Countdown

Class is starting now!

Course Overview

CS1660-CS1620-CS2660
Introduction to Computer Systems Security

Goals

- Provide an introduction to computer security
  - Overview security threats and defenses
- Help you develop a security-aware mindset:
  - Take the big picture and understand the details
  - Learning by practicing
- Consider ethical implications and tradeoffs of using, building, and testing secure systems

What is security ?

Security is a chain…

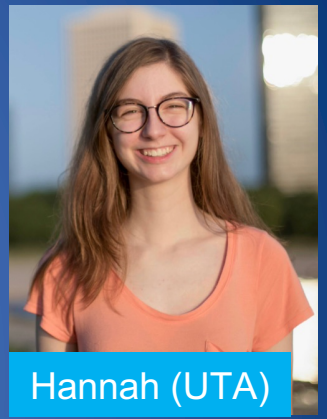
Staff


Bernardo (Prof)

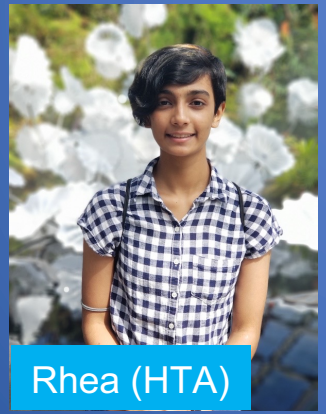

KP (HTA)


Brandon (UTA)


Camille (UTA)

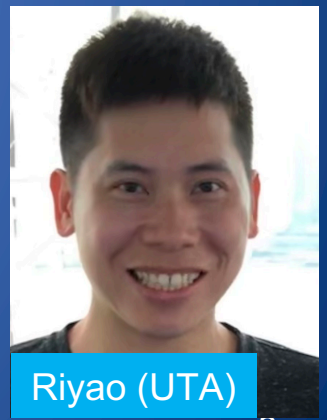

Hannah (UTA)


Nick (Prof)


Rhea (HTA)


Kim (UTA)


Rosa (UTA)


Riyao (UTA)

Security is a chain…

Lectures


Trust
Systems
Authentication
Computer
Crypto
Usability
Demos
Assignments
Security
Social
Attribution
Lockpicking
Operating
Anonymity
Passwords
Networks
Network
lectures
Technology
Pen-Testing

Lectures

- Security Principles
- Cryptography
- Authentication
- Operating Systems Security
- Network Security
- Web Security
- Applications Security
- TBD…

Class Participation

IN PERSON

- Raising your hand and asking question if you have any doubt
- Your question will be repeated by the instructor

ONLINE

- Please if possible keep open the video and mute the microphone
- To ask a question, please raise your hand or type “question” in chat

- Synchronous attendance encouraged, but not required
- All lectures and notes will be recorded
- The deadlines will be the same for all students

Clicker Questions

- Conducted via TopHat (Join Code: **821033**)
- You need to register
- Does not count towards your grade
- Engage with course material during lecture!

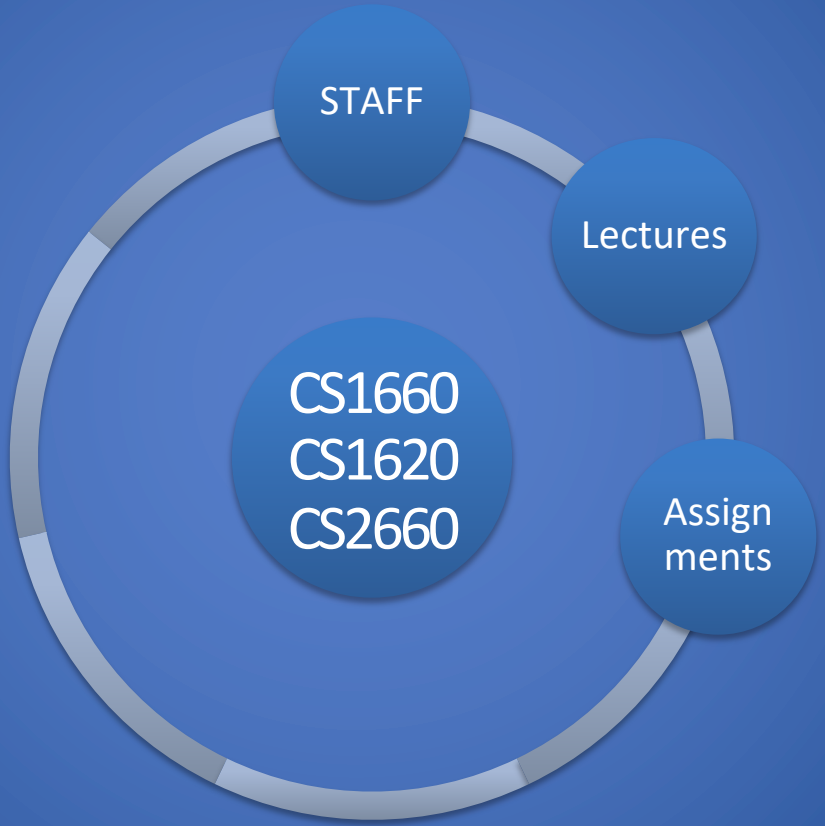
Live Demos

- See in class hands-on demonstrations of basic attack and defense techniques
- Try it yourself and show it to your friends
- Keep in mind that attack demos should be done in an ethical and legal manner

Disclaimer

- Any such techniques are taught only for educational purposes.
- The techniques are taught to you in simulated or isolated environments that prevent harm to other parties.
- You should not use these techniques outside the setting of the course.

Security is a chain…



Assignments

- 4 Homeworks (35%)
  - Written problems + short “labs” on TryHackMe
- Projects (45%)
  - Cryptography: Break some weak crypto
  - Flag: Web Hacking
  - Handin: OS Hacking
- Final project (25%): Design, build, test a secure system

Prerequisites

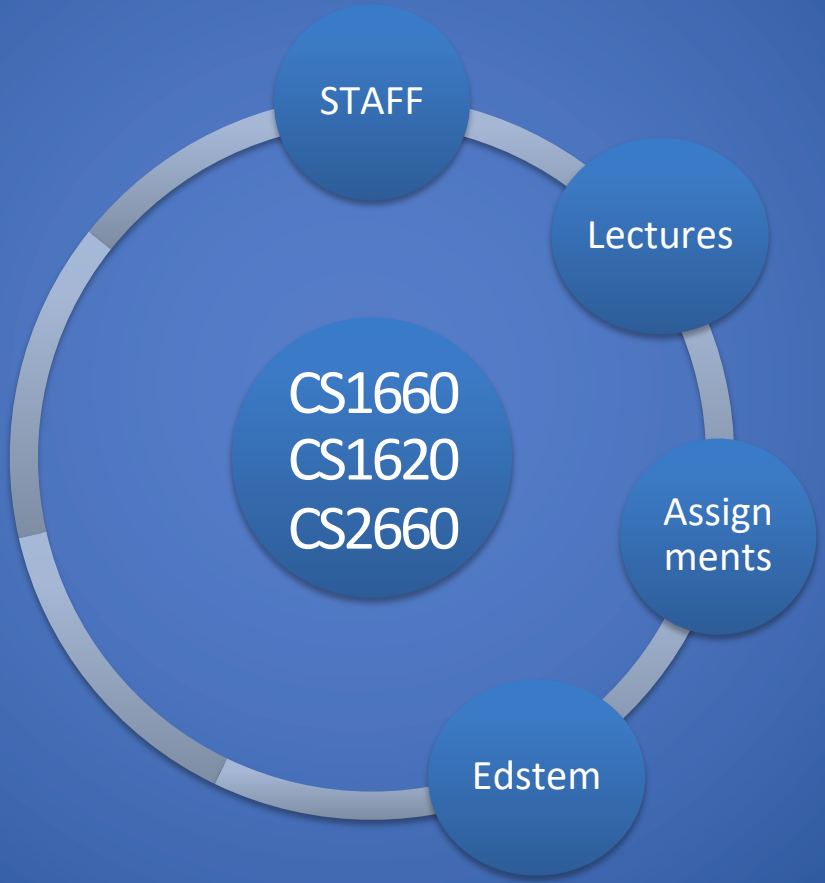
- CS33, CS300, CS1310, CS1330 (or equivalent)
  - You should have *seen* systems concepts like threads, memory management, (basic) networking before

You should also be comfortable with…

- Writing programs/scripts in some language (Python, Go, C/C++, Shell scripting, …)
- Learning new languages you've never seen before, to read code (we'll gain practice with this!)

If you have questions, please ask!

Security is a chain…



Regular Administrivia

- Most material on course website: https://cs.brown.edu/courses/csci1660/

- You are responsible to check the web page and EdStem!
  - All announcements will be there
  - Notes for all lectures (filled and unfilled)
  - Handouts, due dates, programming resources, *etc…*

Asking for help

- Online help: EdStem
- Office hours/clinics: calendar on course website
  - In-person and hybrid

- Can help with..
  - Debugging
  - Assignment/project concepts
  - Systems issues, attack mechanics
  - And more!

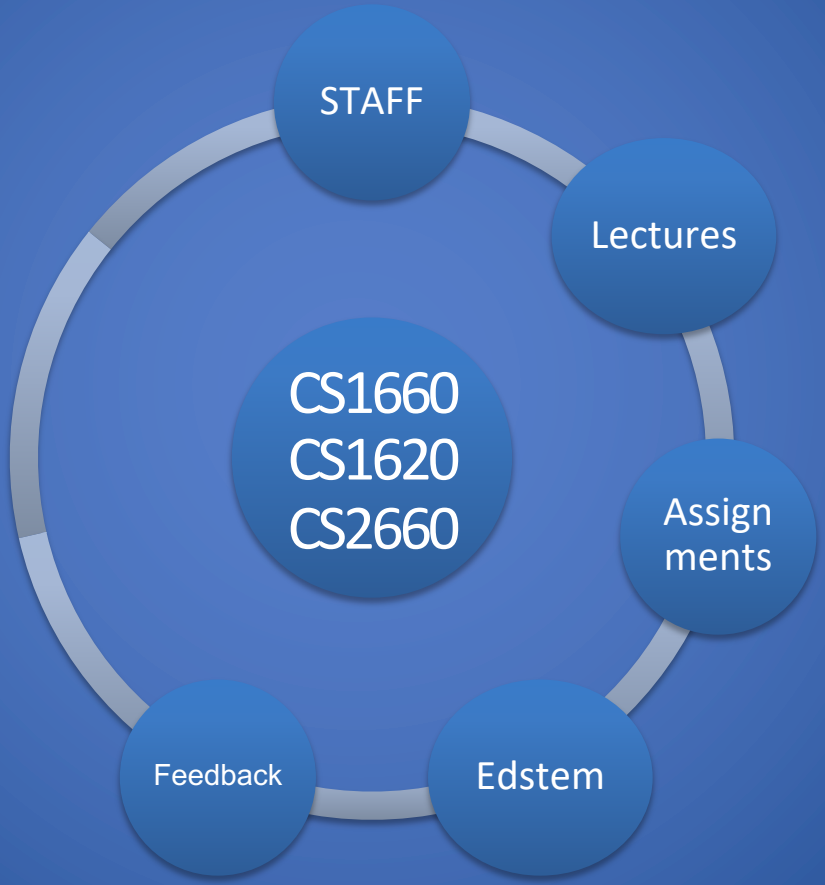
We’re here to help you learn how to solve problems—but please start early!

Asking for help

- Collaboration: work with your peers!
  - Collaboration policy on course website
  - We encourage you to collaborate, **so long as the code you write and vulnerabilities you find are your own**
  - List collaborators in your submission

- Your physical and mental health is important!
  - If you have concerns, feel free to talk to us
  - We encourage you to contact University resources like CAPS

Security is a chain…



Diversity and Inclusion

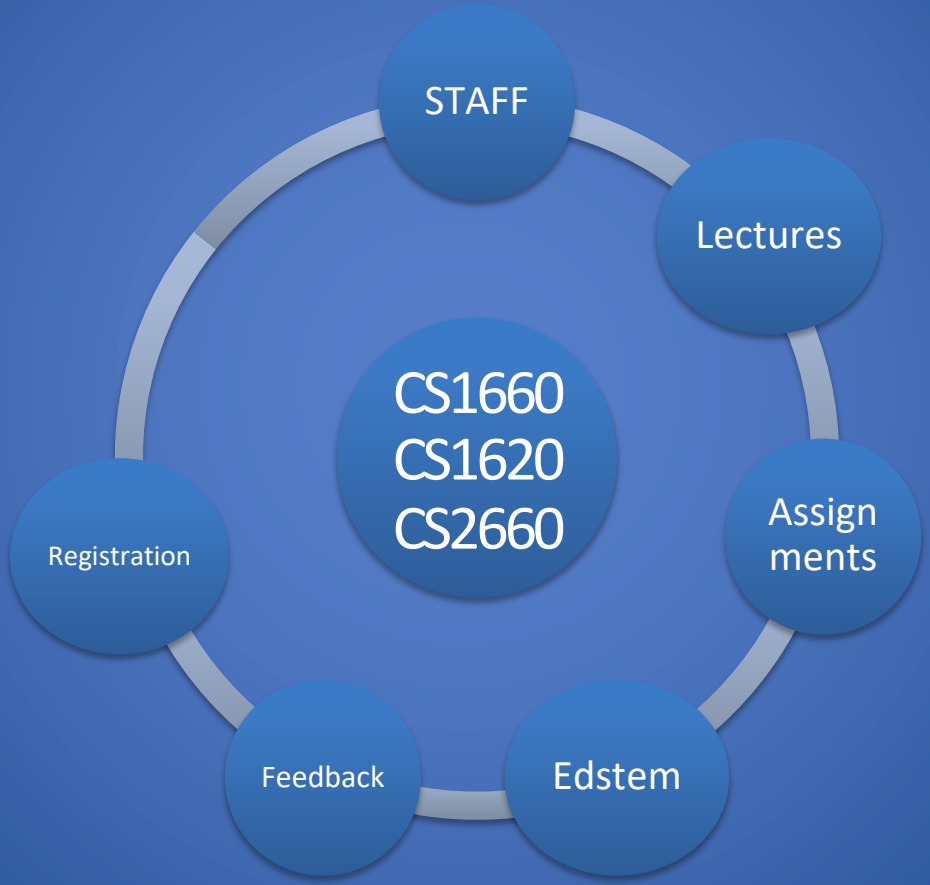
- We welcome diverse ideas and perspectives
- Points of contact:
  - Bernardo, Nick & TAs
  - Anonymous feedback form (website)
  - diversity.advocates@lists.cs.brown.edu
  - wellness.advocates@lists.cs.brown.edu

Feedback

- Anonymous feedback form on course website

- Please tell us how we can improve the course!
  - Clarity of assignments
  - Improving accessibility
  - Concerns about presentation of content, interactions with staff

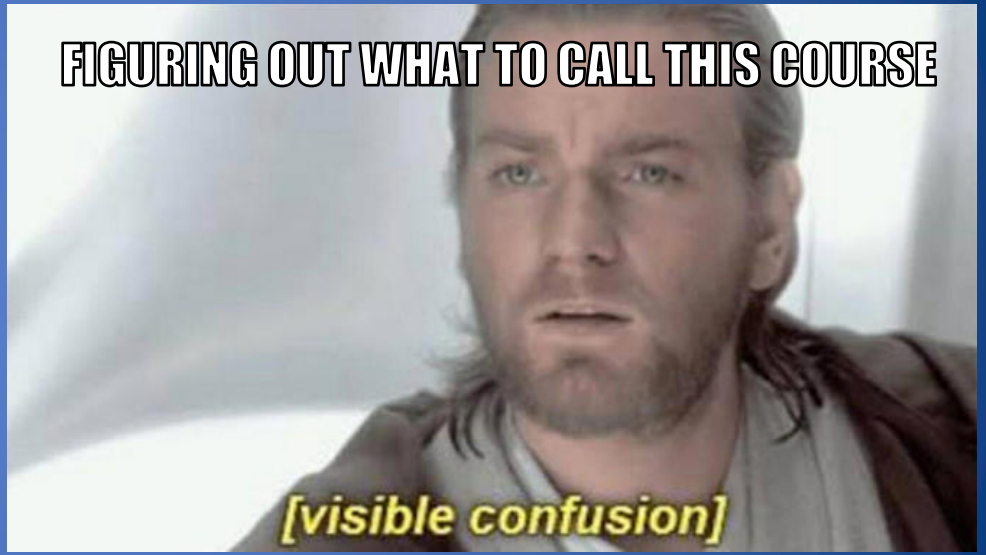
Security is a chain…



Registration Logistics

What's with all the course numbers?

- CS166/CS1660??
- CS162/CS1620??
- CS2660???



CS1660

(was CS166)

- Open to undergraduate and graduate students
- Counts for 1000-level credit

Cybersecurity master's program: this course is designed for the Computer Science track

  - Policy track students should take CS1880 instead

CS1620/CS2660: The "Lab"

(was CS162)

If you are interested, you can work on more challenging problems for additional credit:

- Undergraduates: half-credit lab (+ capstone, if senior)
- Graduate students: 2000-level credit

What changes?

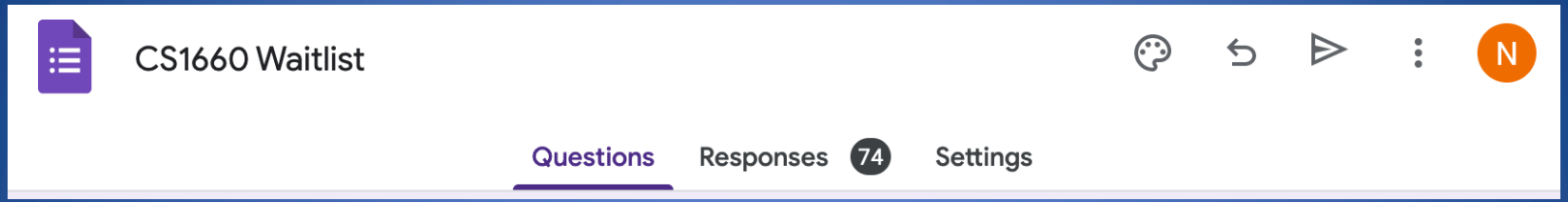
- More problems, tricker vulnerabilities, some outside reading
- No additional prerequisites/background, just requires more time
- Extra late days

CS1620/CS2660: Interested?

If you are a…	Register for…	What you get
Undergraduate	CS1660 + CS1620 (Register for **BOTH**)	Half-credit lab Capstone (if you are a senior, email us)
Graduate student	CS2660	2000-level credit Note: can't drop to 1660 after shopping period!
Undergraduate w/ Concurrent master's	You decide	CS1620: Freedom to drop to 1660 CS2660: 2000-level credit (+capstone)

If you have questions, let us know!

Some honesty



- Huge demand for the course this year!
- We are working hard to scale the class—we appreciate your patience and understanding!

The waitlist

If you are not enrolled do the following:

1. Fill out the waitlist form ASAP
2. Add the course to your cart

As enrollment changes, we will admit students from the waitlist, prioritizing students who:

- Were unable to preregister due to CAB issues
- Cannot take the course again or have strict program req's

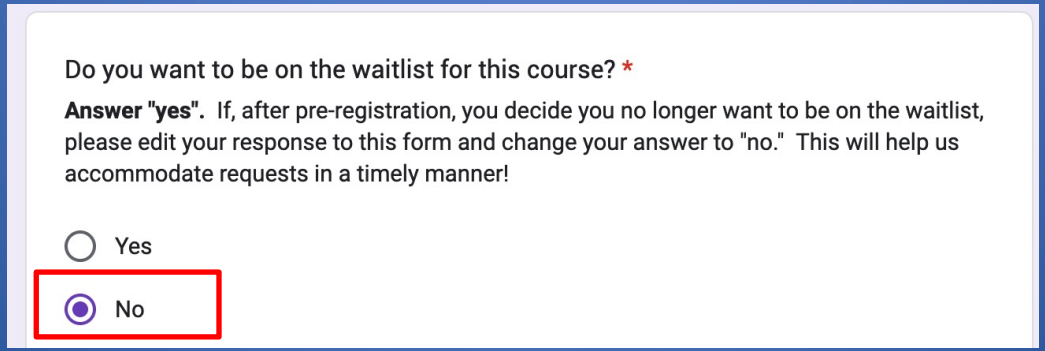
First batch of admissions tonight—look for an email

If you decide not to take this course

That's okay!

Please be respectful to your fellow students--let us know ASAP:

- If you are registered: please drop the course
- If you are on the waitlist: edit your form response



Setup: Homework 0

- Ensure you have access to course resources
- Helps us to gauge your comfort level with various topics and concepts covered in this course
  - We will use this to determine how to scope lectures and provide other resources
- Complete by **Thursday, Feb 2 (sooner if possible!)**

Security is a chain…

Password Cracking Demo

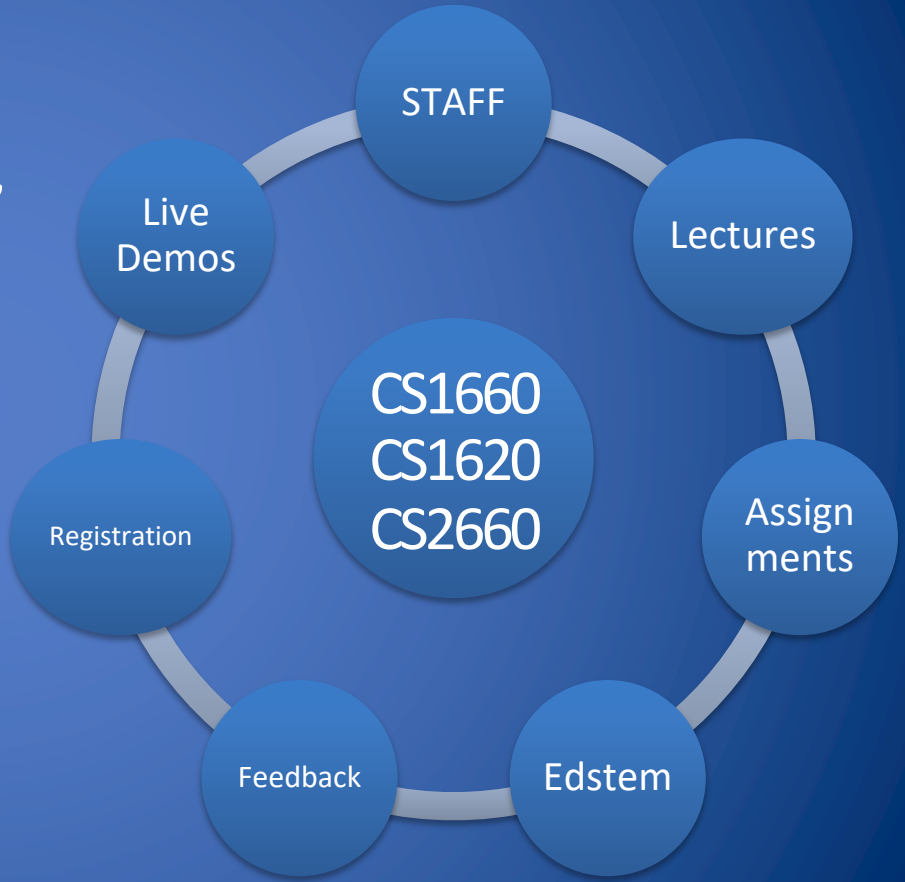
- How to crack some passwords with different strengths
- We will be randomly select a student for creating a password during the lecture in a breakout room
  - One at a time
- We will help the student with the rules for selecting the password

Select a Password

- Choose a case-sensitive alphanumeric password
- That is, your password should use the following characters
  - 0123456789
  - abcdefghijklmnopqrstuvwxyz
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Let's try to crack it!

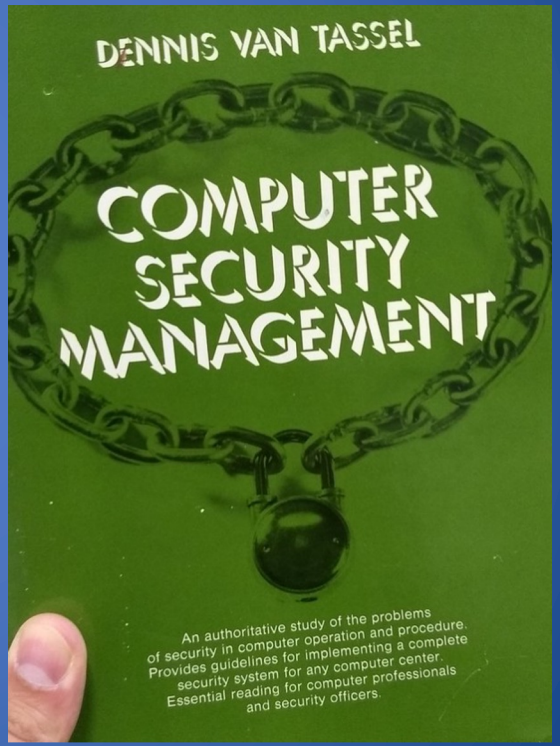
Security is a chain…

- Security is about the “weakest link in the chain”
- You can not overlook any link



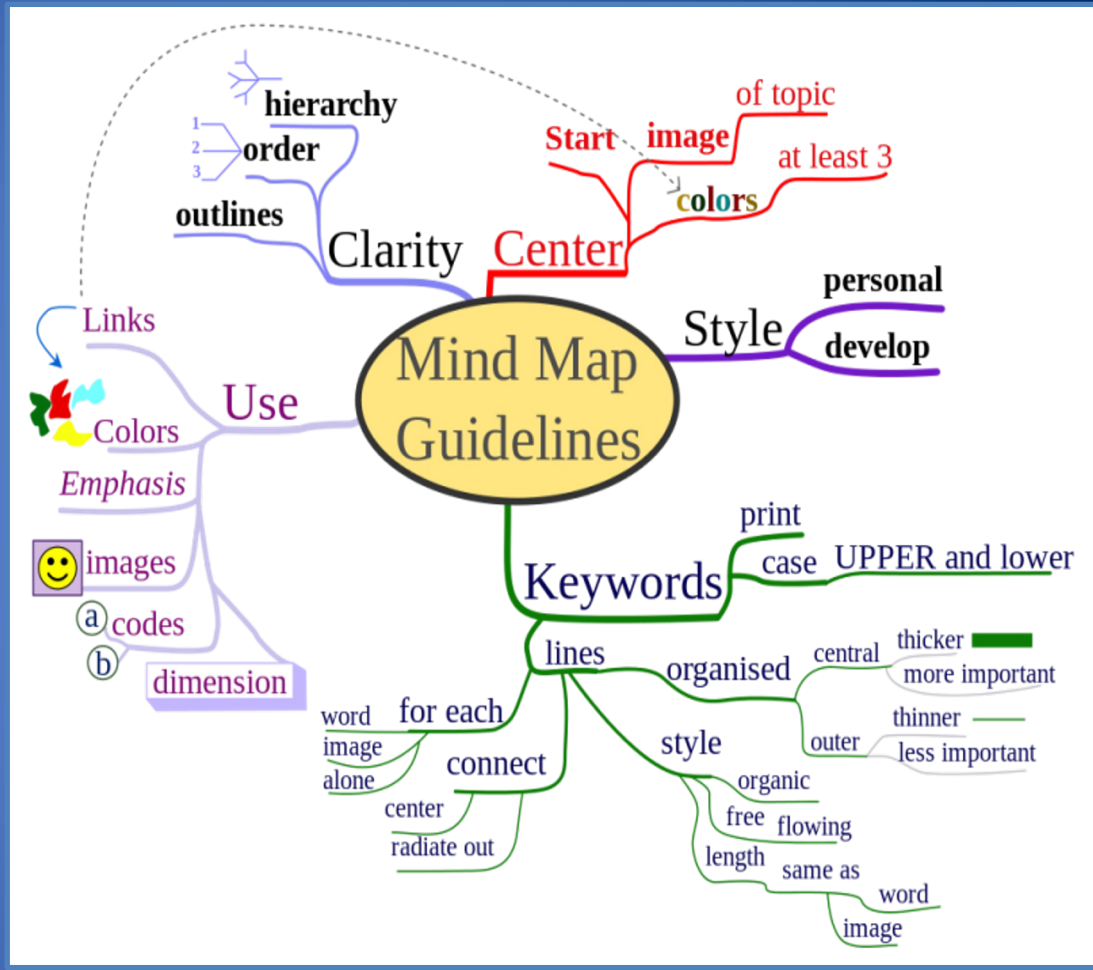
Security is a chain…

- Who said this sentence?
  - Bruce Schneier in…
    Secrets and lies



Mind Map

- A Mind Map is a visual form of:
  - brain storming
  - note-making
- A Mind Map is hierarchical and shows relationships among pieces of the whole



Let's Try Together

- Visit: **https://tinyurl.com/cs1660-mindmap**
- You should not need an account!
  - Password: **csci1660**

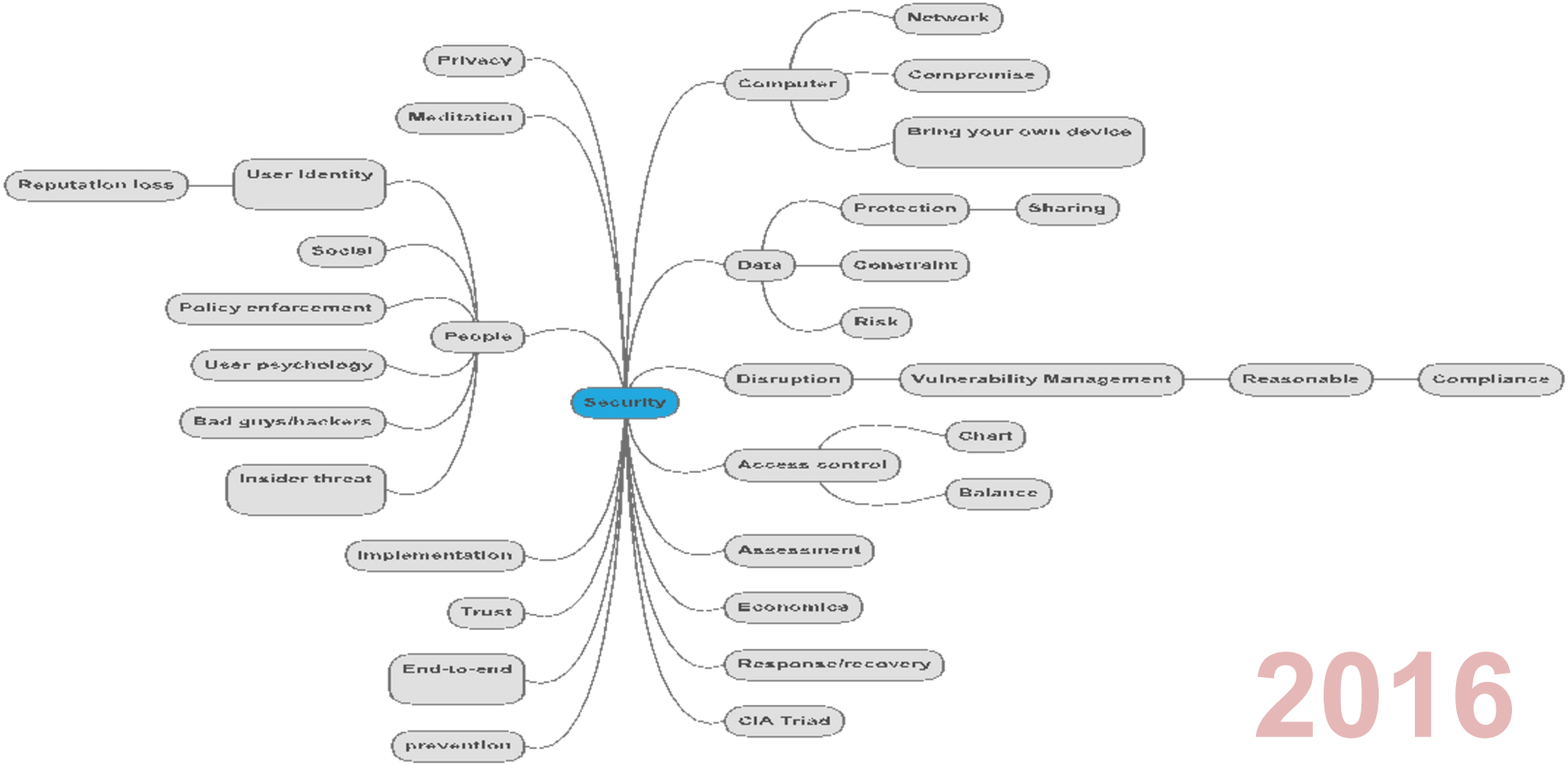
- Add a word in the mind map tool, based on what you associate with security in general. Feel free to add a word to an existing branch or to create a new branch.

- Optionally, include your name in "()" after the word so that we can discuss

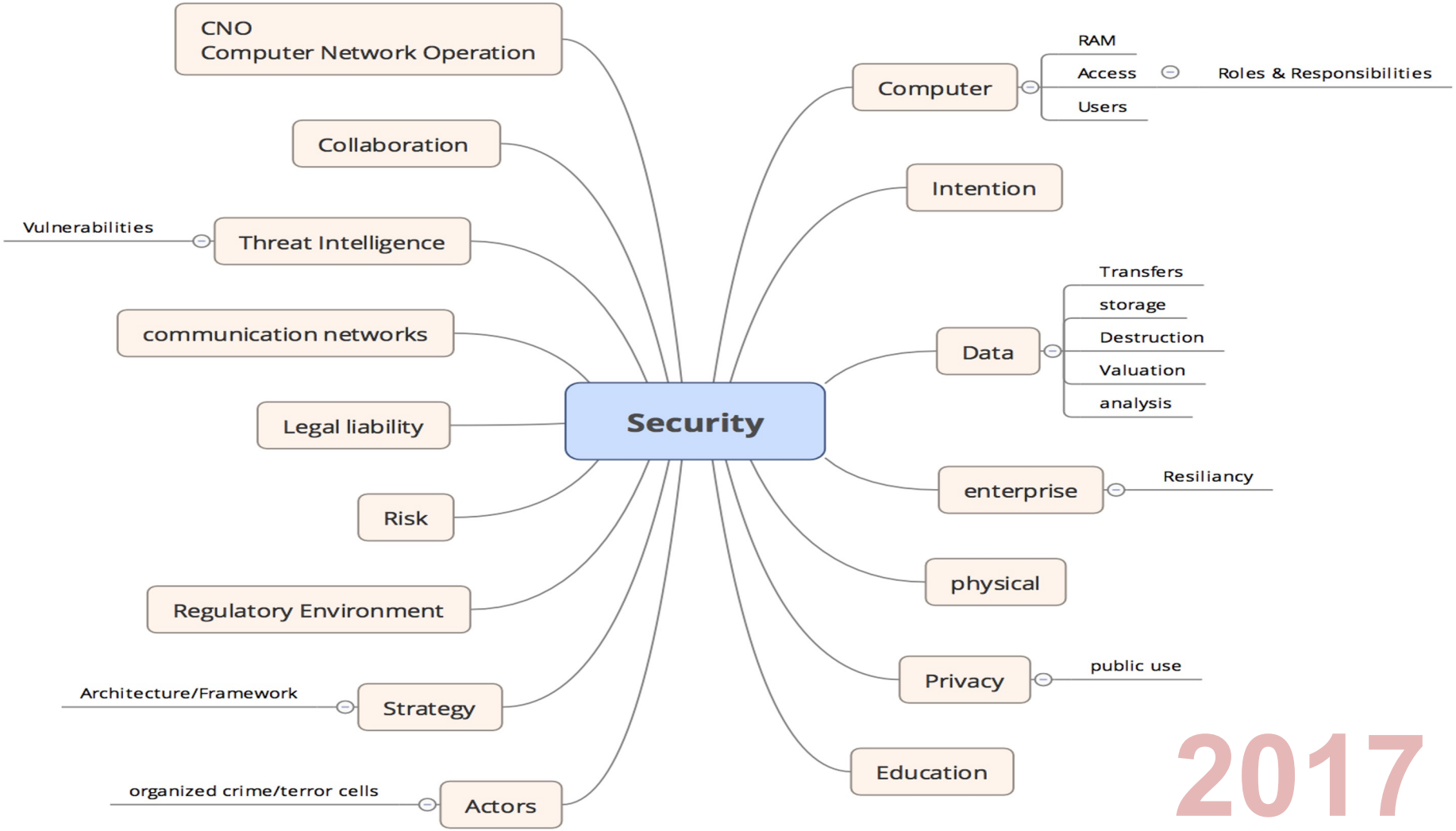
Break!!!!!

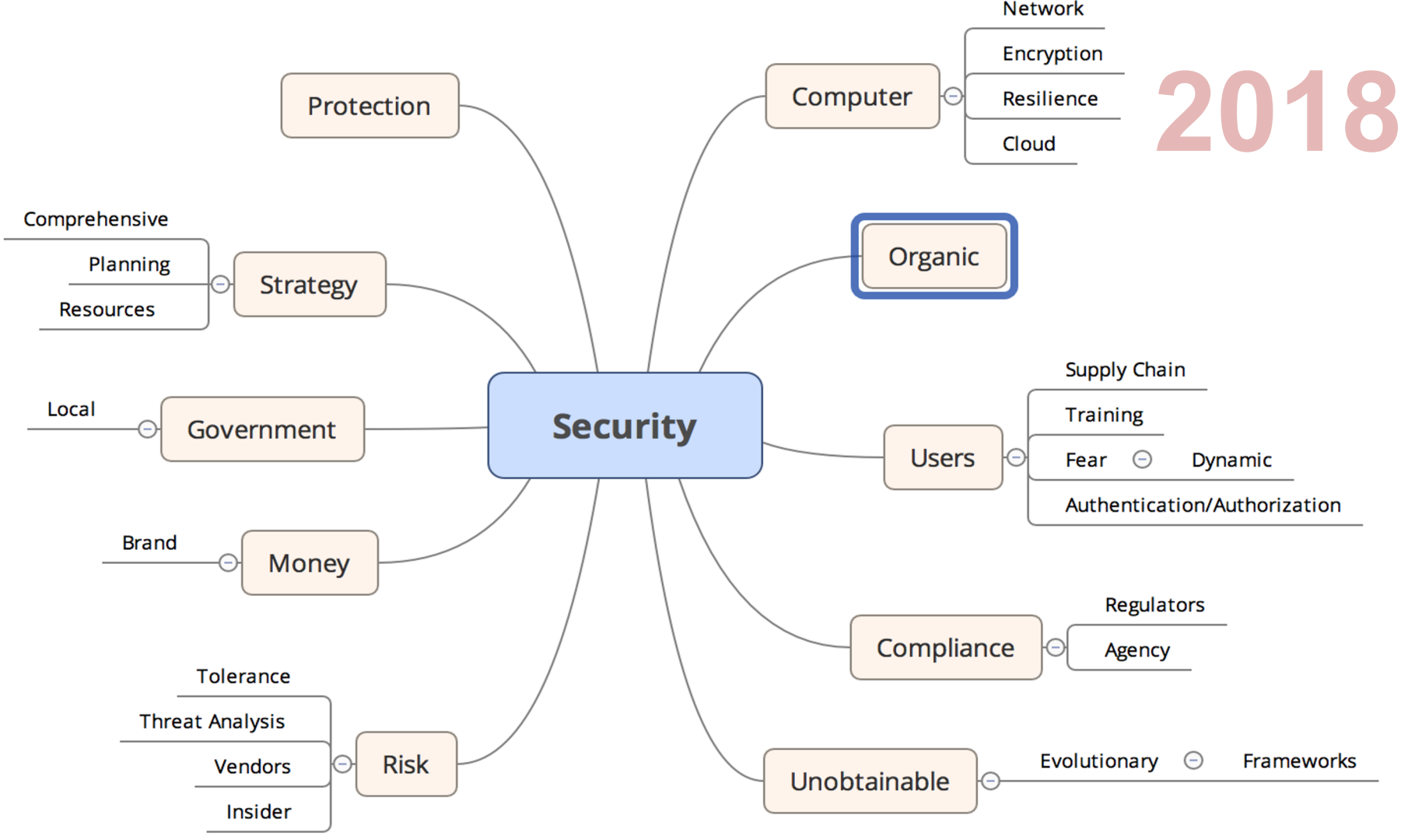
60 60 60 60 60

Class is starting now!


Security
Privacy
Meditation
People
User Identity
Reputation loss
Social
Policy enforcement
User psychology
Bad guys/hackers
Insider threat
Implementation
Trust
End-to-end
prevention
Computer
Network
Compromise
Bring your own device
Data
Protection
Sharing
Confidentiality
Risk
Disruption
Vulnerability Management
Reasonable
Compliance
Access control
Chart
Balance
Assessment
Economics
Response/recovery
CIA Triad

2016


Security
CNO
Computer Network Operation
Collaboration
Vulnerabilities
Threat Intelligence
communication networks
Legal liability
Risk
Regulatory Environment
Architecture/Framework
Strategy
organized crime/terror cells
Actors
Computer
RAM
Access
Roles & Responsibilities
Users
Intention
Data
Transfers
storage
Destruction
Valuation
analysis
enterprise
Resiliancy
physical
Privacy
public use
Education
2017


2018
Security
Protection
Computer
Network
Encryption
Resilience
Cloud
Organic
Strategy
Comprehensive
Planning
Resources
Government
Local
Users
Supply Chain
Training
Fear
Dynamic
Authentication/Authorization
Money
Brand
Compliance
Regulators
Agency
Risk
Tolerance
Threat Analysis
Vendors
Insider
Unobtainable
Evolutionary
Frameworks

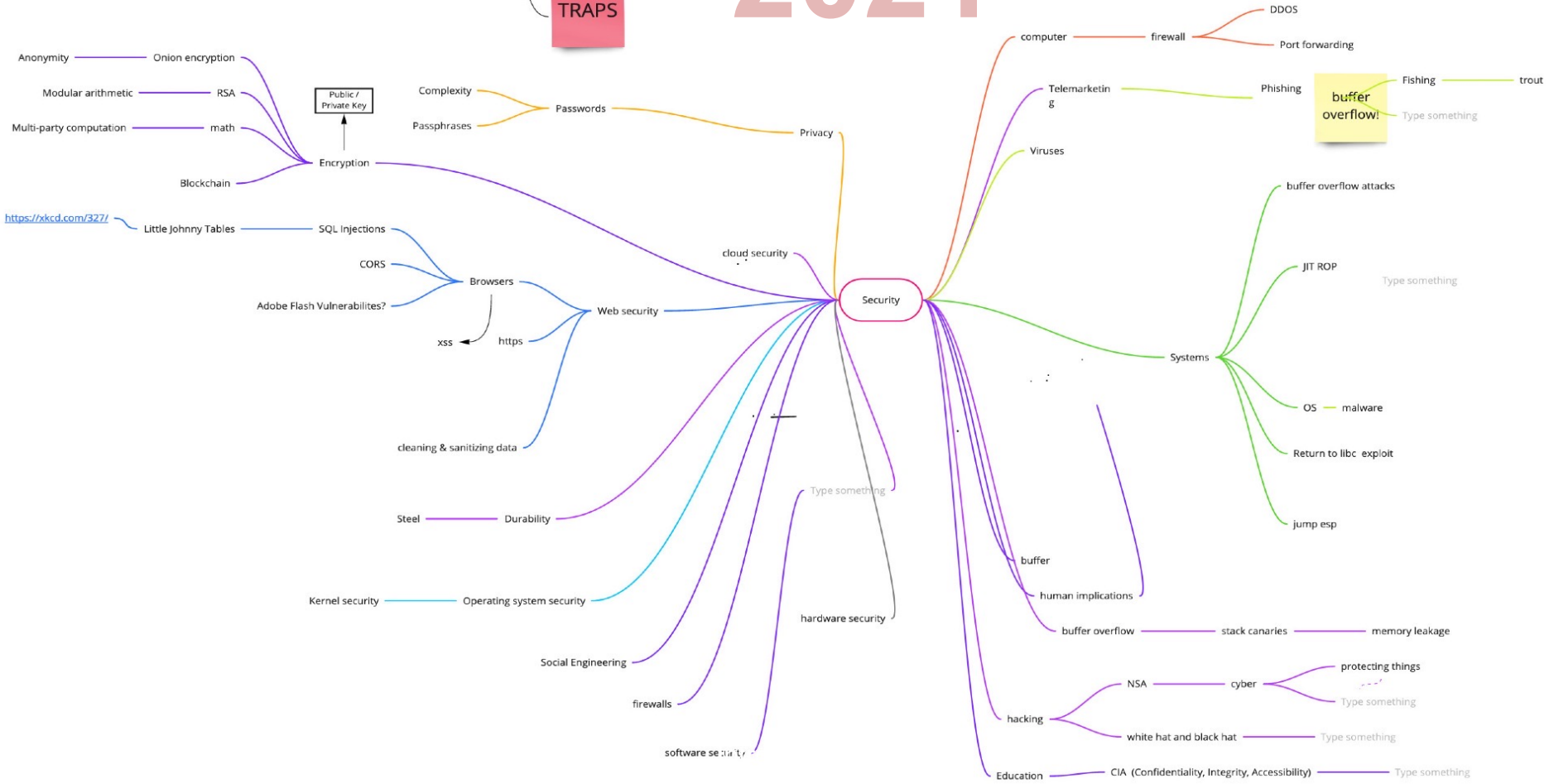

Security
Data
Compliance
Confidentiality
Encryption
Policy/ Liability/ Recourse
Education
Offense
availability
Architecture
Trade-off
Layers
Supply Chain
Confidentiality
Legal
Interconnection Security Agreement
Resilience
Computer
defense
CYBER RISK MANAGEMENT
2019
Peace of mind
User
Process
Behavior
Victims
Player Data
Customers
Cryptocurrency
Compliance
Regulations
Threat
Danger
Vulnerability
Weakness
Physical
Fence
LOCKS

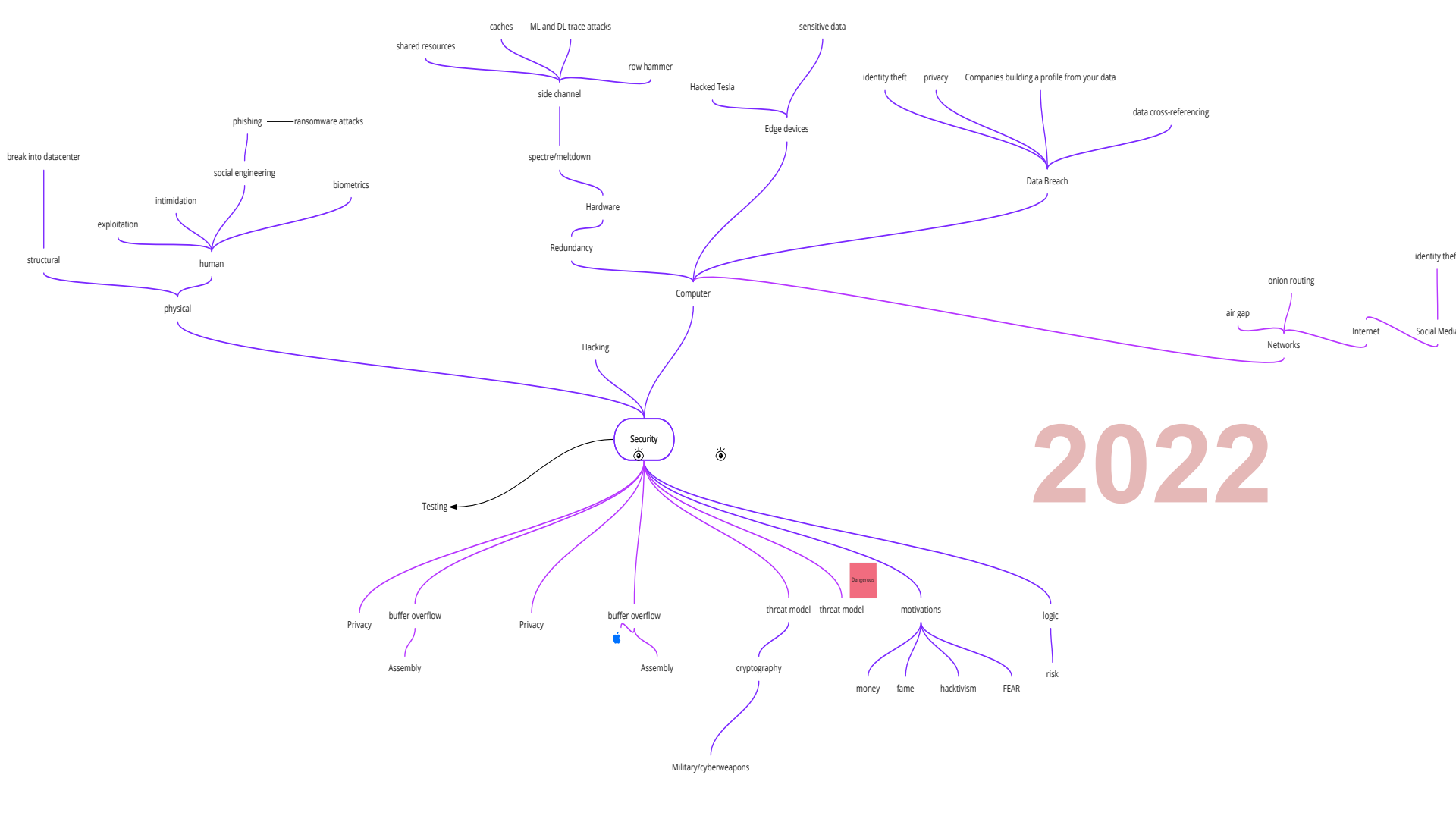
If you want to add a branch to a node on the mindmap, hover over the node and press the "+" button!

PAIN

TRAPS

2021




caches
ML and DL trace attacks
shared resources
row hammer
side channel
sensitive data
Hacked Tesla
Edge devices
identity theft
privacy
Companies building a profile from your data
data cross-referencing
Data Breach
phishing
ransomware attacks
social engineering
break into datacenter
biometrics
intimidation
exploitation
human
structural
physical
spectre/meltdown
Hardware
Redundancy
Computer
onion routing
air gap
Networks
Internet
identity thef
Social Media
Hacking
Security
2022
Testing
Privacy
buffer overflow
Assembly
Privacy
buffer overflow
Assembly
threat model
cryptography
Military/cyberweapons
threat model
Dangerous
motivations
money
fame
hacktivism
FEAR
logic
risk

Introduction to Security

Introduction to Computer Systems Security

CIA Triad

Confidentiality

- Prevent disclosure of information to unauthorized parties

Integrity

- Detect data tampering

Availability

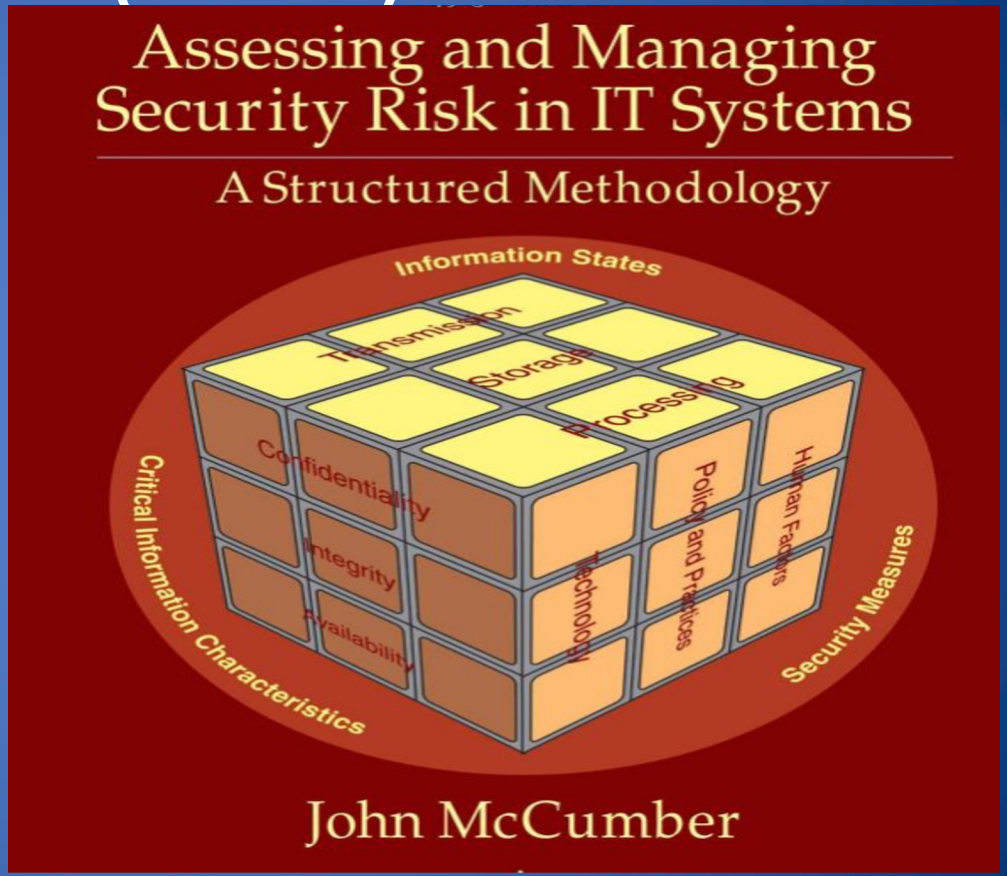
- Guarantee access to data

McCumber Cube (1991)

Security Goals
- Confidentiality
- Integrity
- Availability

Information States
- Storage
- Transmission
- Processing

Security Measures
- Human factors
- Policy and practices
- Technology



Is this enough?

- Parkerian Hexad (2002)
- C-I-A Triad expanded:
  - Authenticity
    - Veracity of the data source and provenance can be assured
  - Utility
    - Security or insecurity of data does not inhibit the practical use of the data
  - Possession or Control
    - Data is only accessible or changeable by those intended
- Non-Repudiation
    - One party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction
- Etc.

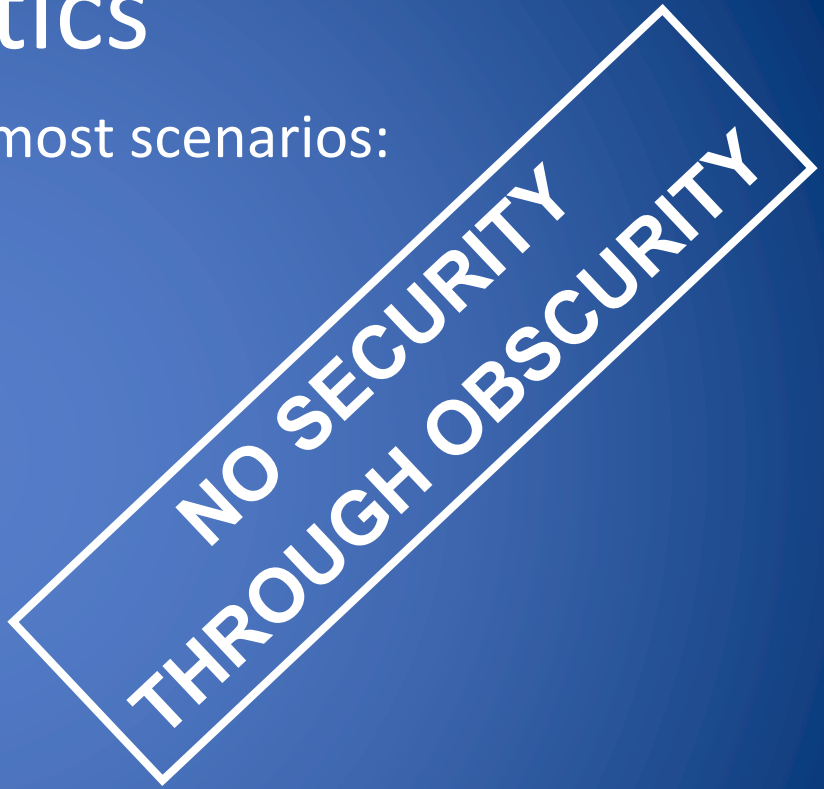
Secure Against What?

- “Security” has no meaning per se
- The security of a system, application, or protocol is always relative to
  - A set of desired properties
  - An adversary with specific capabilities
- In cybersecurity it is difficult to define general rules often we use best practices or heuristics

Heuristics

Just some best practices useful in most scenarios:

- Need to know/Least privileges
- Default secure
- Defence in depth
- Open design/Standard solutions
- Security as a process
- Usability
- …

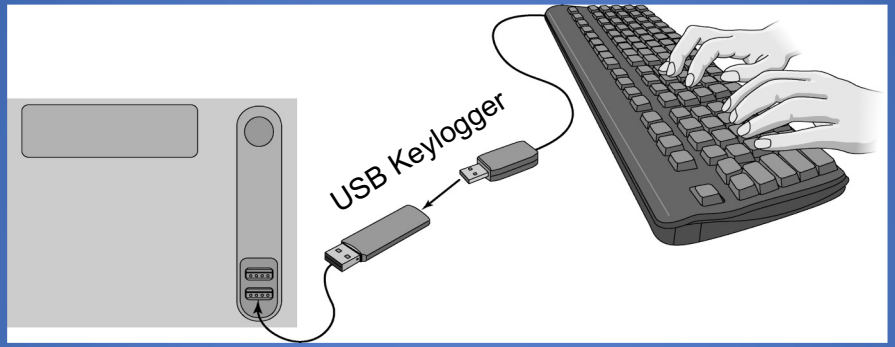


Security Trade-offs

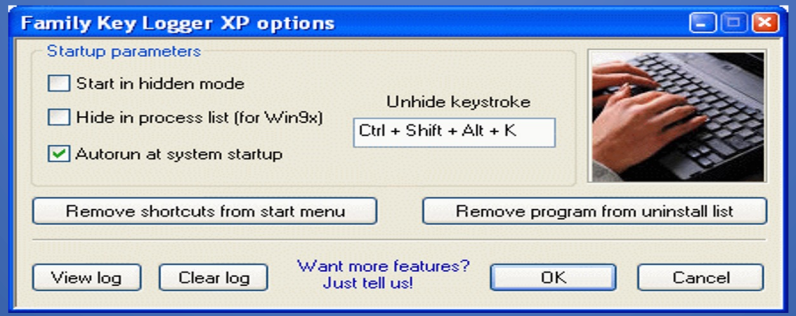
- Complete security against all conceivable adversaries is often unfeasible
- Security implies a tradeoff between risk mitigation and the cost of deploying defense mechanisms
- In addition, human factors such as user acceptance and usability must be taken into account

If Cracking does not Work

Keyloggers



Hardware



Software

Summary

- Security is a chain…
- Security models (CIA)
- There is no a general definition for security you should take in consideration:
  - Adversaries
  - Heuristics
  - Trade-offs
  - Ethics
  - …

Ethics

- Ethics Question & Group Discussion in HWs
  - No right answer
- Many real-world applications, Cybersecurity decisions inherently ethical:
  - Should the government be able to require access to encrypted communications?