Network Security and Risk Analysis Using Attack Graphs

Anoop Singhal
National Institute of Standards and Technology

Coauthors: Lingyu Wang and Sushil Jajodia

Concordia University
George Mason University

Outline

- **Motivation and Related Work**
- **Example of an Attack Graph**
- **Quantitative Security and Risk Analysis**
- **Conclusion and Future Work**

Motivation

- Typical issues addressed in the literature
  - How can the 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 my network architecture so it provides a certain amount of security?
- For this we need a network security modeling and analysis tool

Challenges for Quantitative Analysis

- Counting the number of vulnerabilities is not enough
  - Vulnerabilities have different importance
  - The scoring of a vulnerability is a challenge
    - Context of the Application
    - Configuration of the Application
- How to *compose* vulnerabilities for the overall security of a network system

Sample Vulnerability

symantec.

Symantec Vulnerability Alert

Microsoft SQL Server 2000 Resolution Service Denial of Service Vulnerability

Synopsis

Bugtraq ID: **5312** CVE: CAN-2002-0650

Published: July 25 2002 Last Update: July 25 2002 GMT

Last Update: Initial analysis.

Remote: Yes Local: No

Availability: Always Authentication: Not Required

Ease: No Exploit Available

Vulnerability Classification: Failure to Handle Exceptional Conditions

Urgency Rating: 6.1

Threat Breakdown:

Severity	6.7
Impact	4.0
Ease of Exploit	1
Credibility	Vendor Confirmed

Related Work

- NIST's efforts on standardizing security metric
  - Special publication 500-133 1985, 800-55 2003
  - NVD and CVSS v2
- Attack surface (Howard et. al QoP'06)
- Page Rank (Mehta et. al RAID'06)
- Fred Cohen (1998, 2000)

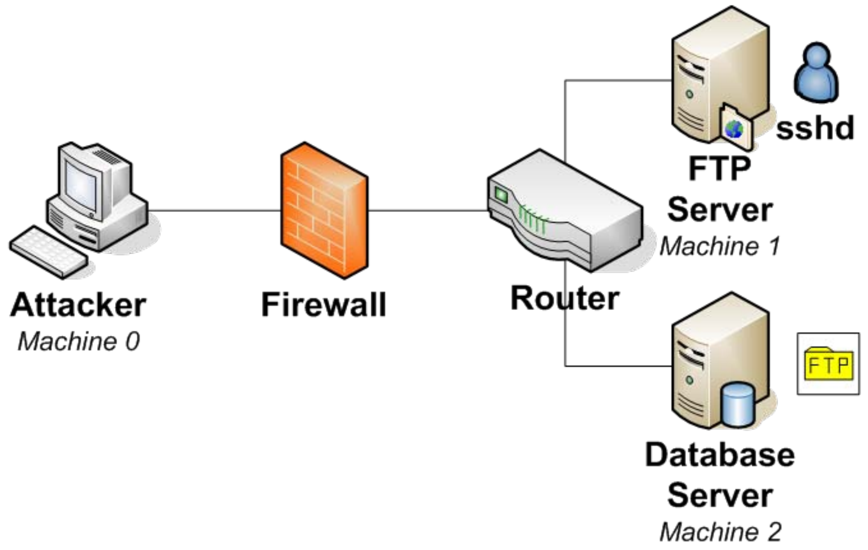
Related Work (Cont'd)

- Attack graph
  - Model checker-based (Ritchey et. al S&P'00, Sheyner et. al S&P'02)
  - Graph-based (Noel et. al ACSAC'03, Singhal et. al DBSEC'06, DBSEC '07)

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

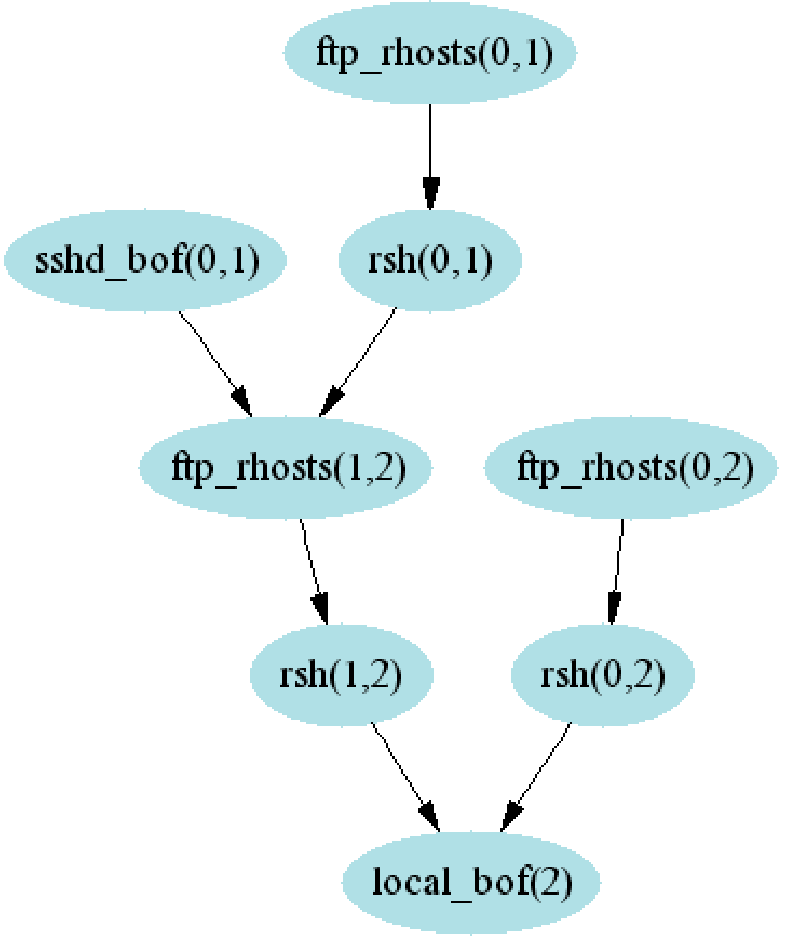
Attack Graph Example



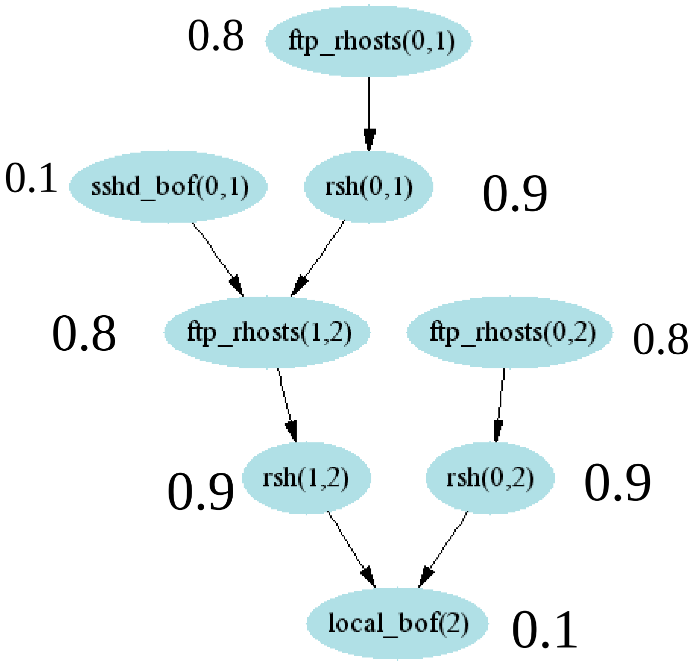
Different Paths for the Attack

- *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

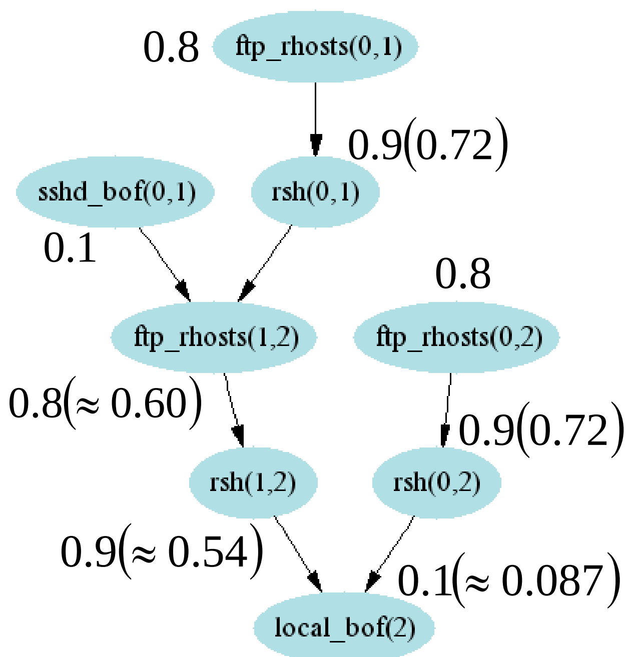


Attack Graph with Probabilities



- 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: $p(A \text{ or } B) = p(A) + p(B) - p(A)p(B)$.

Network Hardening

- When we harden the network, this changes the attack graph, along with the way its probabilities are propagated.
- Our options to block traffic from the *Attacker*:
  - Make no change to the network (baseline)
  - Block ftp traffic to prevent *ftp_rhosts(0,1)* and *ftp_rhosts(0,2)*
  - Block rsh traffic to prevent *rsh(0,1)* and *rsh(0,2)*
  - Block ssh traffic to prevent *sshd_bof(0,1)*

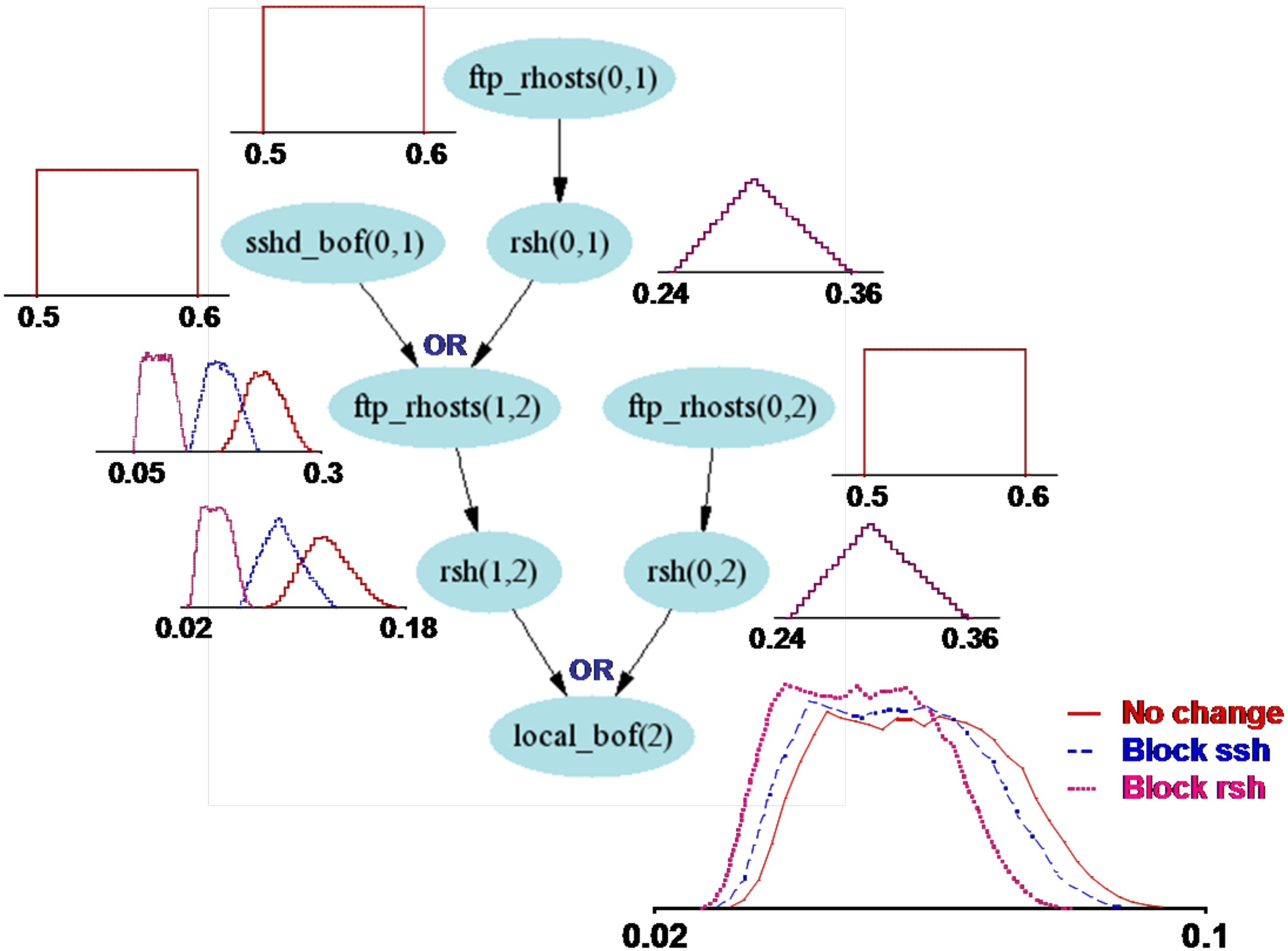
Comparison of Options

- We can make comparisons of relative security among the options
- Make no change p=0.1
- Blocking rsh traffic from *Attacker* leaves a remaining 4-step attack path with total probability $p = 0.1 \cdot 0.8 \cdot 0.9 \cdot 0.1 = 0.0072$
- Blocking ftp traffic, p=0.0072
- But blocking ssh traffic leaves 2 attack paths, with total probability $p \approx 0.0865$, i.e., compromise is *10 times more likely* as compared to blocking rsh or ftp.

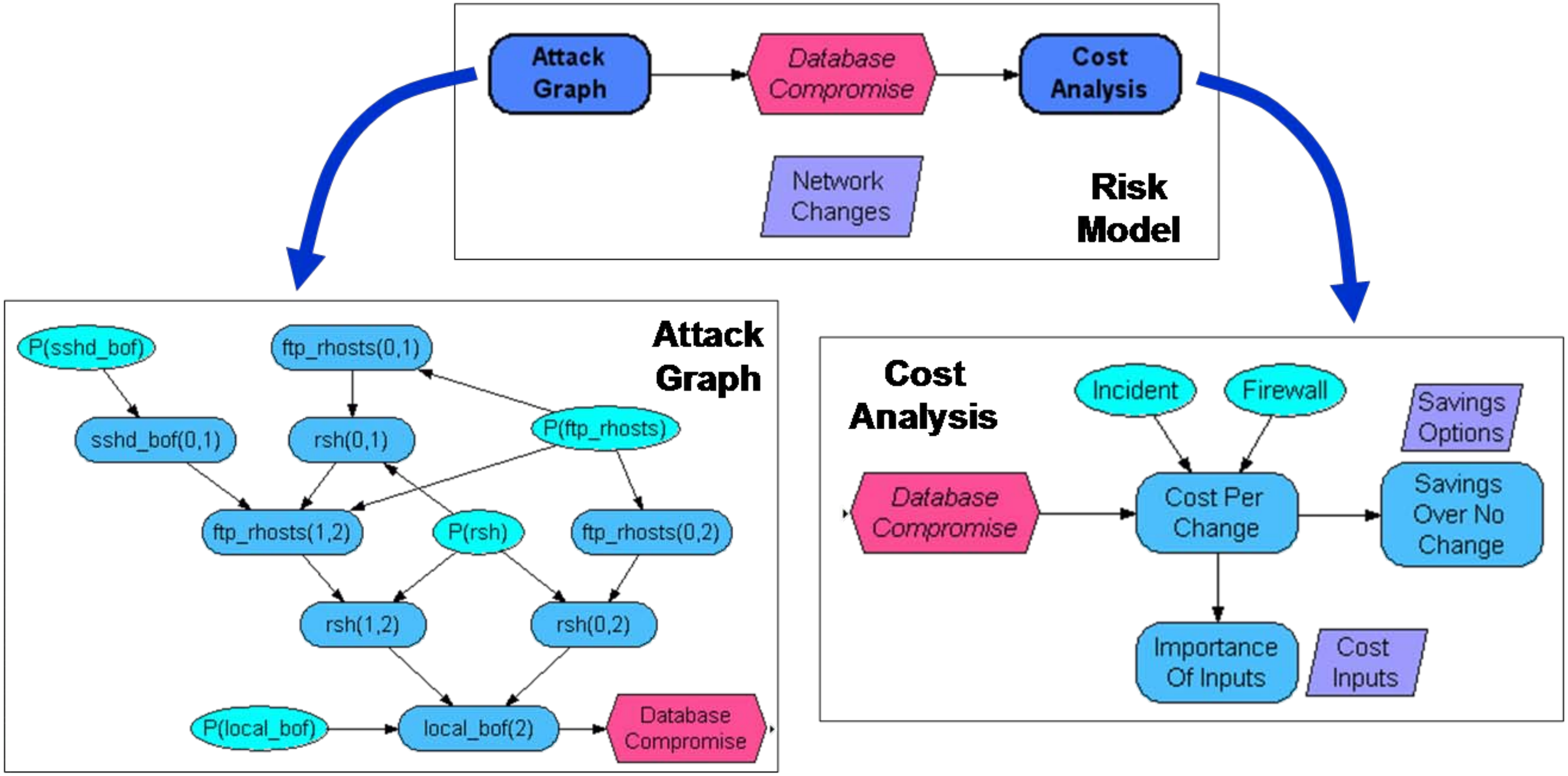
Need for a Modeling Tool

- For a large enterprise network that has hundreds of host machines and several services we need a modeling tool that can
  - Generate the attack graph
  - Use the attack graph for quantitative analysis of the current configuration
  - Help the network administrators to decide what changes to make to improve security

Probability Of DB Compromise for Each Choice



A Model for ROI Analysis



ROI Analysis

- Total Cost = Cost of Firewall Change +
  (Prob. Of DB Compromise) *
  (Cost of DB Compromise)

Assume

Cost of DB Compromise is $20K

Cost of a Firewall Rule Change is 0.5K

Conclusion

- Based on attack graphs, we have proposed a model for measuring the overall security of network systems
- The metric meets intuitive requirements
- It can be useful for ROI Analysis

Future Work

- Build a Network Security Modeling and Planning Tool
- Generalize the model to use probability distributions for each vulnerability
- Apply this technique for ROI Analysis