Information Systems Integration
MIS 4596

Class 2

Agenda

- Threat Environment
- Cybersecurity Risk
- Threat Modeling
- Caution
- Next Week's Assignments
- Next Week's Quiz

Threat Environment

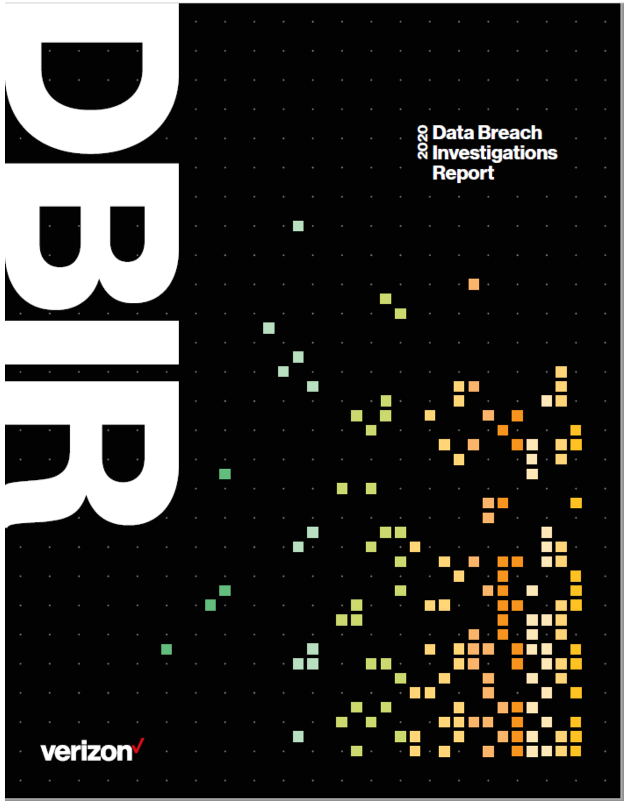
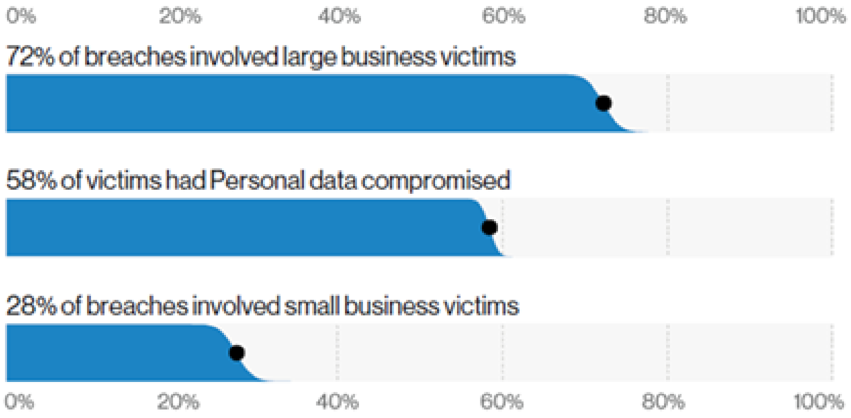


Figure 4. Who are the victims?

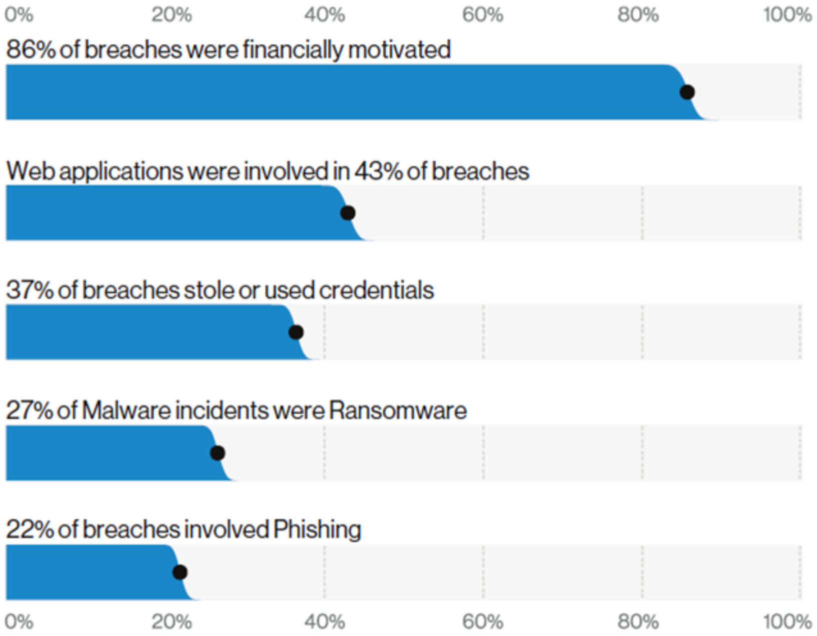


72% of breaches involved large business victims

58% of victims had Personal data compromised

28% of breaches involved small business victims

Figure 5. What are the other commonalities?



86% of breaches were financially motivated

Web applications were involved in 43% of breaches

37% of breaches stole or used credentials

27% of Malware incidents were Ransomware

22% of breaches involved Phishing

Based on analysis of 157,525 security incidents, of which 3,950 were confirmed data breaches

Threat Environment

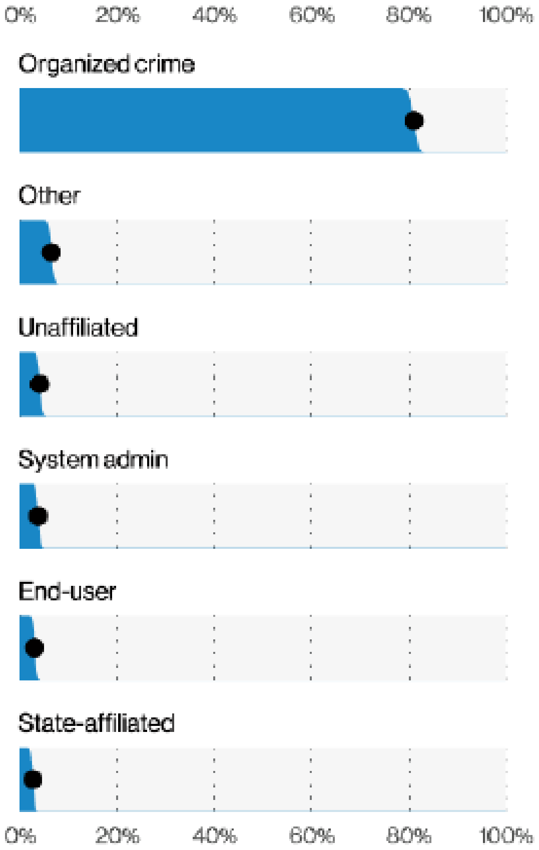


Figure 16. Top threat actor varieties in breaches (n=2,277)

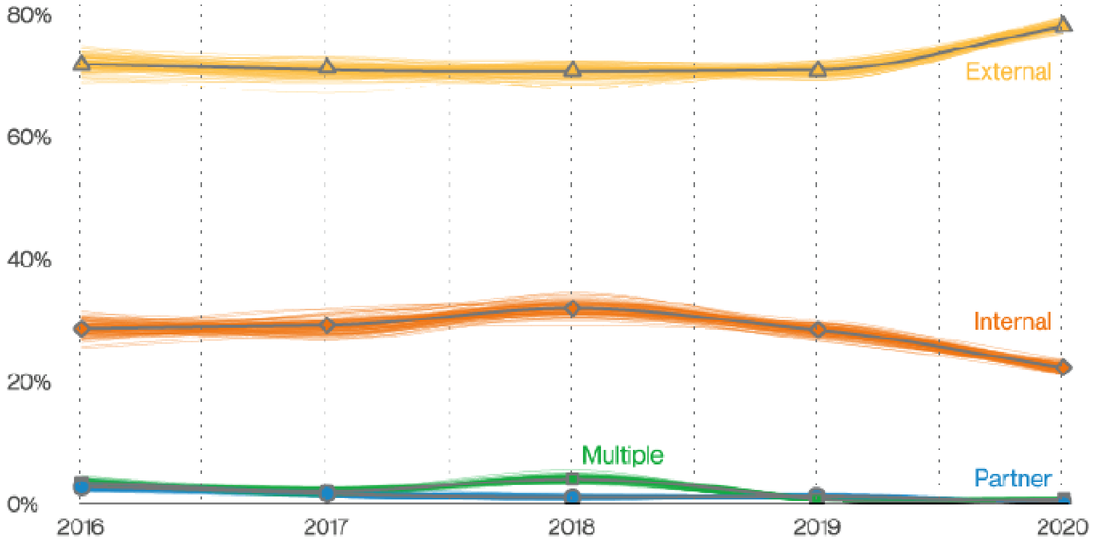


Figure 14. Threat actor over time in breaches

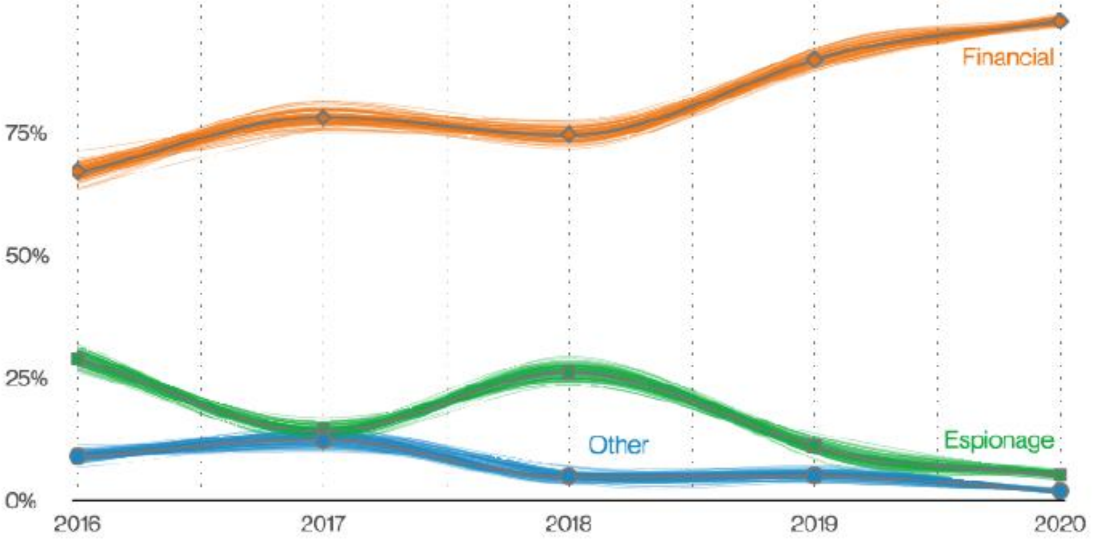
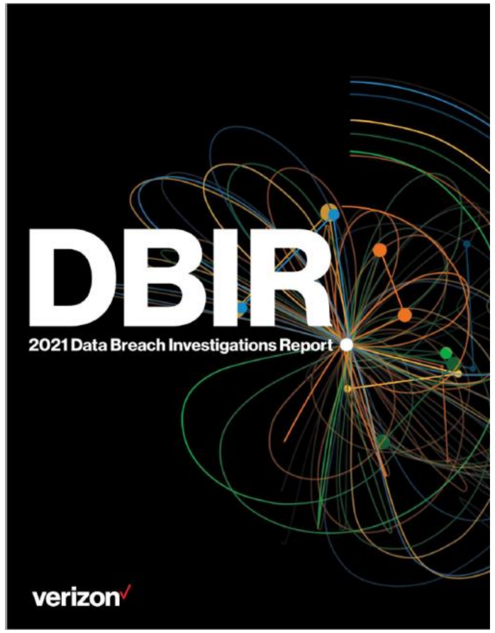


Figure 15. Top threat actor motive over time in breaches



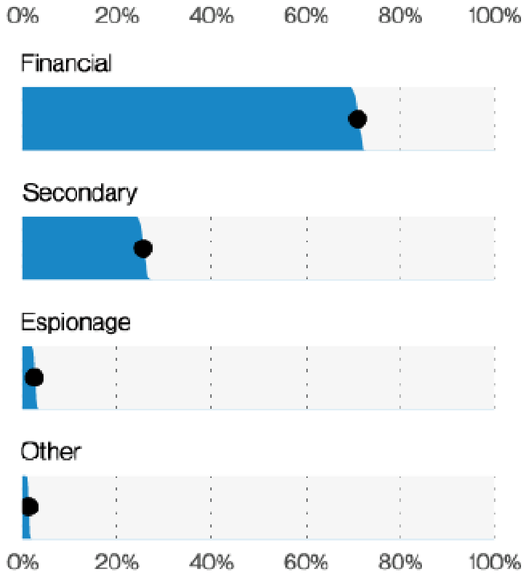
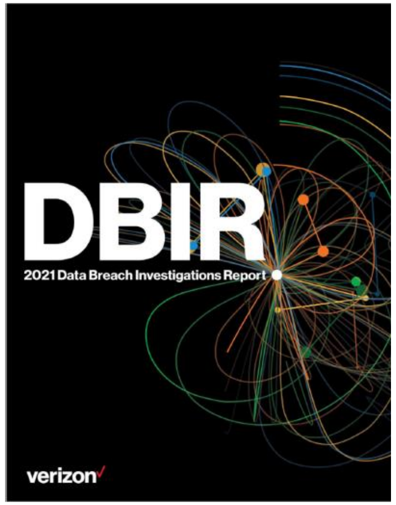


Figure 18. Top Actor motives in incidents (n=5,085)

Threat Environment



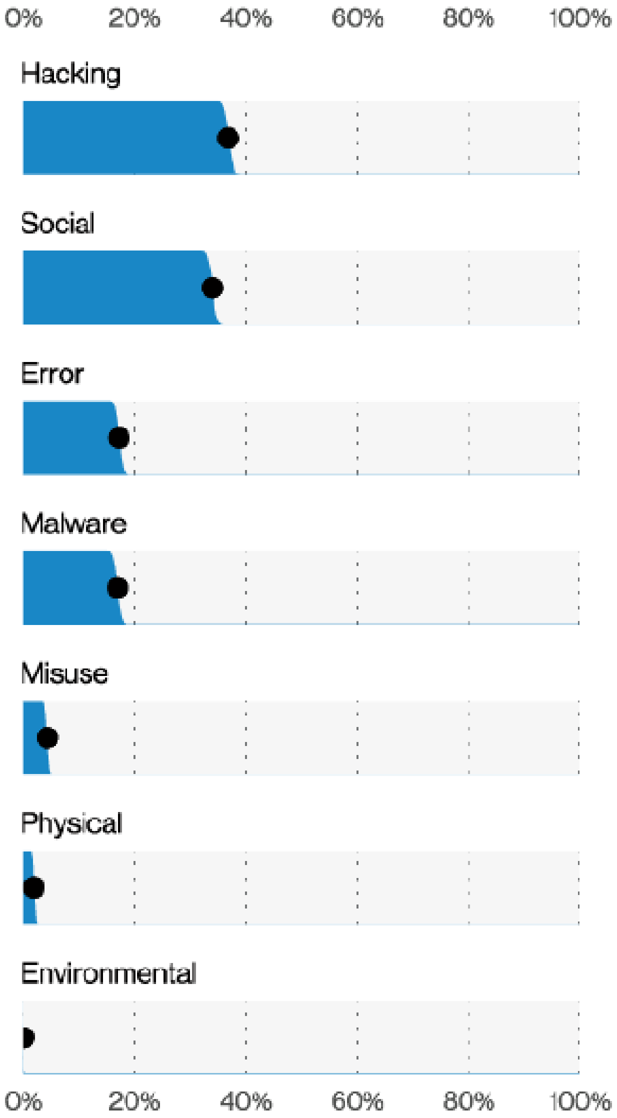


Figure 23. Actions in breaches (n=5,257)

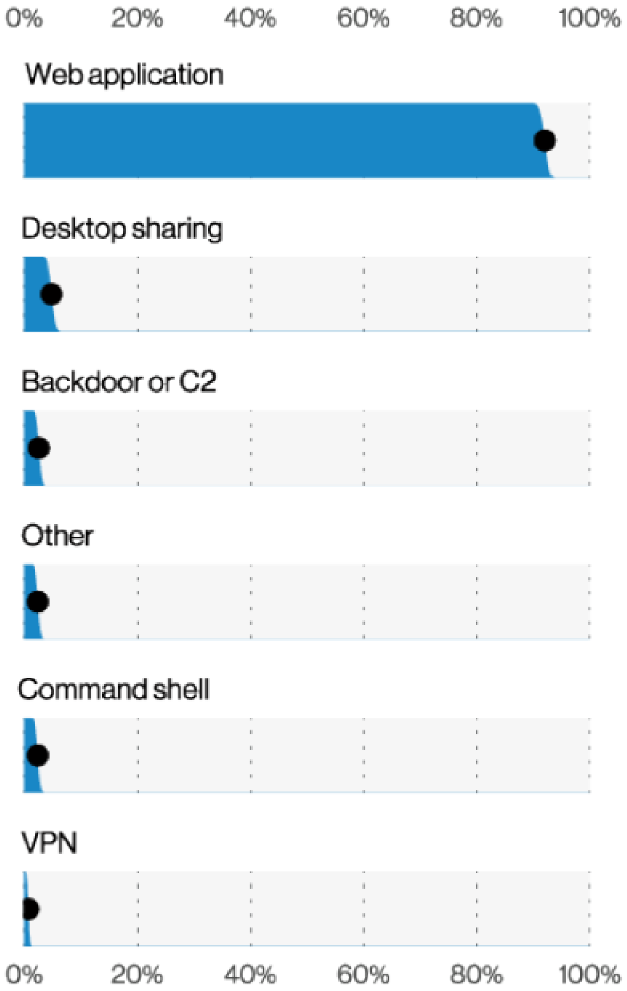
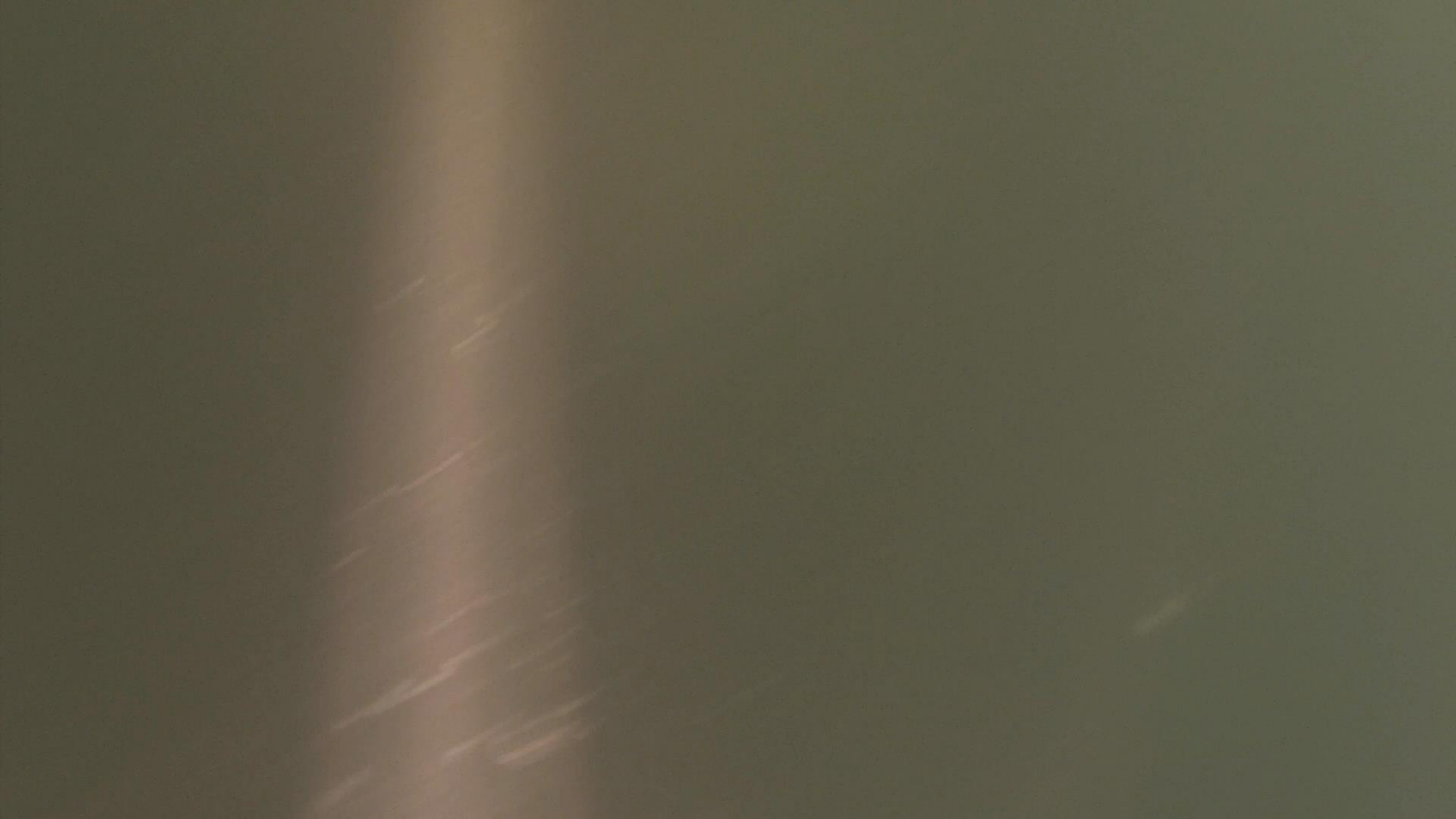


Figure 26. Top Hacking vectors in breaches (n=1,610)

Is this computer 100% secure?

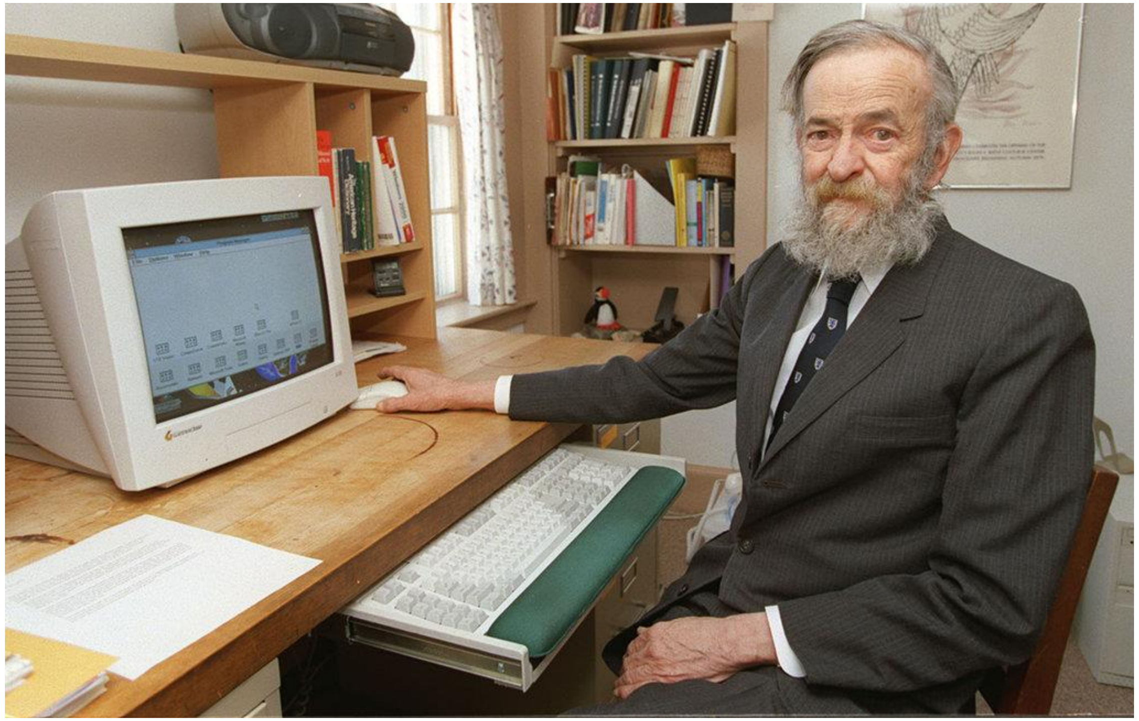
“How can we make a computer 100% secure?”



How can we make a computer 100% secure?

3 Golden Rules to ensure computer security:

1. Do not own a computer
2. Do not power it on
3. Do not use it



Robert Morris

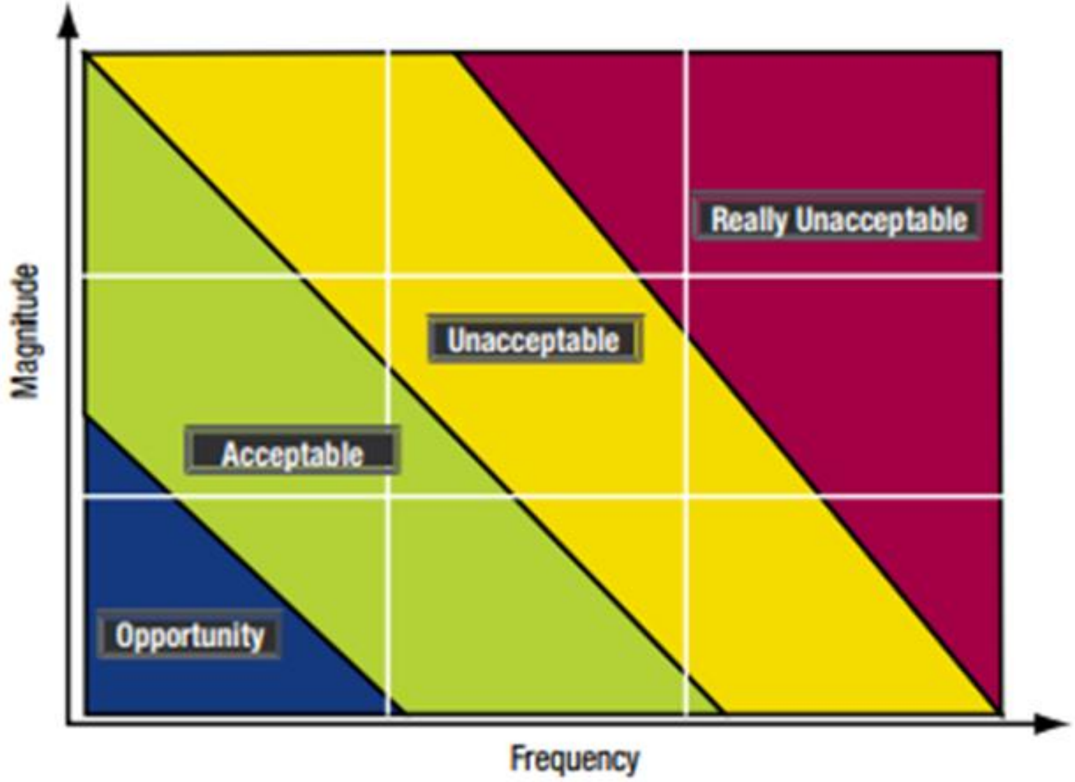
Cryptographer who helped develop the Unix computer operating system, which controls many of the world's computers and touches almost every aspect of modern life

Agenda

✓Threat Environment
- Cybersecurity Risk
- Threat Modeling
- Caution
- Next Week’s Assignments
- Next Week’s Quiz

Businesses cannot eliminate risk, but they can manage to acceptable level of risk, by

1. Avoidance
2. Acceptance
3. Transfer
4. Mitigation (“Controls”)



Quantitative definition of risk

Risk = Impact × Probability

- *Risk is an "expected value", which is a quantitative measure of impact a threat event would have on the organization times the probability that it might happen*

Annualize Loss Expectancy (ALE) = Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)

ALE = SLE X ARO

Single Loss Expectancy (SLE) = Asset value X Exposure factor

- Calculations of SLE consider such things as: replacement cost of the asset, opportunity cost of delays because asset is no longer available, cost for purchasing credit monitoring for customers, fines and other economic impacts of the loss of confidentiality, integrity and availability of the information or information system.

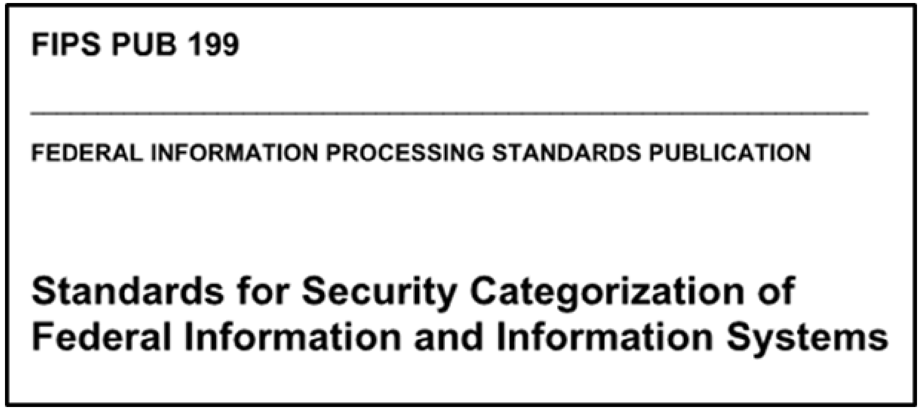
- Exposure factor is the % damage that a realized threat would have on the asset

Annual Rate of Occurrence (ARO) is a probability indicating how many times this is expected in one year?

It is often difficult to put a monetary value that captures the full extent of impacts breaches of confidentiality, integrity or availability have businesses and individuals

Risk is often dependent on the business and organizational context

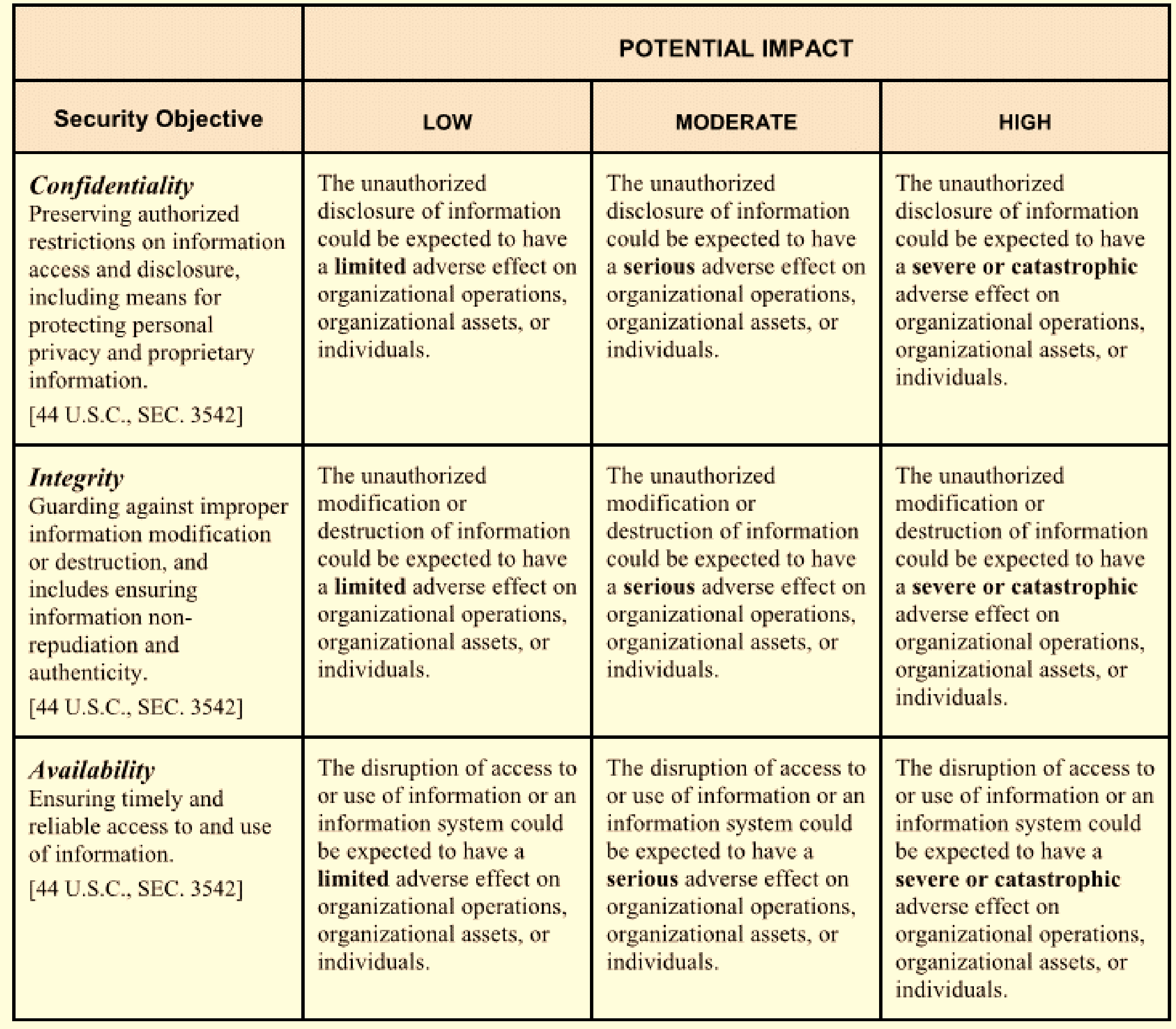
This is where qualitative measures of impact come in to help…



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems



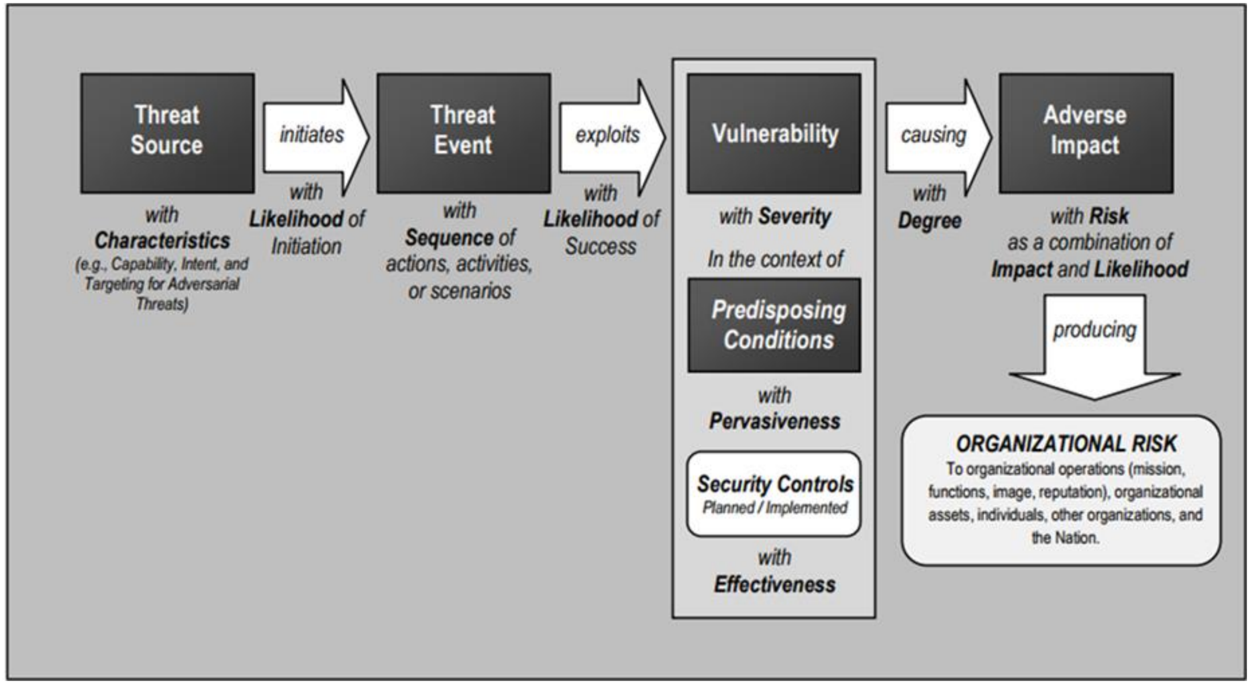
	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Qualitative descriptions of elements of risk can be expressed in quantitative format…

Risk = Asset × Vulnerability × Threat

- An *asset* is a thing that we are trying to protect
- A *vulnerability* is a weakness or gap in our protection efforts
- A *threat* is what we're trying to protect against –
  - a *motivated attacker* with *specific methods* and *resources*

…and can also be described as causal sequences



Threat Source
initiates
Threat Event
exploits
Vulnerability
causing
Adverse Impact
with Characteristics (e.g., Capability, Intent, and Targeting for Adversarial Threats)
with Likelihood of Initiation
with Sequence of actions, activities, or scenarios
with Likelihood of Success
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls Planned / Implemented
with Effectiveness
with Degree
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

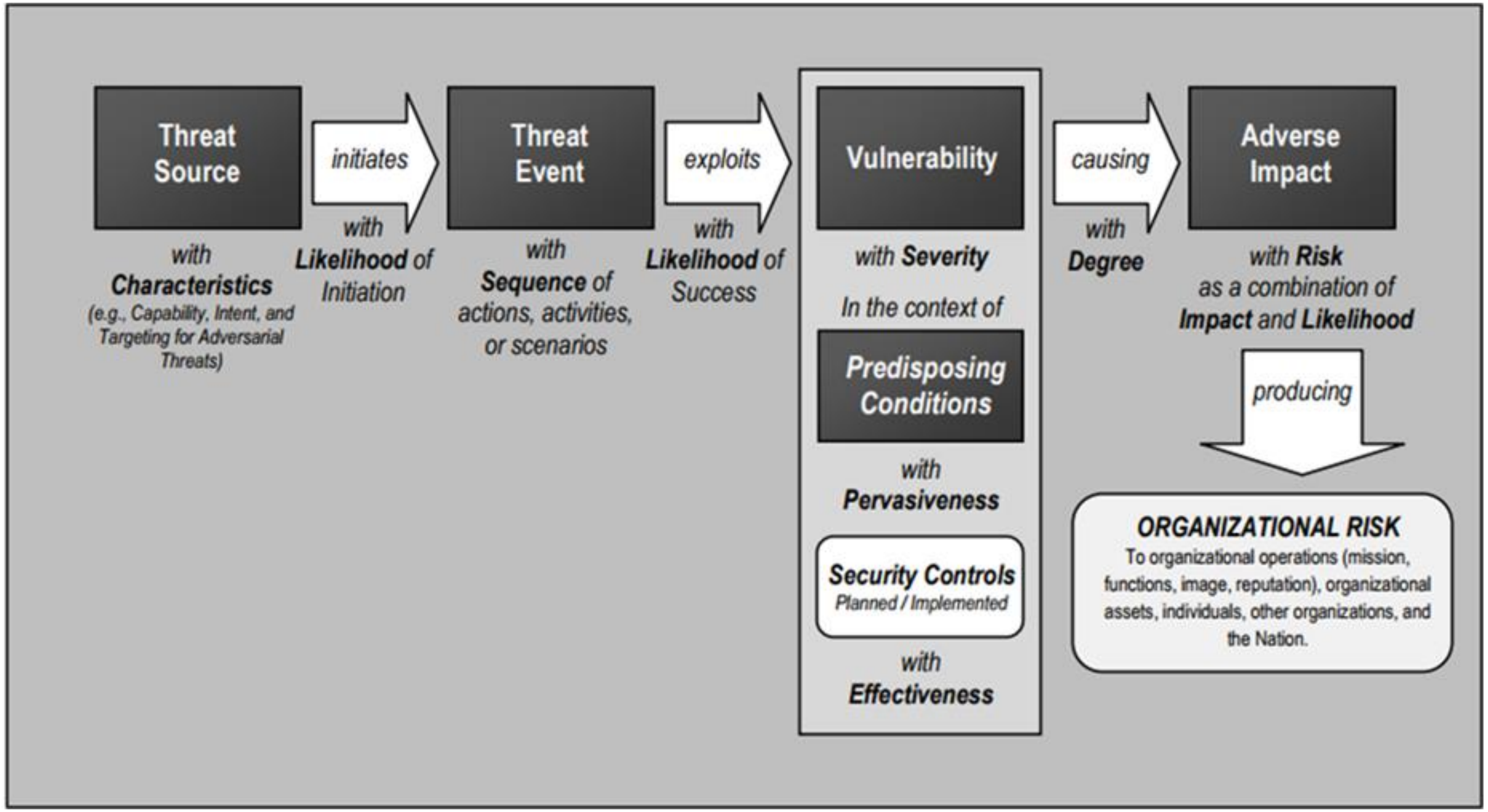
Agenda

- ✓Threat Environment
- ✓Cybersecurity Risk
- Threat Modeling
- Caution
- Next Week’s Assignments
- Next Week’s Quiz

Threat modeling helps us understand vulnerabilities and their relative importance to organizations

The most critical weaknesses can be prioritized for mitigation

assuring rational risk management investments to improve security


Threat Source
with Characteristics
(e.g., Capability, Intent, and Targeting for Adversarial Threats)
initiates
with Likelihood of Initiation
Threat Event
with Sequence of actions, activities, or scenarios
exploits
with Likelihood of Success
Vulnerability
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls
Planned / Implemented
with Effectiveness
causing
with Degree
Adverse Impact
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

Threat Modeling

The purpose of threat modeling is to provide defenders with a systematic analysis of what mitigations (i.e. controls or defenses) need to be included, based on the

- Assets most desired by an attacker
- Nature of the system
- Probable attacker's profile
- Most likely attack vectors

Threat modeling answers:

- *“What are the most relevant threats?”*
- *“Where am I most vulnerable to attack?”*
- *“What do I need to do to safeguard against these threats?”*

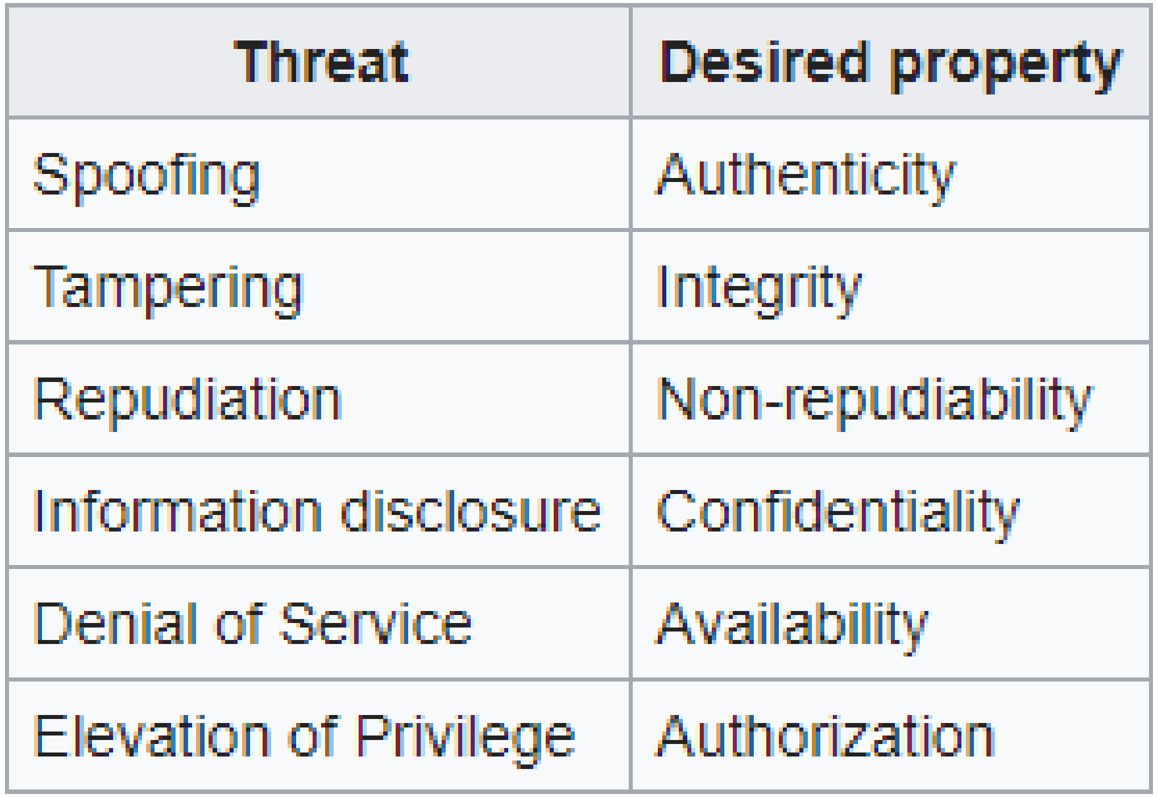
https://en.wikipedia.org/wiki/Threat_model

STRIDE

Threat modeling technique created by Microsoft, based 6 categories of threats:

- **Spoofing** – Can an attacker gain access using a false identity?
- **Tampering** – Can an attacker modify data as it flows through the system?
- **Repudiation** – If an attacker denies doing something, can we prove he/she did it?
- **Information disclosure** – Can an attacker gain access to private or potentially injurious data?
- **Denial of service** – Can an attacker crash or reduce the availability of the system?
- **Elevation of privilege** – Can an attacker assume the identify of a privileged user?

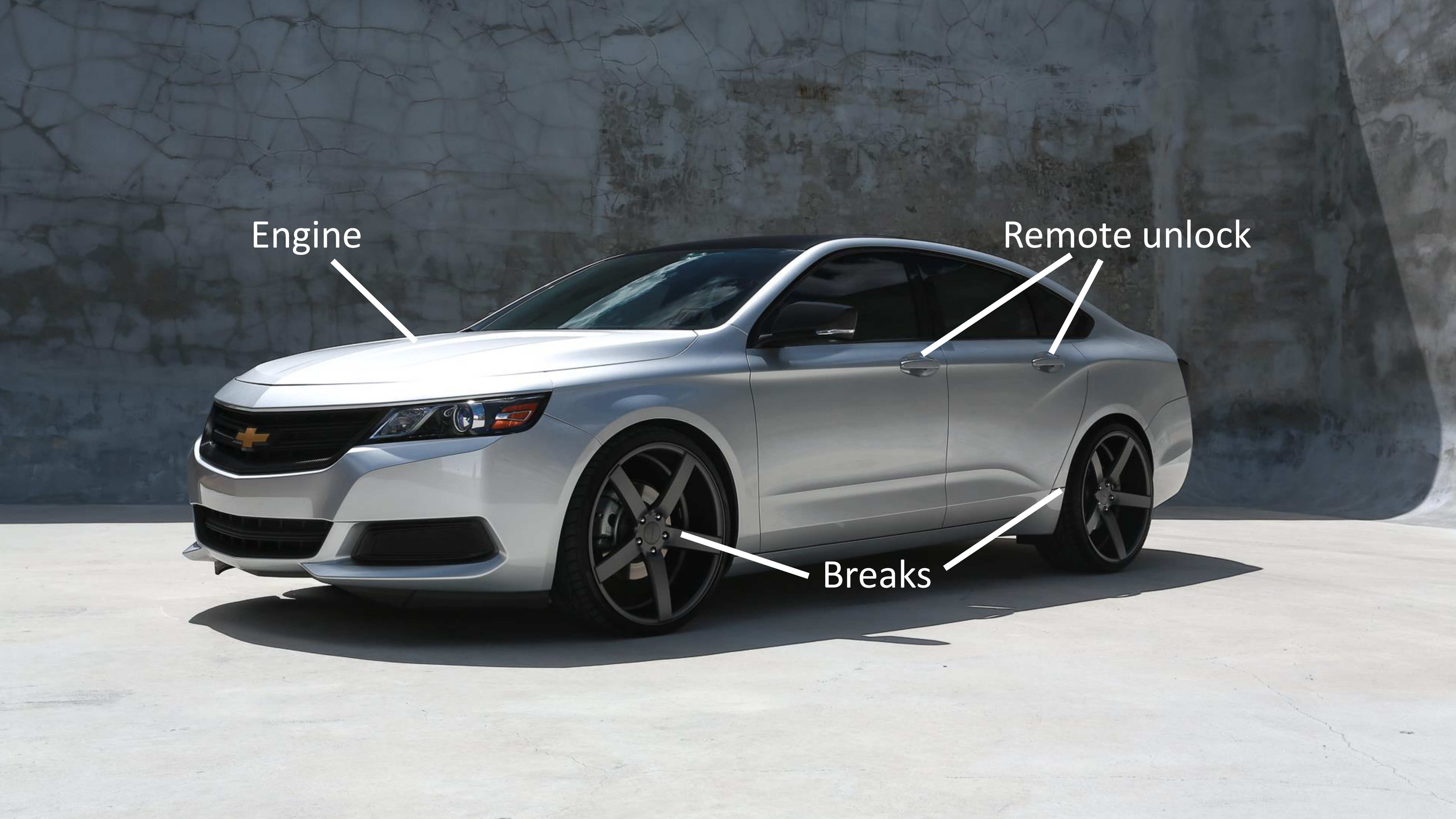
STRIDE threats and desired properties they impact

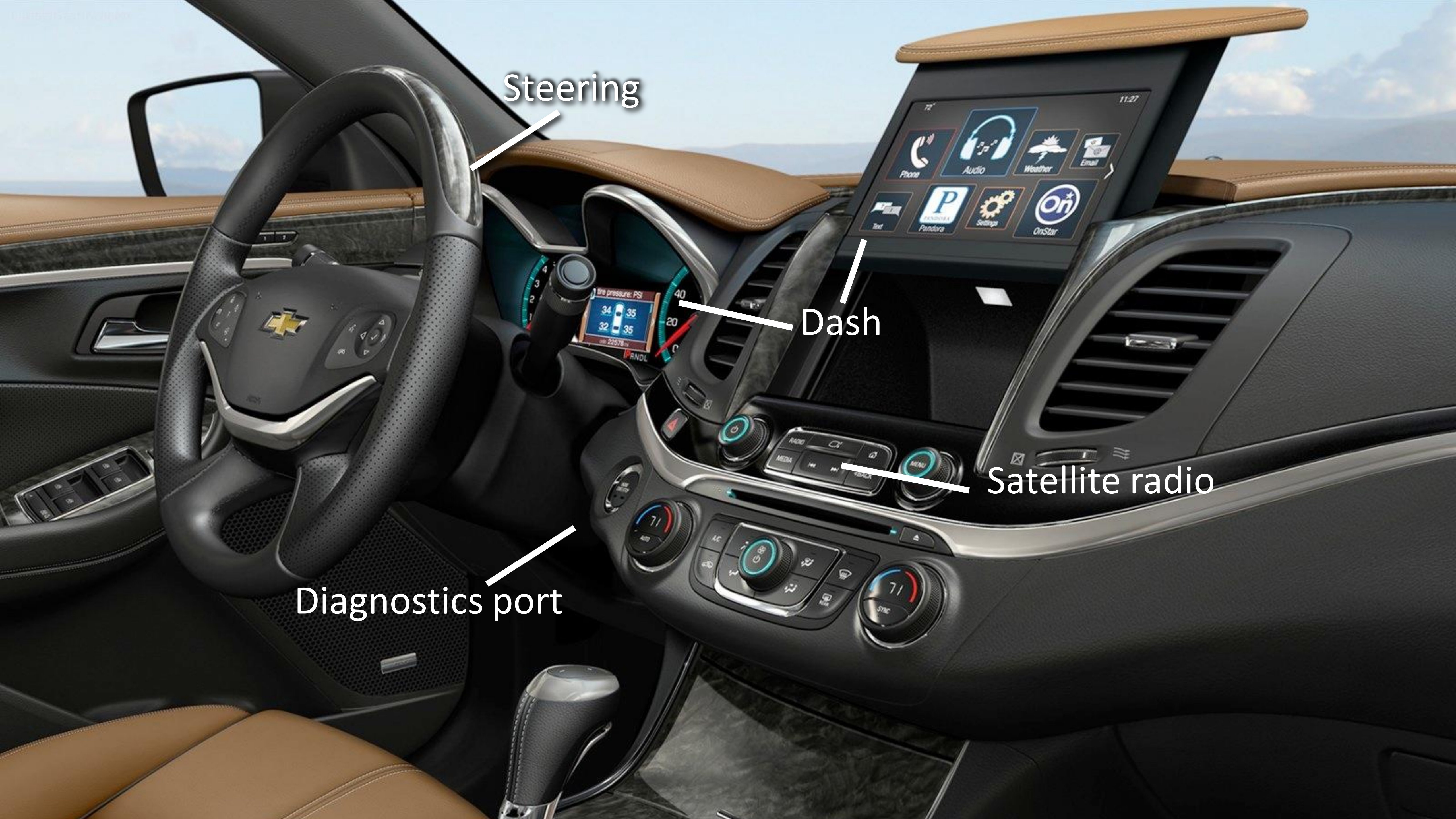


Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Modern Cars

…are computer networks on wheels, with most have many computers that control various aspects of the car


Engine
Remote unlock
Breaks



Steering

Dash

Satellite radio

Diagnostics port

University of Washington Security Cards

A security threat brainstorming activity – Access Cards Here

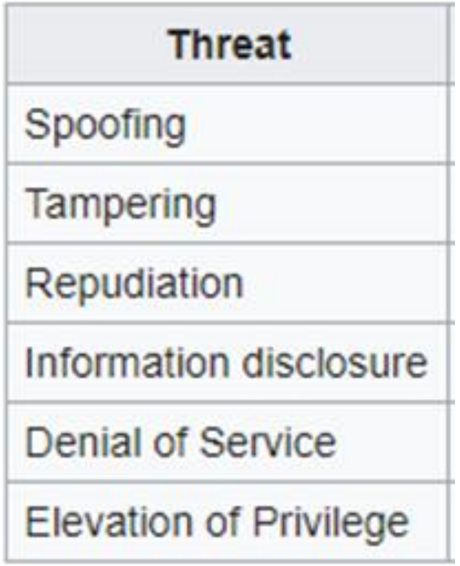
Break up into groups of 3:

- Pretend you are security professionals
  - A car company tasked you with thinking through the security implications of the modern car computer systems
- Start with the blue suit of cards (“Human Impact”), consider what impacts to people would result if an attacker misused modern car systems like the attack you just witnessed
  - Either think about one car, or think about the entire car product line
  - Rank order the cards from most relevant
  - Explain your 3 top choices

STRIDE Threat Modeling

A security threat brainstorming activity

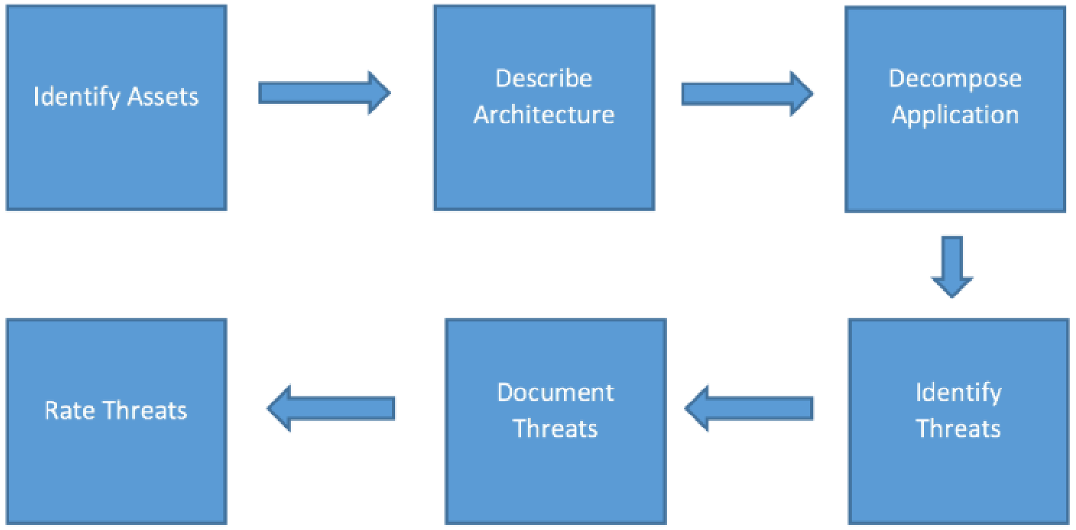
- Set aside the UW Security Cards, and use the STRIDE model
- Consider what methods adversaries might use for attacking modern car systems
  - Either think about one car, or think about the entire car product line
  - Rank order the threats from most relevant
  - Explain your 3 top choices

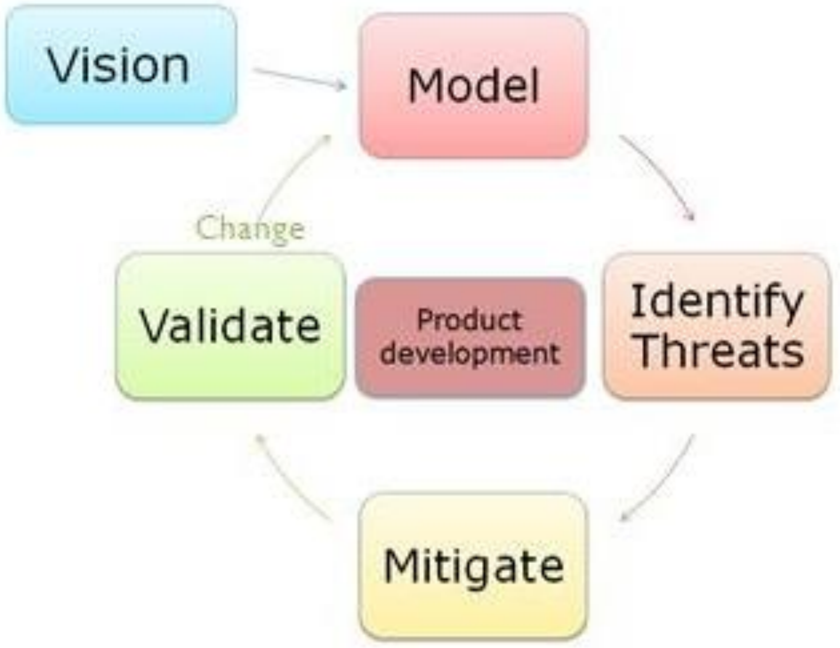


Threat
Spoofing
Tampering
Repudiation
Information disclosure
Denial of Service
Elevation of Privilege

Threat Modeling

- Can be a full-time job for cyber security professionals
- Is now a skill information systems designers, developers and architects need to have





Agenda

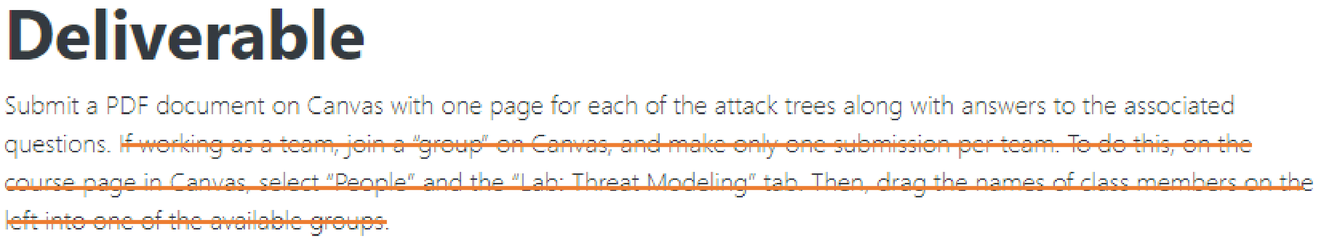
- ✓Threat Environment
- ✓Cybersecurity Risk
- ✓Threat Modeling
- Security Mindset / Caution
- Next Week’s Assignments
- Next Week’s Quiz

Caution

- The tools and techniques discussed and used in this course should only be used on systems you personally own or have written permission to use.
- Some of the tools used have the potential to disrupt or break computer systems.

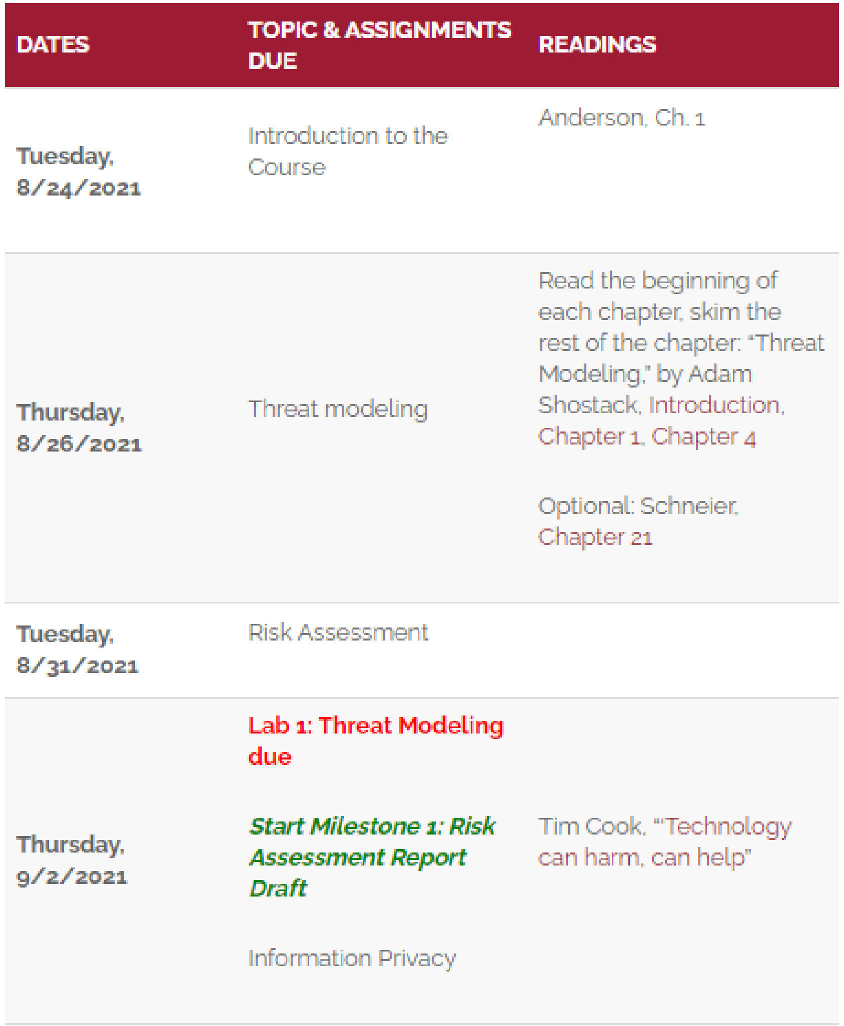
Next Week’s Assignments

1. Complete Lab 1: Threat Modeling
    - See Attack Trees (Chapter 21) by Bruce Schneier
        - Check for numbering scheme used in outline form of PGP Attack tree (Figure 21.7 on page 325)
    - You may work individually or in teams, but you must submit your own Lab 1 assignment as a PDF file in Canvas
    - Be sure to put all the names of the members of your team on your submittal

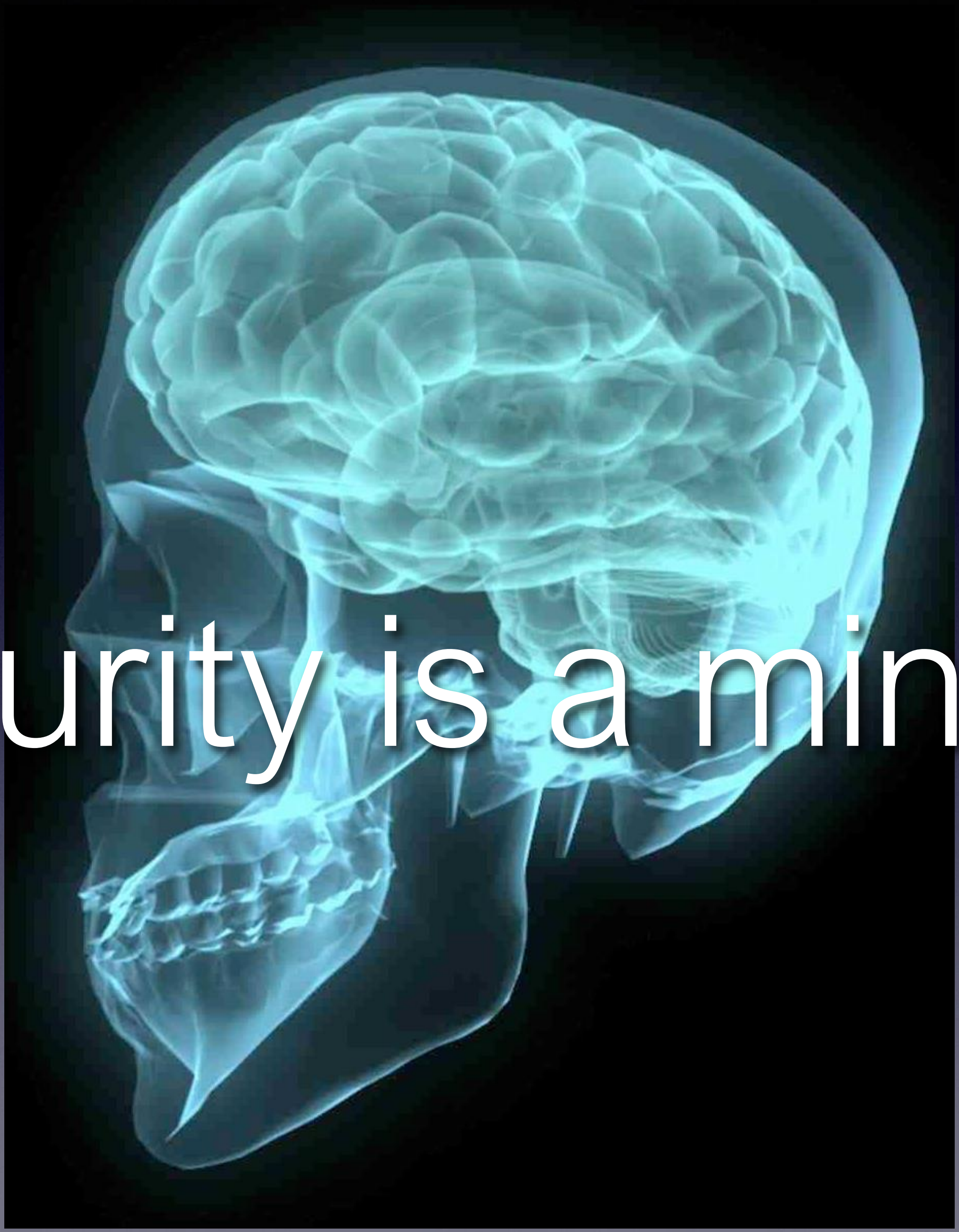


Deliverable

Submit a PDF document on Canvas with one page for each of the attack trees along with answers to the associated questions. ~~If working as a team, join a "group" on Canvas, and make only one submission per team. To do this, on the course page in Canvas, select "People" and the "Lab: Threat Modeling" tab. Then, drag the names of class members on the left into one of the available groups.~~

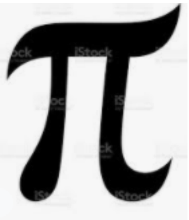


DATES	TOPIC & ASSIGNMENTS DUE	READINGS
Tuesday, 8/24/2021	Introduction to the Course	Anderson, Ch. 1
Thursday, 8/26/2021	Threat modeling	Read the beginning of each chapter, skim the rest of the chapter: "Threat Modeling," by Adam Shostack, Introduction, Chapter 1, Chapter 4 Optional: Schneier, Chapter 21
Tuesday, 8/31/2021	Risk Assessment	
Thursday, 9/2/2021	**Lab 1: Threat Modeling due** ***Start Milestone 1: Risk Assessment Report Draft*** Information Privacy	Tim Cook, "Technology can harm, can help"



Security is a mindset

Next Week's Quiz



At the start of next class, I will give you five minutes to write out the first 100 digits of pi, from memory, on a sheet of paper

- When time is up, you will show the paper to me
- I will not make you clear your desk, but you will need to close your laptop and put your phone face down on the table or away in your bag or pocket
- I do not expect you to actually memorize the digits of pi—**I want you to cheat**.
- How you choose to cheat is entirely up to you. However, I will observe you in Zoom via your camera. If you are caught cheating, you will fail the quiz. Collaborative cheating is also allowed, but everyone involved will fail the quiz if caught.
- The class will vote on the most creative and effective cheating technique.
- The objective of the exercise is to learn how an adversary thinks and operates by deliberately loosening traditional academic rules and tapping personal creativity. To avoid any misunderstanding, this exception to the traditional ban on cheating only applies to this quiz and not to other graded assignments in the course. Cheating outside of this quiz will not be tolerated."

Goal: Help you develop a Security Mindset

Agenda

- ✓Threat Environment
- ✓Cybersecurity Risk
- ✓Threat Modeling
- ✓Caution
- ✓Next Week’s Assignments
- ✓Next Week’s Quiz

Agenda

- ✓Threat Environment
- ✓Cybersecurity Risk
- ✓Threat Modeling
- ✓Caution
- ✓Next Week’s Assignments
- ✓Next Week’s Quiz
- ➢2 extra threat modeling activities… if there is time

University of Washington Security Cards

A security threat brainstorming activity

- Next move onto the **orange** “Adversary Motivation” suit
- Consider what motivations adversaries might have for attacking modern car systems
  - Either think about one car, or think about the entire car product line
  - Rank order the adversary motivations from most relevant to least
  - Explain your 3 top choices

University of Washington (UW) Security Cards

A security threat brainstorming activity

- Next move onto the red “Adversary’s Resources” suit
- Consider what resources adversaries might have for attacking modern car systems
  - Either think about one car, or think about the entire car product line
  - Rank order the cards from most relevant
  - Explain your 3 top choices