Research report at 71st IFIP WG meeting

Graphical Security Models and Their Applications: Research Activities at UC

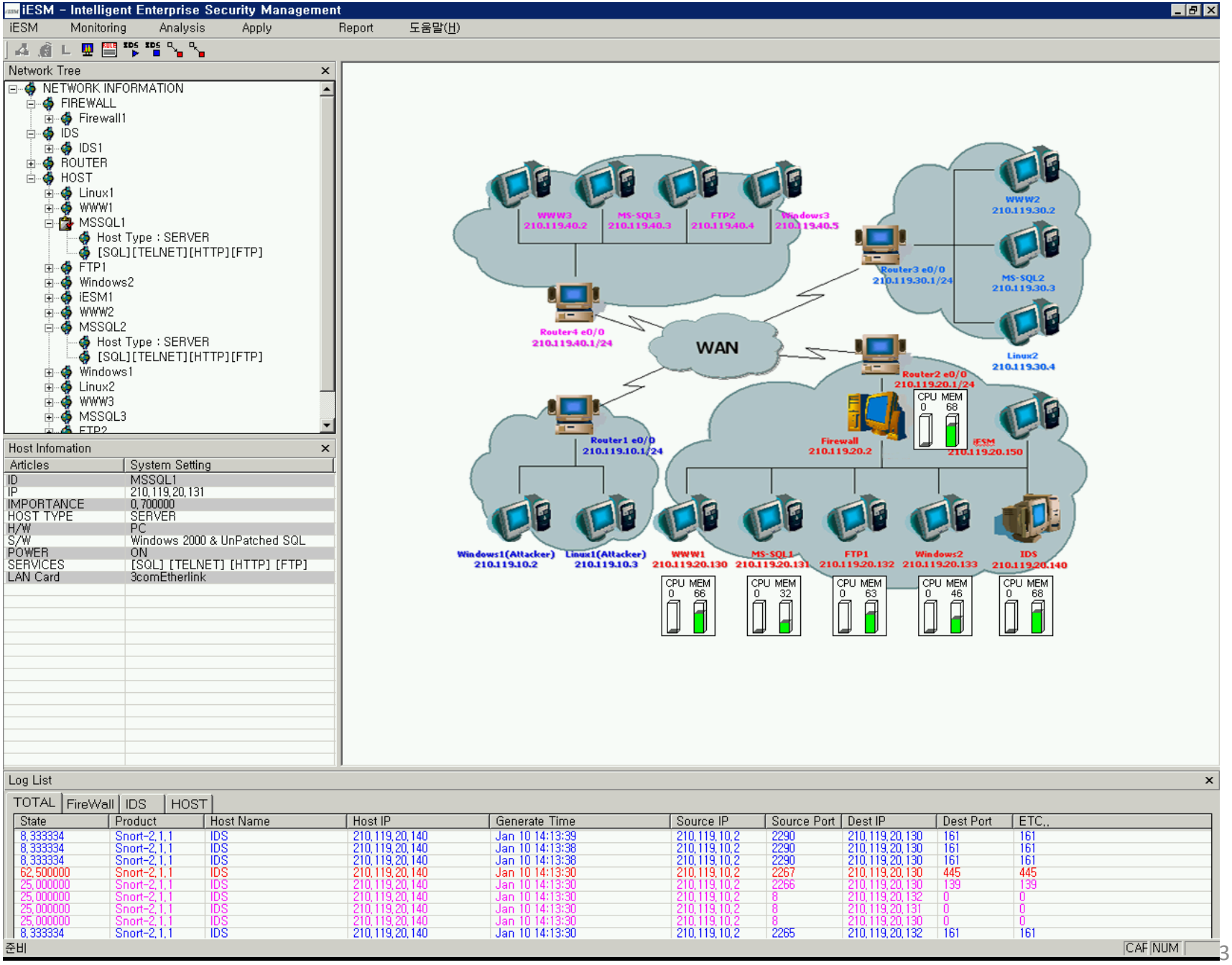
Dong-Seong Kim

University of Canterbury, New Zealand

Email: dongseong.kim@canterbury.ac.nz

My experience in Cybersecurity Modeling and Assessment

- *Intelligent* Enterprise Security Management (*i*ESM) system design and development (2003-2005) at KAU
- NSF MiMANSaS: Metrics, Models and Analysis of Network Security and Survivability at Duke (2008-2010)
- Cloud Security by NATO Science for Peace and Security (SPS) programme at UC (2012-2015)
  - http://cloudsecurity.ece.duke.edu/
- Security modeling tools development at UC (2016-2017)
- Security Assessment for Cloud by Qatar NPRP at UC (2016-2019)

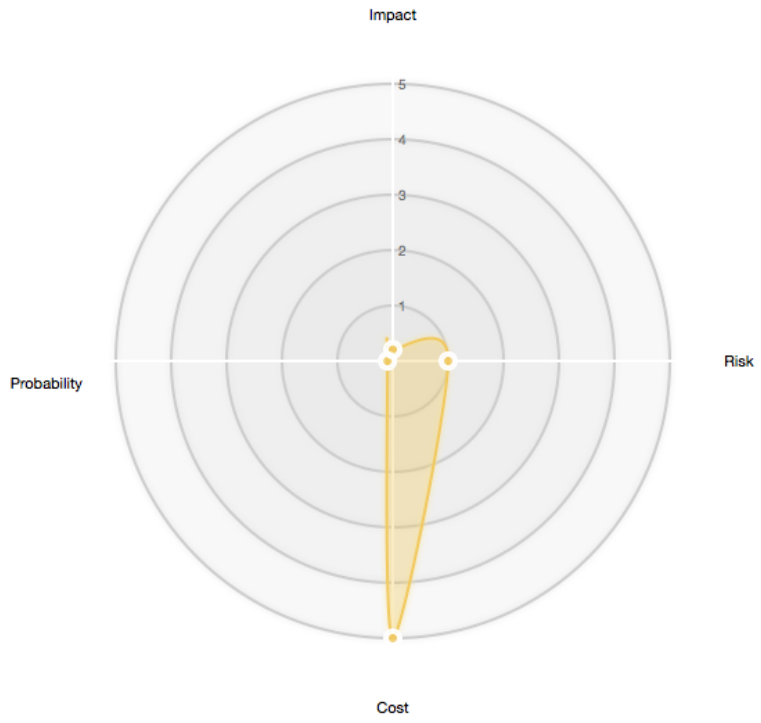

iESM – Intelligent Enterprise Security Management
iESM
Monitoring
Analysis
Apply
Report
도움말(H)
Network Tree
NETWORK INFORMATION
FIREWALL
Firewall1
IDS
IDS1
ROUTER
HOST
Linux1
WWW1
MSSQL1
Host Type : SERVER
[SQL][TELNET][HTTP][FTP]
FTP1
Windows2
iESM1
WWW2
MSSQL2
Host Type : SERVER
[SQL][TELNET][HTTP][FTP]
Windows1
Linux2
WWW3
MSSQL3
FTP2
Host Infomation
Articles
System Setting
ID
MSSQL1
IP
210,119,20,131
IMPORTANCE
0,700000
HOST TYPE
SERVER
H/W
PC
S/W
Windows 2000 & UnPatched SQL
POWER
ON
SERVICES
[SQL] [TELNET] [HTTP] [FTP]
LAN Card
3comEtherlink
WWW3 210.119.40.2
MS-SQL3 210.119.40.3
FTP2 210.119.40.4
Windows3 210.119.40.5
Router4 e0/0 210.119.40.1/24
WAN
Router3 e0/0 210.119.30.1/24
WWW2 210.119.30.2
MS-SQL2 210.119.30.3
Linux2 210.119.30.4
Router2 e0/0 210.119.20.1/24
Router1 e0/0 210.119.10.1/24
Firewall 210.119.20.2
iESM 210.119.20.150
Windows1(Attacker) 210.119.10.2
Linux1(Attacker) 210.119.10.3
WWW1 210.119.20.130
MS-SQL1 210.119.20.131
FTP1 210.119.20.132
Windows2 210.119.20.133
IDS 210.119.20.140
CPU MEM
Log List
TOTAL
FireWall
IDS
HOST
State
Product
Host Name
Host IP
Generate Time
Source IP
Source Port
Dest IP
Dest Port
ETC..
8,333334 Snort-2,1,1 IDS 210,119,20,140 Jan 10 14:13:39 210,119,10,2 2290 210,119,20,130 161 161
8,333334 Snort-2,1,1 IDS 210,119,20,140 Jan 10 14:13:38 210,119,10,2 2290 210,119,20,130 161 161
8,333334 Snort-2,1,1 IDS 210,119,20,140 Jan 10 14:13:38 210,119,10,2 2290 210,119,20,130 161 161
62,500000 Snort-2,1,1 IDS 210,119,20,140 Jan 10 14:13:30 210,119,10,2 2267 210,119,20,130 445 445
25,000000 Snort-2,1,1 IDS 210,119,20,140 Jan 10 14:13:30 210,119,10,2 2266 210,119,20,130 139 139
25,000000 Snort-2,1,1 IDS 210,119,20,140 Jan 10 14:13:30 210,119,10,2 8 210,119,20,132 0 0
25,000000 Snort-2,1,1 IDS 210,119,20,140 Jan 10 14:13:30 210,119,10,2 8 210,119,20,131 0 0
25,000000 Snort-2,1,1 IDS 210,119,20,140 Jan 10 14:13:30 210,119,10,2 8 210,119,20,130 0 0
8,333334 Snort-2,1,1 IDS 210,119,20,140 Jan 10 14:13:30 210,119,10,2 2265 210,119,20,132 161 161
준비
CAP
NUM

Tool development: Safelite/Safeview

- Hierarchical Attack Representation Models

Report Summary

Radar Chart



Report information

METRICS SUMMARY

	Name	Value
1	Total number of vulnerabilities:	63
2	Number of hosts	63
3	Risk of HARM	29
4	Cost of attack	5
5	Mean of attack path lengths	2.5
6	Mode of attack path lengths	3
7	Standard Deviation of attack path lengths	0.7071067811865476
8	Shortest attack path length	2

THE TOP 10 MOST VULNERABLE HOSTS

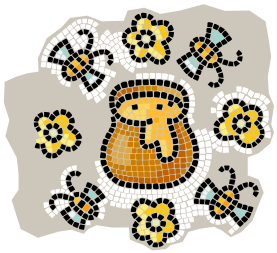
	Name	Value
1	FinanceFileServer	13
2	WebServer	5
3	132.181.14.114	2
4	132.181.14.139	2
5	132.181.14.80	2
6	132.181.14.116	2
7	132.181.14.115	2
8	132.181.14.158	2
9	132.181.14.119	2

GraMSec

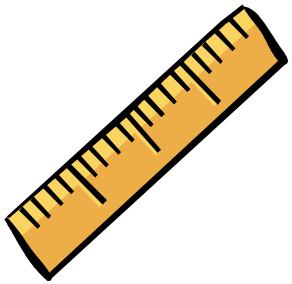
- The Third International Workshop on Graphical Models for Security
  - Lisbon, Portugal - June 27, 2016
  - Co-located with CSF 2016
- Chairs
  - Barbara Kordy, INSA Rennes, IRISA, FR (general chair)
  - Mathias Ekstedt, KTH Royal Institute of Technology, SE (PC co-chair)
  - Dong Seong Kim, University of Canterbury, NZ (PC co-chair)
- GraMSec 2017 with CSF 2017, Aug. 21, 2017, CA, USA
  - http://www.gramsec.uni.lu/

Cybersecurity Assessment via 3Ms

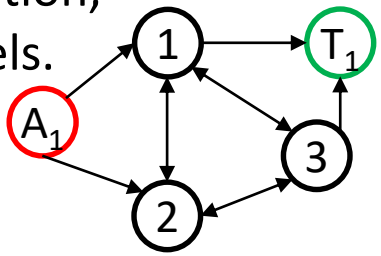
- To assess security, one requires 3**M**s:
  1. Security **M**easures
     - To **collecte** required information.
     - Vulnerabilities, reachability, *etc.*

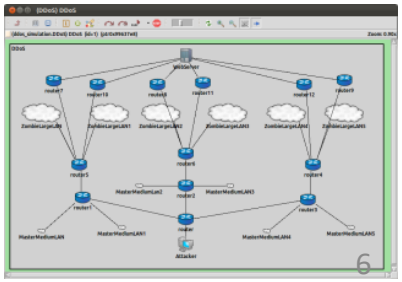


  2. Security **M**etrics
     - To **represent** the analysis of security
     - Attack-defense scenarios, prob. of attack success

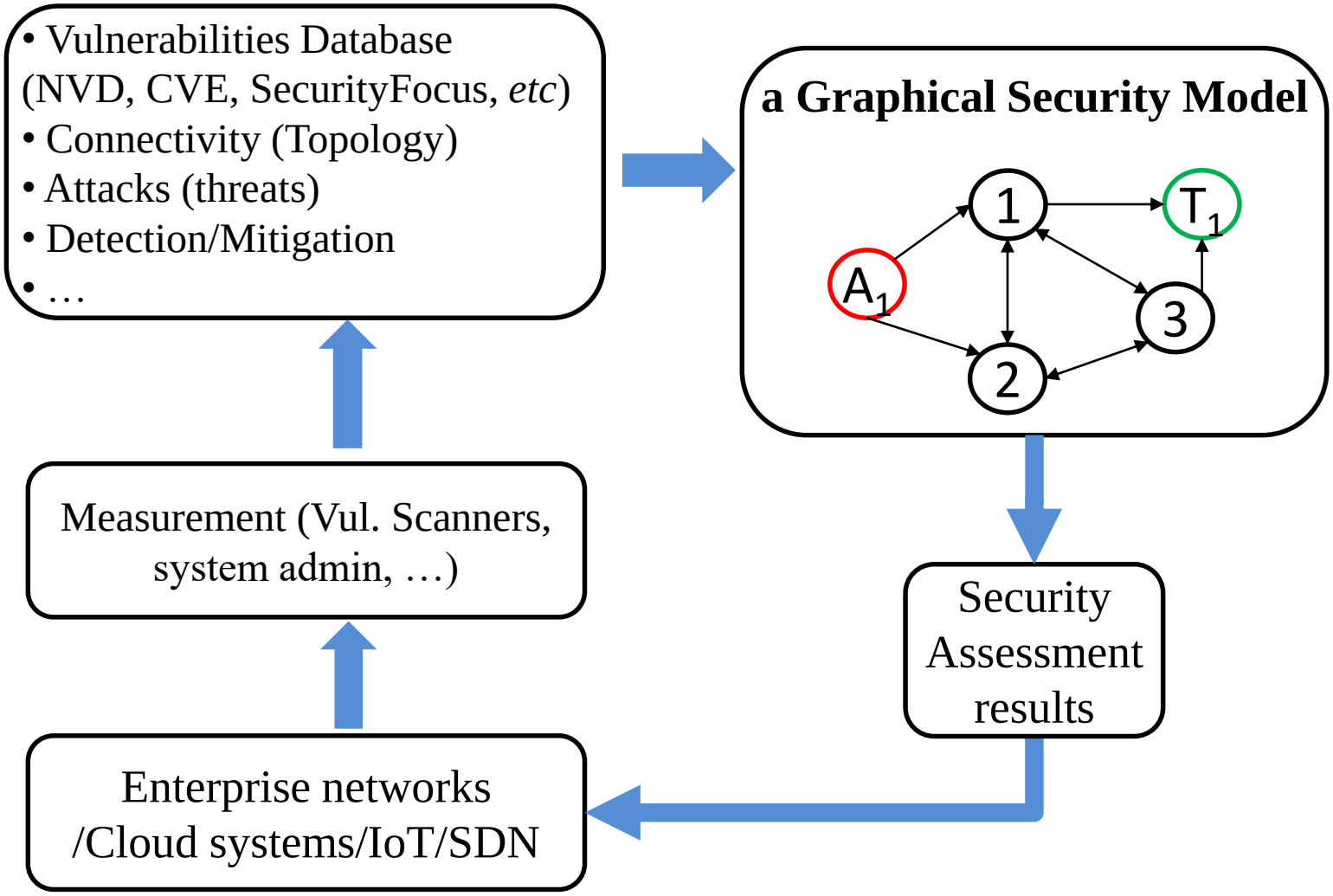


  3. Graphical Security **M**odels (for short, Security Models)
     - To **capture** security using simulation, analytic models, or hybrid models.





An Example of Graphical Security Models

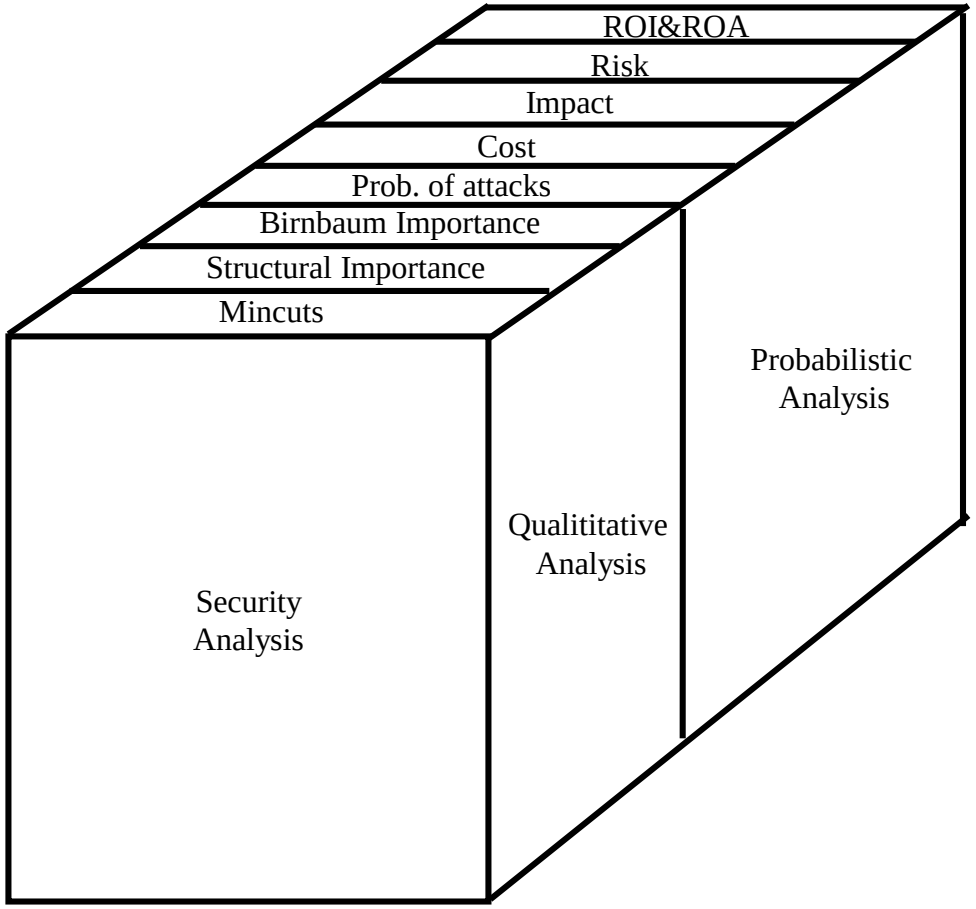


Security Measures

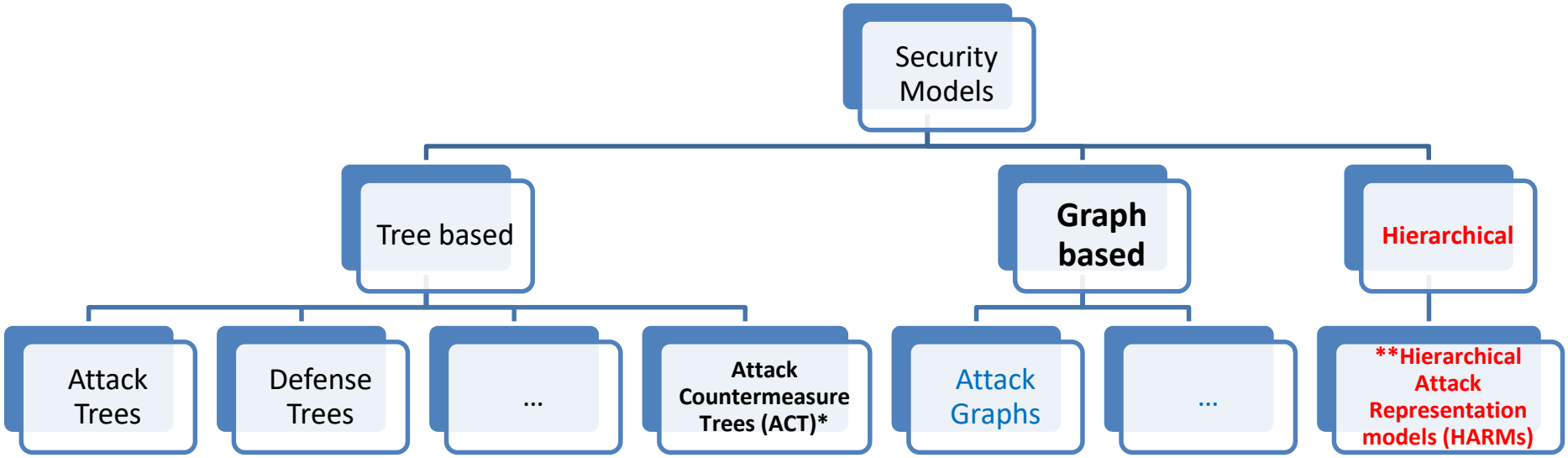
- Vulnerabilities and their scores
  - Common Vulnerability and Exposures (CVE)
  - Common Vulnerability Scoring System (CVSS) Base Score (BS): e.g., 9 out of 10.
- Reachability
  - Nmap (network mapping)
  - Network Configurations (e.g., access control by firewalls)
- Mitigation methods
  - Detection (Intrusion Detection, Vulnerability Identification, …)
  - Countermeasure (Patch, firewall rules changes, …)
  - Moving target defenses
- …

Security Metrics:
Qualitative vs Quantitative

- Qualitative
  - Mincuts (Attack (countermeasure) scenarios))
  - Importance Measures
  - …
- Quantitative
  - Probability of Attacks, Detection,…
  - Adversary's viewpoint
    - Cost of Attack
    - Return on Attack (ROA)
    - …
  - Defender's Viewpoint
    - Risk = Prob.*Impact
    - Security Investment Cost
    - Return on Investment (ROI)
    - …

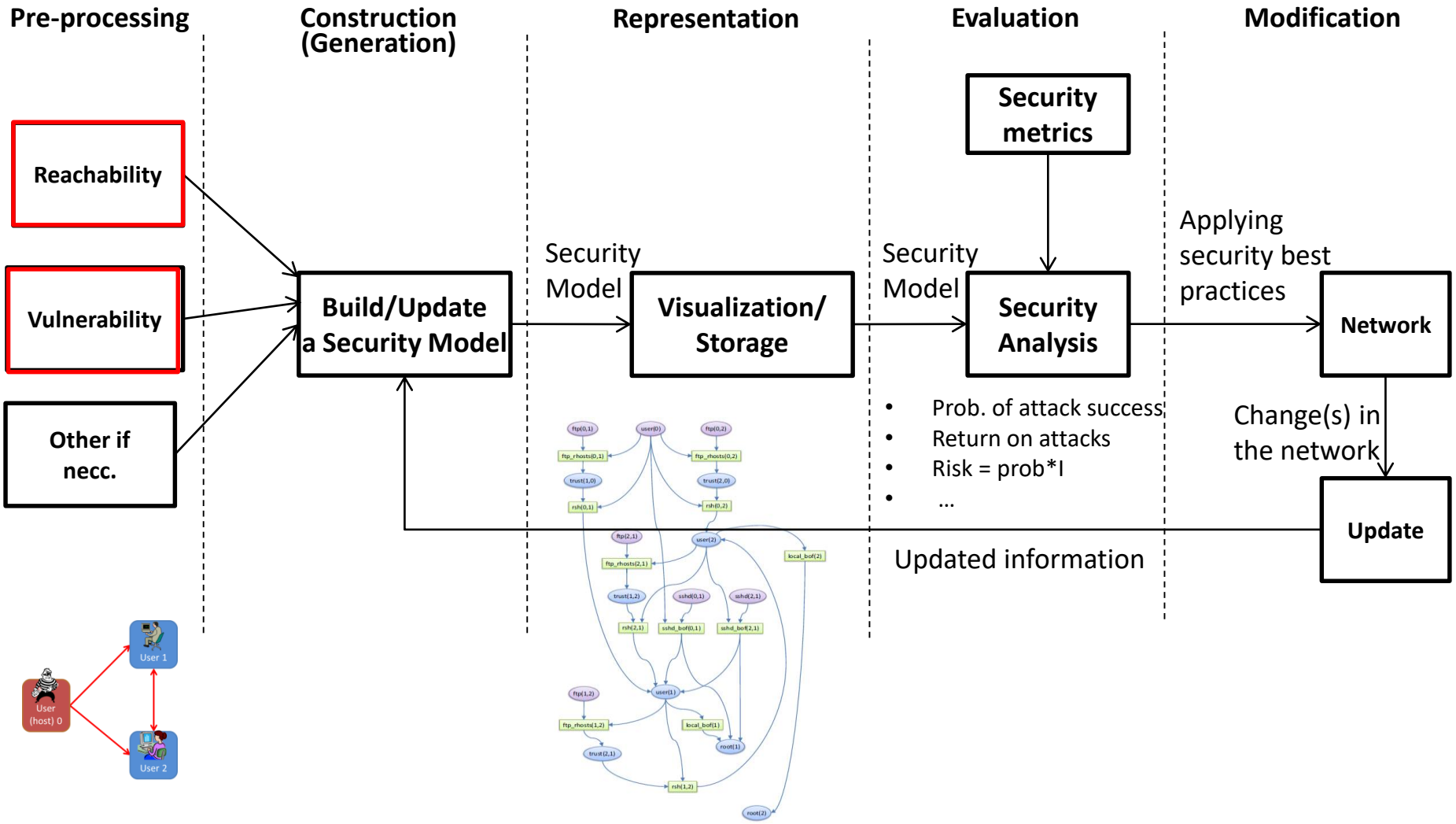


Graphical Security Models: A Classification



- *A. Roy, Dong Seong Kim, Kishor S. Trivedi: **Attack countermeasure trees (ACT)**: towards unifying the constructs of attack and defense trees. ***Security and Communication Networks*** 5(8): 929-943 (2012)
- *A. Roy, Dong Seong Kim, Kishor S. Trivedi: Scalable optimal countermeasure selection using implicit enumeration on attack countermeasure trees. in Proc. DSN 2012
- **J. Hong, Dong Seong Kim, "Assessing the Effectiveness of Moving Target Defense using Security Models" Transactions of Dependable and Secure Computing (TDSC), IEEE, vol.13, no. 2, pp. 163-177, Mar 2016 - Link

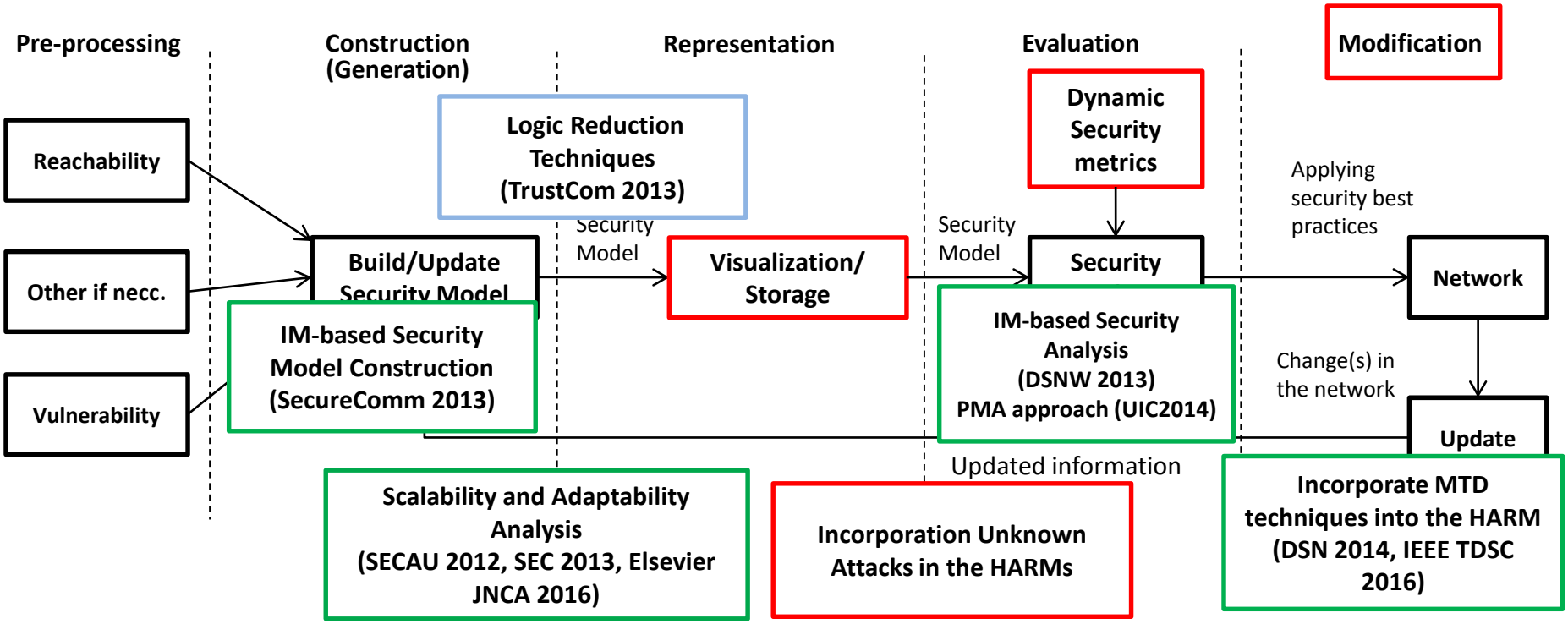
Graphical Security Models: a lifecycle



Research Domains

- Moving Target Defenses
- Cloud computing
- Enterprise Networks (SME, Large.)
  - Risk and Availability evaluation
- Internet of Things
- Software defined networking

Recent Results for Enterprise nets/Cloud

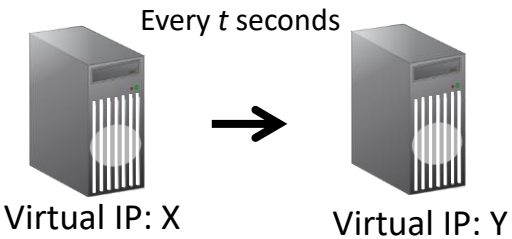


SECAU 2012: ``HARMs: Hierarchical Attack Representation Models for Network Security Analysis"
SEC 2013: ``Performance analysis of scalable attack representation models"
TrustCom 2013: ``Scalable Attack Representation Model Using Logic Reduction Techniques"
DSNW 2013: ``Scalable Security Analysis in Hierarchical Attack Representation Model using Centrality Measures"
SecureComm 2013: ``Scalable Security Model Generation and Analysis using k-importance Measure"
DSN 2014: ``Scalable Security Models for Assessing Effectiveness of Moving Target Defenses"
DSNW 2014: ``What Vulnerability Do We Need To Patch First?"
UIC 2014: ``Scalable Security Analysis using Partition and Merge Approach in an Infrastructure as a Service Cloud"
Elsevier JNCA2016: ``Towards Scalable Security Analysis using Multi-Layered Security Models"
IEEE TDSC 2016: ``Assessing the Effectiveness of Moving Target Defense using Security Models"

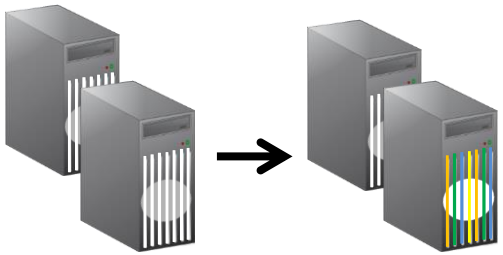
Evaluation of the Effectiveness of Moving Target Defenses

- Moving Target Defense (MTD) techniques continuously **change** the attack surface to thwart attacks.
- Changes in the networked system by deploying MTD techniques are captured via the **HARM**.
- MTD techniques are divided into three categories:

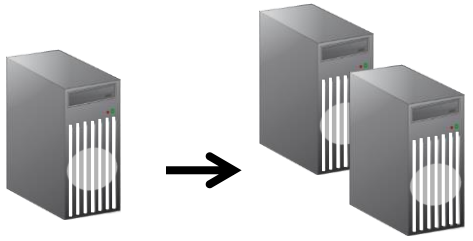
Shuffle



Diversity



Redundancy



- Evaluation of the Effectiveness of MTD techniques
  - **J Hong, D Kim,** "Assessing the Effectiveness of Moving Target Defenses using Security Models",
  - **IEEE TDSC 2016**

Evaluation of the Effectiveness of Moving Target Defenses: extensions

- A classification of MTD at layers
- A combination of
  - Two of MTD
  - Three
- Take into account other metrics (e.g., system performance, user-perceived availability)
- …

Security Risk Modeling and Assessment of Cloud Computing

- On-going research project
- Funded by the Qatar National Research Fund (2016-2018)
- Objectives
  - Security threat/countermeasure classification
  - Graphical Security modeling and analysis
  - Defense and mitigation mechanisms
  - Security framework and tools development

Model based Evaluation of Security Risk and Capacity oriented Availability (CoA)

- Why security and availability need to be taken into account together
- Examples:
  - patch management (when patching, the system is down affecting the availability; but patching may improve security);
  - increasing redundancy may increase both the availability and the attack surface
- How to balance between security risk and availability

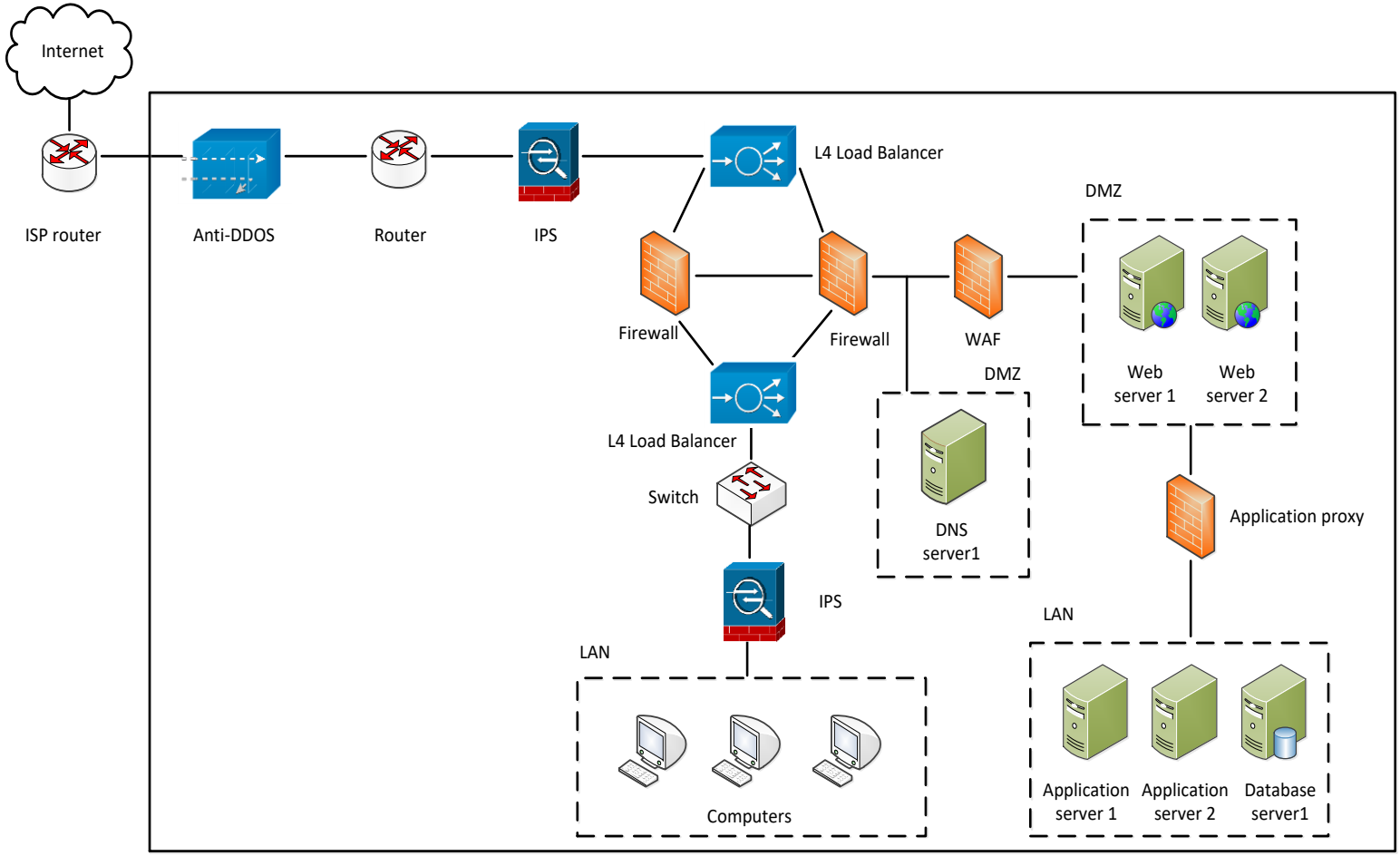
Related work summary

- Security modeling using graphical security models
  - Attack countermeasure trees [Roy et al. 2011 SCN]
  - Attack countermeasure trees [Roy et al. 2012 DSN]
  - Attack graphs [Albanese et al. 2012 DSN]
  - HARM [Hong et al. 2015 DSN]
- Availability modeling using stochastic models
  - Availability modeling and analysis [K Trivedi, DS Kim et al. 2009 PRDC]
  - Performance and dependability modeling with Mobius [Gaonkar et al. 2009 SIGMETRICS]
  - Probability and statistics [Trivedi 2008 John Wiley & Sons]
  - System availability assessment [Trivedi et al. 2013 ASMBI]
- A few research on security and availability/performance
  - In sensor nets, crypto vs. available resources (power consumption, performance degradation…)
  - Dependability and Security models [Trivedi et al. 2009 DRCN]
  - Mobius 2.3 for dependability and security evaluation [Courtney et al. 2009 DSN]
  - Security in terms of availability
    - SITAR [Madan et al. 2004 DSN-PDS]
    - SCIT [Anantha et al. 2009 DEPEND]
    - ITS using standby clusters [Aung et al. 2005]
    - Intrusion tolerant database system [Peng Liu et al., ESORICS 2006]
    - Self-healing MANETS [Ann Tai et al. 2010 DSN]

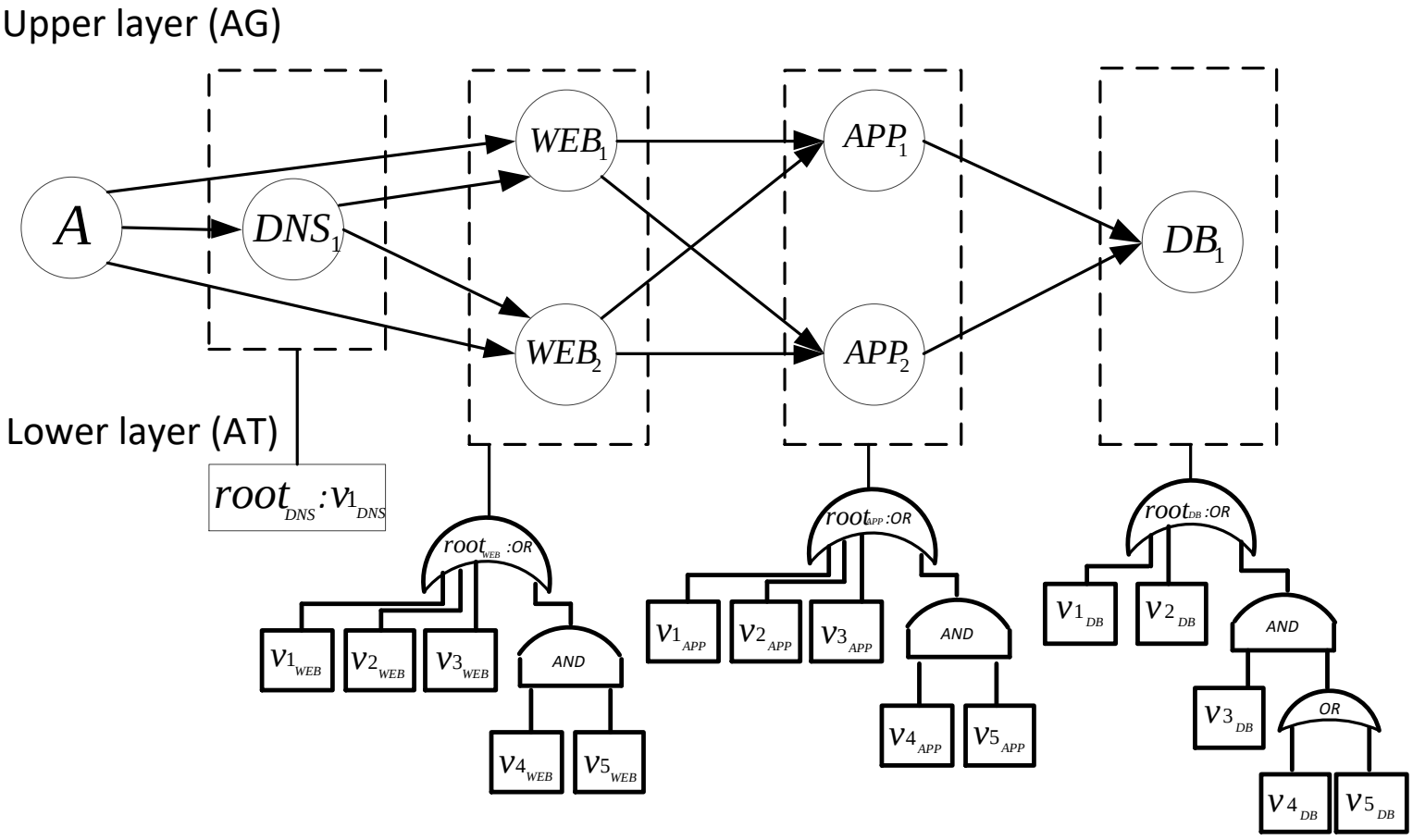
Approach

- To build a graphical security model and an availability model separately
  - Security models using AGs and HARMs
  - Availability models using Stochastic Reward Nets
- To consider security and availability together (not a composite model but interpret them using security/availability metrics)
- Benefit: find sub-optimal operation points to meet a certain level of security and availability requirements

An example: enterprise network (1 DNS, 2 Web, 2 APP, 1 DB)

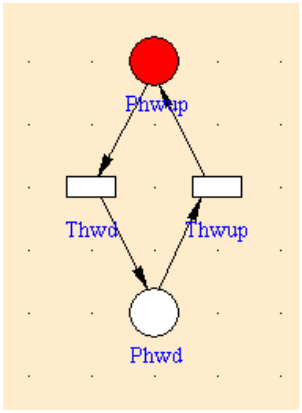


A HARM of the example network (1 DNS, 2 Web, 2 APP, 1 DB server)

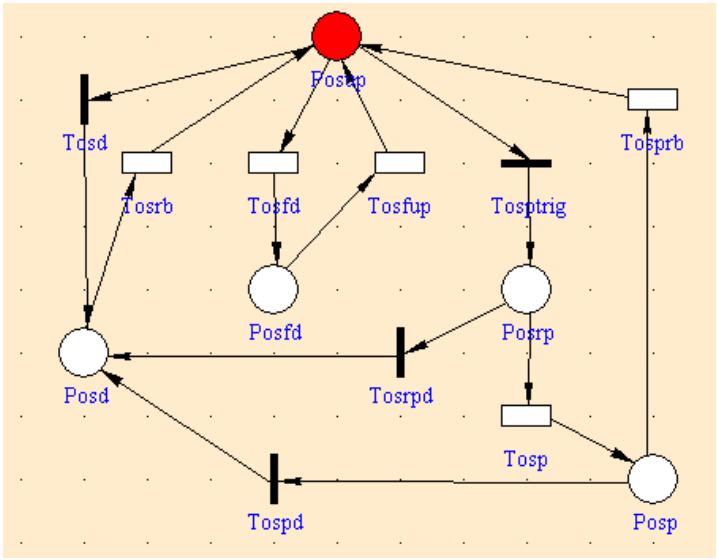


SRN models of a DNS server

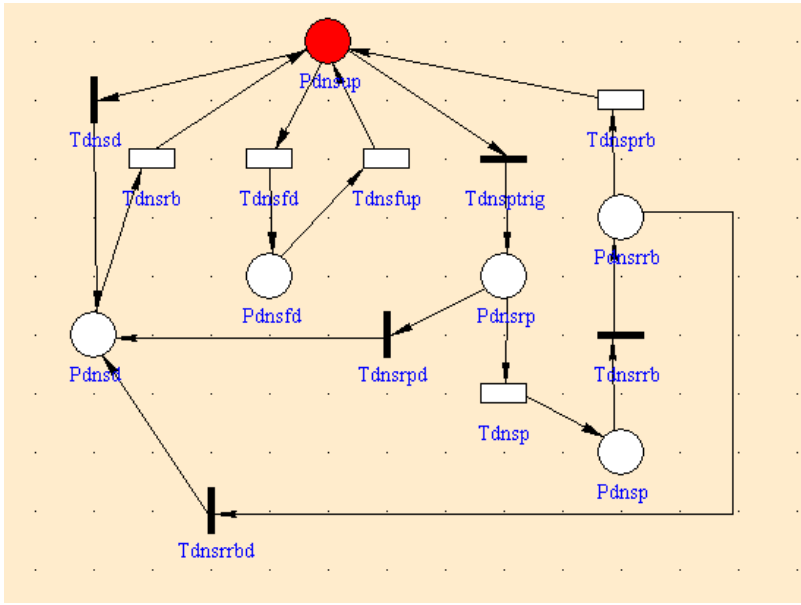
Hardware



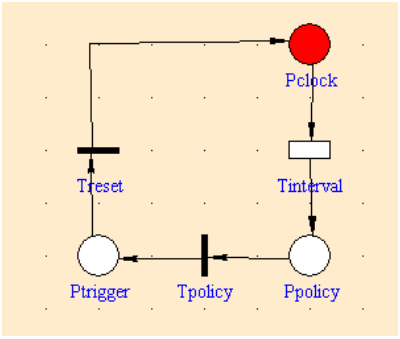
OS



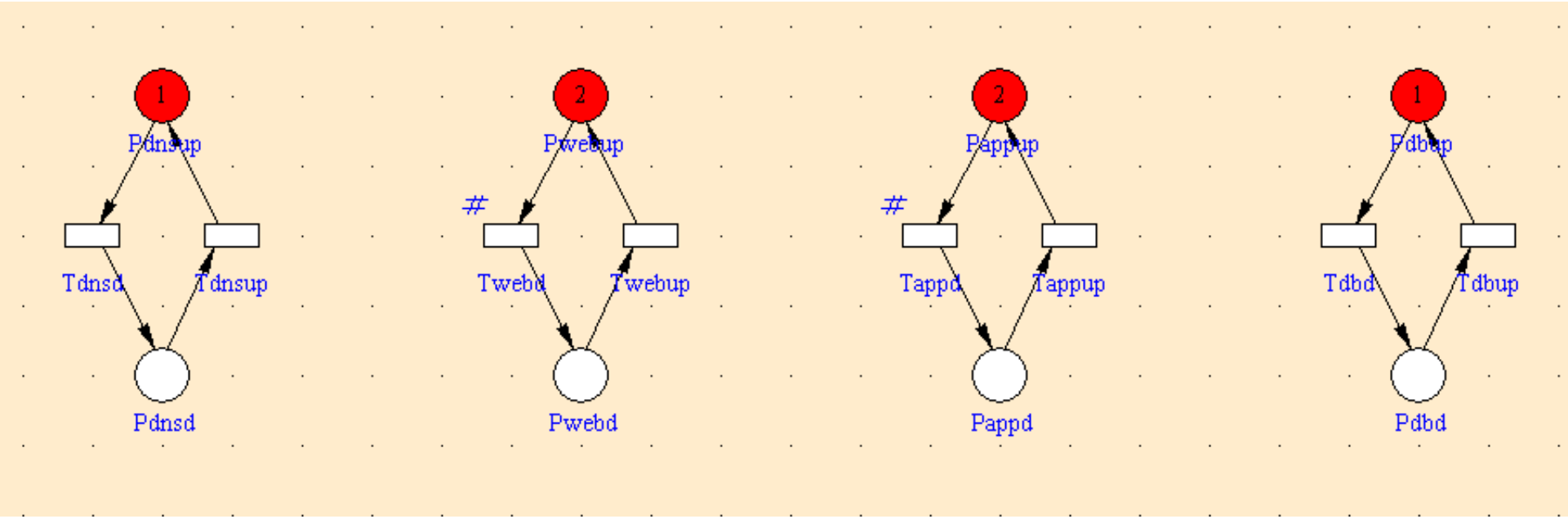
DNS app



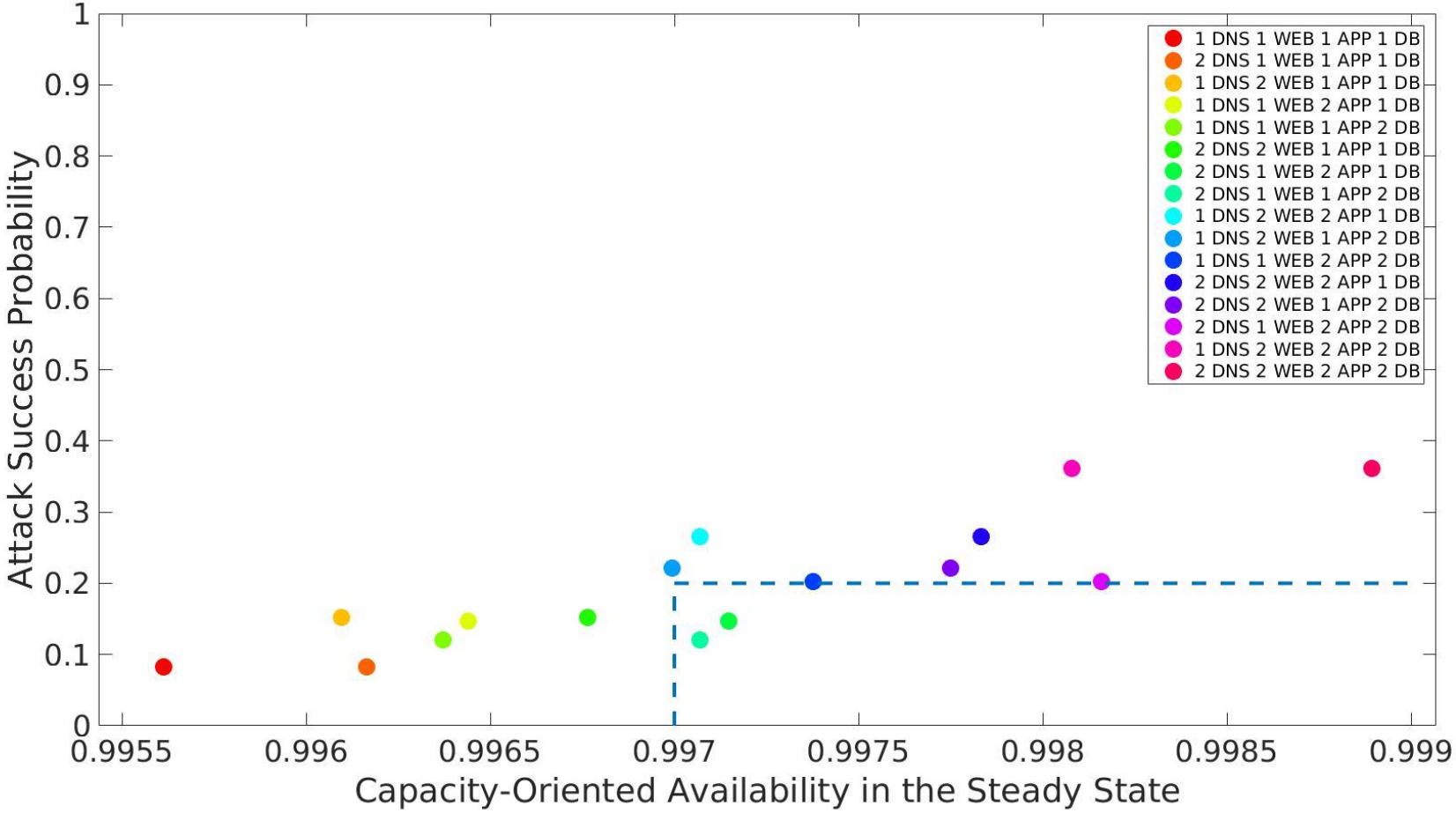
a Clock



A SRN model of the example network (1 DNS, 2 Web, 2 APP, 1 DB server)

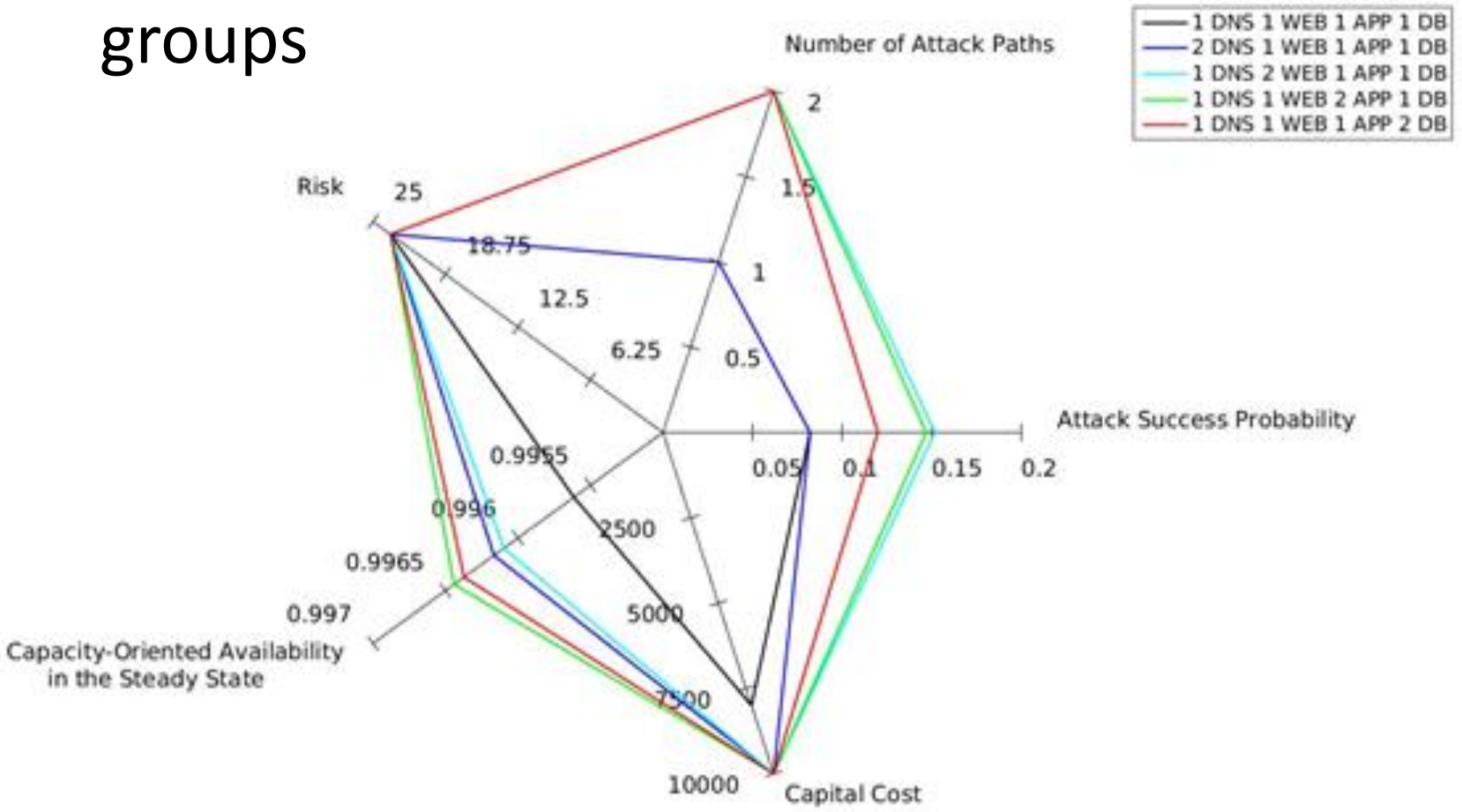


Capacity oriented availability analysis vs. Attack Success Probability



A Radar chart of Security/availability metrics

- Radar chart and comparison in different groups



Graphical Security Models for IoT

- Problems
  - Three types of vulnerabilities: known, zero-day, forever
  - Heterogeneity
  - mobility
- Proposed ideas
  - A Security analysis framework
  - Software defined IoT (proactive, reactive reconfiguration)
  - Security optimization

Other on-going research

- Security Models and Metrics for Dynamic Networks
- Security Assessment as Service using the Cloud
- Security Modeling and Analysis of Software Defined Networking
- Reliability and Resilience Analysis of Smart Grid

Thank you!

Hagley Park, Christchurch,
New Zealand

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