## CSC 438/539 Systems and Software Security, Dr. N. Meghanathan, Spring 2014

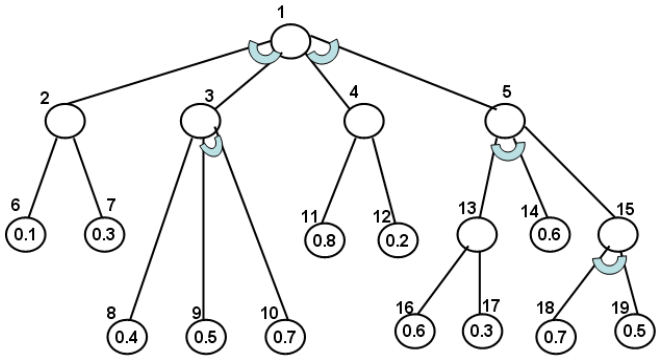
## Module 7 – Risk Analysis for Secure Software Design

1) Define the following terminologies in the context of risk analysis for secure software design:
(a) Vulnerability; (b) Threat; (c) Attack; (d) Risk; (e) Control; (f) Asset; (g) Likelihood; (h) Impact; (i) Risk exposure

2) What are the six threat categories of the STRIDE model and which property of an information asset does each category target? Explain. Discuss one strong potential countermeasure to mitigate each of these threats.

3) Consider the case study "Denial of Service – Decompression Bomb" that was discussed in class to illustrate how to come up with an attack pattern. In the context of this attack, answer the following questions:
a. What are the two pre-requisites to be able to launch the Decompression Bomb attack?
b. Briefly explain the Decompression Bomb attack.
c. What applications are typically targeted with the Decompression Bomb attack?
d. Explain some of the solutions that were discussed to mitigate the Decompression Bomb attack.

4) Consider the case study "Shell Command Injection – Command Delimiters" that was discussed in class to illustrate how to come up with an attack pattern. In the context of this attack, answer the following questions:
a. What is the pre-requisite to be able to launch the Shell Command Injection attack?
b. Briefly explain the Shell Command Injection attack.
c. What is typically considered as the motivation to launch the Shell Command Injection attack?
d. Explain some of the solutions that were discussed to mitigate the Shell Command Injection attack.




5) Consider the attack tree shown to the left. The integer outside a circle represents the node ID and the real number inside a circle represents the probability of apprehension when an attack is attempted on the node.

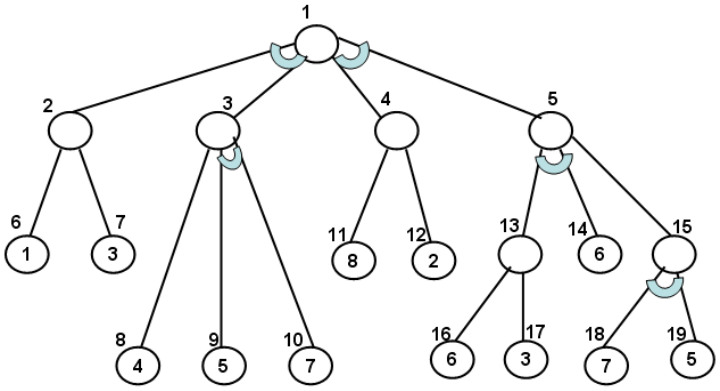
Note that larger the probability of apprehension on a node, the lower the difficulty in detecting an attack on the node and vice-versa.

(1) Identify all the possible paths (i.e., the sequence of nodes in each path) for the attack tree. For clarity, label each path with a unique number.
(2) For each of the paths identified, compute the probability of apprehension for the attack leading to the root node

Based on the paths, and the probability of apprehension determined, identify the paths according to each of the following criterion:

(3) The path of least apprehension
(4) The path that is the least difficult to detect
(5) The attack path that involves the maximum # of leaf nodes (break any tie by choosing the path that is more difficult to detect an attack)
(6) The attack path that involves the minimum # of leaf nodes (break any tie by choosing the path that is least difficult to detect an attack)

6) Consider the attack tree shown below. The integer outside a circle represents the node ID and integer inside a circle represents the cost of an attack is attempted on the node.




(1) Identify all the possible paths (i.e., the sequence of nodes in each path) for the attack tree. For clarity, label each path with a unique number. Note: It is the same attack tree as in the previous question.
(2) For each of the paths identified, compute the cost for the attack leading to the root node

Based on the paths, and the probability of apprehension determined, identify the paths according to each of the following criterion:

(3) The most expensive path
(4) The least expensive path
(5) The attack path that involves the maximum # of leaf nodes (break any tie by choosing the most expensive path)
(6) The attack path that involves the minimum # of leaf nodes (break any tie by choosing the least expensive path)

7) Briefly explain the three types of vulnerability analysis (you can use an appropriate example for each type) that could be conducted as part of assessing the security risks associated with software architecture?

8) How would you define the "High", "Medium" and "Low" ratings for each of the following in the context of software security qualitative risk assessment models: (a) Likelihood of the risk and (b) Risk exposure? Complete the table below for Risk Exposure.

| Likelihood of the Risk | Impact of the Risk | | |
|---|---|---|---|
| | Low | Medium | High |
| Low | | | |
| Medium | | | |
| High | | | |

9) Consider the following application scenario of a *Student Faculty Appointment System for Course Registration*, discussed in class, and briefly described below.

> Through this application, students can login and request for appointments from their faculty/academic advisors to register for their classes. Care will be taken to ensure that there is no denial of service attacks wherein a student makes multiple fake appointments for a particular faculty during a particular time period. The financial aid opportunities available to the student for the particular semester are also displayed when the student makes the appointment for registration.

(a) List two threats (other than the threat mentioned in parts (b) and (c)) for the above system and classify them under the STRIDE model. Justify your grouping of the threat to the STRIDE category.

(b) One of the threats for the above system is *students trying to make multiple fake appointments* and launching a ***Denial of service attack***. Conduct a DREAD analysis of this threat and compute the Risk Score associated with the threat. Justify your rating of the threat under the different components of the DREAD model.

(c) Another threat associated with the above system is the ***Spoofing the Identity*** threat related to *login attempts using the username and password (either reset or original password) corresponding to a different user*. Construct an attack tree for this threat. The attack tree should involve at least four attack paths and at least one of these paths should involve an AND node. You can use OR nodes as well as AND nodes for your attack paths. The nodes of the attack tree should be clearly labeled and described as illustrated in the "Spoofing the Identity" threat in the slides.