CSC 580
Cryptography and Computer Security

Security Basics, Threat Modeling, and Attack Trees

January 18, 2018

Overview

Today: Discuss security principles and system/threat modeling

Handout: Homework problems

- Representative problems
- Work through them!
- Think about generalizations and practice those

On Tuesday: Will discuss solutions

On Thursday: First quiz

I hear … I forget
I see … I remember
I do … and I understand
- Ancient Chinese Proverb

Becoming a security expert

Language

- An expert is someone who “speaks the language”
- Terminology develops to capture key concepts
- In this class: Work on always using professional terminology - practice!

Mindset

- Extreme paranoia (that’s not a joke)
  - Remember: Attackers only need to find one vulnerability - you have to cover every possibility
- Security breaches are very different from random faults
- Locks on top of locks: **defense in depth**

Next: Let’s start learning the language

Computer Security - Big Picture

Setting the Stage...

Basic Goals (CIA)

- **Confidentiality**: Information only available to authorized parties
- **Integrity**: Information is precise, accurate, modified only in acceptable ways, consistent, meaningful, and usable
- **Availability**: Services provide timely response, fair allocation of resources, quality of service

Sometimes added (esp. in talking about “Information Assurance”)

- **Non-repudiation**: Messages or actions are accompanied by proof which cannot be denied
- **Authentication**: Establishing the validity of a transmission, message, or originator (including verifying the identity of a participant)

Terminology 1

A **vulnerability** is a weakness in a security system.

- Can be in design, implementation, or procedures

A **threat** is a set of circumstances that has the potential to cause loss or harm.

Threats can be

- Accidental (natural disasters, human error, …)
- Malicious (attackers, insider fraud, …)

  NSA “major categories of threats”: fraud, hostile intelligence service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, and HUMINT

An **attack** is when a vulnerability is exploited to realize a threat - types:

- **Passive attack** (look but don’t touch) - **eavesdropping**, **traffic analysis**, ...
- **Active attack** (go crazy) - **masquerade**, **replay**, **tampering**, **denial of service**, ...

Terminology 2

A **security mechanism** is a process or technology used to prevent, detect, or recover from an attack.

Examples (very basic list):

- **Encryption** / encipherment: Prevents attacks on confidentiality
- **Digital signatures** / other **data integrity mechanisms**: detects attacks on integrity
- **Access control**: grants access to data only for authorized parties
- (Note… others in book)

Mechanisms are low-level - sometimes used to provide higher-level **services**

- Example: **AAA** (Authentication, Authorization, Accounting)
    - Sometimes Authentication, Access Control, Audit

Secure Design Principles

Best practices for not doing something stupid

Classic Design Principles [Saltzer & Schroeder 1973]

- Economy of Mechanism (KISS!)
- Failsafe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability

Newer additions:

- Isolation
- Encapsulation
- Modularity
- Layering (defense in depth)
- Least astonishment

Many secure design principles are just "building a reliable system" principles!

System / Security Modeling

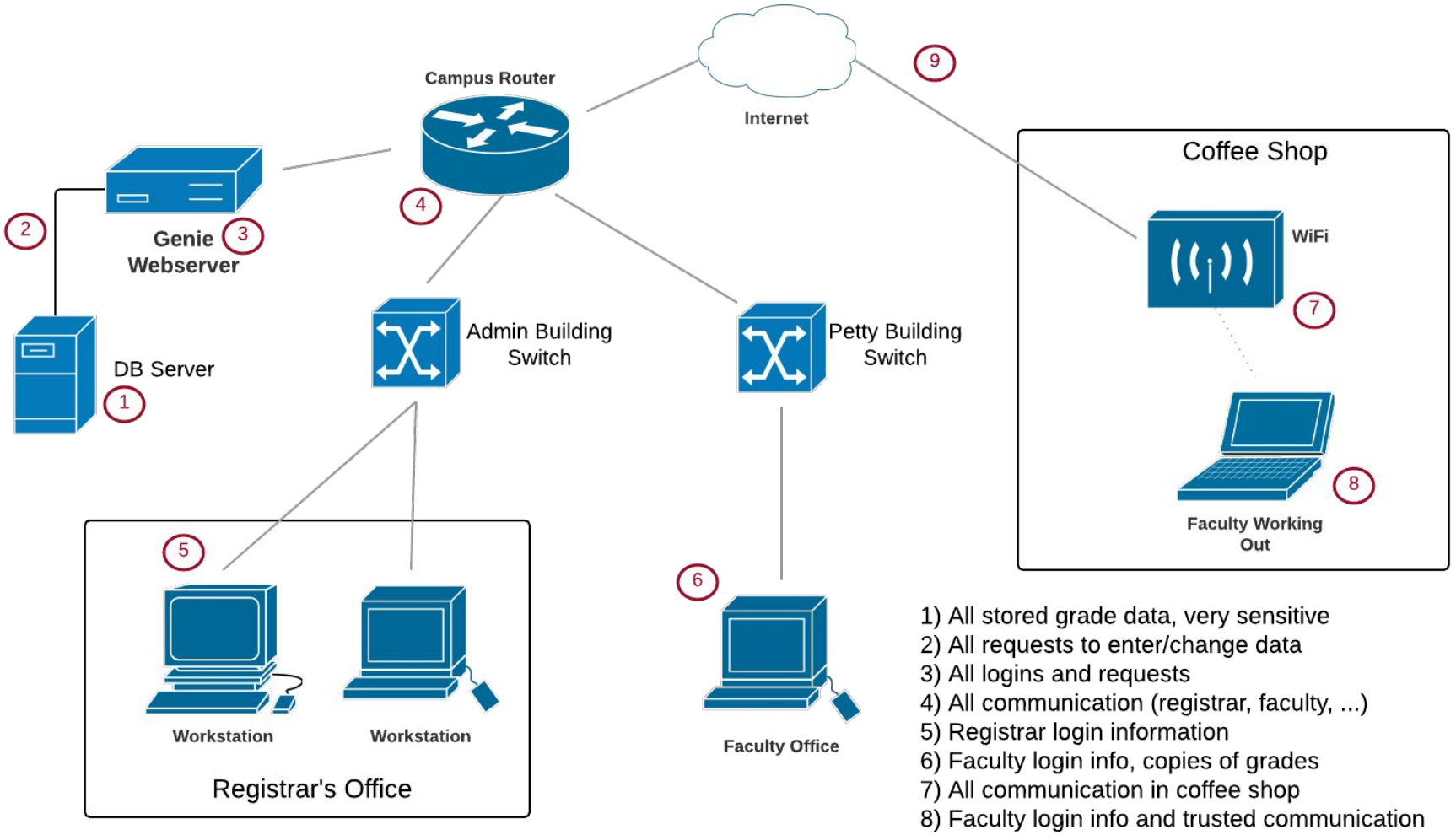
Purpose: Understand data flow through a system and security requirements

What to do

- Draw diagram showing key participants and technology
- Identify what data is at different points in system
  - Characterize by sensitivity level
  - Characterize systems/links by protection level
- Next step: Understand threats
- Then: Identify controls against threats

Example: Think about grade recording system at a university...

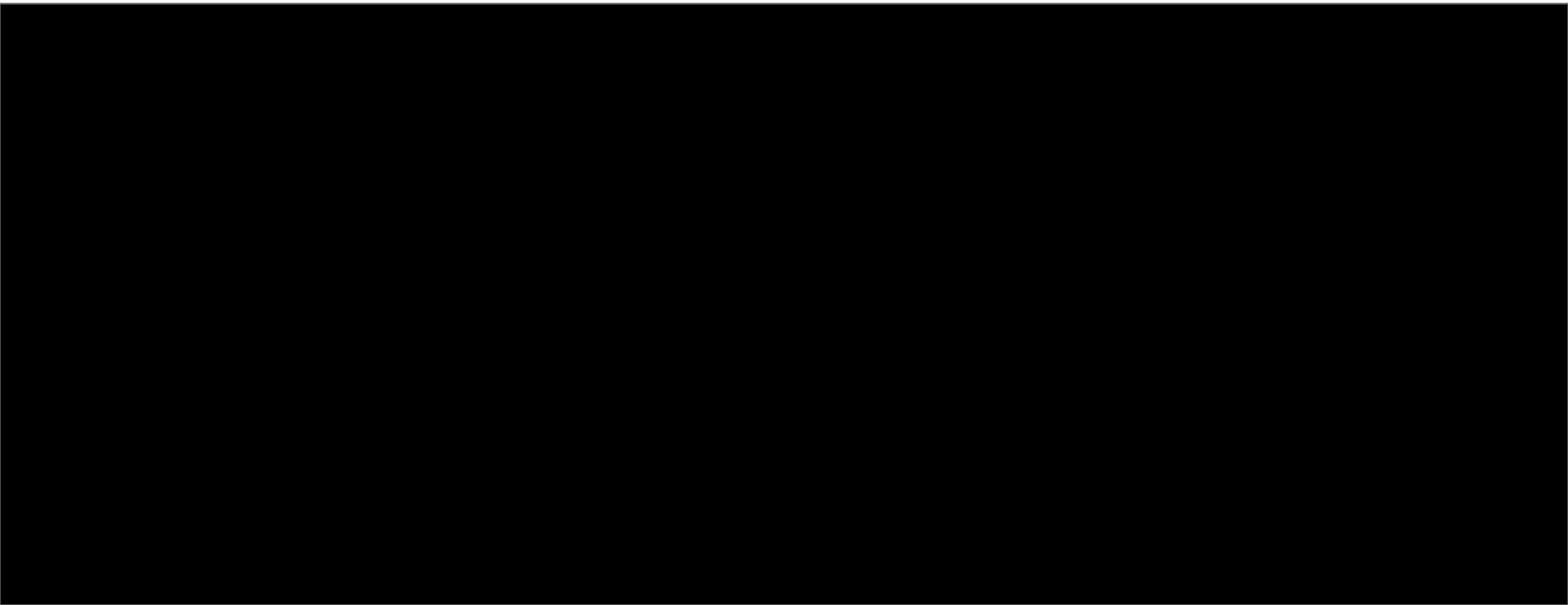
System / Security Modeling



1) All stored grade data, very sensitive
2) All requests to enter/change data
3) All logins and requests
4) All communication (registrar, faculty, ...)
5) Registrar login information
6) Faculty login info, copies of grades
7) All communication in coffee shop
8) Faculty login info and trusted communication
9) All Internet traffic

Your turn!

Sketch system for ATMs (and connection with bank).



Attack Trees

Try to identify all attacks on some valuable resource

- Technical attacks, but also people, physical, …
- Understand dependencies / requirements for attacks
- Goal: Thwart more dangerous attacks

Learn how attackers work and think like an attacker!

> If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.
>
> — Sun Tzu, *The Art of War*

Attack Tree

Example: Stealing customer data from company

Step 1: How to get to customer data (where does it exist)?

On the company fileserver ◈ on system backups ◈ in email being transmitted

Source: etutorials.org - Secure Linux-based servers

Attack Tree

Example: Stealing customer data from company

Step 1: How to get to customer data (where does it exist)?

On the company fileserver ◈ on system backups ◈ in email being transmitted

Step 2: Start tree - goal at root, avenues to the goal as children

Step 3: Located sensitive data, so how do we get to it?

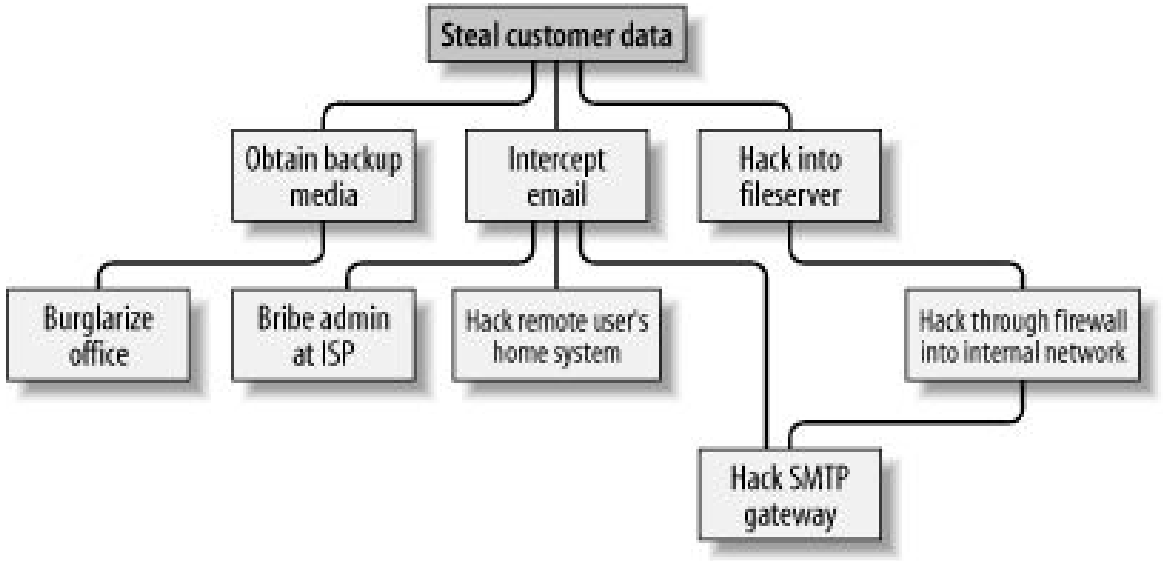
Become children of these leaf nodes

Can have “AND” and “OR” nodes - most attack trees are just OR nodes...

Source: etutorials.org - Secure Linux-based servers

Attack Tree

Example: Stealing customer data from company



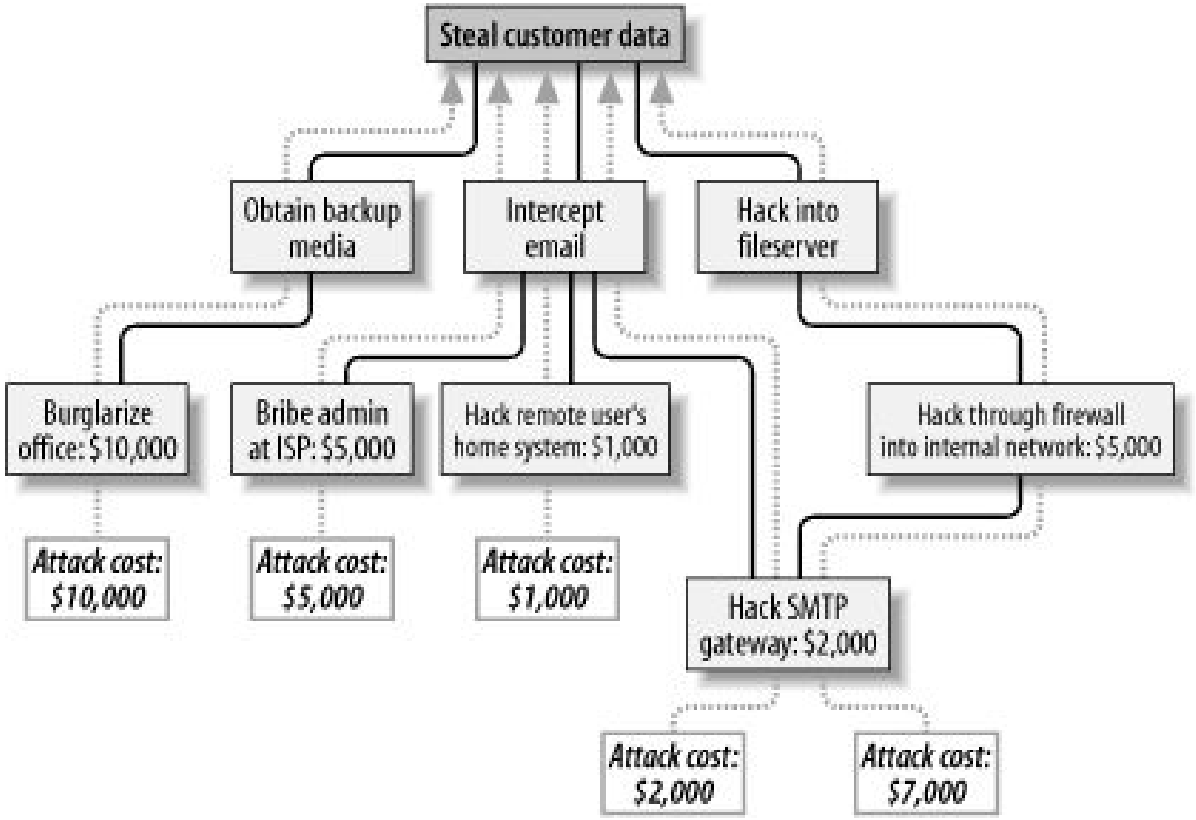
Next: Can estimate costs for each bottom-level action

Then: Propagate up (OR nodes are “min” ; AND are “plus”)

Source: etutorials.org - Secure Linux-based servers

Attack Tree

Example: Stealing customer data from company

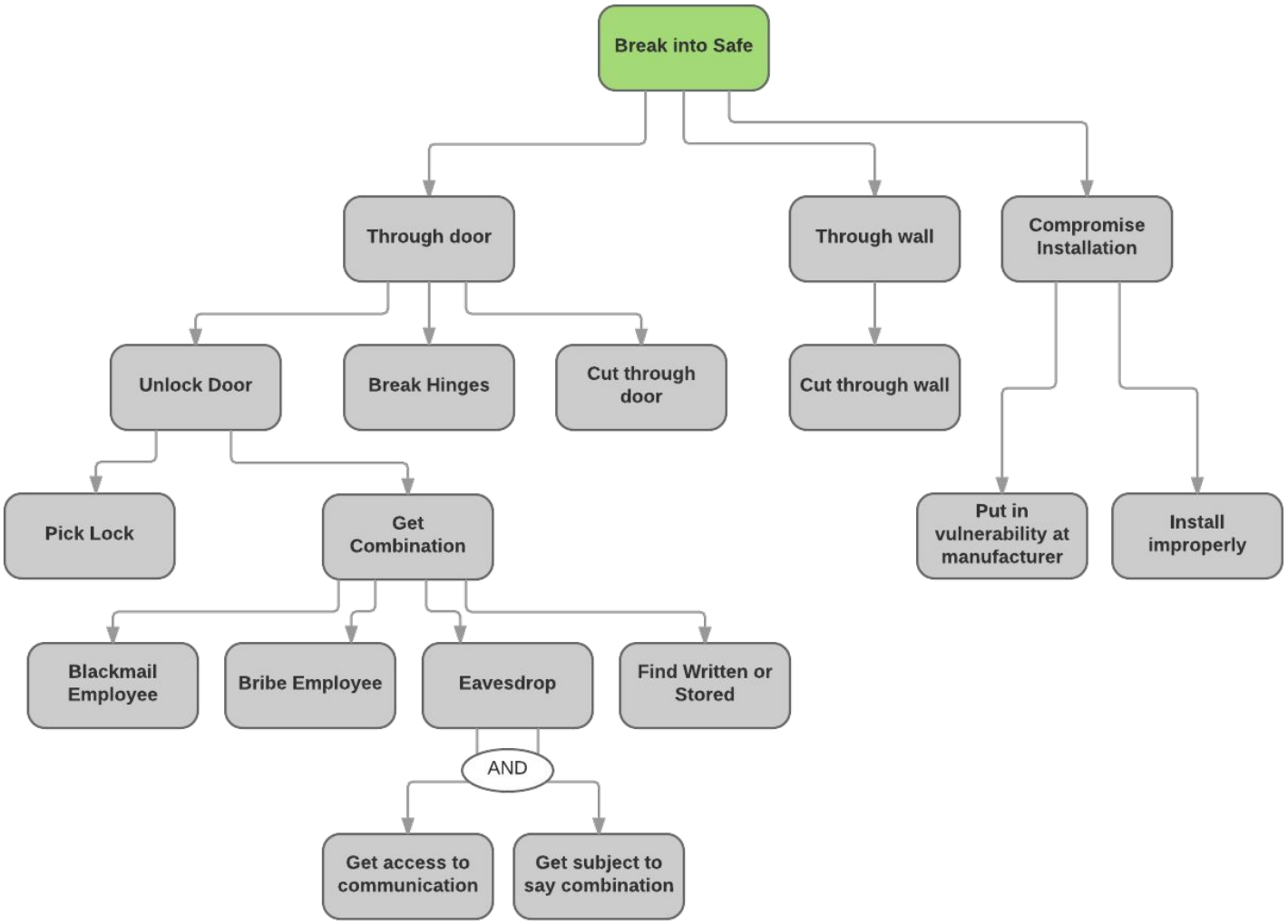


Goal: Maximize cost to attacker - where to put controls?

Source: etutorials.org - Secure Linux-based servers

Attack Tree

Example: Breaking into a safe



Your turn!

Make an attack tree for changing grades in student records.