Attack Graph Generation for Optimal Sensor Placement

Manoj Valeti B160091CS
Rakesh Chowdary Y B160710CS

Department of Computer Science and Engineering
NIT Calicut

24 October 2019

Outline

1. Topological Vulnerability Services
   - TVA
   - Adjacency Matrix Visualization
2. Security Metrics
   - Introduction
   - Probabilistic Security Metrics
   - Attack Resistance
3. Minimum cost for Network Hardening
   - Approach
   - Examples
4. Intrusion Detection Systems
   - Correlating Intrusion Events and Building attack Scenarios through Attack Graph Distance
   - Intrusion Detection Systems
   - Optimal Sensor Placement
   - Alarm Prioritization and Attack Response

Problem Statement

- To performance comprehensive literature survey on *Attack Graphs* and implement a system for automatically generating an attack graph.

Outline

TVA

- Analysis of vulnerabilities and building a complete map showing all possible paths of multi-step penetration into the network, organized as an attack graph, is known as Topological vulnerability analysis.
- Single vulnerability may not pose a threat but combination of vulnerabilities may allow attackers reach critical network assets.
- TVA considers dependencies among vulnerabilities and combines them in a real way as real attackers might do.

Outline

Adjacency Matrix Visualization

- Attack graph of n vertices can be represented by matrix of n x n.
- Rows and columns of matrix can be placed in any order, but orderings that capture regularities are desired.
- Regularities include cluster of vertices that have a common edge.
- Adjacency matrix shows reachability within single step.
- Adjacency matrix raised to power of P gives number of p-step paths between vertices.

Contd.

- Native Matrix multiplication can be improved by spectral decomposition of A into V and D.
- D contains eigen values as diagonal elements and V is matrix of eigen vectors. Now, Large powers of A can be computed by raising D to large powers.
- Transitive closure of A gives for each pair of vertices, whether attacker can reach one graph vertex to another over all possible number of steps.
- Reachability matrix contains minimum no. of steps required to reach one vertex from another.

Outline

Introduction

- No widely accepted security metrics
- Every metric is qualitative rather than quantitative
- 3 factors that account to quantitative security metrics are
  (i) *Significance of resource* - Prioritizes the resources
  (ii) *Reconfiguration cost* - Provides the relative overhead for network hardening
  (iii) *Attack Resistance* - Removes the idea of qualitative measure.

Outline

Probabilistic Security Metrics

- It gives the likelihood of an attack
- For each exploit e and condition c we will be having individual probabilities p(e), p(c) and cumulative probabilities P(e), P(c).
- Individual probability is the likelihood of exploiting exploit e given all it's preconditions are satisfied.
- Cumulative probability represents the likelihood of reaching a state in which attacker can successfully exploit a given exploit.

Cummulative Probability

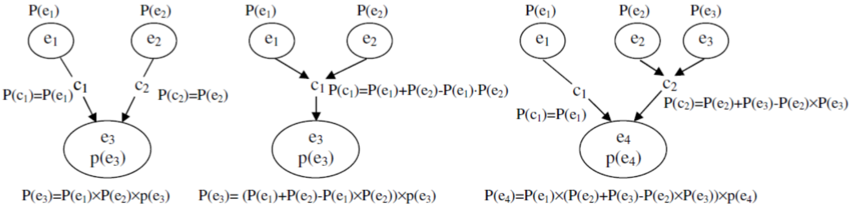


Fig. 2. Examples Showing the Need for Cumulative Scores of Conditions

[7] Wang, L., Islam, T., Long, T., Singhal A., & Jajodia, S. (2008, July). *An attack graph-based probabilistic security metric.*

Probabilistic Security Metrics

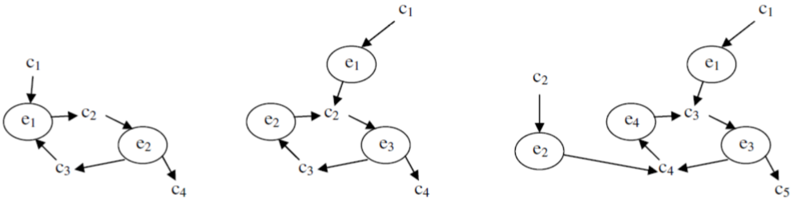


Fig. 3. Cycles in Attack Graphs

[7] Wang, L., Islam, T., Long, T., Singhal A., & Jajodia, S. (2008, July). *An attack graph-based probabilistic security metric.*

Probabilistic Security Metrics

- We follow 3 methods to avoid difficulties
  a) Remove cycles.
  b) Break edges
  c) Neither remove cycles nor break edges

Outline

Attack Resistance

- Metrics are quantified based on the time and effort taken to compromise a given critical resource
- More the no.of attack paths the less secure is the network.
- Metrics are quantified by
  (i)Assigning the real number values to attack resistances
  (ii)Attack resistances are represented as set of intial conditions.

Real values assignment

- The attack resistance is quantified by a real number
- For an exploit e the attack resistance value is denoted by r(e)
- Cumulative attack resistance is similar to that of effective resistance in an electrical circuit
- Cumulative attack resistance is calculated using $\oplus$, $\otimes$ between two resistances.
- $1/r1 \oplus r2 = 1/r1 + 1/r2$ - parallel condition
- $r1 \otimes r2 = r1 + r2$ - series condition
- $R'()$ function gives the modified attack resistance values when a particular exploit occurs.

Set of Initial Conditions

- Attack resistance is completely different from the previous approach
- Resistance here means set of initial conditions to be satisfied before an intrusion is possible.
- More the no.of initial conditions more the resistance

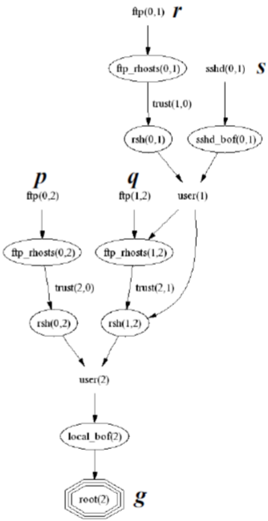
Outline

Network Hardening

- This is one of the first method to quantify the metrics
- Vulnerabilities should not be taken in isolation
- Every exploit is represented as a Boolean value and attack path is represented as a function of these Boolean values
- We start building a dependency graph with initial conditions as post conditions.
- In forward building of dependency graph we avoid redundancies by avoiding cycles.
- Once we reach the goal we do a backward processing in order to get those states that are not reachable from initial state but are relevant to the attack goal.
- This results in a set of minimal attack paths.
- $g = p + qr + qs$
  $=(p+q+r+s).(p+q+r+s').(p+q+r'+s).(p+q+r'+s').(p+q'+r+s)$

Outline

Examples for Hardening



[8] Noel, Steven, et al.*"Efficient minimum-cost network hardening via exploit dependency graphs."*

Outline

Correlating Intrusion Events

- Network vulnerability is ignored in most of the cases
- Joint model of attacker exploit and network vulnerability is created.
- Graph distance between the events is used to measure the correlation between the events.
- If an event is unreachable from previous one then it will be taken as a new event.

Correlating contd

- For easy calculations we take inverse of distance as it lies in the range of [0,1]
- We pass this distance function through an exponential weighted function in-order to take care of false alarms.
- This exponential weighted function is called low-pass-filter function.
- After passing through low-pass filter threshold value helps us to correlate the events.
- if d_k is the distance between events then consider

$$x_k = 1/d_k$$

$$\bar{x_k} = P.\bar{x_{k-1}} + (1-p)x_k \quad 0 \leq p \leq 1$$

$\bar{x_k}$ represents the filtered version of original sequence

[6] Noel, Steven, Eric Robertson, and Sushil Jajodia. *"Correlating intrusion events and building attack scenarios through attack graph distances."*

Outline

Sensors

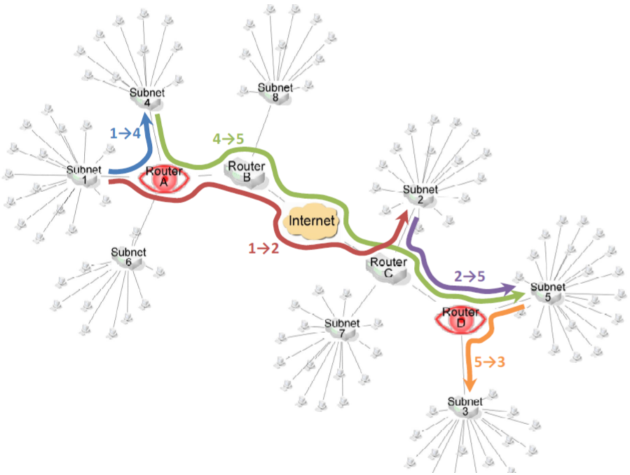
- Traditionally sensors are placed at network perimeters.
- Sensors report all malicious traffic without any regard to actual network configuration, vulnerabilities and mission impact.
- To reduce false alarms, attack graphs are built based upon network configuration, vulnerabilities and attacker exploits.
- Sensors are placed in minimal number to protect mission critical assets.

Outline

Sensor Placement

- Even though firewalls,routers ACLs are present still residual vulnerabilities are present.
- To minimize costs, Minimum no of sensors are placed to cover all critical paths. This is an instance of NP Hard Problem.
- Greedy algorithm for NP Hard Minimal set cover problem gives polynomial time solution.
- Algorithm is as follows
  - At every stage, select the set with large no. of elements.
  - If there are more sets with equal large no. of elements, select the one with more infrequent elements.

Optimal Sensor Placement



[9] Noel, Steven, and Sushil Jajodia. *"Optimal ids sensor placement and alert prioritization using attack graphs."*

Outline

Alarms Prioritization and Attack Response

- Attack graphs are used to correlate IDS alarms, prioritize them and predict the future steps and respond accordingly.
- Attack origin and goal can be predicted from alarms and adjacency matrix.
- For an alarm, non-zero elements along the projected row show all possible single steps forward. Projection along column gives attack origin.
- Alarms are prioritized based on distance from critical networks assets. Closer to critical assets are given higher priority.
- If attack is detected, we can predict the next steps and block that particular machines and ports

For Further Reading I

Jajodia, Sushil, and Steven Noel.
Advanced cyber attack modeling analysis and visualization.
GEORGE MASON UNIV FAIRFAX VA, 2010.

Jajodia, Sushil, Steven Noel, and Brian O'berry.
"Topological analysis of network attack vulnerability."
Managing Cyber Threats. Springer, Boston, MA, 2005. 247-266.

Jajodia, Sushil, and Steven Noel.
"Topological vulnerability analysis: A powerful new approach for network attack prevention, detection, and response."
Algorithms, architectures and information systems security. 2009. 285-305.

For Further Reading II

Wang, Lingyu, Anoop Singhal, and Sushil Jajodia.
"Measuring the overall security of network configurations using attack graphs."
IFIP Annual Conference on Data and Applications Security and Privacy. Springer, Berlin, Heidelberg, 2007

Wang, Lingyu, Anoop Singhal, and Sushil Jajodia.
"Toward measuring network security using attack graphs."
Proceedings of the 2007 ACM workshop on Quality of protection. ACM, 2007.

Noel, Steven, Eric Robertson, and Sushil Jajodia.
"Correlating intrusion events and building attack scenarios through attack graph distances."
20th Annual Computer Security Applications Conference. IEEE, 2004.

For Further Reading III

Wang, L., Islam, T., Long, T., Singhal A., & Jajodia, S. (2008, July).
An attack graph-based probabilistic security metric.
In IFIP Annual Conference on Data and Applications Security and Privacy (pp. 283-296). Springer, Berlin, Heidelberg

Noel, Steven, et al.
"Efficient minimum-cost network hardening via exploit dependency graphs."
19th Annual Computer Security Applications Conference, 2003. Proceedings.. IEEE, 2003.

Noel, Steven, and Sushil Jajodia.
"Optimal ids sensor placement and alert prioritization using attack graphs."
Journal of Network and Systems Management 16.3 (2008): 259-275.

For Further Reading IV

Noel, S., & Jajodia, S. (2007, November).
Attack graphs for sensor placement, alert prioritization, and attack response.
In Cyberspace Research Workshop (pp. 1-8).

Thank You