

CS1660/CS2660

Intro to Computer Security

<https://brown-csci1660.github.io>

Staff



Bernardo (Prof)



Rhea (HTA)



Oren (UTA)



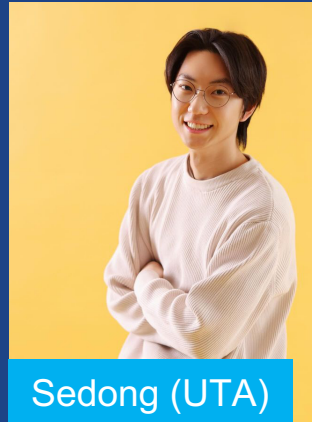
Chen (UTA)



Nick (Prof)



Siming (HTA)



Sedong (UTA)



Min (UTA)

Yuntian (UTA)

Rosalie (UTA)

Learning goals

Develop a security mindset: learn how to *understand* and *communicate* about security principles

- Learn by implementing (and breaking) real systems
- Learn about historical examples that have shaped modern security

What is security?



BROWN UNIVERSITY

Authentication Required

Enter your Brown credentials

Username

Password


Log In

You have asked to log in to:



bannersomgr.brown.edu


Why do we need this?



BROWN UNIVERSITY

Authentication Required

Your account requires that you provide an additional factor of authentication. Please select from one of the options below.

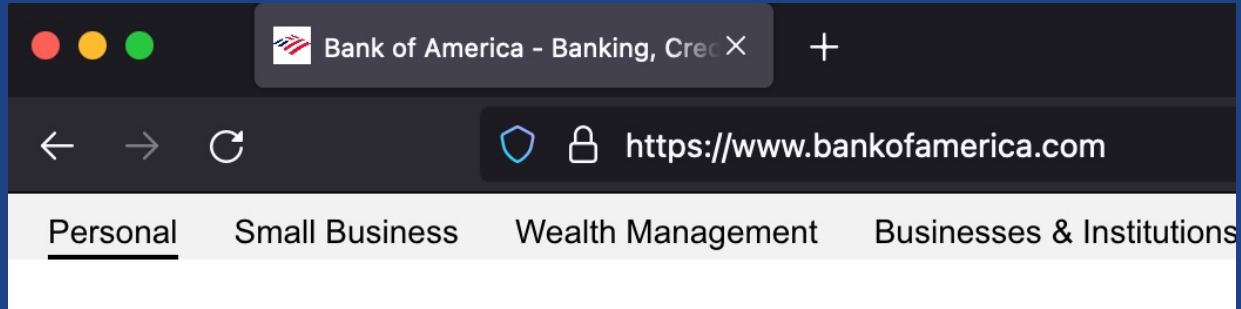


[What is this?](#) [Need help?](#)

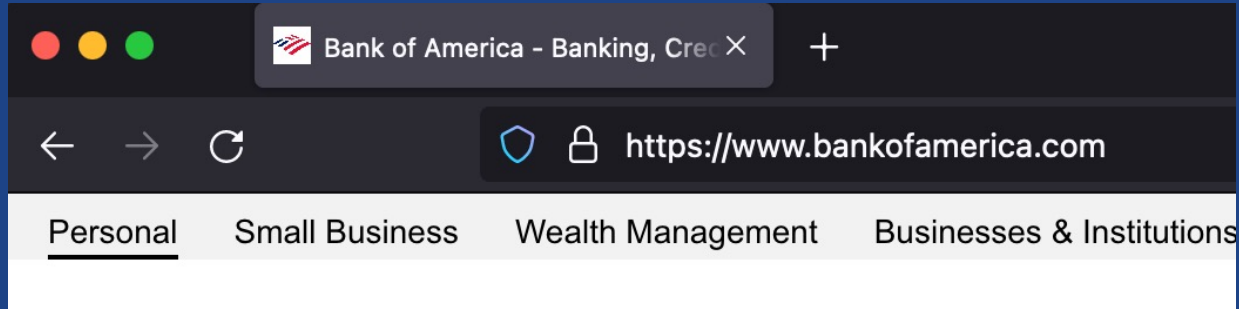
Secured by Duo

Remember me for 30 days

What makes something secure?

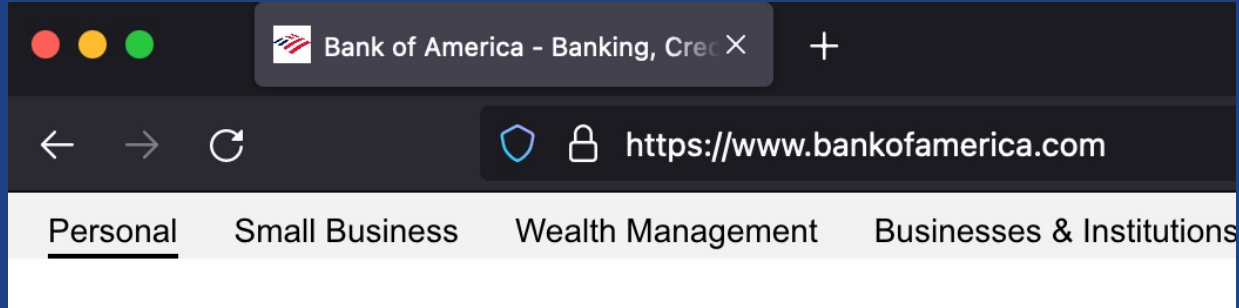


What makes something secure?



- What do we need to secure?
- What security mechanisms do we need?
- How do they work?

What makes something secure?



- What do we need to secure?
- What security mechanisms do we need?
- How do they work?

Need to understand the system, how it will be used,
and the technical details

What are all these warnings?

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **nd.isacc.net**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

User Account Control

Do you want to allow this app to make changes to your device?

Microsoft Management Console

Verified publisher: Microsoft Windows

Show more details

Yes No

Allow "Maps" to access your location while you are using the app?

Your current location will be displayed on the map and used for directions, nearby search results, and estimated travel times.

Allow While Using App

Allow Once

Don't Allow



Do you trust the authors of the files in this folder?

Code provides features that may automatically execute files in this folder.

If you don't trust the authors of these files, we recommend to continue in restricted mode as the files may be malicious. See [our docs](#) to learn more.

~/Development/csci1680/proj/ipstack-reference

Trust the authors of all files in the parent folder 'proj'

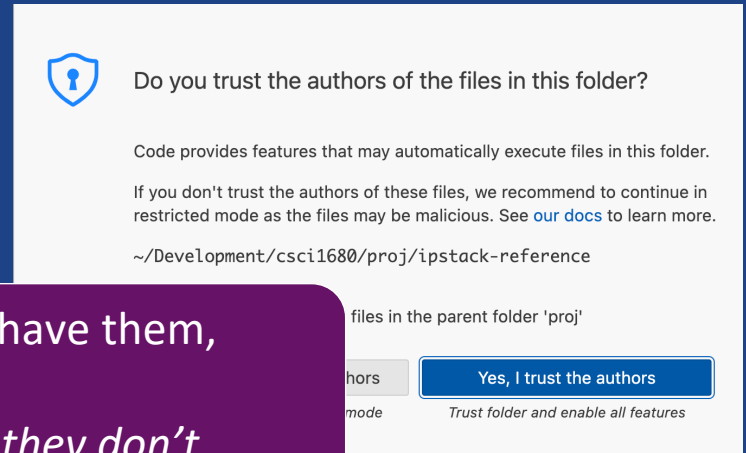
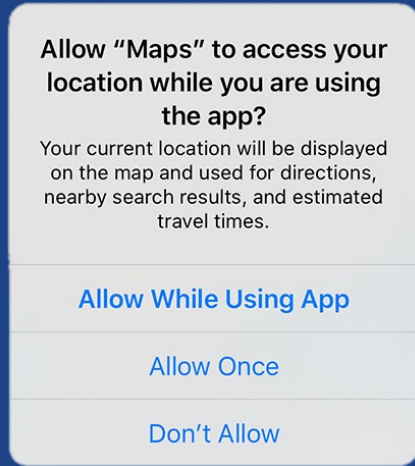
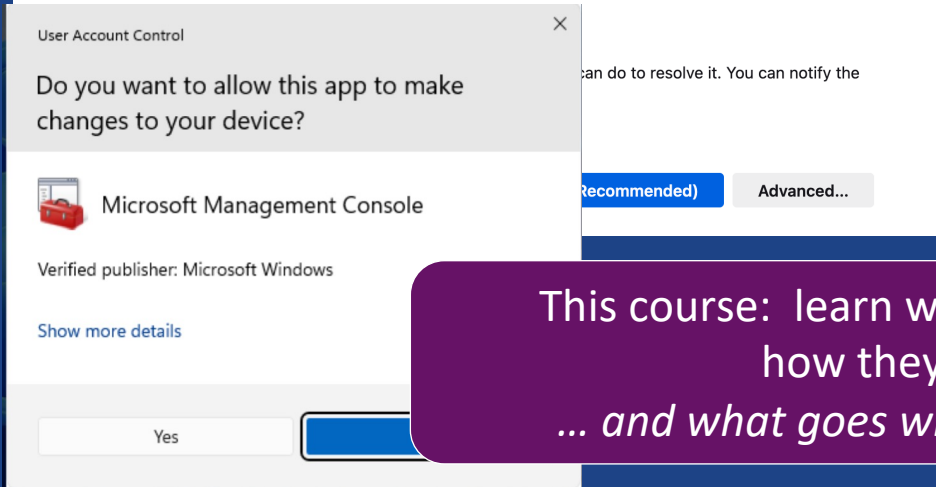
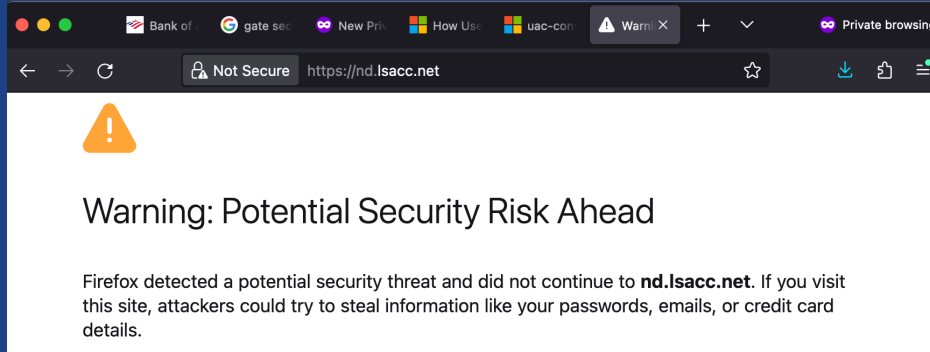
No, I don't trust the authors

Yes, I trust the authors

Browse folder in restricted mode

Trust folder and enable all features

What are all these warnings?



This course: learn why we have them, how they work, ... and what goes wrong if they don't

What can go wrong?

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS POLITICS SCIENCE MORE SIGN IN SUBSCRIBE


KIM ZETTER SECURITY NOV 3, 2014 6:38 AM


An Unprecedented Look at Stuxnet, the World's First Digital Weapon

In an excerpt from her new book, "Countdown to Zero Day," WIRED's Kim Zetter describes the dark path the world's first digital weapon took to reach its target in Iran.

Your new smart car is an IoT device that can be hacked

Updated on: November 15, 2023 12:53 PM

 Pierluigi Paganini, Contributor



Editor's choice



Ransomware landscape overview 2022
by Cybernews Team · 16 January 2024

In 2023, the ransomware groups that we track claimed that they successfully targeted a total of 1,000 victims, signifying an exceptional year of cyberattacks.

The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

Feature
Mar 09, 2018 · 7 mins

Internet of Things Malware Security

Emergency rooms in at least 3 states diverting patients after ransomware attack

Ardent Health Services, which oversees 30 hospitals across the U.S., said it had shut down a significant number of its computerized services.

Limitations of secure (or not so secure...) systems

Home > Tech > Tech News

These Malicious Android Apps Can Steal Your Private Data

Cybersecurity researchers have found that multiple Android apps on the Google Play Store include malware that lead users to phishing websites.

BY KISHALAYA KUNDU PUBLISHED NOV 3, 2022

F.B.I. Asks Apple to Help Unlock Two iPhones

The request could reignite a fight between the Silicon Valley giant and law enforcement over access to encrypted technology.

NEWS & COMMENTARY

Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress

Congress must take this opportunity rein in the pervasive government surveillance enabled by Section 702.



Learning goals

Develop a security mindset: learn how to *understand* and *communicate* about security principles

- Learn by implementing (and breaking) real systems
- Learn about historical examples that have shaped modern security

Learning goals

Develop a security mindset: learn how to *understand* and *communicate* about security principles

- Learn by implementing (and breaking) real systems
- Learn about historical examples that have shaped modern security
- How to assess security threats, identify ways to defend
- How attacks work in practice
- Discuss tradeoffs and impact of security mechanisms, policies, enforcement, ...

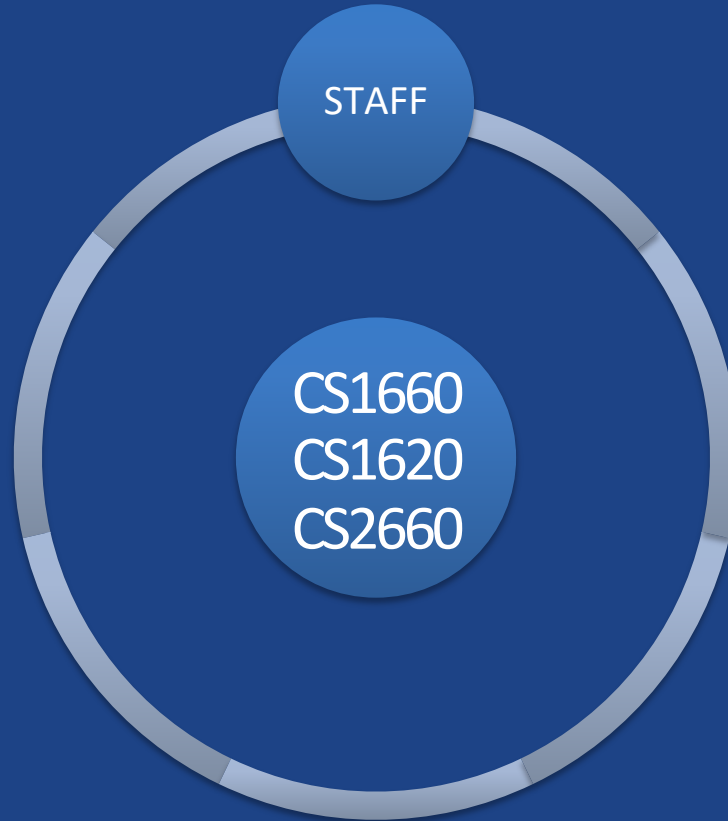
Learning goals

Develop a security mindset: learn how to *understand* and *communicate* about security principles

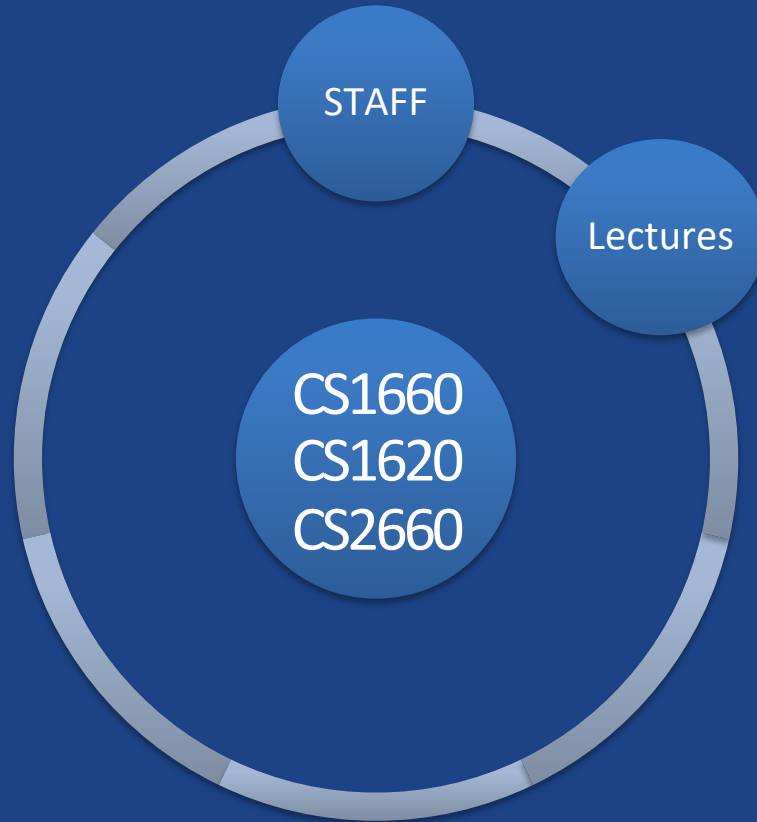
- Learn by implementing (and breaking) real systems
- Learn about historical examples that have shaped modern security
- How to assess security threats, identify ways to defend
- How attacks work in practice
- Discuss tradeoffs and impact of security mechanisms, policies, enforcement, ...

Many examples of what NOT to do!

Security is a chain...



Security is a chain...



Lectures

Overview of security principles

- Cryptography
- Authentication

Lectures

- Security Principles
- Cryptography
- Authentication

- Security for the web

- How operating systems provide security

- How to secure networks/the Internet

Lectures

- Security Principles
- Cryptography
- Authentication

- Security for the web

- How operating systems provide security

- How to secure networks/the Internet

- Special topics (cloud platforms, AI security, ...)

Class Participation

- Synchronous attendance encouraged, but not required
- All lectures and notes will be recorded => posted within 24hrs
- 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

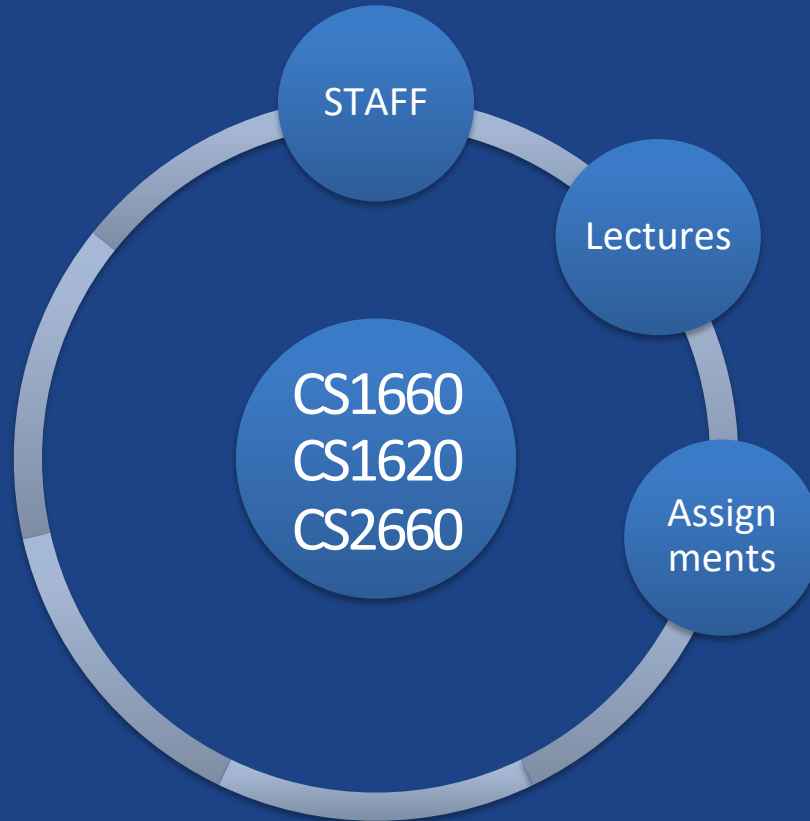
- See in class hands-on demonstrations of basic attack and defense techniques
- Usually: code released so you can try yourself
- Any attack demos should be done in an ethical and legal manner

Disclaimer

We will teach you how to break things, so that you can learn how to make systems more secure

- Use your skills responsibly
- Do not conduct attacks outside the setting of the course, or on systems that you do not own
- You are responsible for adhering to collaboration policy, Brown's Academic code, state/federal laws...

Security is a chain...



Assignments

- 4 Homeworks (35%)
 - Written problems + short “labs”
- Projects (45%)
 - Cryptography: Learn cryptographic principles
 - Flag: Break a web application
 - Handin: Circumvent OS privileges
- Final project (25%): Design, build, test a secure system

Prerequisites

- CS330, CS300, CS1310, CS1330 (or equivalent)
 - You should have *seen* systems concepts like threads, memory management, (basic) networking before

Prerequisites

- CS330, 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 ...)
- Learning new languages you've never seen before, to read code (we'll gain practice with this!)

Prerequisites

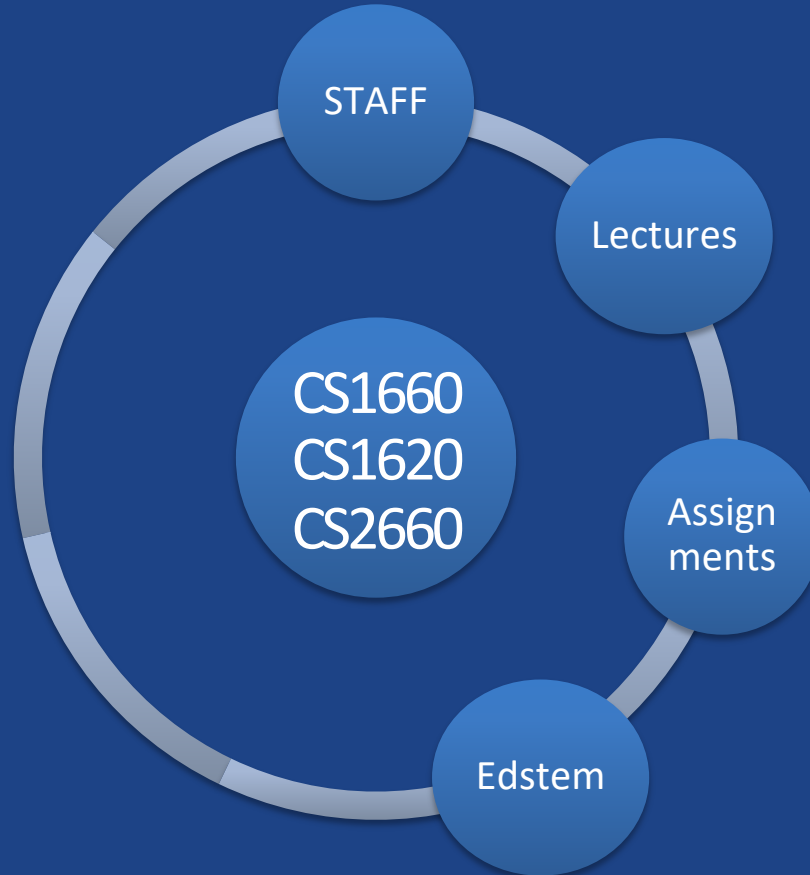
- CS330, CS300, CS1310, CS1330 (or equivalent)
 - You should have *seen* systems concepts like threads, memory management, (basic) networking before

You should also be comfortable with...

- Writing programs/scripts in some language (Python, Go, C/C++, Shell ...)
- 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://brown-csci1660.github.io>

- 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: 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
- Use online resources, AI tools, etc. to find resources or code snippets, but *it's up to you to pieces together*

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**

- 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

Late days

- Everyone gets five (5) late days to apply to most assignments, extends deadline by one full day
 - +2 for CS1620/CS2660 students
- Max 2 late days per assignment
- Weekends/University holidays don't count
(If deadline Fri 11:59pm, Monday 11:59pm is 1 day late)

Late days

- Everyone gets five (5) late days to apply to most assignments, extends deadline by one full day
 - +2 for CS1620/CS2660 students
- Max 2 late days per assignment
- Weekends/University holidays don't count

We want you to rest => take time to think about things

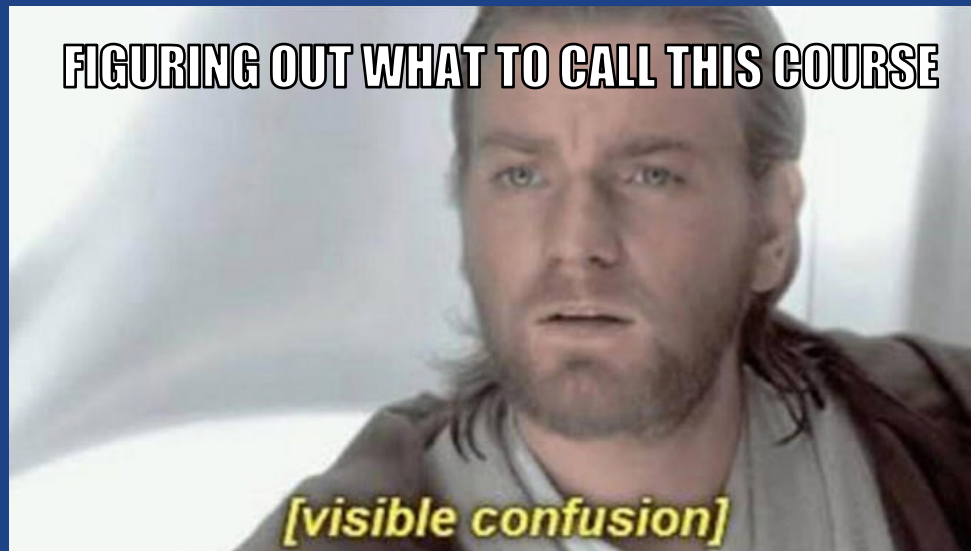
Feedback

- 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

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

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

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

CS1620/CS2660: Interested?

If you are a...	Register for...	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 <u>Note</u> : 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!

Interested?

Please do the following...

- Fill out the registration form on the course website
- Request an override (form will help you pick a section)
- Add the course to your cart (adds you to Ed)

The waitlist



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

More admissions tonight—watch your 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

Do you want to be on the waitlist for this course? *

Answer "yes". If, after pre-registration, you decide you no longer want to be on the waitlist, please edit your response to this form and change your answer to "no." This will help us accommodate requests in a timely manner!

Yes

No

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 next lecture

Setup: Project 0

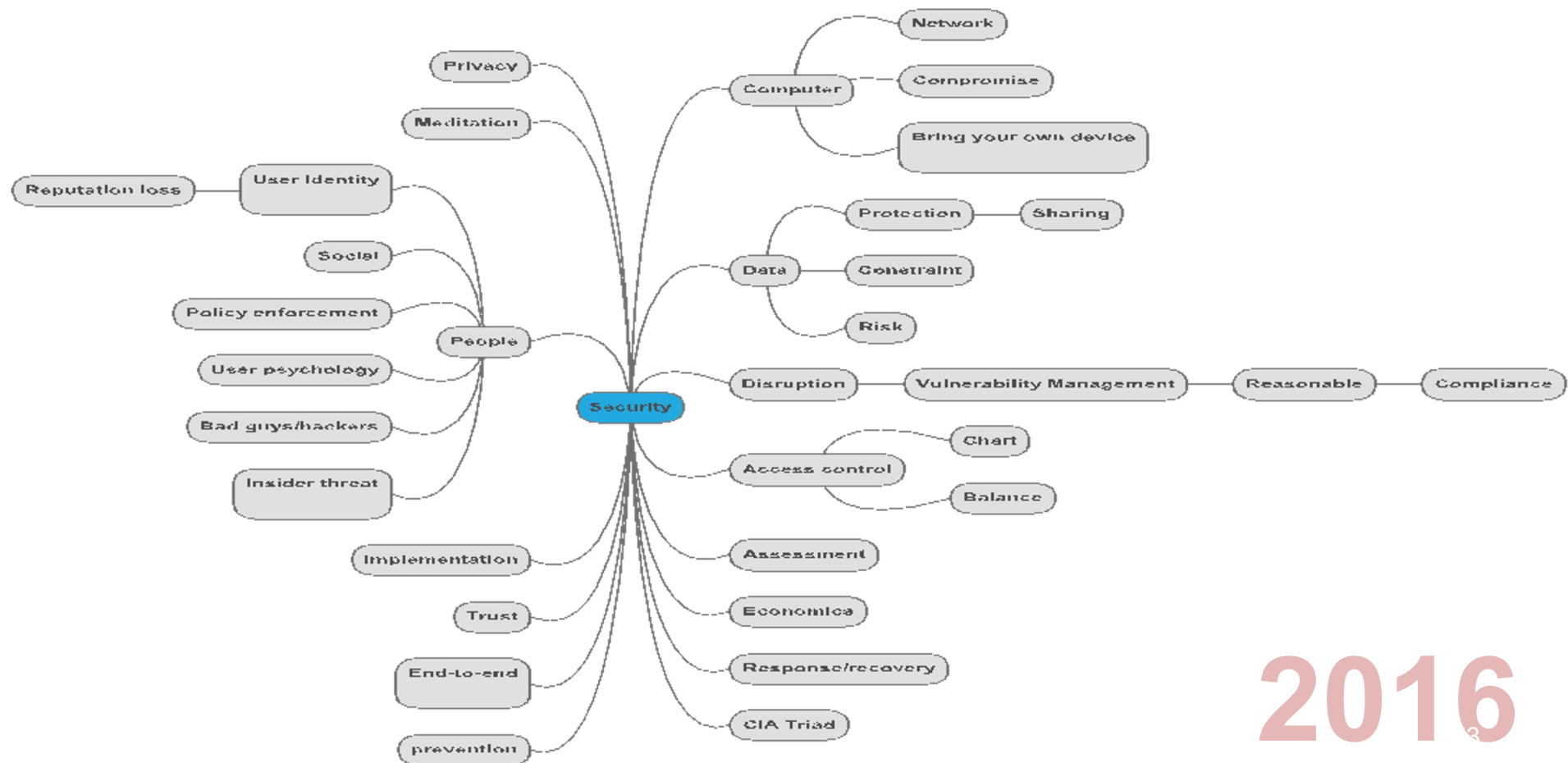
- Set up course container environment
- You'll use this to develop all subsequent projects
- Do by next Thursday (for release of first project)

Out soon--look for announcement tonight/tomorrow

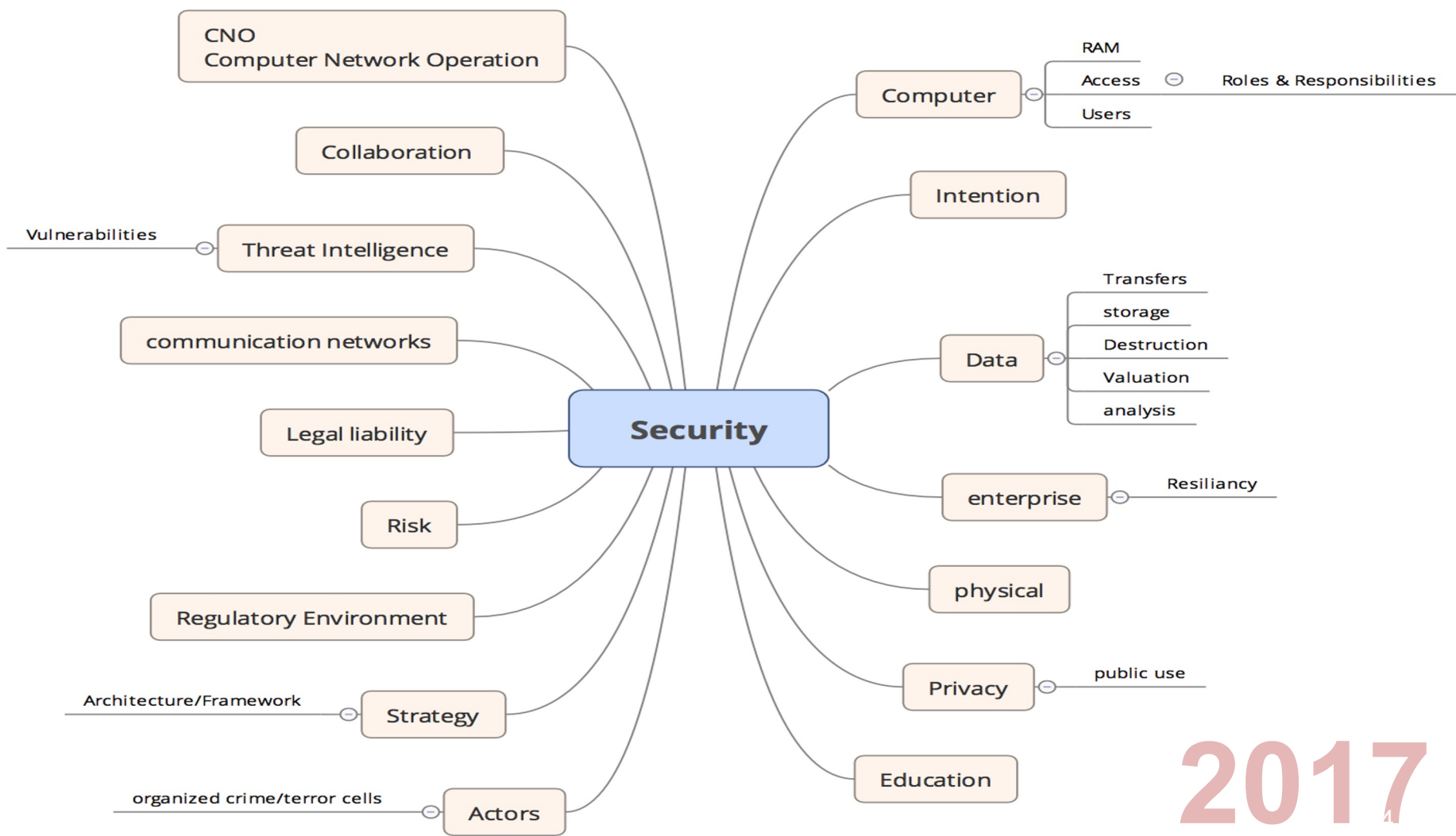
Security is a chain...



Break!

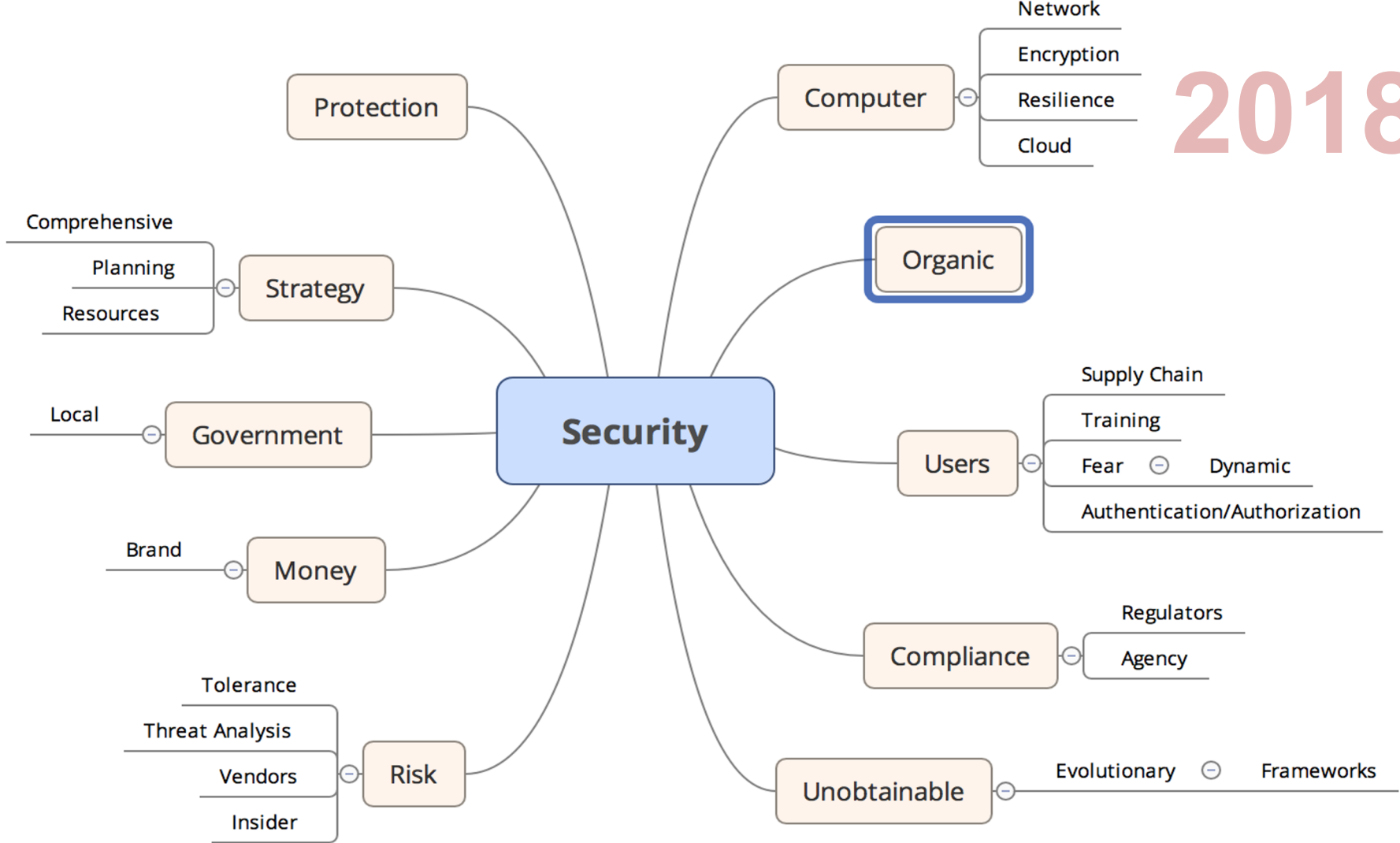


2016



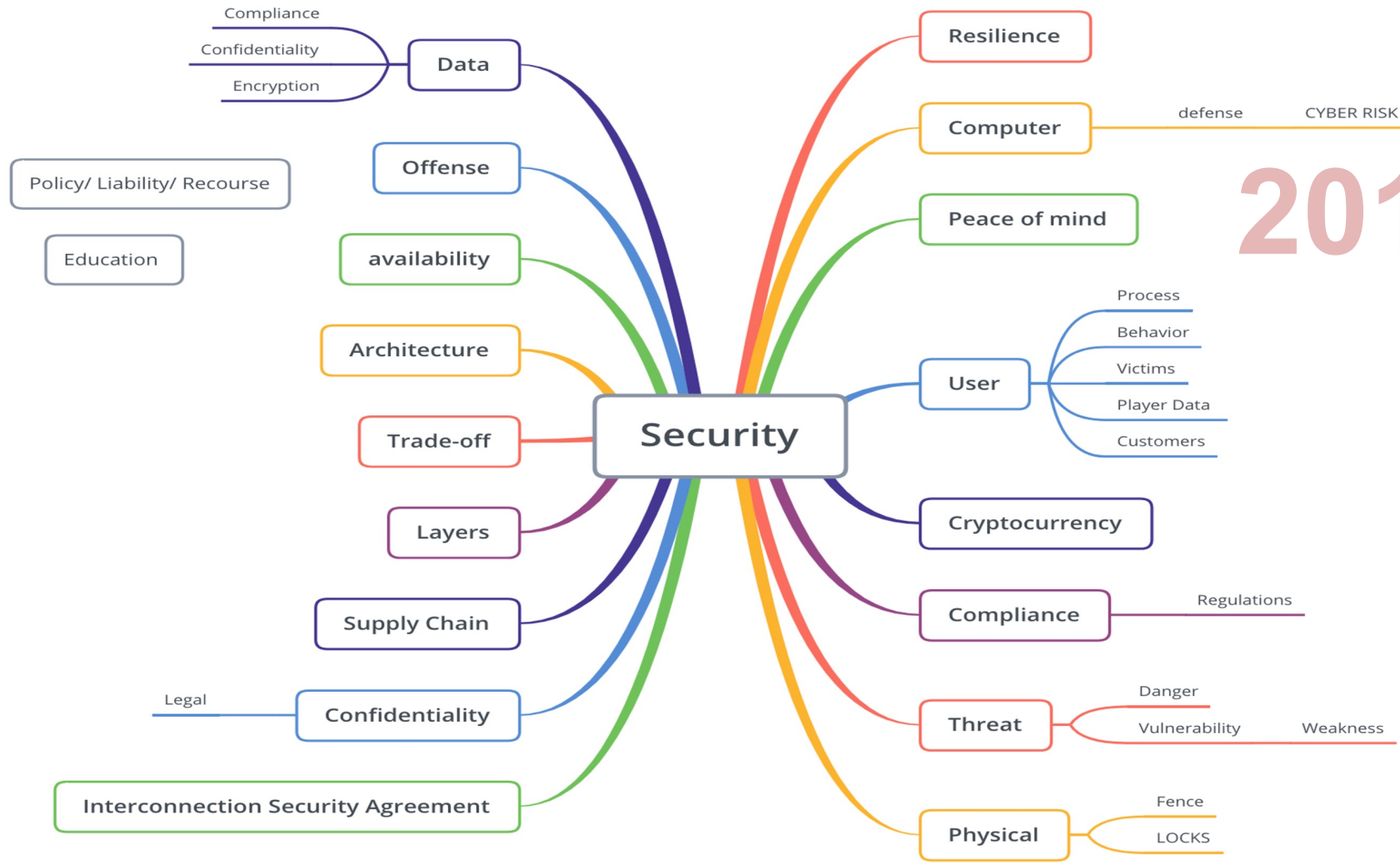
2017

2018



2019

defense CYBER RISK MANAGEMENT

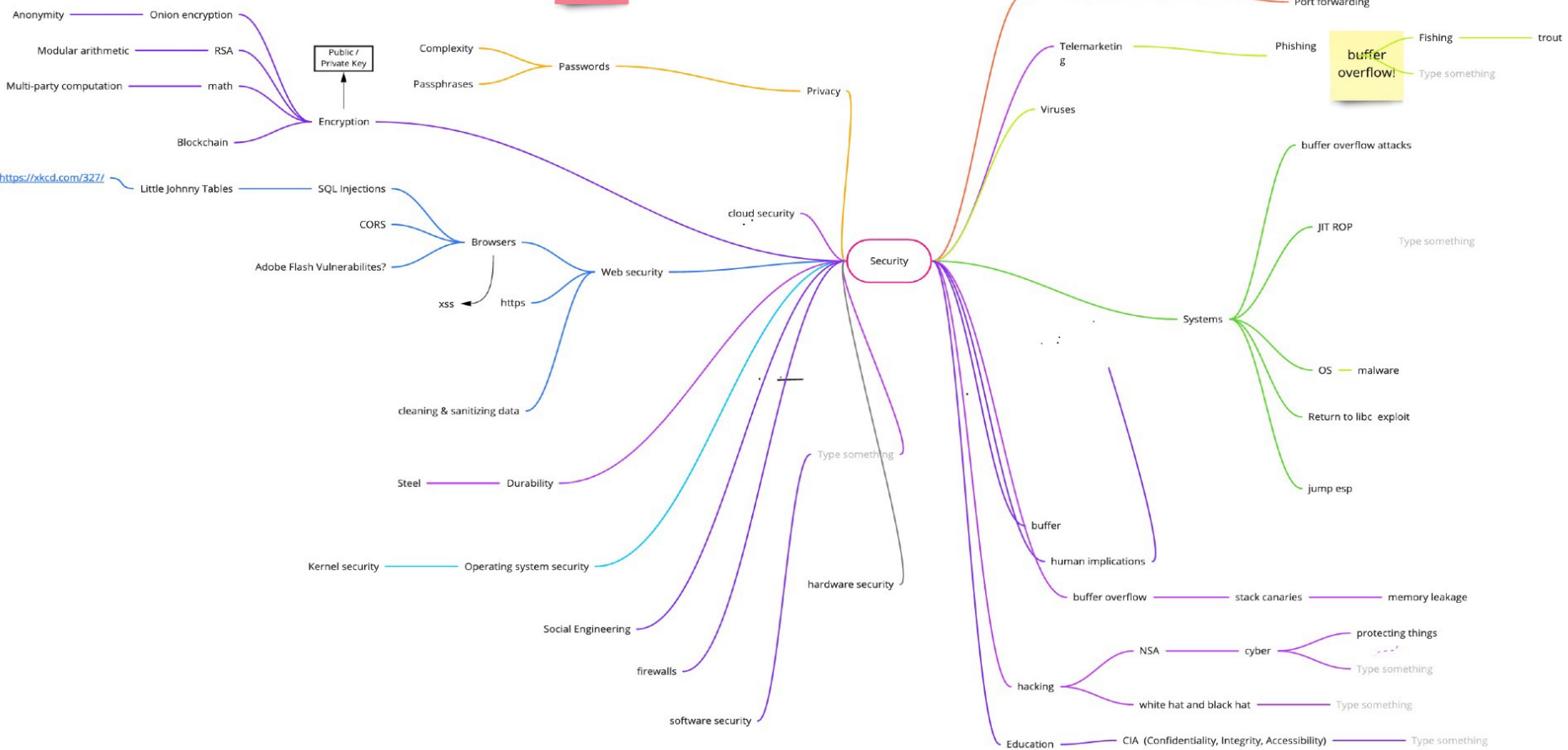


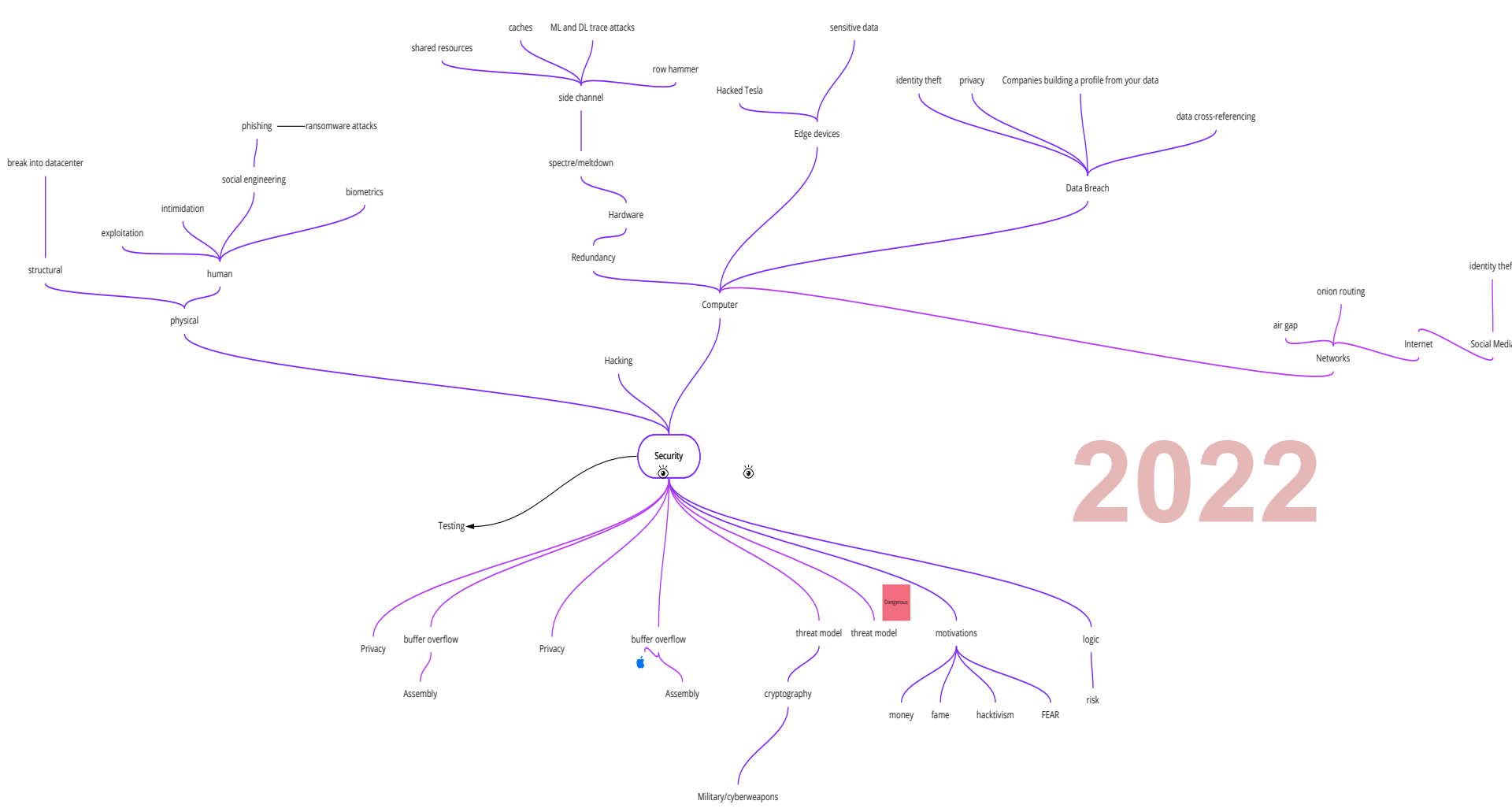
press the "+" button!

2021

PAIN

TRAPS





2022

Introduction to Security

Introduction to Computer Systems Security



Search 🔍

[Checking](#) [Savings & CDs](#) [Credit Cards](#) [Home Loans](#) [Auto Loans](#) [Investing](#) [Better Money Habits®](#)

User ID

Password

Save User ID

[Log In](#)





[Forgot ID/Password?](#) [Security & Help](#) [Enroll](#)

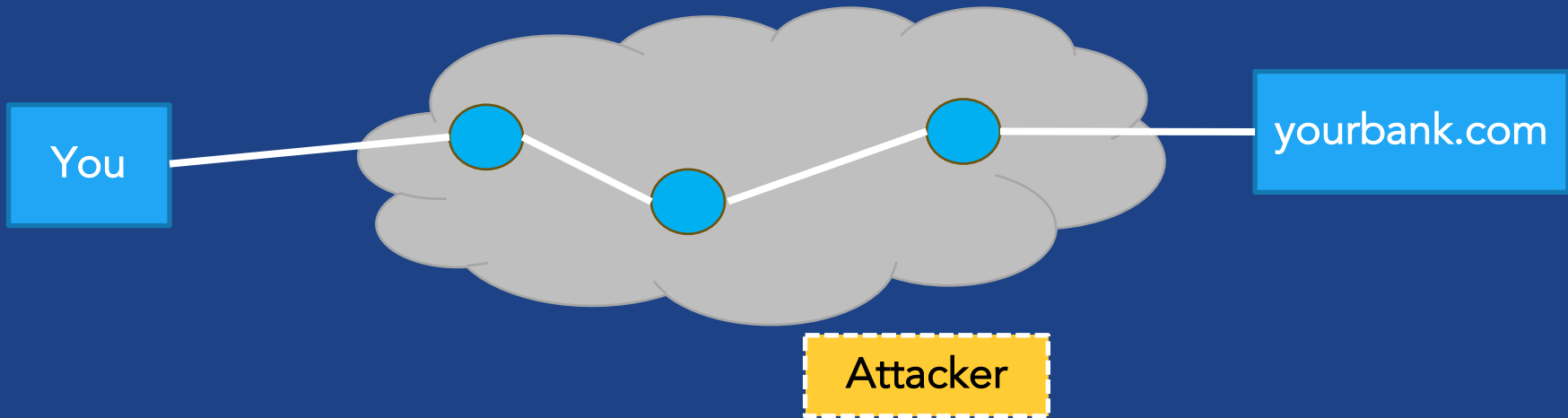
[Open an Account](#)

Find your closest financial center or ATM

Schedule an Appointment

Choose the card that works for you

<p>\$200</p> <p>online bonus offer</p> <p>No annual fee.</p> 	<p>\$200</p> <p>online bonus offer</p> <p>No annual fee.</p> 	<p>25,000</p> <p>online bonus points offer</p> <p>No annual fee.</p> 	<p>0%</p> <p>intro APR offer</p> <p>No annual fee.</p> 
<p>Customized Cash Rewards</p> <p>3% cash back in the category of your choice ></p>	<p>Unlimited Cash Rewards</p> <p>Unlimited 1.5% cash back on all purchases ></p>	<p>Travel Rewards</p> <p>Unlimited 1.5 points for every \$1 spent on all purchases ></p>	<p>BankAmericard®</p> <p>Intro APR offer for 18 billing cycles ></p>



(some) Key security properties

- Confidentiality
- Authentication
- Integrity

(some) Key security properties

- **Confidentiality**: prevent adversary from reading the data
=> Protect against *eavesdropping, sniffing*
- **Authentication**: verifying the identity of a message or actor
=> Protect against *spoofing, impersonation*
- **Integrity**: make sure messages arrive in original form
=> Protect against *tampering*

(some) Key security properties

- **Confidentiality**: prevent adversary from reading the data
=> Protect against *eavesdropping, sniffing*
- **Authentication**: verifying the identity of a message or actor
=> Protect against *spoofing, impersonation*
- **Integrity**: make sure messages arrive in original form
=> Protect against *tampering*

These are just a few!

CIA Triad

Confidentiality

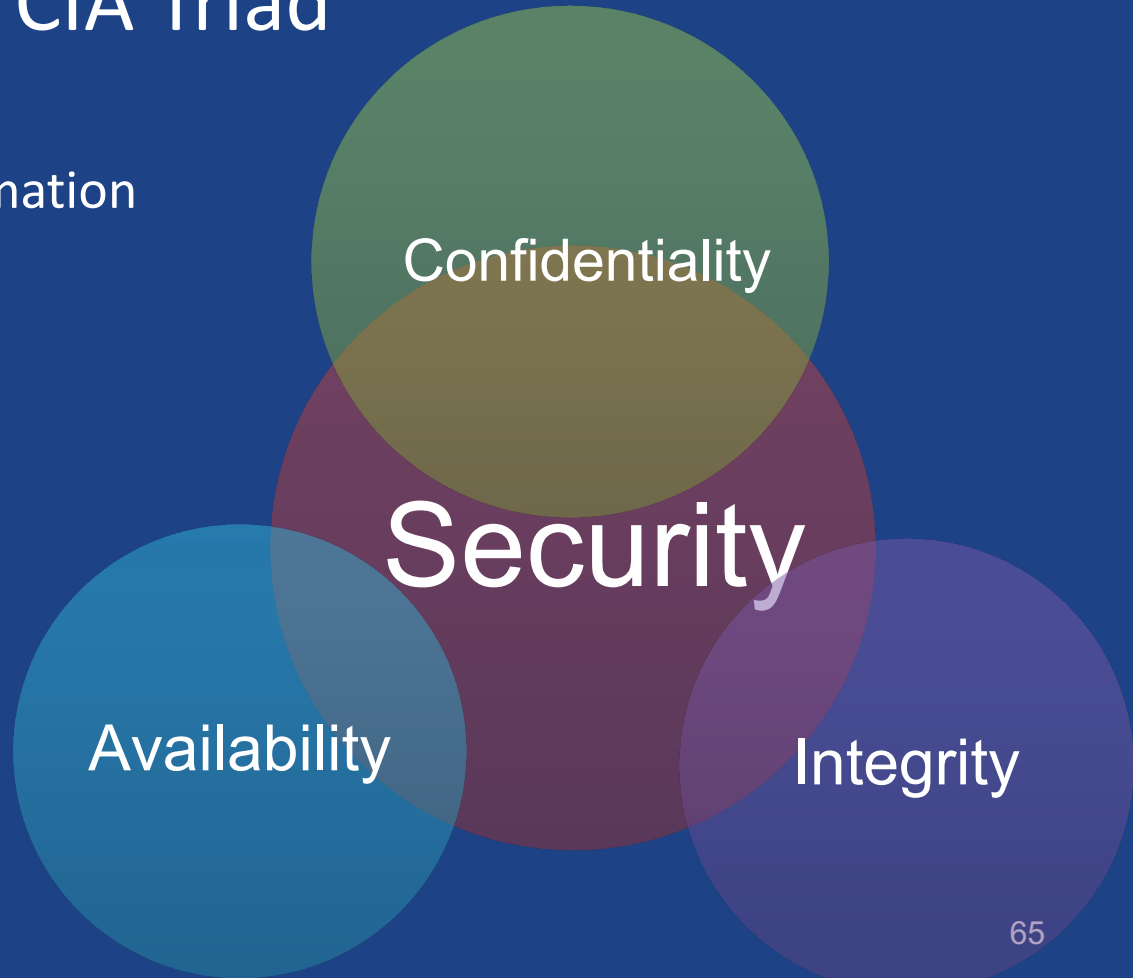
- Prevent disclosure of information to unauthorized parties

Integrity

- Detect data tampering

Availability

- Guarantee access to data



Other important security properties

- **Availability:** Will the network deliver data?
 - Protect against infrastructure compromise, DDoS
- **Authorization:** is actor allowed to do this action?
- **Appropriate use:** is action consistent with policy? (spam, copyright, ...)
- **Anonymity:** can someone tell who is connecting?

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

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

Difficult to define general rules for security => adapt best practices, heuristics based on the system we are considering!

Example: physical safes



TL-15 (\$3,000)
15 minutes with
common tools



TL-30 (\$4,500)
30 minutes with
common tools



TRTL-30 (\$10,000)
30 minutes with
common tools and a
cutting torch



TXTL-60 (>\$50,000)
60 minutes with
common tools, a
cutting torch, and up
to 4 oz of explosives

Example: physical safes



TL-15 (\$3,000)
15 minutes with
common tools



TL-30 (\$4,500)
30 minutes with
common tools



TRTL-30 (\$10,000)
30 minutes with
common tools and a
cutting torch



TXTL-60 (>\$50,000)
60 minutes with
common tools, a
cutting torch, and up
to 4 oz of explosives

Security also about economics

Security tradeoffs

- Complete security against all conceivable adversaries is often unfeasible
- 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

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
 - ...

Best practices

Just some best practices useful in most scenarios:

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