COMP435: *SECURITY CONCEPTS!*

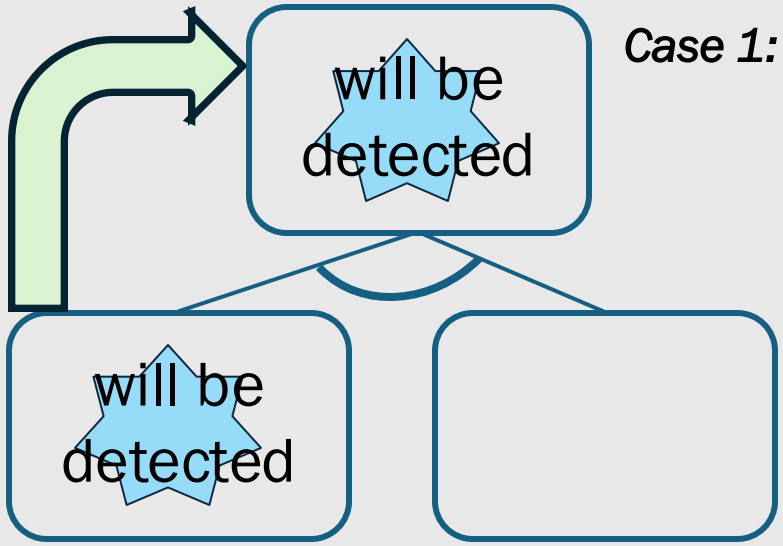
Lecture 3: More Threat Modeling, Risk

Please don’t sit in the back 4 rows ☺

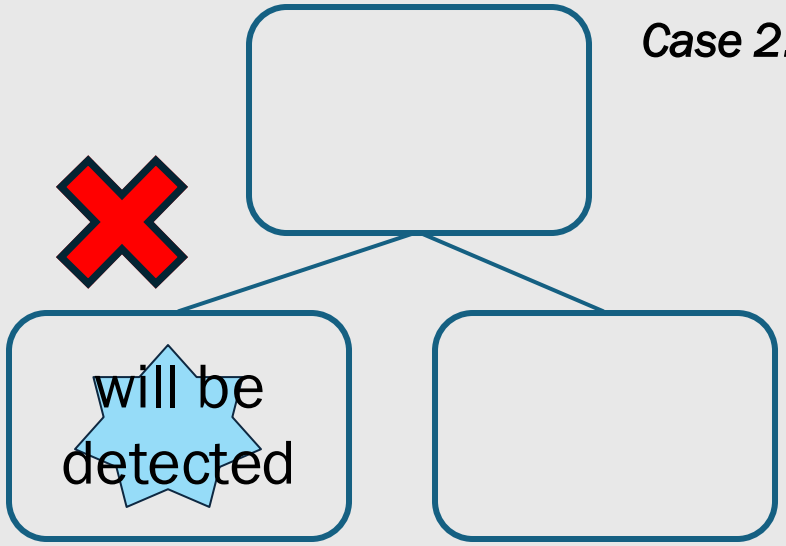
Logistics Update!

- Quiz topics:
  - Threat Modeling Terminology
  - Security Primitives
  - Security Policies: Writing them, analyzing them
  - Attack Trees
  - Risk Analysis
- Review Session
  - Tomorrow!
  - Recorded: Yes
- Office Hours in SN137
  - Schedule Posted
- Written Assignment 1 Posted.
  - *Due Thurs at 11:59pm in Gradescope*
  - If you submit by tomorrow night, we will grade it before the quiz!

Will be detected?



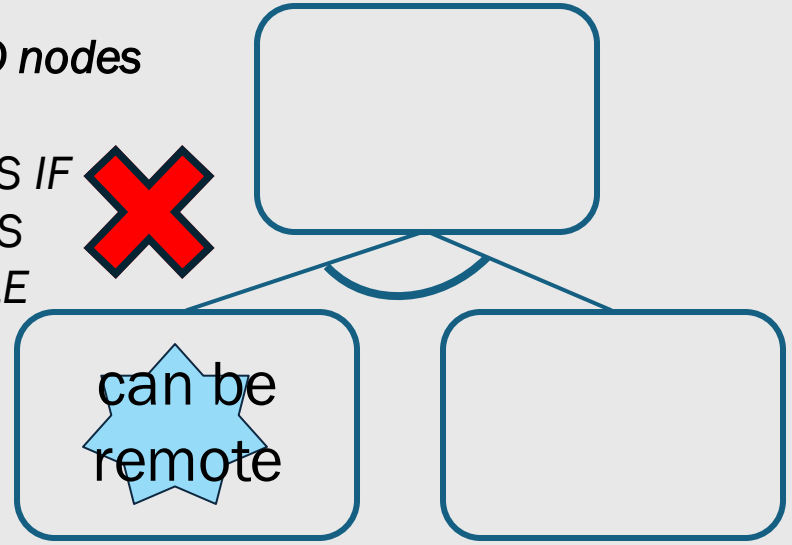
Case 1: AND nodes



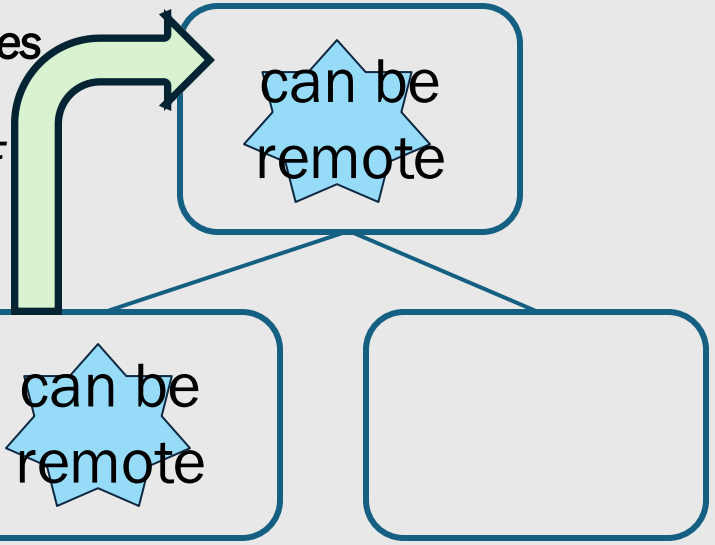
Case 2: OR nodes

Can be launched remotely?

Case 1: AND nodes
LABEL PROPAGATES IF BOTH NODES LAUNCHABLE REMOTELY



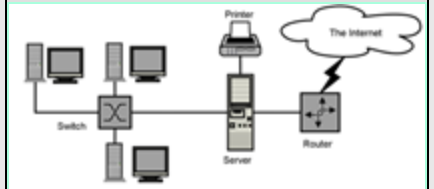
Case 2: OR nodes
** LABEL PROPOGATES IF ANY NODE LAUNCHABLE**



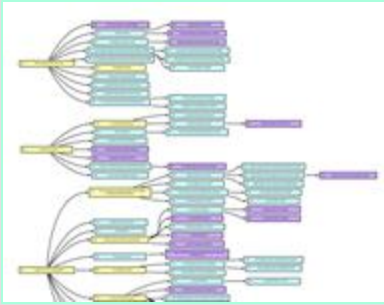
THREAT MODELING

Threat Modeling

Trees



Diagrams



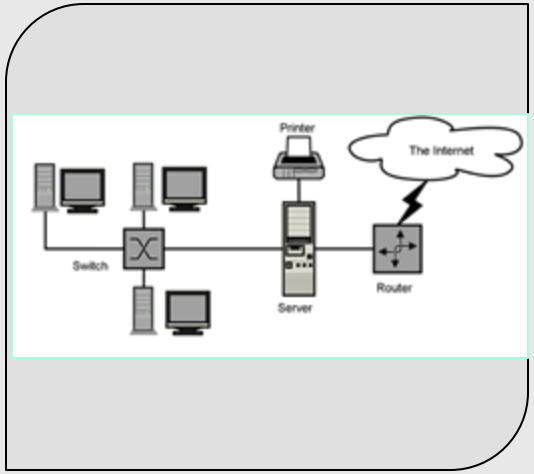
Lists

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Escalation of privilege

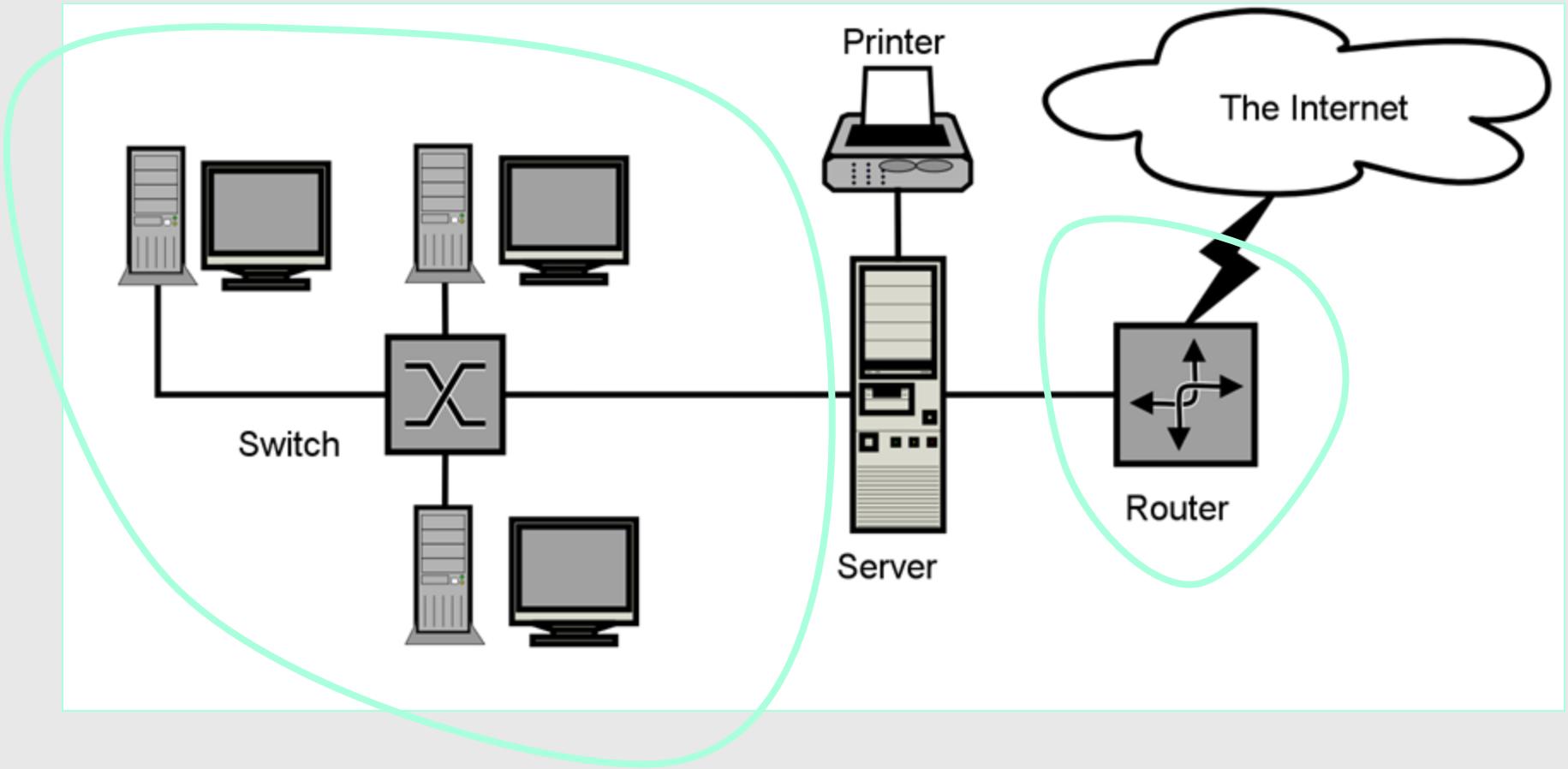
STRIDE

https://commons.wikimedia.org/wiki/File:Attack_tree_virus.png
https://en.wikipedia.org/wiki/File:Sample-network-diagram.png

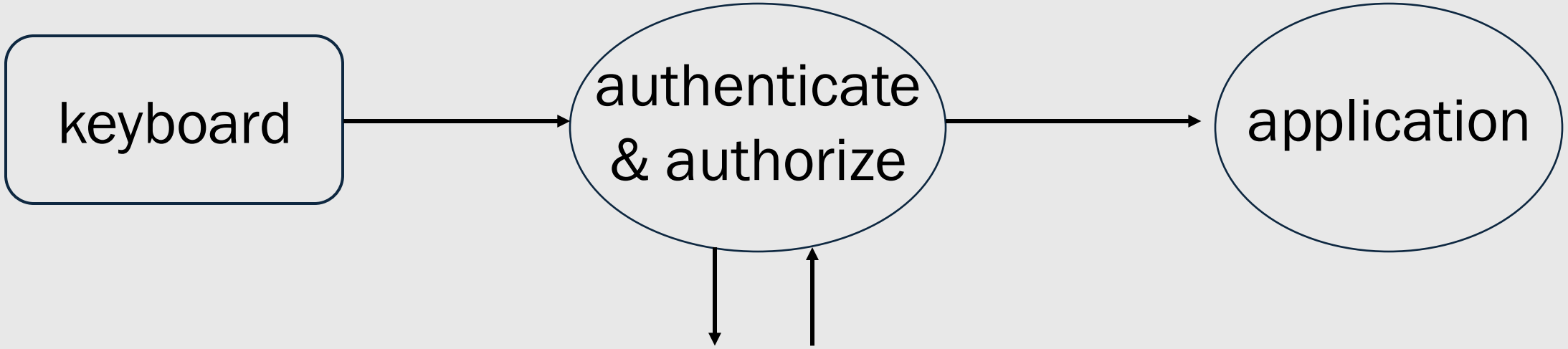
DIAGRAMS



Architectural Diagrams

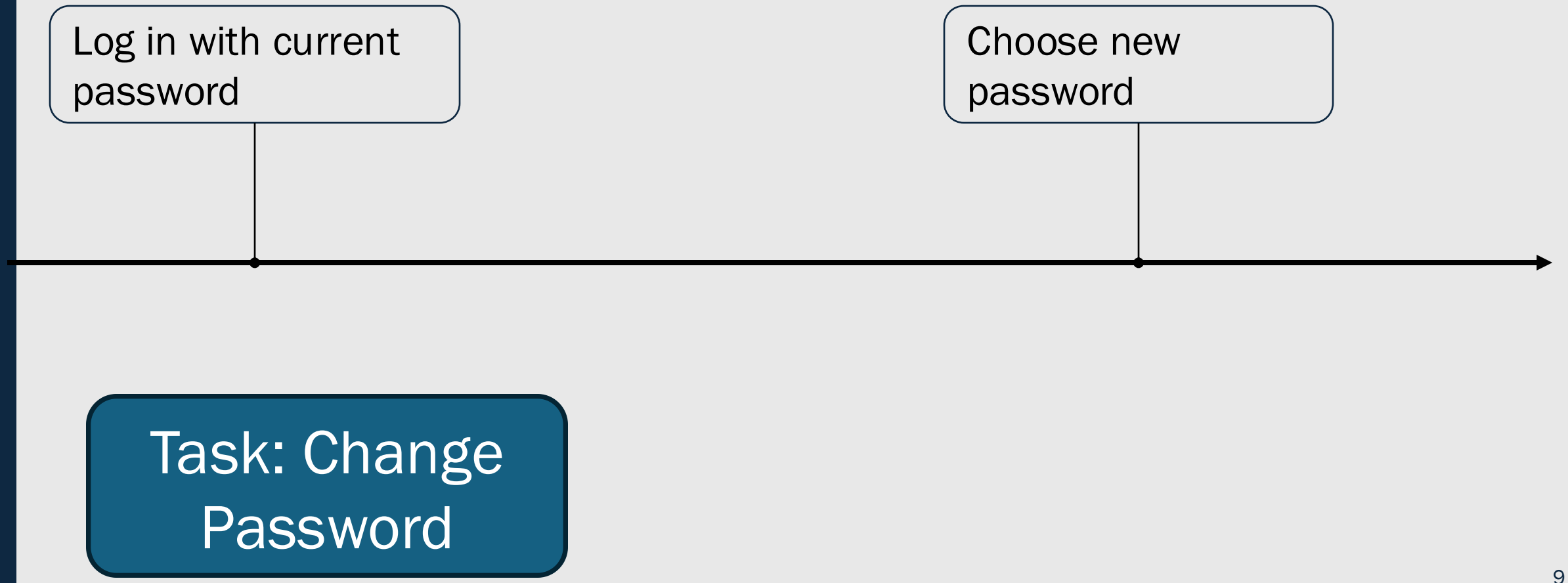


Dataflow Diagram

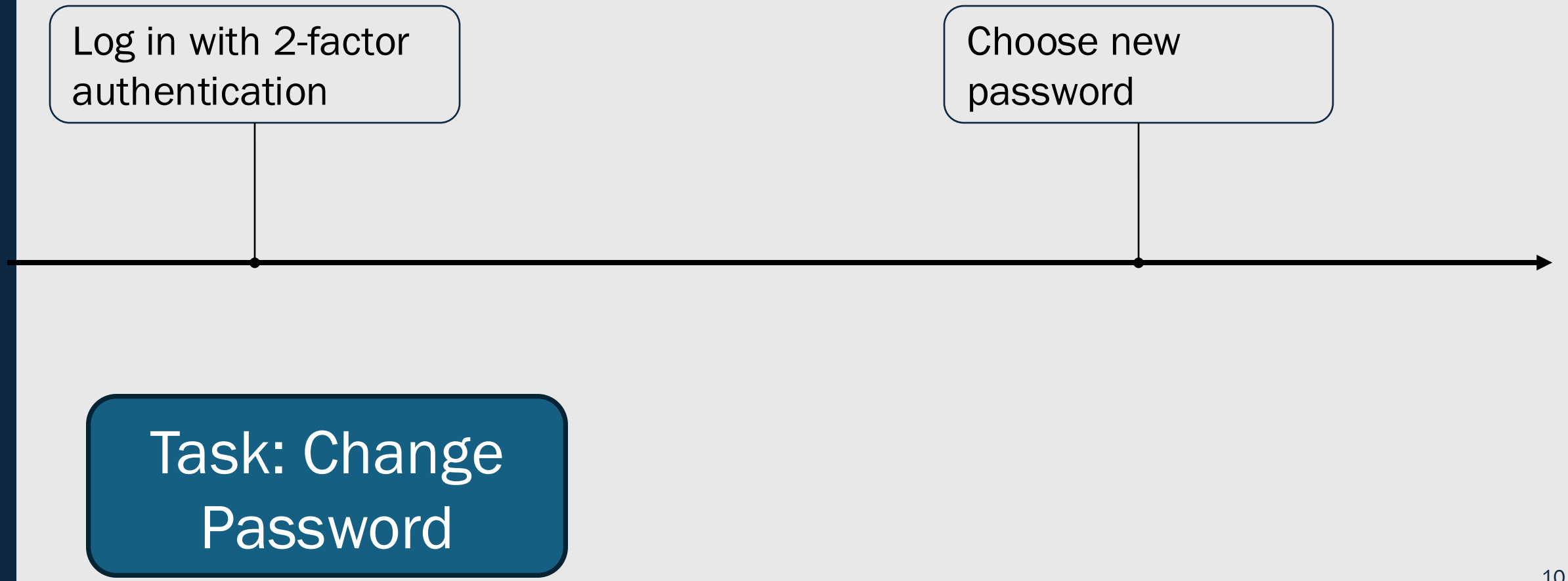


Task: Log in

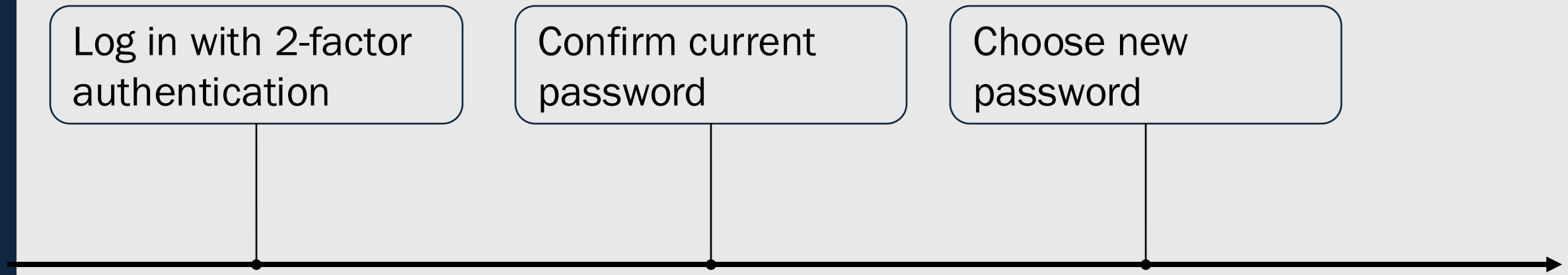
User Workflow Diagram



User Workflow Diagram

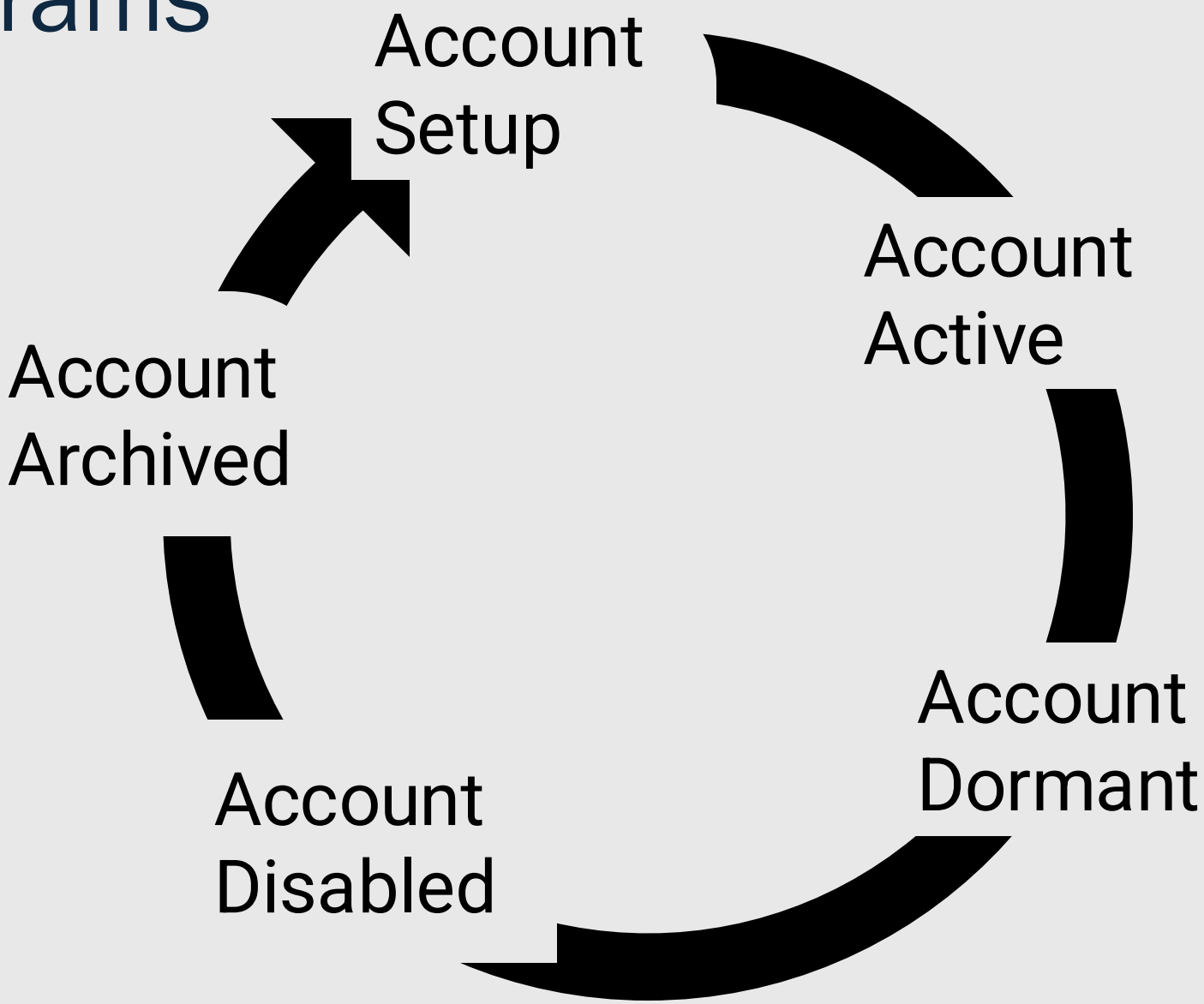


User Workflow Diagram



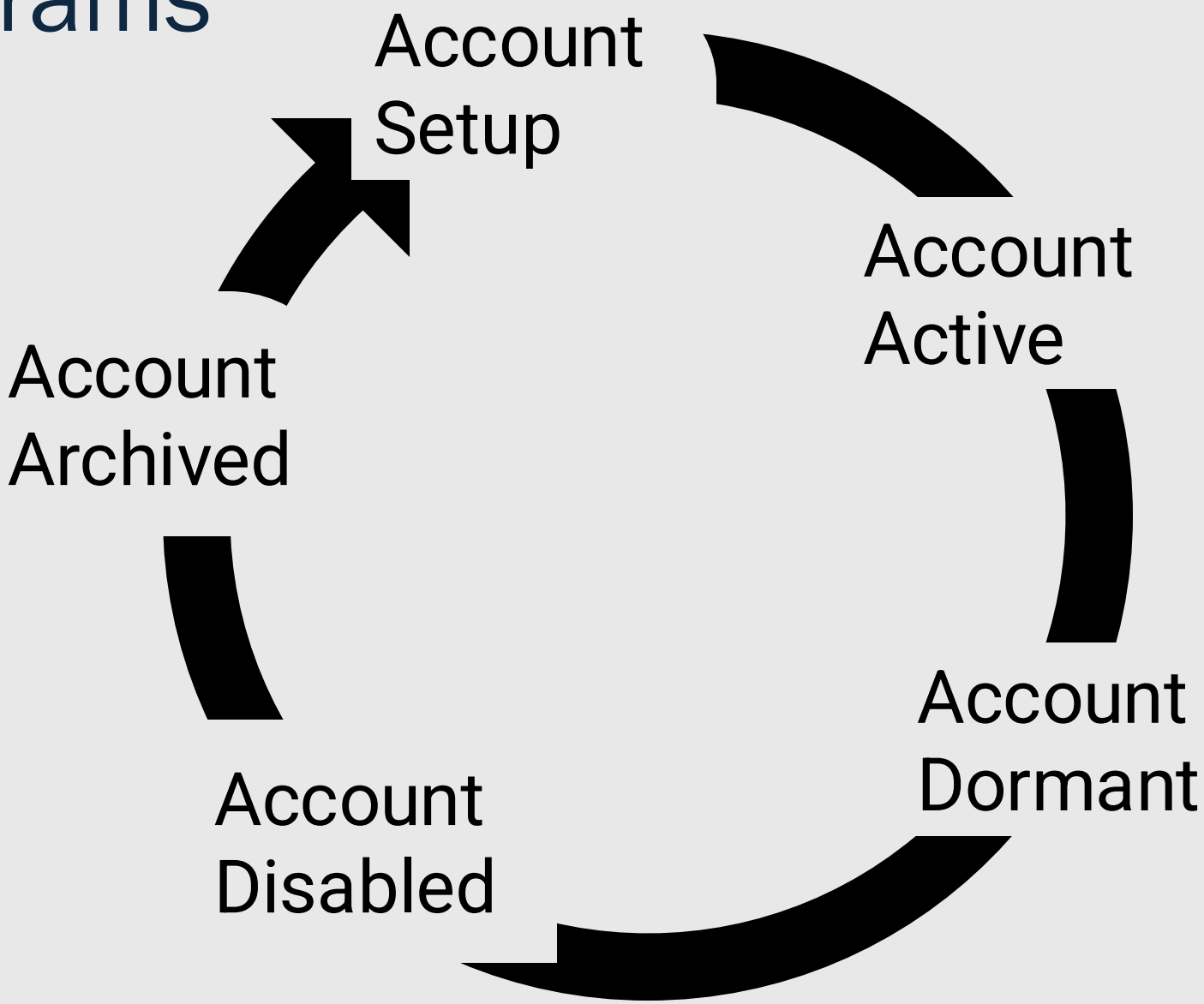
Task: Change Password

Lifecycle Diagrams

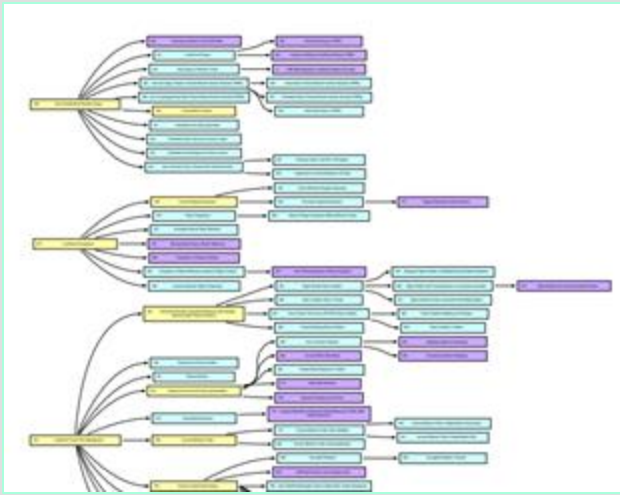


Lifecycle Diagrams

- Data
- Software
- Hardware
- Accounts



LISTS



MITRE Lists

- https://cwe.mitre.org/index.html
- https://cve.mitre.org/index.html

STRIDE

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service
- **E**scalation of privilege

STRIDE

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service
- **E**scalation of privilege

STRIDE

- ***Spoofing***  Impersonating an entity
- **T**ampering
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service
- **E**scalation of privilege

STRIDE

- Spoofing
- ***Tampering***  Unauthorized alteration
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service
- **E**scalation of privilege

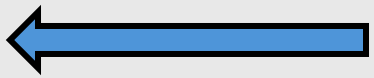
STRIDE

- Spoofing
- Tampering
- ***Repudiation***  Denying responsibility
- Information disclosure
- Denial of service
- Escalation of privilege

STRIDE

- Spoofing
- Tampering
- Repudiation
- ***Information disclosure***  Unauthorized release of data
- Denial of service
- Escalation of privilege

STRIDE

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- ***Denial of service***  Loss of availability
- Escalation of privilege

STRIDE

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- ***Escalation of privilege***  Gaining unwarranted privilege to resources

RISK

Risk

- Def: A possible event with a negative outcome; a potential problem
- I.e., Crossing the street

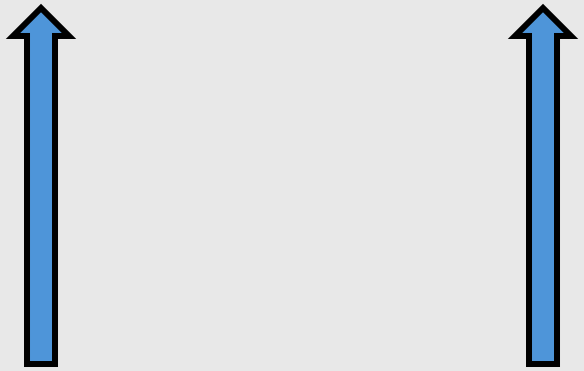
Risk Impact

- Def: a loss associated with the event
- E.g., loss of life, lost time, lost money, bad publicity

Risk Probability

Def: the likelihood an event will occur in a given timeframe

$$0 \leq Pr[Event] \leq 1$$



Impossible Certain

Risk Exposure

Def: risk exposure = risk impact x risk probability

E.g., A projected impact of $5000 in hardware replacement costs, times a risk probability of 10% gives the risk exposure (for a particular event in a particular time frame) at $500.

$5000 x .1 = $500

Risk Control

- Def: actions taken to reduce or eliminate risk exposure
  - *E.g., Adding two-factor authentication*
- 3 main ways to handle risk
  - *Avoid*
  - *Transfer*
  - *Assume*

Handling Risk

- ***Avoid***
- Transfer
- Assume

change something to avoid the risk

Handling Risk

- Avoid
- ***Transfer***  reallocate the risk or buy insurance
- Assume

Handling Risk

- Avoid
- Transfer
- ***Assume***  Accept the risk

Risk Analysis

1. Identify assets
2. Determine vulnerabilities
3. Estimate likelihood of exploitation
4. Compute expected annual loss
5. Survey applicable controls and their costs
6. Project annual savings of control

1. Identify Assets

hardware

software

data

people

supplies

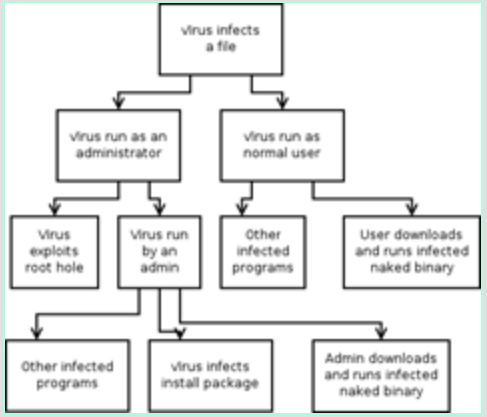
reputation

documentation

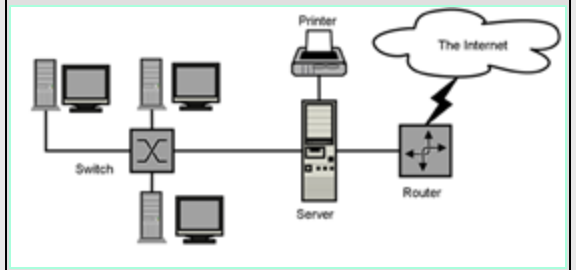
availability

2. Determine Vulnerabilities

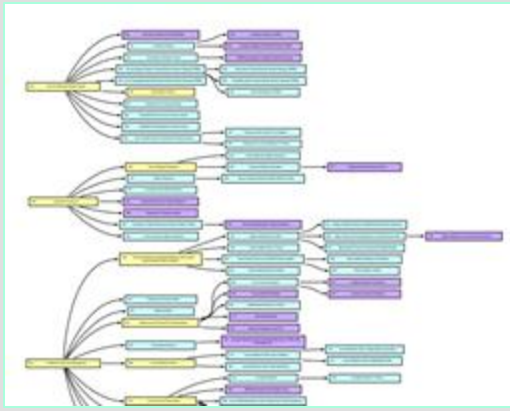
This is threat modeling



Trees



Diagrams



Lists

- **S**poofing
- **T**ampering
- **R**epudiation
- **I**nformation disclosure
- **D**enial of service
- **E**scalation of privilege

STRIDE

3. Estimate Likelihood of Exploitation

Calculate risk probability

- Model-based probability measure
- Frequency-based probability measure
- Expertise-based probability measure

3. Estimate Likelihood of Exploitation

Calculate risk probability

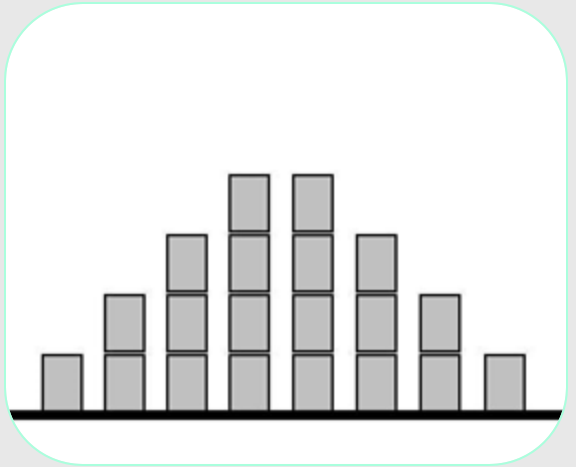
- ***Model-based probability measure***
- Frequency-based probability measure
- Expertise-based probability measure

$$Pr[E] = \frac{n(E)}{n(S)}$$

3. Estimate Likelihood of Exploitation

Calculate risk probability

- Model-based probability measure
- ***Frequency-based probability measure***
- Expertise-based probability measure



3. Estimate Likelihood of Exploitation

Calculate risk probability

- Model-based probability measure
- Frequency-based probability measure
- ***Expertise-based probability measure***

4. Compute Annual Expected Loss

Calculate risk exposure

hardware

software

data

people

supplies

reputation

documentation

availability

5. Survey and Select Controls

- Prevention vs detection
- Set of risks mitigated
- One-time vs ongoing costs
- Ease of use

6. Project Costs and Savings

annual

Risk Impact	$500,000
Risk Probability	.01
Risk Exposure	$5,000
Cost of Control	$300
Reduction of Risk	50%
Expected Costs	$2,800
Expected Savings	$2,200

6. Project Costs and Savings

Risk Impact	$500,000
Risk Probability	.01
Risk Exposure	$5,000
Cost of Control	$300
Reduction of Risk	50%
Expected Costs	$2,800
Expected Savings	$2,200

expected annual cost (500,000 x .01)

6. Project Costs and Savings

Risk Impact	$500,000
Risk Probability	.01
Risk Exposure	$5,000
Cost of Control	$300
Reduction of Risk	50%
Expected Costs	$2,800
Expected Savings	$2,200

6. Project Costs and Savings

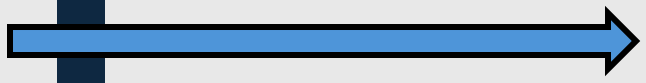
Risk Impact	$500,000
Risk Probability	.01
Risk Exposure	$5,000
Cost of Control	$300
Reduction of Risk	50%
Expected Costs	$2,800
Expected Savings	$2,200

remaining exposure = $2500

6. Project Costs and Savings

Risk Impact	$500,000
Risk Probability	.01
Risk Exposure	$5,000
Cost of Control	$300
Reduction of Risk	50%
Expected Costs	$2,800
Expected Savings	$2,200

new risk exposure + control cost



6. Project Costs and Savings

Risk Impact	$500,000
Risk Probability	.01
Risk Exposure	$5,000
Cost of Control	$300
Reduction of Risk	50%
Expected Costs	$2,800
Expected Savings	$2,200

($5000-$2800)

Calculating Risk Exposure (Q1)

Calculate the hospital’s annual risk exposure

Calculating Costs (Q2)

Considering the costs of risk mitigation, what should the hospital do?

Risk Analysis

- Increase awareness of risk
- Justify security expenditures
- Identify assets and their values

Pros

- False sense of accuracy & precision
- Never final
- Time consuming

Cons