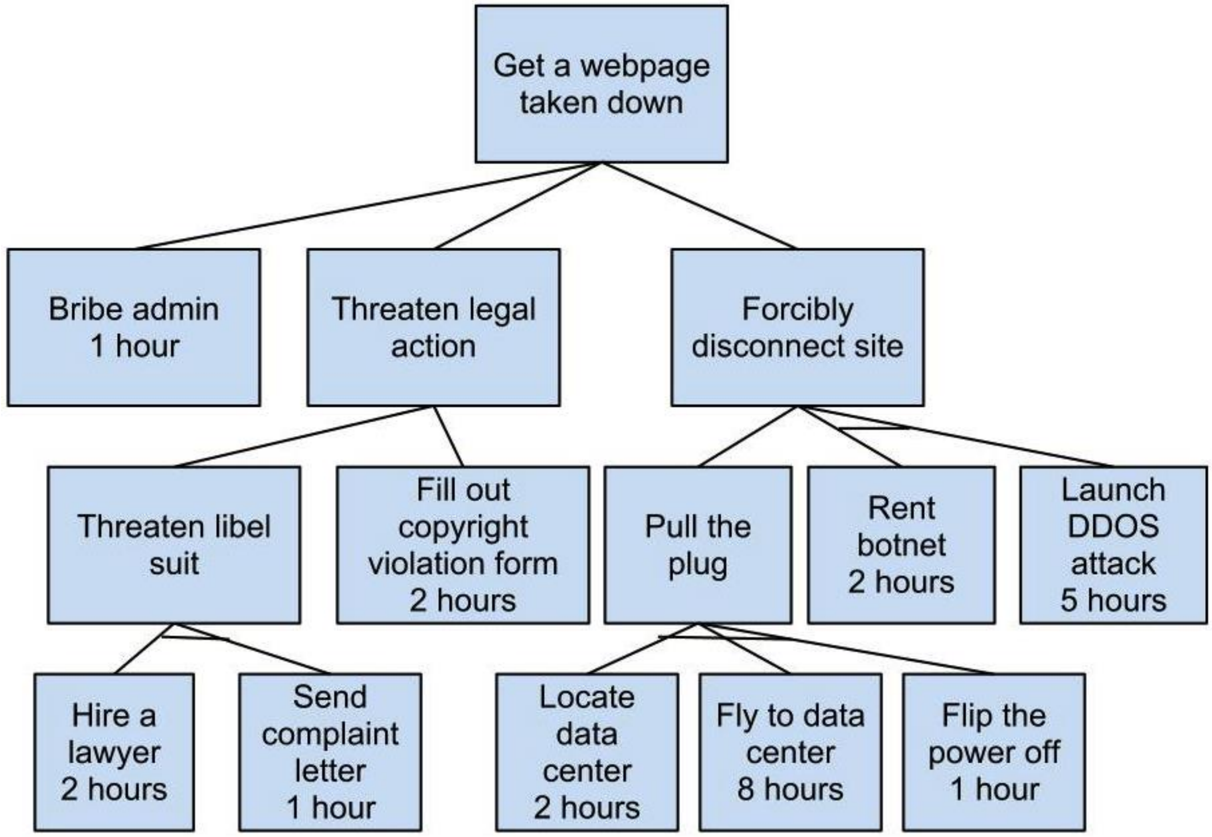
Information Security and Privacy Assignment – 1.3

Name: Srinivas Piskala Ganesh Babu **NetID: spg349 (N13138339)**

This assignment is worth 60 points (6% of your total grade).

1) **Below is an example attack tree for getting a webpage taken down. The child nodes are annotated with the amount of time needed to perform an action. [2 points each]**


Get a webpage taken down
Bribe admin 1 hour
Threaten legal action
Forcibly disconnect site
Threaten libel suit
Fill out copyright violation form 2 hours
Pull the plug
Rent botnet 2 hours
Launch DDOS attack 5 hours
Hire a lawyer 2 hours
Send complaint letter 1 hour
Locate data center 2 hours
Fly to data center 8 hours
Flip the power off 1 hour

a) Propagate the minimum amount of time needed up the tree – ***1 Hour – Bribe Admin***

b) Annotate the child nodes of the attack tree that require money with ($). Annotate free child nodes with (Free). Propagate these symbols up the tree. (Note that you should not consider the amount of time when considering how to propagate these symbols

Layer 3:

**** Hire a Layer - $2000 –*** *Lawyer and Document Fee Estimate*

**** Send complaint letter - $100 –*** *Stamp, Documents and Carrier Charges*

**** Locate data center – $0 – Free*** *Social Engineering or Review Organization Locations (Assuming possessing a computer and social engineering skills)*

**** Fly to data center - $1000 –*** *Travel expenses*

Information Security and Privacy Assignment – 1.3

**** Flip the power off – $100 –*** *Accessing the organization power switch or building power as an electrician – (Charge to fake a service men)*

Layer 2:

**** Threaten libel suit - $2100 –*** *And Functionality of previous layers*

**** Fill out copyright – $0 - Free -*** *Claiming for Copyright violation*

**** Pull the plug - $1100 -*** *And Functionality of previous layers*

**** Rent Botnet - $1000 –*** *Buy a Botnet*

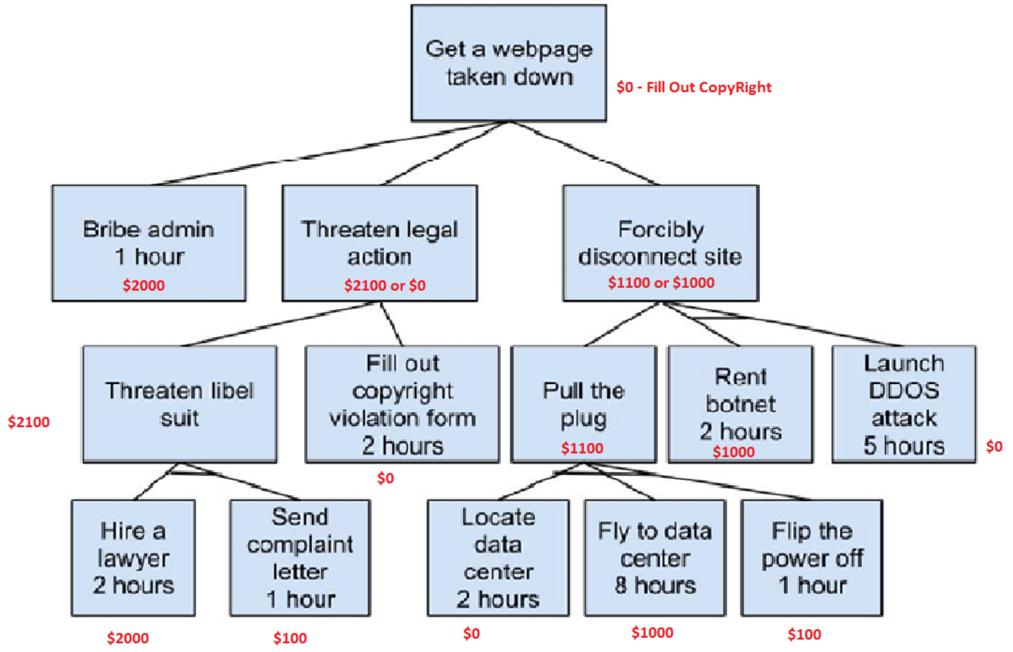
**** Launch DDOS Attack – $0 - Free*** *(Use the Botnet to do DOS – Assuming possession of required skills for successful DOS attack using the Botnet)*

Layer 1:

**** Bribe Admin – 2000$ -*** *Bribing is expensive*

**** Threaten Legal Action – 0$ or 2100$ -*** *OR Functionality of previous layers*

**** Forcibly disconnect site - $1100 or $1000 -*** *OR Functionality of previous layers*



c) What is the path that takes the least amount of time and is Free?

*** Fill out copyright violation and submit**

d) Describe a policy that the organization could employ to minimize the impact of an attacker using the path described in the previous question.

Policy To Overcome Copyright Violation:

** Patent new technology invented or open source it with proper license.*

** Have legalized and patented technology data, obtain permission rights and proper verification of ownership before incorporating any data or technology in the website.*

Information Security and Privacy Assignment – 1.3

** Have a legal opinion on a regular basis from any legal or copyright consultants*

** Be elaborate and clear in terms and condition and necessary agreements in the content used.*

** Maintain a database with proper agreements, licenses and verifications made with the respective authorities*

** Ensure verification of content presented in the webpage with a team or content manager – Perform regular audit for verification of information*

2) Security models:
The Bell–LaPadula Model (BLP) is a state machine based model for enforcing access controls.
https://en.wikipedia.org/wiki/Bell–LaPadula_model
The Biba Integrity Model is another type of state machine based model for enforcing access controls.
https://en.wikipedia.org/wiki/Biba_Model
[2 points each]

a) Circle the security model that forbids write-up. (BLP or [✓ Biba])
b) Circle the security model that forbids read-up. ([✓ BLP] or Biba)
c) Circle the property that is preserved by BLP. ([✓ confidentiality], integrity, or availability)
d) Circle the property that is preserved by Biba. (confidentiality, [✓ integrity], or availability)
e) Which security model discussed in the class is primarily used to prevent conflict of interest?
**** Chinese Wall Model***

3) Please classify each of the following as a violation of confidentiality, of integrity, of availability or of some combination of those:
[2 points each]

a) Mallory forges her father's signature on an application form – **Integrity** *(Authorized by some other person than the original source)*
** Can also be considered as **Confidentiality** to some extent as Mallory is revealing her fathers signature to some application form which can be used to forge in evil hands, as well as Mallory gets access to certain information based on the application that she is not authorized which compromises confidentiality.*

b) John Doe registers the domain name "citibank.com" and does not allow the real CitiBank to buy or use the domain name. **Availability** *(Brings down the availability of the domain – online banking)*

c) Wendy obtained Bob's customer identification number for the cable service and cancelled Bob's cable service. **Confidentiality** *(Identification number a secret id for customer)* **and Availability** *(Service of Bob's cable brought down)*

d) Alice copies Bob's assignment and turns it in as her own. ***Confidentiality*** *(Copied the information in Bob Assignment without legal or valid access)* **and Integrity** *(False source of work and tampered with a* *false identity Alice)*

4) Categorize the following as primarily policy or mechanism.
[2 points each]

a) A padlock on a door.   Circle: policy or [✓ mechanism]

b) A law providing a stiff punishment for littering. [✓ policy] or mechanism

c) The written rules for appropriate Internet access at NYU. [✓ policy] or mechanism

d) A firewall that blocks sites to enforce Internet access rules. policy or [✓ mechanism]

5) QR codes, like the one to the right, are used to encode strings.   This often is used to make a physical item (like a poster or box) contain a URL that links to a website that gives extended information about the physical item.
A recent Slashdot article summary noted:
"Invisible nano QR codes have been proposed as a way to stop forgery of U.S. currency by students of the South Dakota School of Mines and Technology. Unfortunately QR codes are easy to forge and can send you to a site that infects your system. Banks would most likely need to scan currency that have QR codes to ensure the authenticity of the bill. If the QR code was forged it could infect the bank with a virus."
How could the bank protect against this threat? [10 points]

- **Restricted DNS Server - Only the Valid Domain to check authenticity gets Resolved (Other Domain Resolution is restricted)**
  Restricting the DNS Server Used in the internal network to only resolve to the valid authentication domain, Other domains won't get resolved. Making the DNS Resolution only for the QR Verification Domain. All other domains will lead to error. (Easy way is to use etc/hosts with only the Valid QR Verification URL)

- **Isolating the machine (to check QR validation) from the Bank Network**
  Removing the QR Code validating machine from the Bank's Network and using it as a standalone computer dedicated to verification of the currency. Using a separate Internet connection (Different ISP) for the validating machine isolating them from the bank network.

- **Validating the URL before making a Web request**
  A Validation Script or a validation Server running as a mediator, checks for any url other than the valid QR validation url before making a request. If the request is made to some other URL it forbids making a request.

- **No Internet in the Validating Machine: Preventing Internet Access and Setting up an Intra-Network**
  Maintaining no internet connection with the validating machine. Setting up an Internal Network with QR Code Validation Server. Maintaining a central QR Code Validating Server unit in each bank internal network. Hence no internet connection and the validation is achieved.

- **Firewall**
  Setting up firewall policies to block file downloads and irrelevant URL communication. Firewall blocks malicious urls and file downloads. (Ingress/Egress Filtering)

- **Antivirus:**
  Using an Antivirus to protect against the virus. The Antivirus monitoring the file downloads and the url communication efficiently alerts and blocks an url or a file, ultimately deletes them from the system.

- **Check Physical properties of valid currency before making the QR Check**
  Checking the physical properties of the currency visually for authenticity like the images, stamp and seal in the currency, before making a QR Code Validation. It makes it quite harder for the attacker to forge the currency similar to multiple step verification – (2 step verification in gmail)

6) Give an example of a high level security policy and describe how your example may be represented in a lower level security policy. [5 points]

Example Problem Statement:

Say a company called “X” like Apple maintains the current project working on very secretive.
There exists a Lab where the research is going on for the current project.

Objectives:

- Confidentiality – on Research resources, technology and idea
- Integrity – on using the resources and communication between teams
- Availability – for services like Internet, Lab/Machine Access

High Level Security Policy:

- To maintain the CIA triad on the Research Project of company X
- Be most secretive/isolated until the product is released by company X
- Organize the entities as Subjects/Objects and provide authorization
- Isolate the Subjects/Objects in the project from anything else in the organization
- Build trust with the subjects relating to the Project before getting subjects involved
- Make resource available all time for research
- Protect the research and technology in a strict manner
- Restrict any chances of leakage of information without any trigger from the inside

- Maintain Subject/Object relation top down for both READ/WRITE

Low Level Security Policy:

- **LAB Access:**
    - Construct the lab in least accessible part of the organization
    - Provide Lab access to the required personnel only
    - Have a separate timing when the lab will be OPEN/CLOSE
    - Maintain access/timings to lab based on the levels of the subjects – Bottom Up (Engineer will have more access privilege and time to spend in lab than Manager)
    - Maintain access to resources top down, with more authority and access to Manager and less to employee

- **Employee's in the Project**:
    - Establish trust with the subject with proper agreement, bonds
    - Verify the background of the subject

- **Resources for the Project:**
    - Maintain a separate Intra Network for the team with isolated entities like expensive firewall, separate Databases.
    - Provide greater backup for data and power in the lab
    - Restrict Internet usage to a session and verify the information at ingress/egress of the lab

- **Communication:**
    - Isolate the subject at different levels to avoid any personal discussion
    - Provide a secure mail and message platform with strict verification on the information exchanged
    - Maintain very little transparency as we go down the subject levels

- **Technology:**
    - Execute regular verification of the technology used and patent it based on the road map.
    - Establish a strict relation with any third party company involved in the project with proper agreements and license requirements.

7) Several popular news articles have discussed that many users tend to choose the same PIN numbers (4 digit numeric codes often used by ATM cards and automated phone services). The articles say that PIN 1234 is used most often and 8068 is the least frequently used. As a result, a friend suggests that a good idea would be to change your PIN to 8068 because it is the least likely to be guessed. Explain why you agree or disagree. [11 points]

Information Security and Privacy Assignment – 1.3

Disagree. Explanation below

- The fact that an article has the information of 8068 being the least common pin number itself **makes it more vulnerable.**
- Being **ambiguous** comes with **random** or different combination that is nowhere documented or used before and not publicly exposed.
- Using a harder PIN exactly as it is documented will result in being hacked with almost the same chances as using 1234.
- It would also be a very bad idea to take advice from another person while setting the pin as that **compromises confidentiality** in the first place. A Password/Pin should be confidential only to the person possessing the authority (owner of the account).
- Selecting a PIN with random and **no relation to any personal identity** like birthdays/occasions will be the toughest to crack
- PIN being a **4 digit number from 0-9 has (10x10x10x10) 10000 combinations** in total. Given that there is a particular number of times (say 4) a wrong pin be entered before successful login or locked out, a person interested in cracking would select from a list of most common pin, pin publicly exposed (as in 8068) claiming to be hardest, social engineering the person for any birthday/occasion combinations.
- Some tips on consideration of setting a tough PIN would be,
  - Not using repetitive digits
  - Not using round numbers
  - Not using continuous digits
  - Not using any publicly exposed PIN combinations
- PIN 8068 would have guaranteed some toughness to crack if it had not been publicly exposed and created from within the individual itself
- Drawbacks of the statement -> Violates Confidentiality – Friend Suggestion and Using from Article that is publicly documented, There is also a chance to violate Integrity as the Friend may be suggesting based on some fake article.