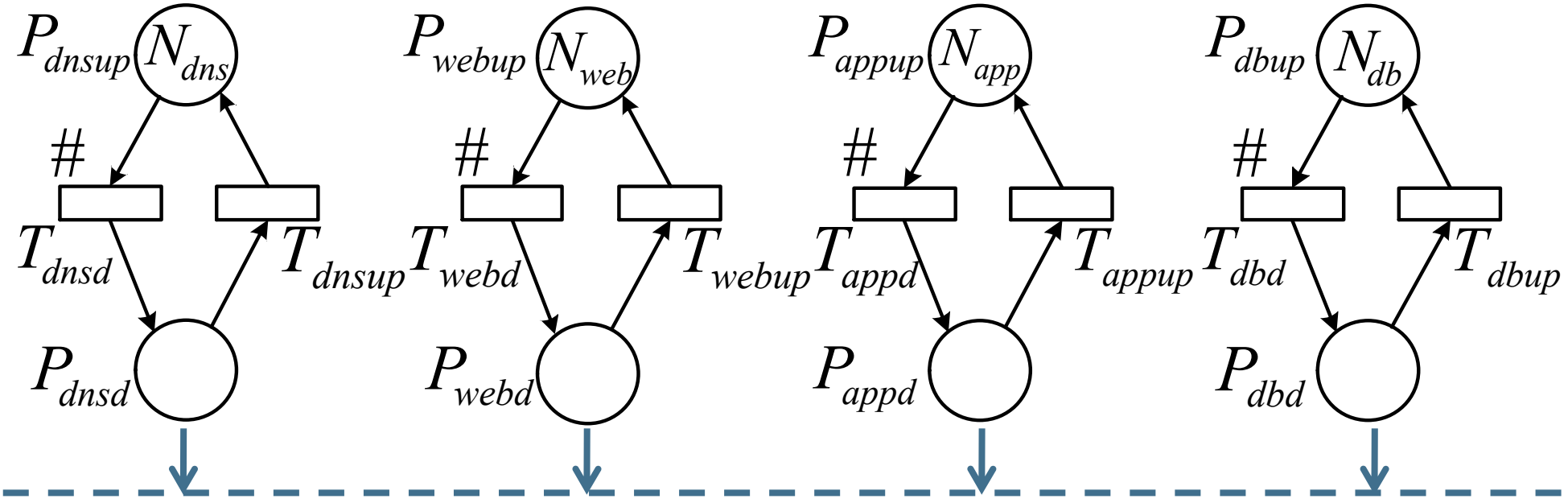


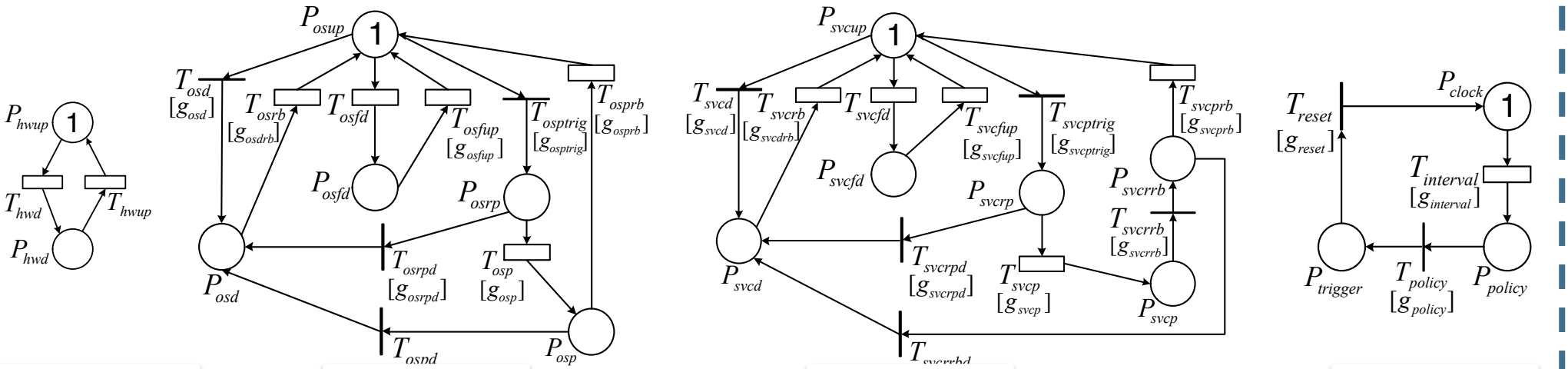
Construction of HARMs (cont.)

- Security metrics for the security analysis:

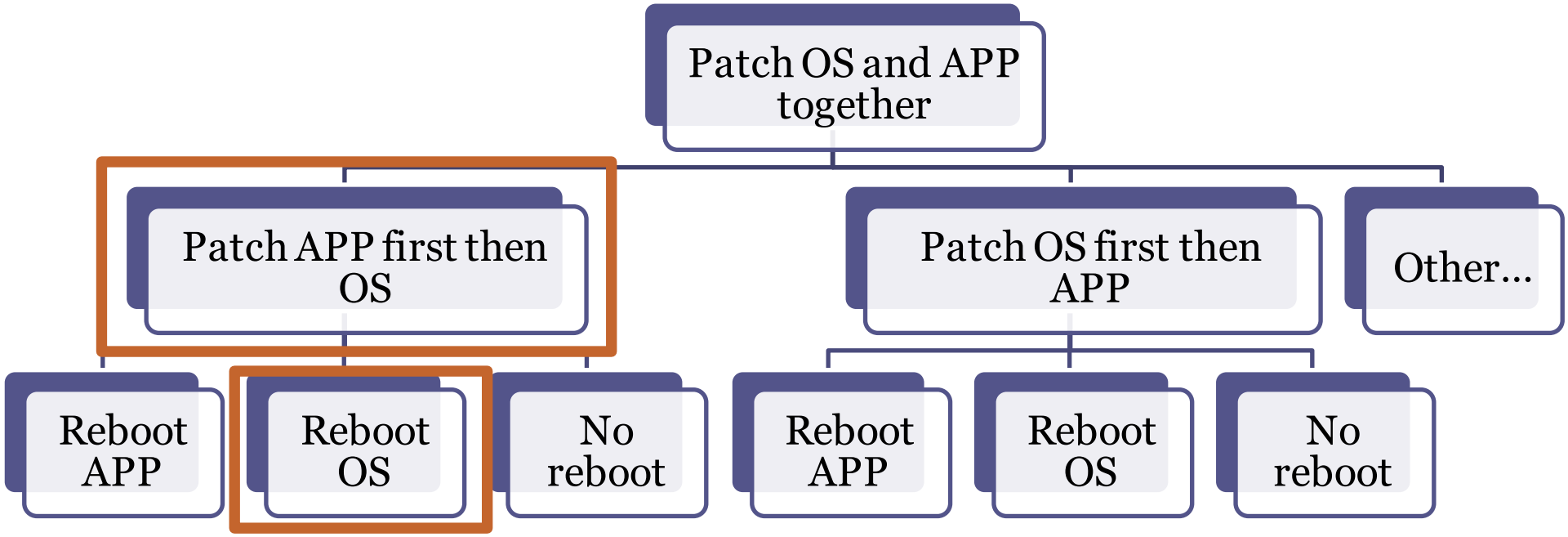


Construction of SRN models





Construction of SRN models (cont.)



Construction of SRN models (cont.)

- Output measure of SRN sub-models for the network
  - Capacity oriented availability (COA)

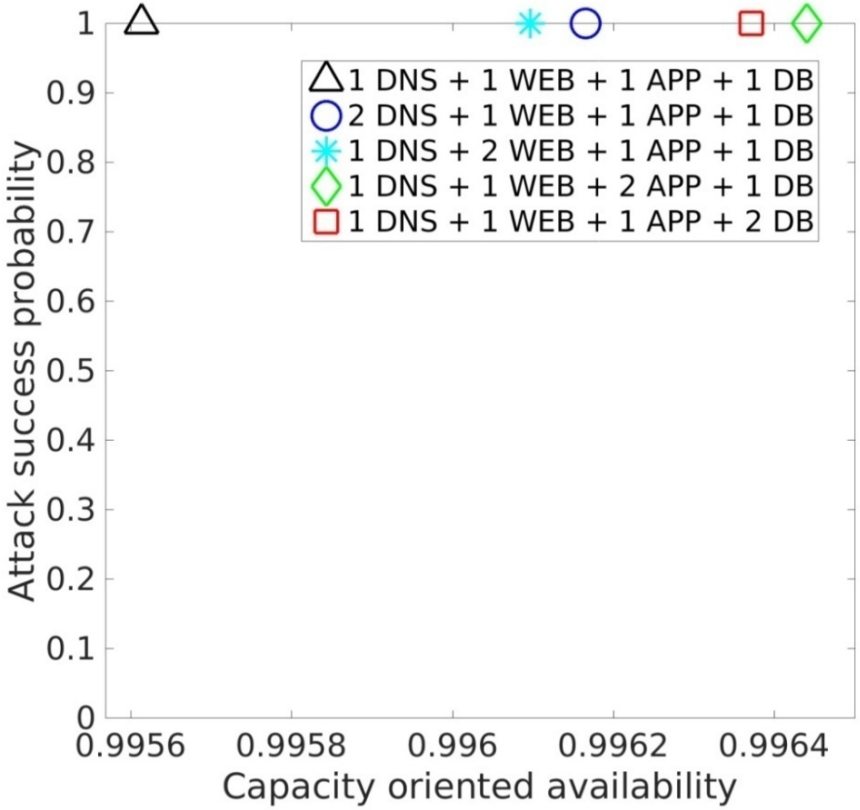
Reward	Definition
COA	if ($\#P_{dnsup} == 1$ && $\#P_{webup} == 2$ && $\#P_{appup} == 2$ && $\#P_{dbup} == 1$) 1 else if ($\#P_{dnsup} == 1$ && $\#P_{webup} == 1$ && $\#P_{appup} == 2$ && $\#P_{dbup} == 1$) 0.83333 else if ($\#P_{dnsup} == 1$ && $\#P_{webup} == 2$ && $\#P_{appup} == 1$ && $\#P_{dbup} == 1$) 0.83333 else if ($\#P_{dnsup} == 1$ && $\#P_{webup} == 1$ && $\#P_{appup} == 1$ && $\#P_{dbup} == 1$) 0.66667 else 0

Reward rate is the number of running servers during patch divided by the total number of servers.
0.83333 (5/6)
0.66667 (4/6)

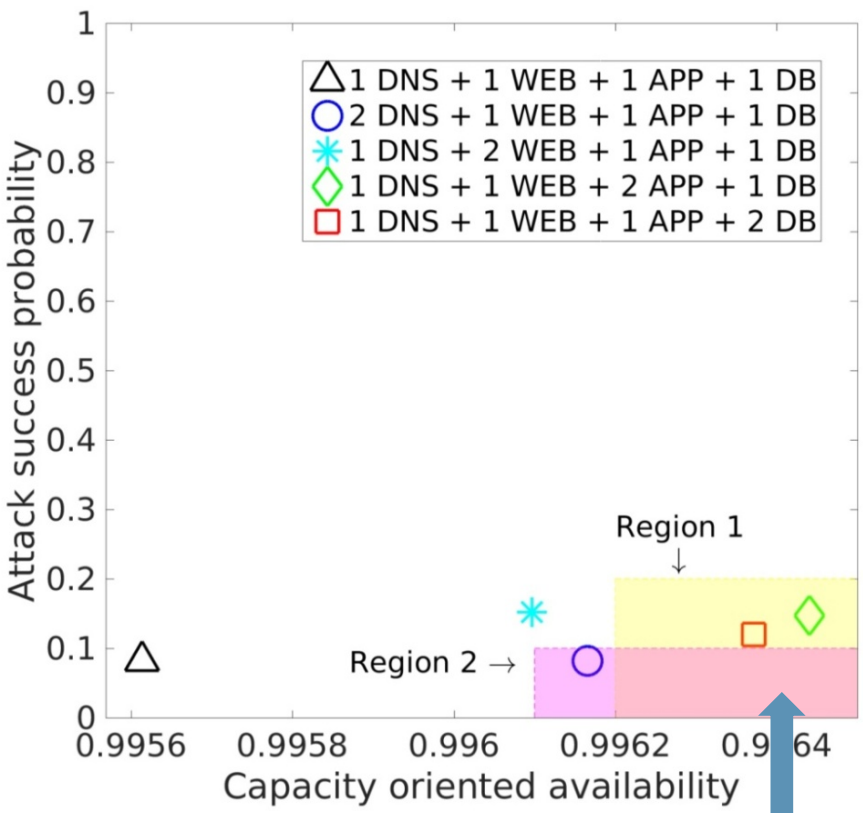
COA≈0.99707

Numerical Analysis

Before patch



After patch



$$f(ASP, COA) = \begin{cases} 1, & \text{if } ASP <= \phi \text{ and } COA >= \psi \\ 0, & \text{if } ASP > \phi \text{ or } COA < \psi \end{cases}$$

Limitations and Potential Extensions

- Measurement using Testbed (we have a Software Defined Cloud at UC)
- Systems
  - Large scale; heterogeneous redundancy
- SRN availability models
  - Patch schedules; reboot cases;…
- User oriented performance/performability
  - Queuing network (e.g., mean response time, mean waiting time, dropping probability) …
- Other Dependability and Security Metrics
  - Opex/capex as output measure
  - Economic metrics (e.g., gain of high availability vs. cost of redundancy; loss of successful attacks vs. cost of security patch) …

My previous work on Availability and performability:
Dong Seong Kim, Fumio Machida, Kishor S. Trivedi: Availability Modeling and Analysis of a Virtualized System. PRDC 2009: 365-371
Rahul Ghosh, Kishor S. Trivedi, Vijay K. Naik, Dong Seong Kim: End-to-End Performability Analysis for Infrastructure-as-a-Service Cloud: An Interacting Stochastic Models Approach. PRDC 2010: 125-132
Fumio Machida, Dong Seong Kim, Kishor S. Trivedi: Modeling and analysis of software rejuvenation in a server virtualized system with live VM migration. Perform. Eval. 70(3): 212-230 (2013)
Tuan Anh Nguyen, Dong Seong Kim, Jong Sou Park: Availability modeling and analysis of a data center for disaster tolerance. Future Generation Comp. Syst. 56: 27-50 (2016)

Evaluating the Effectiveness of Security Metrics for Dynamic Networks

Simon Enoch Yusuf, Mengmeng Ge, Jin Hong, and Dong-Seong Kim

University of Canterbury
Christchurch, New Zealand

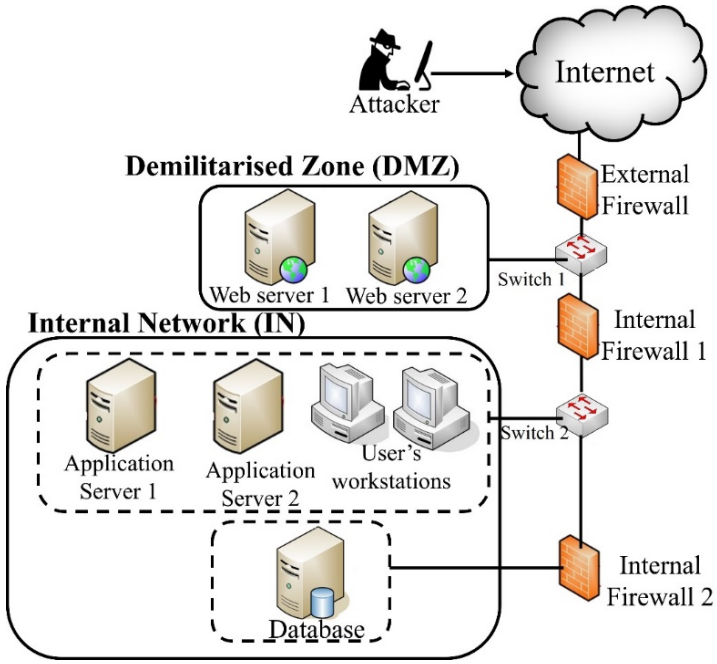
Our approach

- Previous graphical security model – Hierarchical Attack Representation Model (HARM)[1,2]
- Need to incorporate changes in the networks
- propose to use a ***Temporal***-Hierarchical Attack Representation Model (T-HARM)*
- to investigate the varying effects of security metrics when changes are observed in a dynamic network (e.g. enterprise nets, Cloud).
  - T-HARM is a layered and scalable security model that captures the temporal changes.

[1]Jin B. Hong, Dong Seong Kim: Assessing the Effectiveness of Moving Target Defenses Using Security Models. ***IEEE Trans. Dependable Sec. Comput.*** 13(2): 163-177 (2016)

[2]J. B. Hong and D. S. Kim, "Towards Scalable Security Analysis using Multi-layered Security Models," ***Elsevier Journal of Network and Computer Applications***, vol. 75, pp. 156 – 168, 2016.

Example network and Attacker Model



List of vulnerabilities at t_2

Host	Vul.	Base score
WS_1	CVE-2015-3566 CVE-2000-1247	4.3 2.1
WS_2	CVE-2015-3566 CVE-2000-1247	4.3 2.1
AS_1	CVE-2013-0638 CVE-2016-0763	10.0 4.3
AS_2	CVE-2013-0900 CVE-2015-3566	4.3 4.3
DB	CVE-2012-1675 CVE-2016-3201	7.5 4.3
User's	CVE-2016-2834 CVE-2016-7218	8.8 1.9

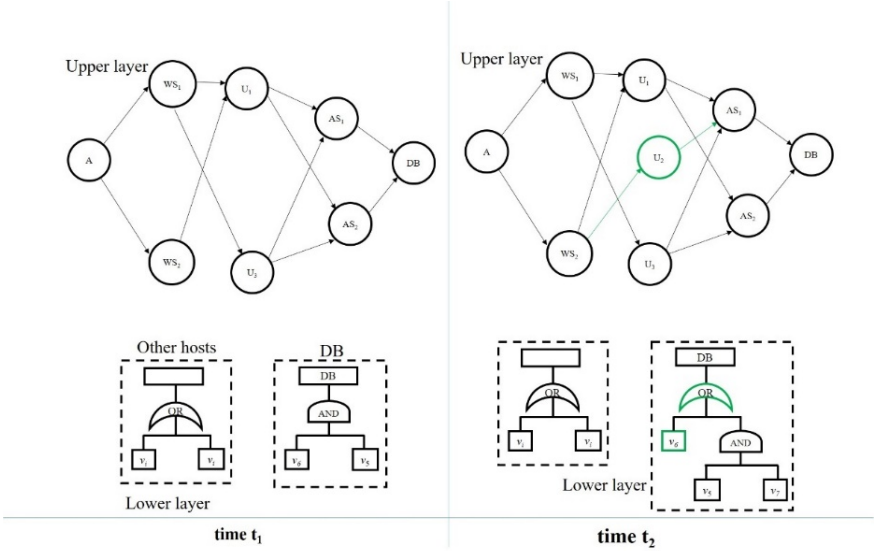


Fig: T-HARM

Table 1: OSs and Applications on hosts

Host	OS	Service
WS_1	Redhat Enterprise Linux 6	Apache http server 2.4
WS_2	Redhat Enterprise Linux 6	Apache http server 2.4
AS_1	Windows 10	WebLogic server 12.1
AS_2	Redhat Enterprise Linux 6	Apache tomcat 7.0
DB	Windows 10	Oracle database 11g
WTs	Redhat Enterprise Linux 6	Mozilla firefox 31.1.0

Changes at at t_2

Host	Vul.	Base score
DB	CVE-2015-2465	2.1
New User	CVE-2016-2834 CVE-2016-7218	8.8 1.9

Security metrics

- We investigate the following security metrics (ten security metrics):

Metrics	Notations
Risk on attack paths	R
Cost on attack paths	AC
Probability of attack success on paths	Pr
Return on attack paths	ROA
Standard deviation of attack path lengths [6]	SDPL
Mean of attack path lengths [14]	MAPL
Number of attack paths [12]	NAP
Mode of attack path lengths [6]	MoPL
Shortest attack path [12]	SAP
Normalised mean of attack path lengths [6]	NMPL

Security metrics (cont.)

- Based on Common Vulnerability Scoring System (CVSS) based score, we assigned values to:
  - the probability of attack success (pr),
  - attack impact (aim) and
  - attack cost (ac) to each vulnerability in the network
    - The CVSS provides standardised vulnerability score which is ranging from 0.0 to 10.0 (with 10.0 being the most severe level).
- We introduce time for each metric, we then use them for the security analysis (e.g., for Risk on attack paths (R), we use it as Risk on attack paths at time t (R_t) to compute the metric at a specific time).

Host (h)	Vul.	Base score	ac_h	aim_h	Pr_h
WS_1	CVE-2015-3566 CVE-2000-1247	4.3 2.1	5.7 7.9	5.0 3.0	0.43 2.1
WS_2	CVE-2015-3566 CVE-2000-1247	4.3 2.1	5.7 7.9	5.0 3.0	0.43 2.1
AS_1	CVE-2013-0638 CVE-2016-0763	10.0 4.3	0.1 7.9	10.0 5.3	1.0
AS_2	CVE-2013-0900 CVE-2015-3566	4.3 4.3	7.9 7.9	5.3 5.3	0.43 0.43
DB	CVE-2012-1675 CVE-2016-3201	7.5 4.3	2.5 7.9	8.0 5.0	0.75 0.43
User's	CVE-2016-2834 CVE-2016-7218	8.8 1.9	1.2 8.1	9.0 2.0	0.88 0.19

Defense model

- We use the patching of vulnerabilities as the defense for our simulation.
- In particular, we adopt the prioritised set of vulnerabilities using the hybrid method* to determine important vulnerability to patch first (since it is infeasible to patch all vulnerability)
  - the Prioritized set of vulnerabilities (PSV) is defined as a set of vulnerabilities which are most important to enhance security (e.g., to minimize the system risk).

*J. B. Hong, D. S. Kim, and A. Haqiq. What Vulnerability Do We Need to Patch First? In Proceeding of the DSNW 2014.

Changes

- investigate the varying effects of security metrics when changes are observed in the network, we conduct various analysis with different types of changes via the T-HARM.
  - Emergence of new vulnerabilities
  - Patching of vulnerabilities with the emergence of vulnerabilities
  - Addition of new hosts (hosts having vulnerabilities)
  - Removal of existing hosts
  - Change of firewall rules.

Summary

- the existing security metrics response to changes in different ways when we introduced time to them.
  - We found that, depending on the types of security change the different security metrics (except the SAP) can show change in their value when there is a change in the network system and configuration.

Security metrics	Emergence of vulnerabilities	Patching and emergence of vulnerabilities	Addition of hosts	Removal of hosts	Firewall rules change
R	✓	✓	✗	✗	✓
AC	✓	✓	✗	†	†
Pr	✓	✓	✗	✗	†
ROA	✓	✓	✗	†	✓
SAP	✗	✗	✗	✗	✗
NAP	✗	✓	✓	✓	✓
MAPL	✗	✓	✓	✓	✓
NMPL	✗	✓	✓	✓	✓
SDPL	✗	✓	✓	✓	✓
MoPL	✗	✓	✓	✗	✓

Legend
- Significant change(✓)
- Small change(†)
- No change(✗)

On-going work

- Time-independent Security models
  - T-HARM takes snapshots of a dynamic network at t_i *(event, users, batch…)*
  - Issues
    - we may miss some states.
    - infeasible to cover all possible states.
- For each state (lets stay we choose sampling method (1)), we can compute the risk of the given Network (e.g., Cloud) state.
- Two ideas:
  - (a) we aggregate all the states and compute security metrics.
  - (b) we give weights to each state based on the observation and aggregate risk based on the weight of each state.
    - Make a state space model (Markov, Petri net models) to capture the state transitions and other info.

Thank you!

Hagley Park, Christchurch, New Zealand

Dong-Seong Kim
dongseong.kim@canterbury.ac.nz

University of Canterbury, New Zealand