Security Metrics and Risk Analysis for Enterprise Systems

August 2017
GramSec

Anoop Singhal
Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD
USA

Outline

- Challenges for Cyber Security Risk Analysis
- NIST Cyber Security Framework
- Attack Graphs and Tools for generating Attack Graphs
- Quantifying Security Analysis
- Mission Impact Analysis
- Conclusions

National Institute of Standards and Technology

About NIST

- Part of the U.S. Department of Commerce
  - Charter for public and private sectors
  - Non-regulatory
- NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.
  - 3,000 employees
  - 2,700 guest researchers
  - 1,300 field staff in partner organizations
  - Gaithersburg, MD and Boulder, CO
- Role in cybersecurity began in 1972 with the development of the Data Encryption Standard

NIST Priority


Advanced Manufacturing


IT and Cybersecurity


Healthcare


Forensic Science


Disaster Resilience


Cyber-physical Systems


Advanced Communications

NIST Computer Security Division

- National Institute of Standards and Technology
- Information Technology Lab
- Computer Security Division
  - http://csrc.nist.gov
  - Cryptography standards
  - Guidelines for Federal Agencies in the areas such as Mobile Device Security, Web Security and so on.
  - Research in the area of Cloud Computing, Biometrics, Network Security and so on.
  - About 60-70 computer scientists

Enterprise Security Management

- Networks are getting large and complex
- Vulnerabilities in software are constantly discovered
- Network Security Management is a challenging task
- Even a small network can have numerous attack paths

Enterprise Security Management

- Currently, security management is more of an art and not a science
- System administrators operate by instinct and learned experience
- There is no objective way of measuring the security risk for an enterprise
- “If I change this network configuration setting will my network become more or less secure?”

NIST Cyber Security Risk Management

- Identify
  - What are the assets?
  - How is the network configured?
- Protect
  - Access Control
  - Authentication
  - Data Security
- Detect
  - Intrusion Detection Systems (IDS)
  - Security Continuous Monitoring

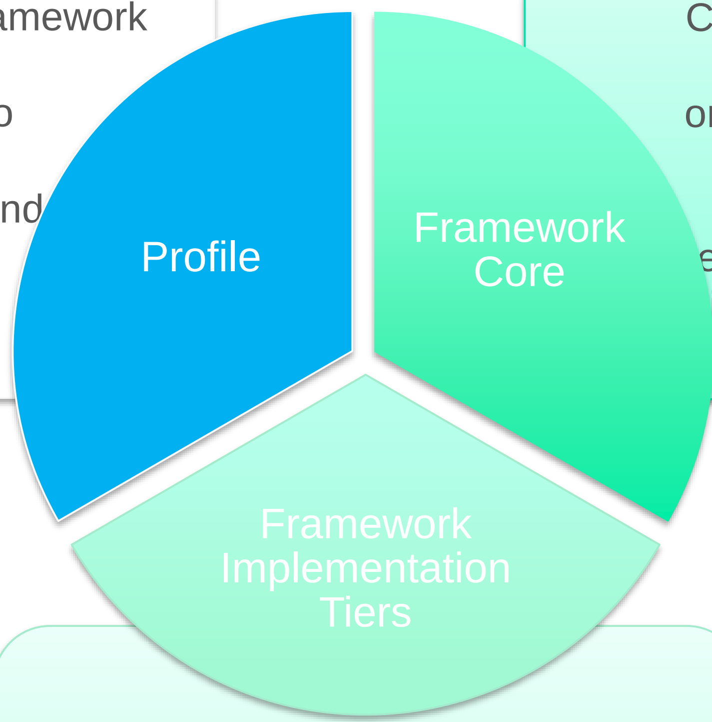
NIST Cyber Security Risk Management

- Respond
  - Response Planning
  - Analysis
  - Mitigation
- Recover
  - Timely recovery to normal operations
  - Recovery Planning
- NIST Special Publication 800-39 “Managing Information System Risk”, March 2011

NIST Cybersecurity Framework Components

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs



Cybersecurity activities and informative references, organized around particular outcomes

es communication of cyber isk across an organization

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Core

Cybersecurity Framework Component

Function	Category	Category Unique ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-5: Resilience requirements to	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3

Improving a Cybersecurity Program

- **Step 1: Prioritize and Scope**
  - Identifies its business/mission objectives and high level organization priorities
- **Step 2: Orient**
  - The organization identifies systems, assets, threats and vulnerabilities
- **Step 3: Create a Current Profile**
  - Create a profile indicating which Category and Subcategory from the Framework Core are currently being used.
- **Step 4:Conduct a Risk Assessment**
  - The organization analyzes the operational environment in order to determine the impact of an attack on the organization. It can be guided by the organization's overall risk management process.
- **Step 5:Create a Target Profile**
  - The organization creates a Target Profile that focusses on the assessment of the Framework Categories and Subcategories for the desired outcome.

Improving a Cybersecurity Program

- **Step 6: Determine, Analyze and Prioritize Gaps**
  - The organization compares the Current Profile and the Target Profile to determine gaps. It then creates an action plan to address those gaps.
- **Step 7: Implement Action Plan**
  - The organization determines which actions to take to address the gaps.
  - It monitors the cybersecurity practices against the target profile.

Key Attributes

- **It's a framework, not a prescription**
  - It provides a common language and systematic methodology for managing cyber risk
  - It is meant to be adapted
  - It does not tell a company *how* much cyber risk is tolerable, nor does it claim to provide "the one and only" formula for cybersecurity
  - Having a common lexicon to enable action across a very diverse set of stakeholders will enable the best practices of elite companies to become standard practices for everyone

- **The framework is a living document**
  - It is intended to be updated over time as stakeholders learn from implementation, and as technology and risks change
  - That's one reason why the framework focuses on questions an organization needs to ask itself to manage its risk. While practices, technology, and standards will change over time—principals will not

Resources

Where to Learn More and Stay Current

The National Institute of Standards and Technology Web site is available at http://www.nist.gov

NIST Computer Security Division Computer Security Resource Center is available at http://csrc.nist.gov/

The *Framework for Improving Critical Infrastructure Cybersecurity* and related news and information are available at www.nist.gov/cyberframework

For additional Framework info and help
cyberframework@nist.gov

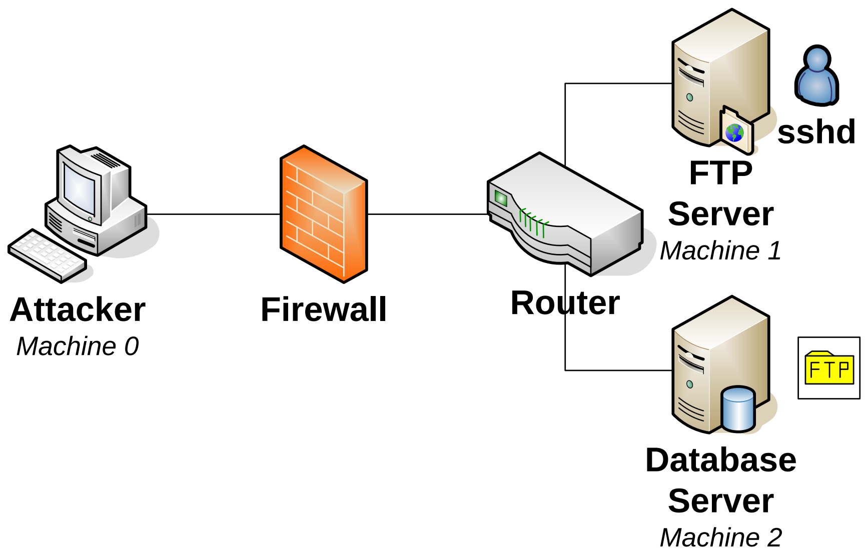
Challenges in Security

- Typical issues addressed in the literature
  - How can a database server be secured from intruders?
  - How do I stop an ongoing intrusion?
- Notice that they all have a qualitative nature
- Better questions to ask:
  - How secure is the database server in a given network configuration?
  - How much security does a new configuration provide?
  - How can I plan on security investments so it provides a certain amount of security?
- For this we need a system security modeling and analysis tool

What is an Attack Graph

- A model for
  - How an attacker can *combine* vulnerabilities to stage an attack such as a data breach
  - *Dependencies* among vulnerabilities

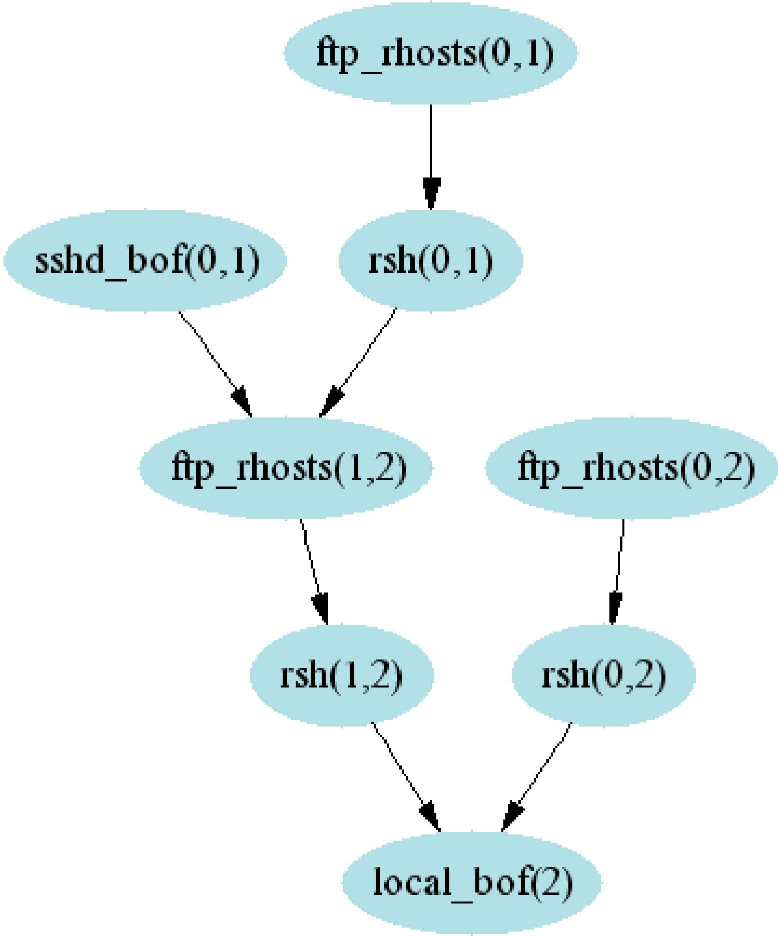
Attack Graph Example



Different Paths for the Attack

- *sshd_bof(0,1)* $\rightarrow$ *ftp_rhosts(1,2)* $\rightarrow$ *rsh(1,2)* $\rightarrow$ *local_bof(2)*
- *ftp_rhosts(0,1)* $\rightarrow$ *rsh(0,1)* $\rightarrow$ *ftp_rhosts(1,2)* $\rightarrow$ *rsh(1,2)* $\rightarrow$ *local_bof(2)*
- *ftp_rhosts(0,2)* $\rightarrow$ *rsh(0,2)* $\rightarrow$ *local_bof(2)*

Attack Graph from machine 0 to DB Server

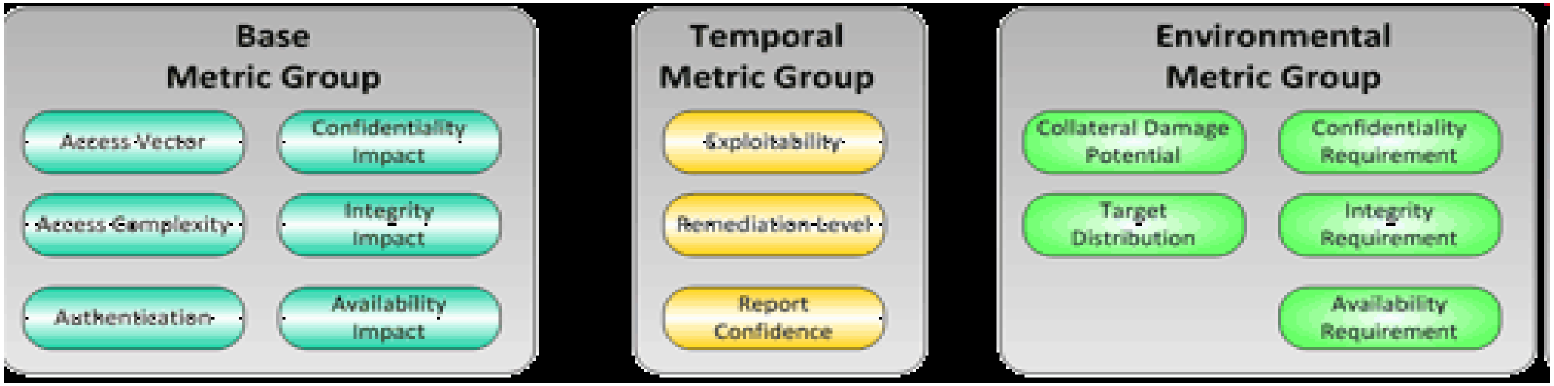


- Stands for *Common Vulnerability Scoring System*
- An open framework for communicating characteristics and impacts of IT vulnerabilities
- Consists three metric groups: *Base, Temporal,* and *Environmental*

CVSS (Cont'd)

- Base metric：constant over time and with user environments
- Temporal metric：change over time but constant with user environment
- Environmental metric：unique to user environment

CVSS (Cont'd)



CVSS metric groups

- Each metric group has sub-matricies
- Each metric group has a score associated with it
- Score is in the range 0 to 10

Base Score

Base Score = Function(Impact, Exploitability)

Impact = 10.41 * (1-(1-ConImp)*(1-IntImp)*(1-AvailImpact))

Exploitability = 20*AccessV*AccessComp*Authentication

Base Score Example CVE-2002-0392

- Apache Chunked Encoding Memory Corruption

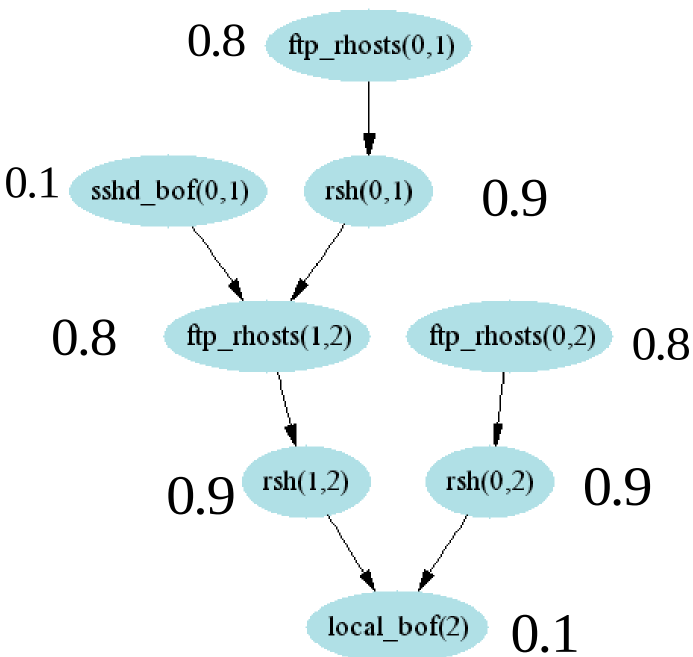
BASE METRIC	EVALUATION	SCORE
Access Vector	[Network]	(1.00)
Access Complex.	[Low]	(0.71)
Authentication	[None]	(0.704)
Availability Impact	[Complete]	(0.66)

Impact = 6.9

Exploitability = 10.0

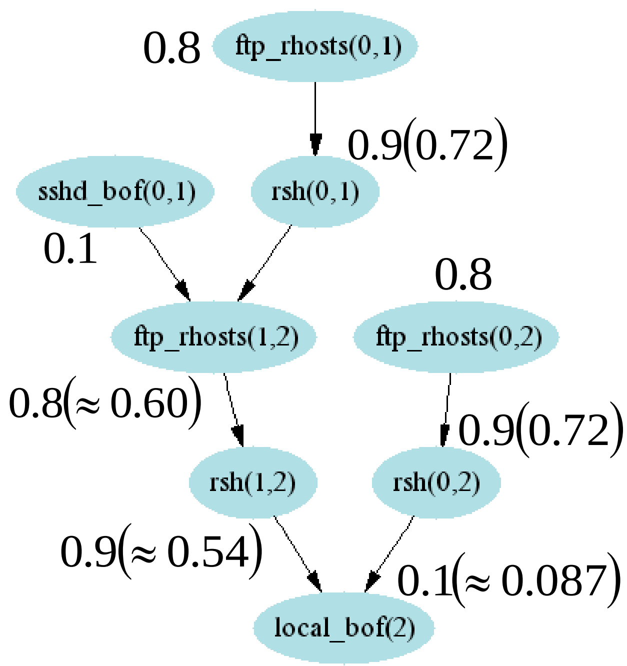
BaseScore = (7.8)

Attack Graph with Probabilities



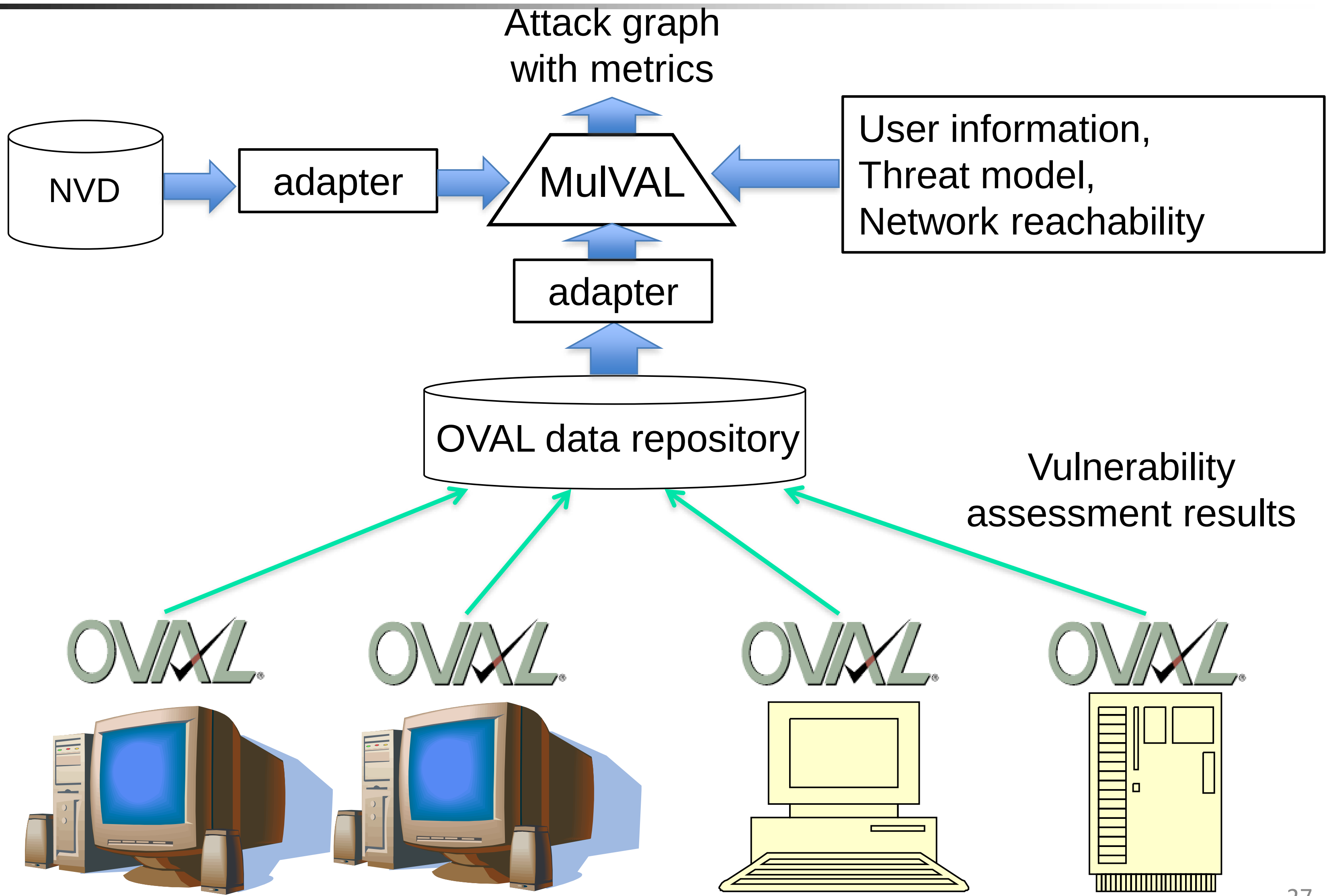
- Numbers are estimated probabilities of occurrence for individual exploits, based on their relative difficulty.
- The *ftp_rhosts* and *rsh* exploits take advantage of normal services in a clever way and do not require much attacker skill
- A bit more skill is required for *ftp_rhosts* in crafting a .rhost file.
- *sshd_bof* and *local_bof* are buffer-overflow attacks, which require more expertise.

Probabilities Propagated Through Attack Graph

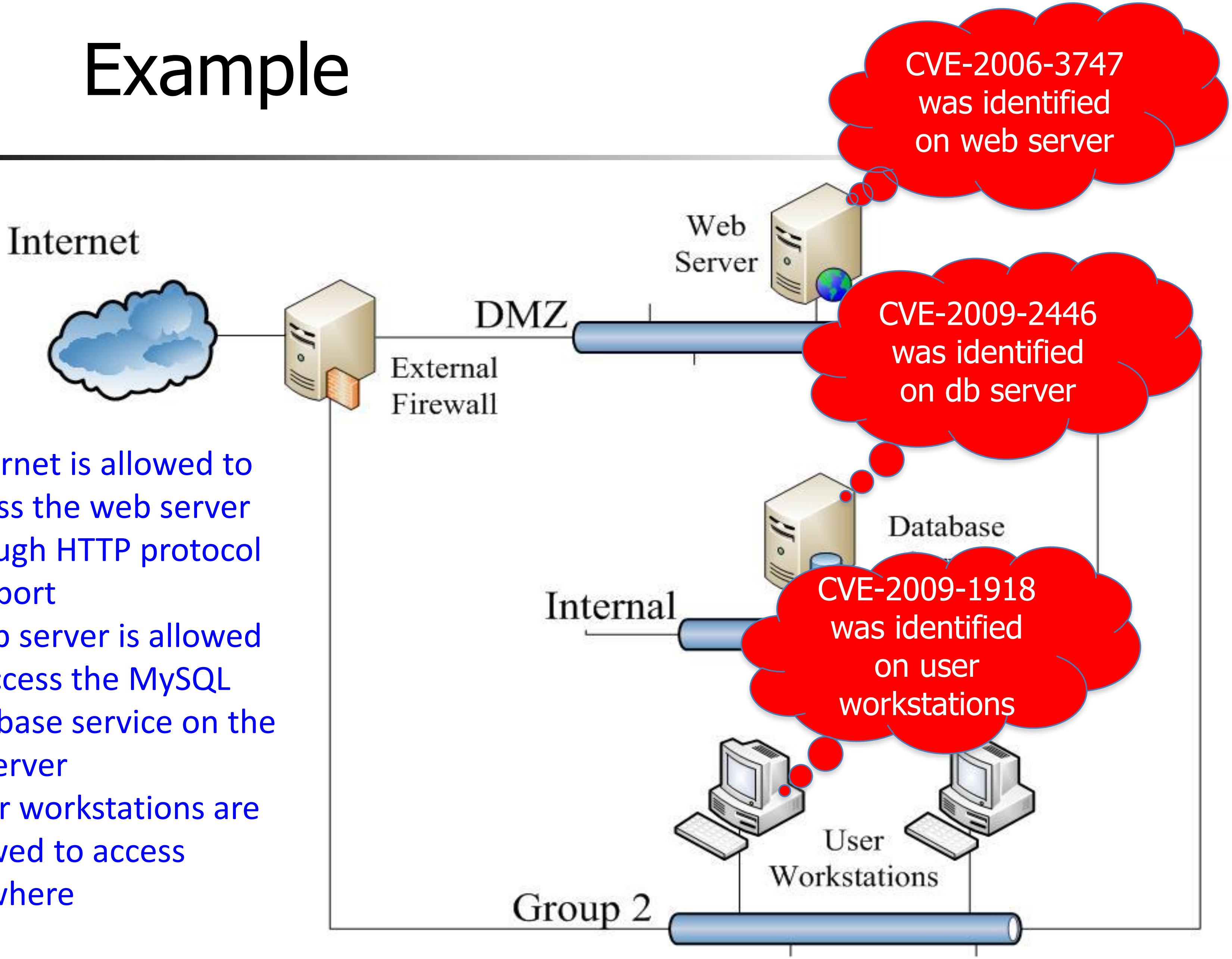


- When one exploit must follow another in a path, this means **both** are needed to eventually reach the goal, so their probabilities are multiplied: $p(A \text{ and } B) = p(A)p(B)$
- When a choice of paths is possible, **either** is sufficient for reaching the goal: $p(A \text{ or } B) = p(A) + p(B) - p(A)p(B)$.

MulVAL attack-graph tool-chain

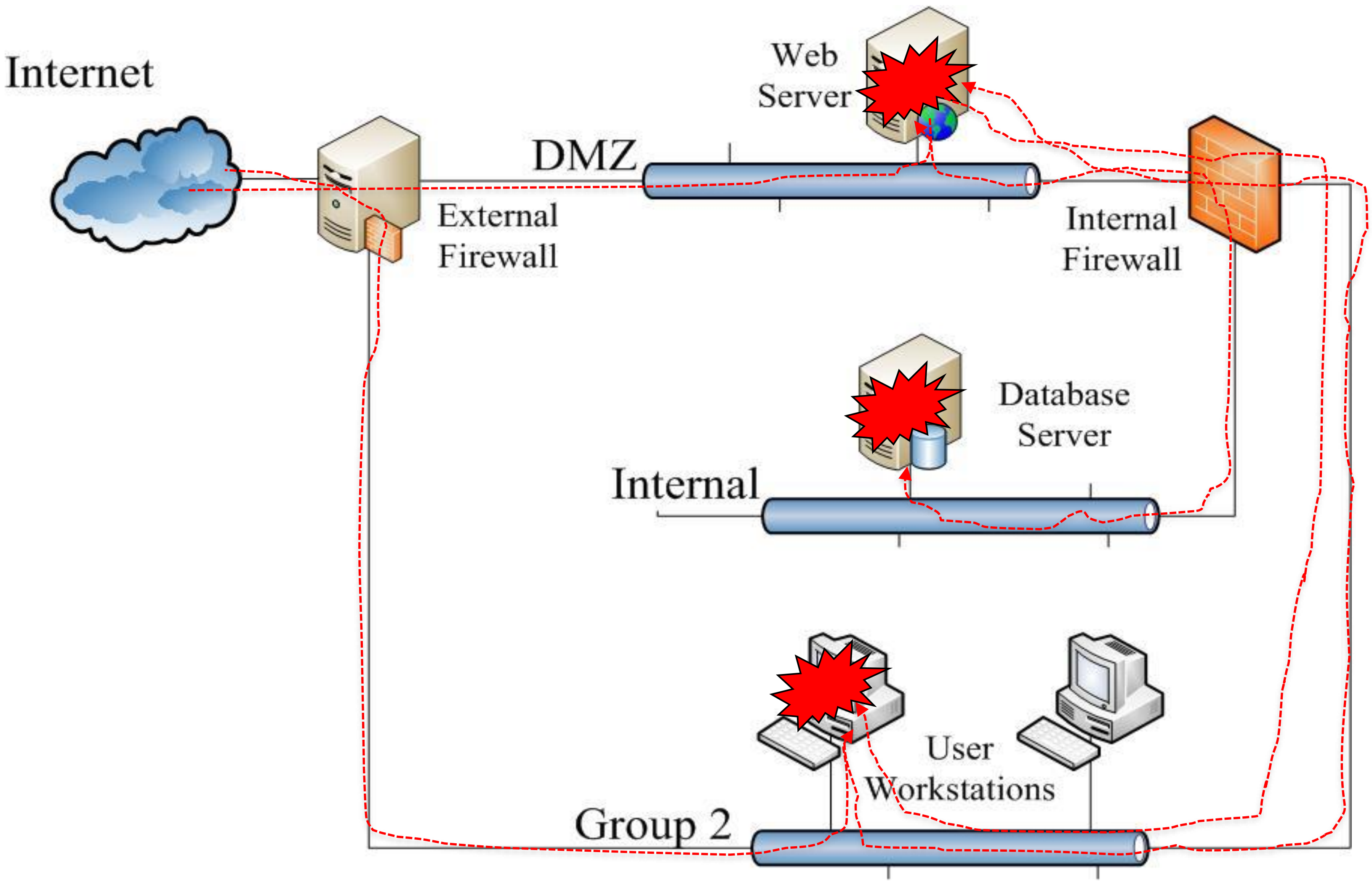


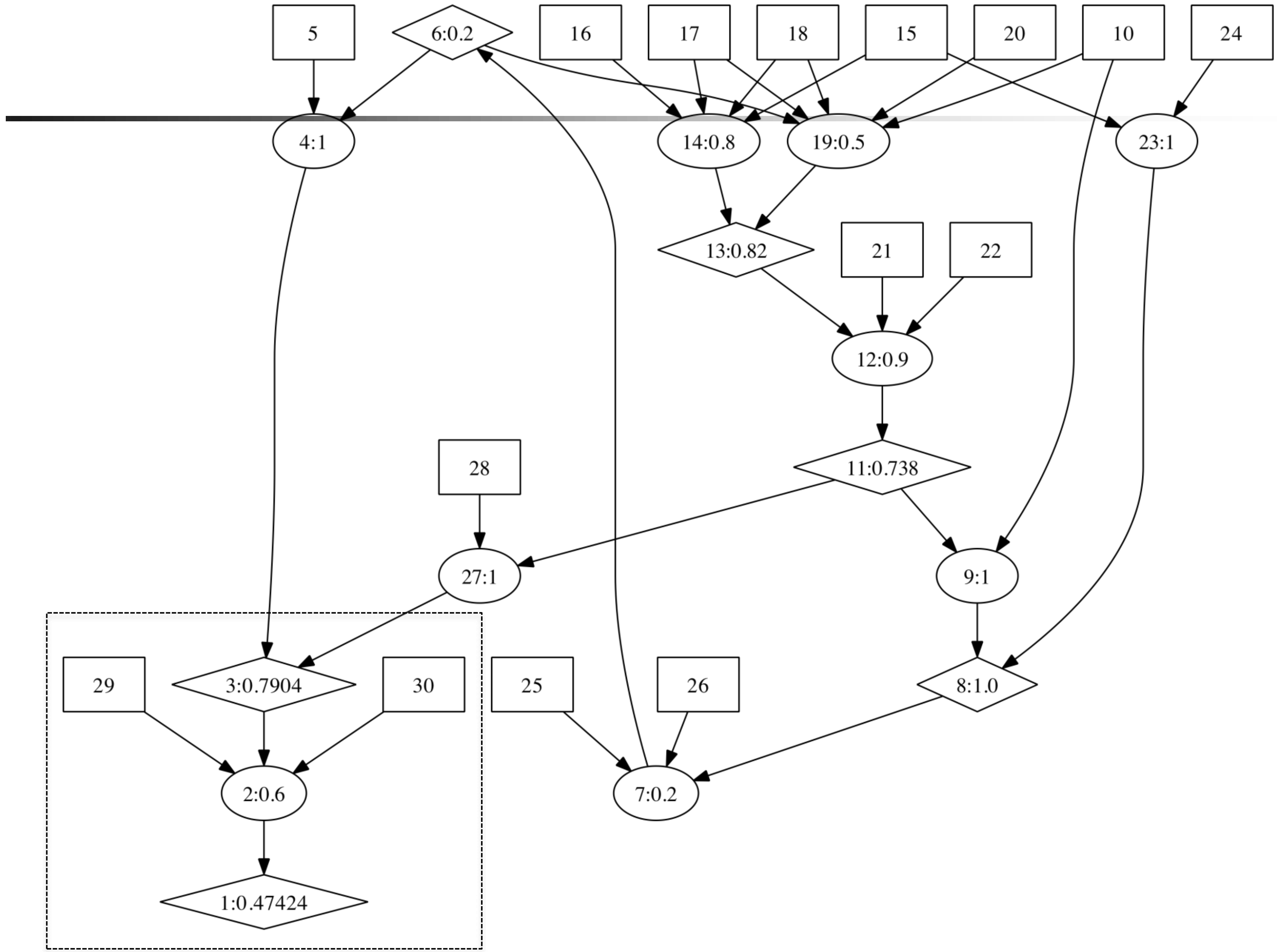
Example



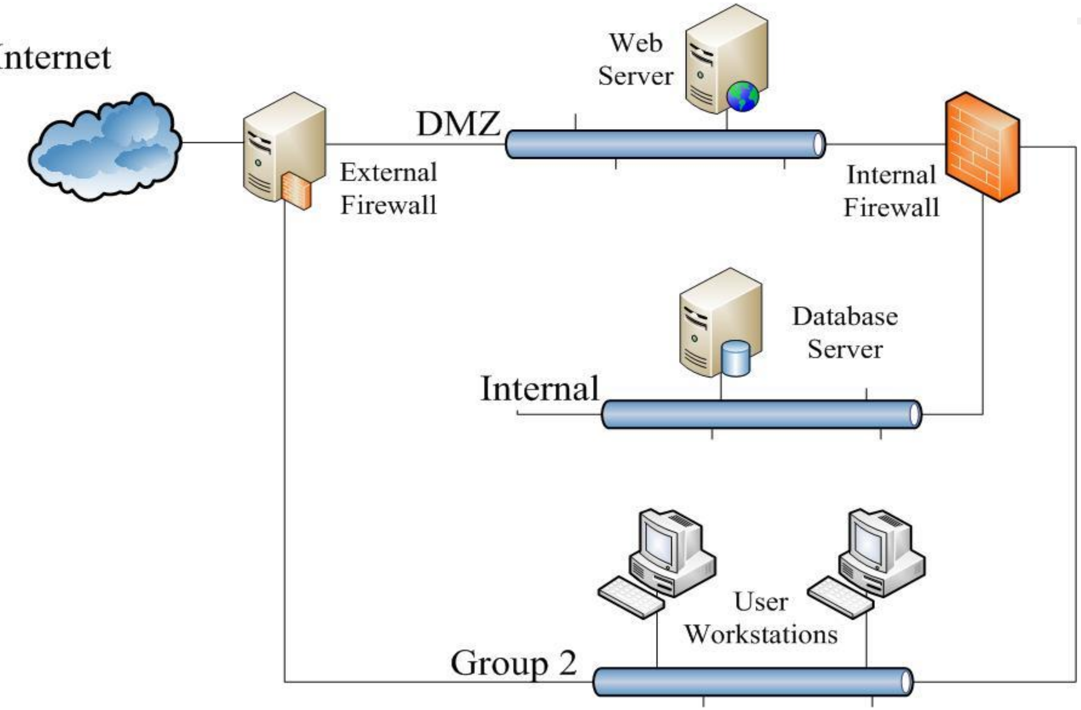
- Internet is allowed to access the web server through HTTP protocol and port
- Web server is allowed to access the MySQL database service on the db server
- User workstations are allowed to access anywhere

Possible attack paths




5
6:0.2
16
17
18
15
20
10
24
4:1
14:0.8
19:0.5
23:1
13:0.82
21
22
12:0.9
28
11:0.738
27:1
9:1
29
3:0.7904
30
25
26
8:1.0
2:0.6
7:0.2
1:0.47424

Result



execCode(dbServer,root): 0.47
execCode(webServer,apache): 0.2
execCode(WS,normalAccount): 0.74

Without Group2: execCode(dbServer,root): 0.12
execCode(webServer,apache): 0.2

Mission Impact Analysis in the Context of Cloud Computing

Cyber Resilience

Cyber resilience:

Capabilities to take cyber defense actions, including network and host hardening actions, quarantine actions, adaptive MTD (Moving Target Defense) and so on.

Mission Impact Assessment and Cyber Resilience

Overlooked Gap between Mission Impact Assessment and Cyber Resilience

- All existing cyber resilience techniques are unfortunately *not mission-centric*.
- Mission impact analysis becomes more complex in the cloud environment.
- Most mission impact assessment techniques are generally *one-dimensional*, without explicitly considering the dimension of service dependency.

Challenges to Bridge the Gap

- It is very challenging to develop a graphical model that can integrate mission dependency graphs and attack graphs

- A cloud environment gives rise to new challenges in bridging the gap

Existing Techniques

For ***mission impact assessment***:

- Different types of mission dependency graphs have been developed to associate missions with component tasks and assets
- However,
  - Dependency relations are usually very loose and not well defined
  - Possibility of multi-step attacks are not considered

Existing Techniques

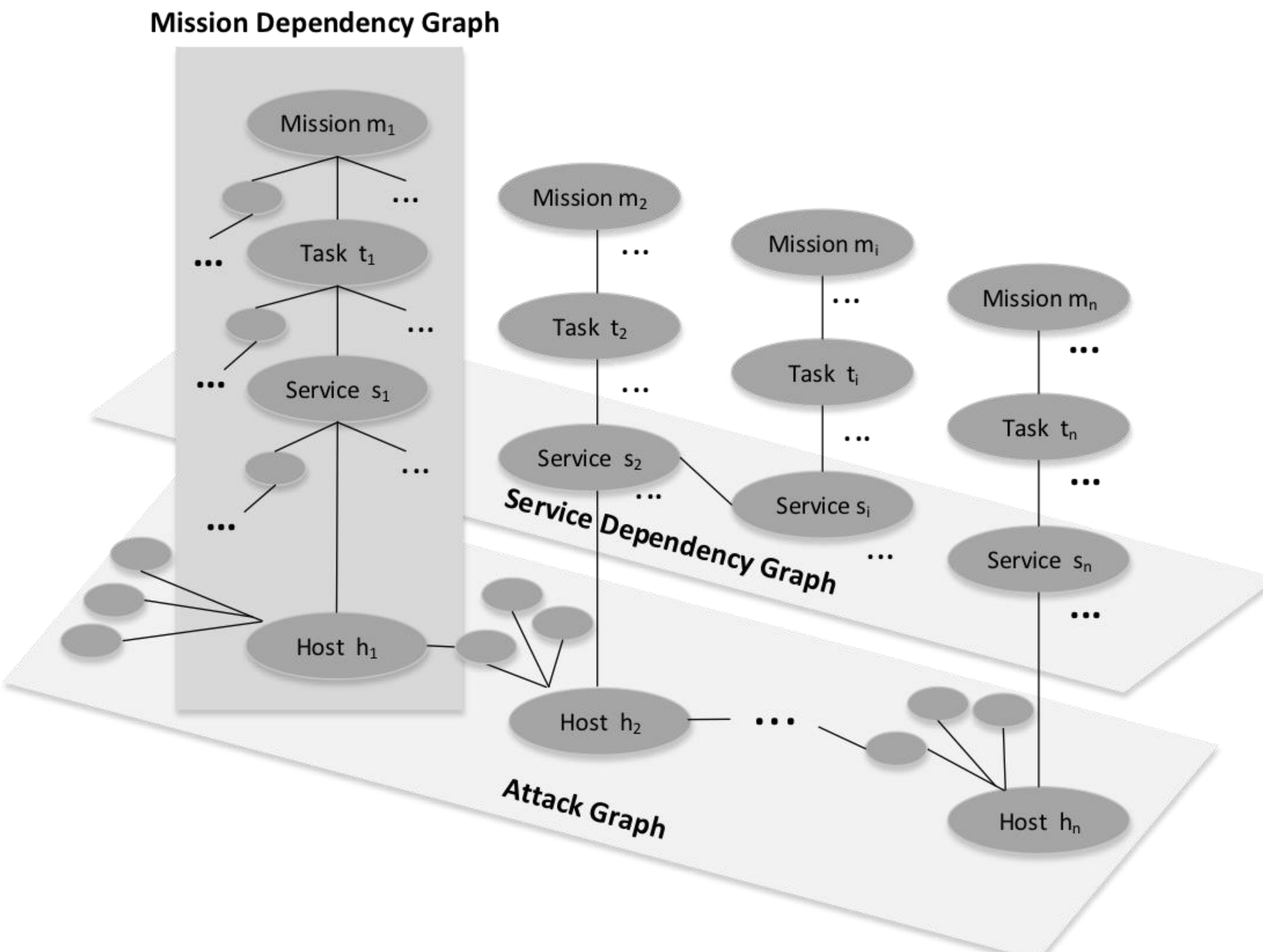
For ***cyber resilience***:

- Attack graphs have become mature techniques for analyzing the causality relationships between vulnerabilities and exploitations
- However,
  - It is not mission-centric
  - Traditional attack graphs do not consider potential attacks enabled by some special features of public *cloud environment* (e.g., virtual machine image sharing and virtual machine co-residency).

Our Approach

- Develop a logical graphical model
  - called *attack graph based mission impact analysis*
  - to integrate mission dependency graphs, service dependency graphs, and cloud-level attack graphs

Our Approach



Our Approach

- Three steps:
  - Unify the representation of nodes and edges in mission dependency graphs and attack graphs
  - Extend traditional attack graphs into cloud-level attack graphs
  - Implement a set of interaction rules in MulVAL to enable automatic generation of logical mission impact graph

The Semantic Gap Between the Attack Graph And the Mission Dependency Graph

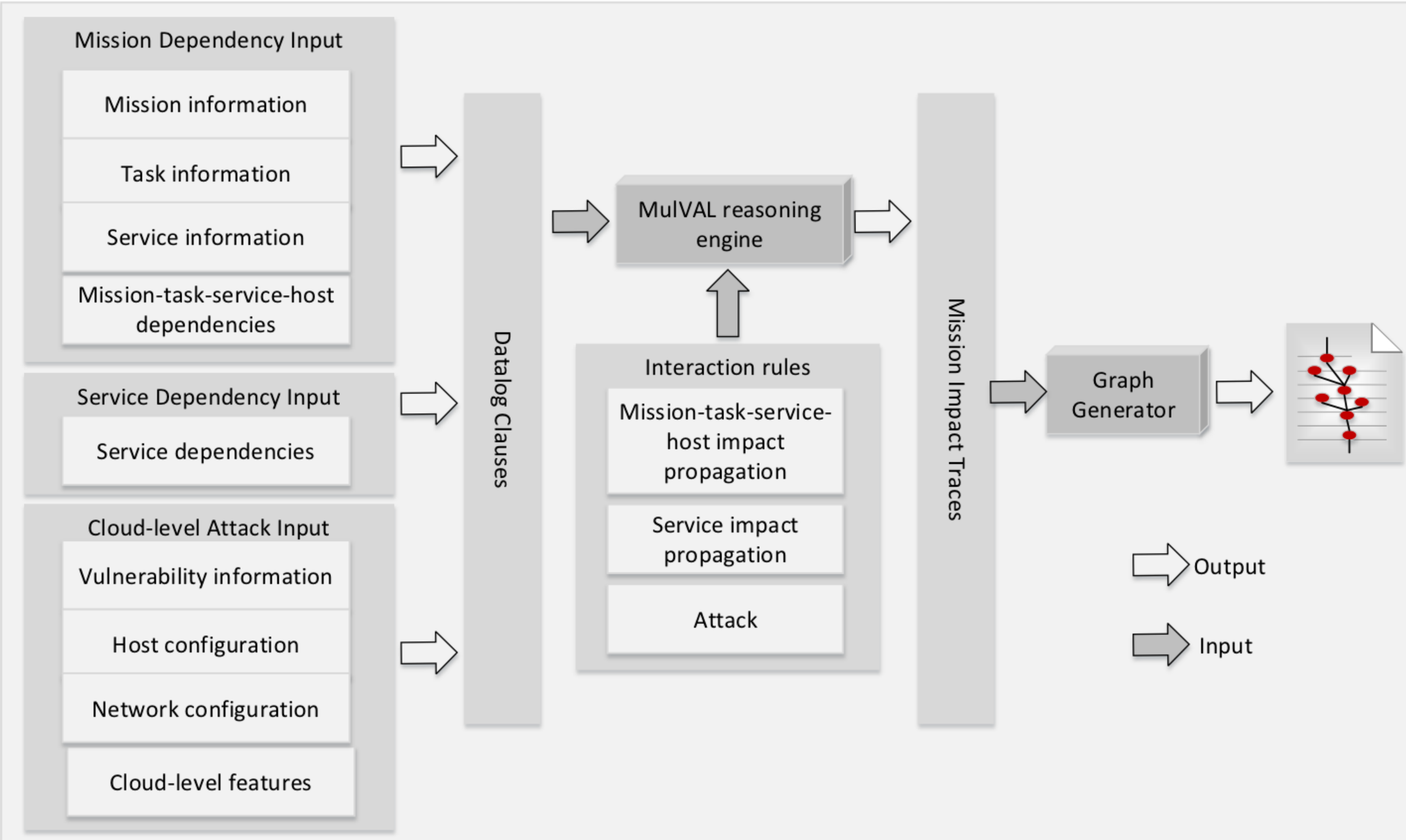
- A mission dependency graph is a mathematical abstraction of assets, services, mission steps (also known as tasks) and missions, and all of their dependencies

- The attack graph usually shows the potential attack steps leading to an attack goal

Mission Impact Graph Definition

- It is a directed graph that is composed of three parts: attack graph part, service dependency part and mission-task-service-host dependency part.
- It contains two kinds of nodes: derivation nodes and fact nodes.
- The edges in the mission impact graph represent the causality relations among nodes.

Logical Mission Impact Graph Generation

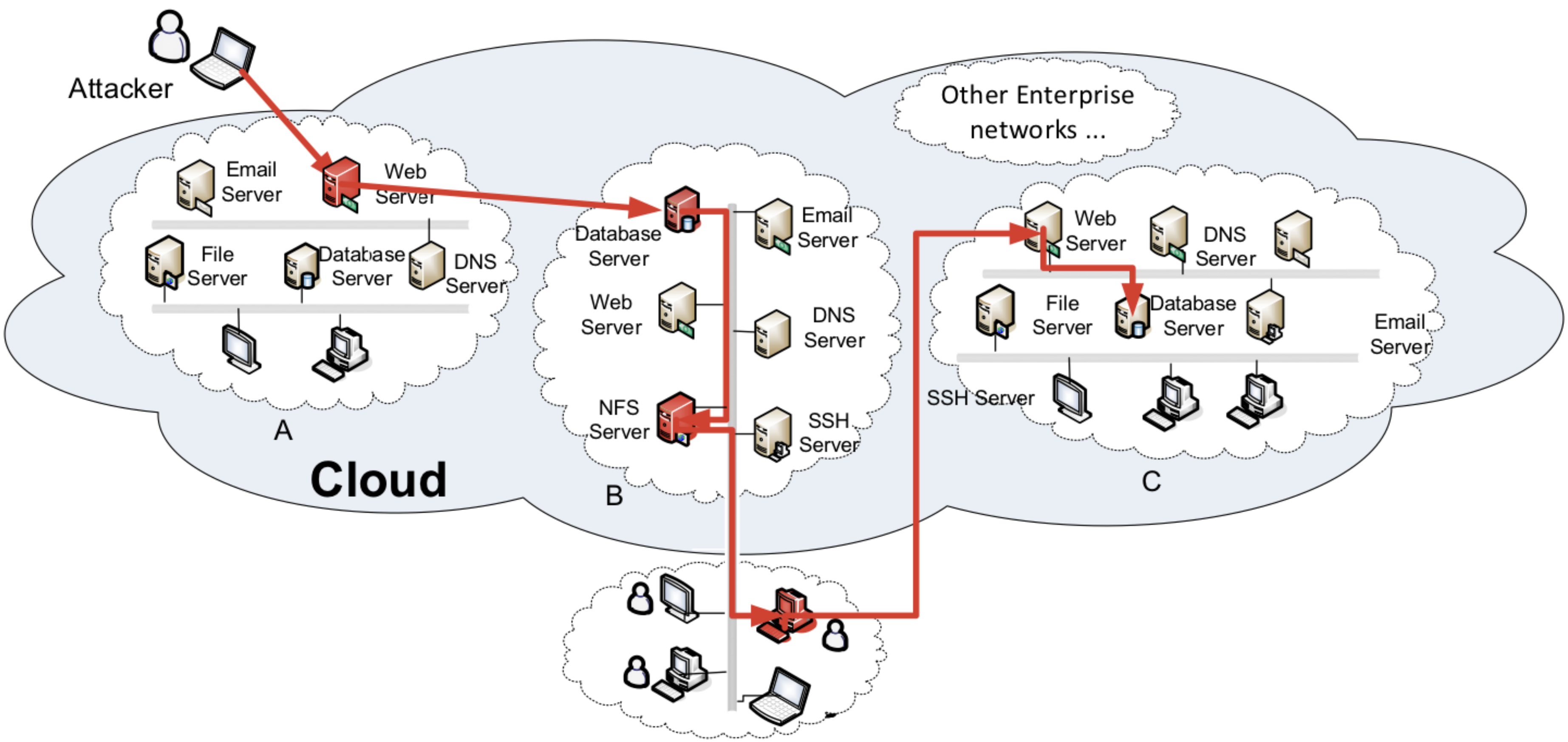


Automatic Generation of Mission Impact Graphs

- Create new Datalog clauses in MulVAL
  - mission dependencies,
  - service dependencies,
  - cloud-level attacks
- Example interaction rules:

interaction rule(
(serviceImpacted(Service, H, Perm):-
hostProvideService(H, Service),
execCode(H, Perm)),
rule_desc('An compromised server will impact the dependent
service')).

Case Study: Attack Scenario

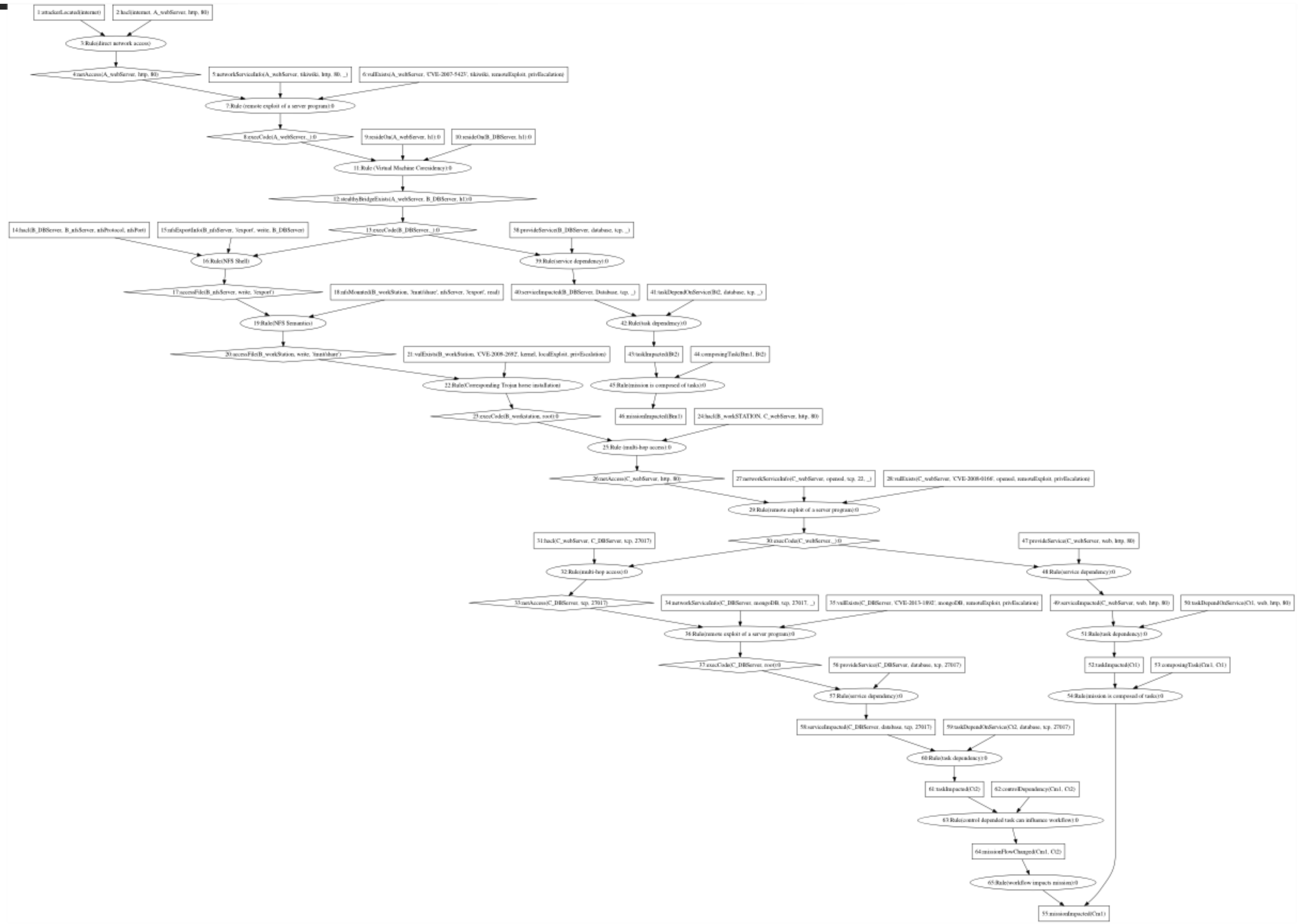


Case Study: Attack Scenario

7-step attack:

- 1) Mallory compromises A’s webserver by exploiting a vulnerability
- 2) Mallory leverages the co-residency relationship to take over B’s database server, based on a side channel attack in cloud.
- 3) Mallory uploads a software tool.deb with a Trojan horse to a directory that is shared by all the servers and workstations inside the company.
- 4) The innocent Workstation user from B downloads tool.deb from NFS server and installs it. This creates an unsolicited connection back to Mallory.
- 5) The Workstation has access to C’s webserver as a trusted client. Mallory then managed to take over it via a brute-force key guessing attack;
- 6) Mallory leverages C’s webserver as a stepping stone to compromise C’s MongoDB database server, which allows Mallory successfully steal credential information from an employee login database table;
- 7) Mallory logins into C’s webserver as a collaborator of C, and accesses the project proprietary documentation to collect formula-related vaccine research and development records.

Case Study: Generated Mission Impact Graph



Case Study: Analysis

- The result cloud-level mission impact graph is very helpful for understanding potential threats to missions in this scenario.
- One function of our mission impact graph is to perform automated “taint” propagation through logical reasoning.
- The generated mission impact graph enables effective mission-centric cyber resilience analysis.

Case Study: Analysis

- Automated “taint” propagation
  - Given a “taint”, be it a vulnerability, a compromised machine, or a disabled service, the impact of the “taint” can be analyzed through logical reasoning
  - The mission impact graph is able to reflect affected entities such as assets, services, tasks, and missions.

Case Study: Analysis

- Mission-centric cyber resilience analysis
  - Performing proactive “what-if” mission impact assessment. Which tasks or missions will be impacted?
    - E.g., what if we remove a server?
    - E.g., what if we patch a vulnerability on a host?

References

- A. Singhal, S. Ou, Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs, NISTIR 7788, September 2011.
- A. Singhal and X. Ou, "Quantitative Security Risk Assessment of Enterprise Networks", Springer Brief Book in Computer Science, December 2011.
- M. Albanese, S. Jajodia, A. Singhal, and L. Wang, "An efficient approach to assessing the risk of zero-day vulnerabilities," Proc. 10th International Conference on Security and Cryptpgraphy (SECRYPT 2013), Reykjavik, Iceland, July 29-31, 2013
- L. Wang, S. Jajodia, A. Singhal, P. Cheng and S. Noel, "K Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities", IEEE Transactions on Dependable and Secure Computing (TDSC) January 2014.
- C. Liu, A. Singhal, D. Wijesekara, "A Logic Based Network Forensics Model for Evidence Analysis", IFIP International Conference on Digital Forensics, Orlando, Florida, January 24th-26th 2015.
- C. Liu, A. Singhal and D. Wijesekera, "A Reasoning Based Model towards Using Evidence from Security Events for Network Forensics Analysis", International Workshop on Security of Information Systems, Lisbon, April 27th 2014.

References

- X. Sun, A. Singhal, P. Liu, "Who Touched My Mission: Towards Probabilistic Mission Impact Assessment", ACM Workshop on Automated Decision Making for Active Cyber Defense, October 12th 2015, Denver, Colorado.
- L. Wang, S. Jajodia, A. Singhal, M. Albanese, "Network Diversity: A Security Metric for Evaluating the Resilience of Networks Against Zero Day Attacks", IEEE Transactions on Information Forensics and Security, 2016.
- C. Liu, A. Singhal, D. Wijesekara, "A Probabilistic Network Forensics Model for Evidence Analysis", IFIP International Conference on Digital Forensics, New Delhi, India, January 4th-6th 2016.
- D. Borbor, L. Wang, S. Jajodia and A. Singhal. "Diversifying Network Services under Cost Constraints for Better Resilience against Unknown Attacks", IFIP WG 11.3 International Conference on Data and Applications Security and Privacy (DBSEC) July 18th-20th 2016.
- X. Sun, J. Dai, P. Liu, A. Singhal, J. Yen, "Towards Probabilistic Identification of Zero Day Attack Paths", IEEE Conference on Communication and Network Security, October 10th-14th 2016.
- C. Liu, A. Singhal, D. Wijesekara, "Identifying Evidence for Cloud Forensics Analysis", IFIP International Conference on Digital Forensics, Orlando, FL, January 29th- Feb 1st 2017.
- X. Sun, A. Singhal, P. Liu, "Towards Actionable Mission Impact Assessment in the Context of Cloud Computing", 31st IFIP WG 11.3 Conference on Data and Application Security and Privacy, Philadelphia, July 19th to 21st 2017.

Conclusions

- Based on attack graphs, we have proposed a model for security risk analysis of information systems
  - Composing individual scores to more meaningiful cumulative metric for overall system security
- Future work is how to apply these techniques for security of cloud computing and for cyber resilience