Science of Cybersecurity: Introduction

CS 459/559: Science of Cyber Security
1st Lecture

Instructor:
Guanhua Yan

Thanks for taking CS459/559!

Survey

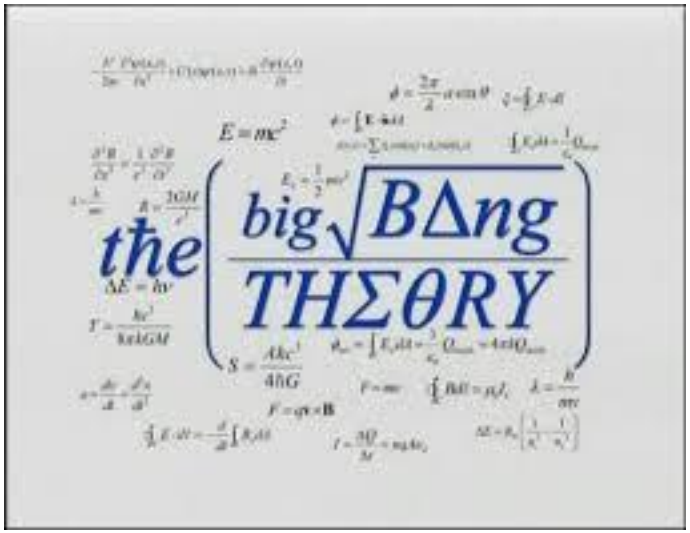
Cybersecurity background

- **How many of you have taken a cybersecurity-related course before?**
  - Introduction to computer security
  - Network security
  - Data security
  - System security
  - AI security
  - …

Interests

- How many of you would like math (or theory) better than systems?

- How many of you would like systems better than math (or theory)?



vs.

Why take the science of cybersecurity?

- I just want to **earn my credit** towards my degree
- I want to **protect my information** on the Internet
- I want to **do research on computer security** later
- I want to **work in the computer security industry**
- I want to **be a hacker**, and make money out of it

Self Introduction

Cybersecurity

Security

- **Security: the state of being free from danger or threat**
  - National security
  - Financial security
  - Job security
  - …
- **Information security: information is free from danger or threat**
- **Cybersecurity (computer security): information security as applied to computing devices**

What is Computer Security?

Ensure that an asset (controlled-by, contained-in) a computer system

1. is accessed only by those with the proper authorization (confidentiality);
2. can only be modified by those with the proper authorization (integrity);
3. is accesible to those with the proper authorization at appropriate times (availability).

Challenge to find a balance:

1. put the asset in a safe, throw a way the key (confidential but not available).

Cybersecurity goals

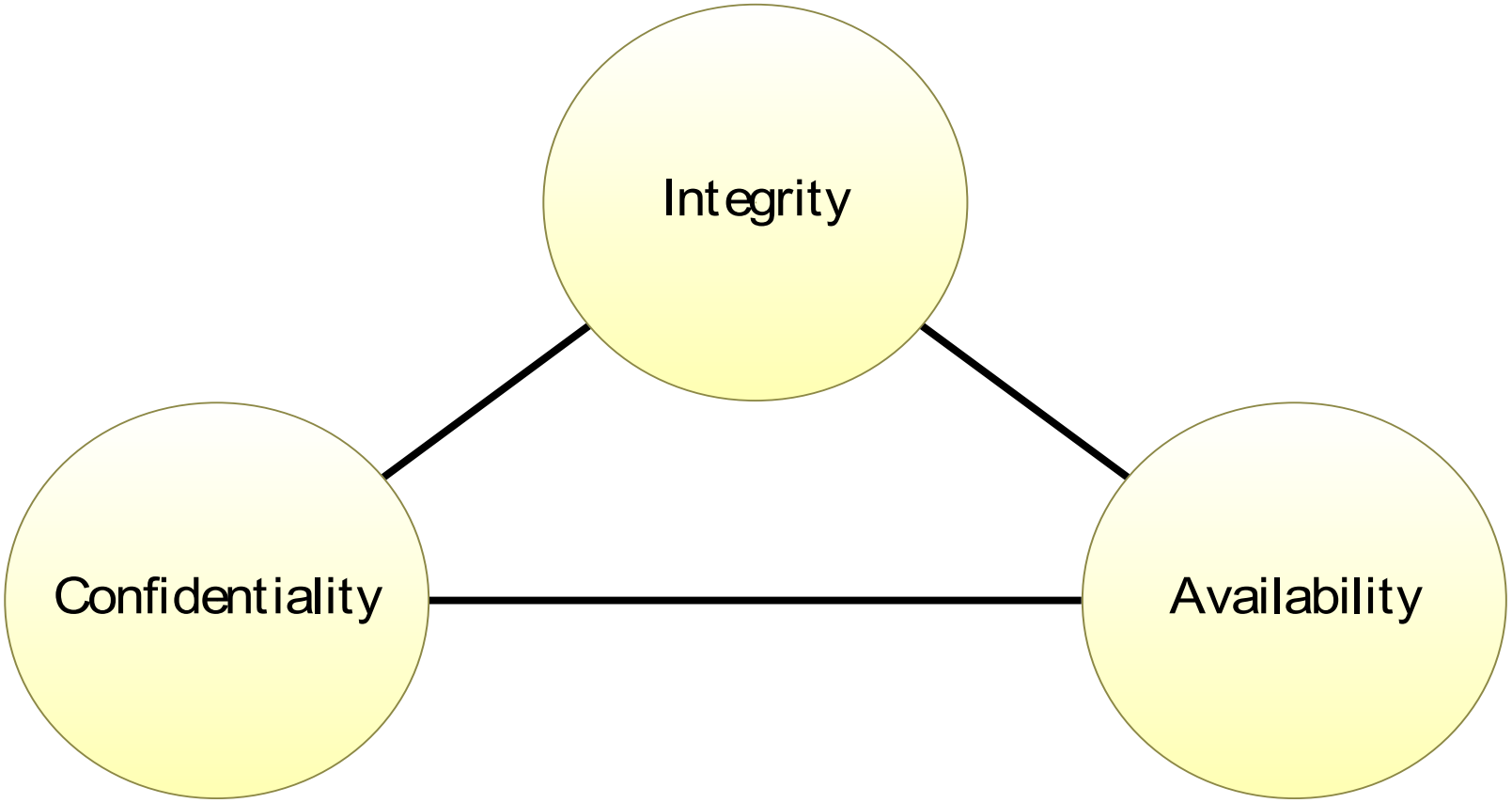
- **Primary goals: CIA**
  - Confidentiality
  - Integrity
  - Availability
- **Secondary goals**
  - Assurance
  - Authenticity
  - Anonymity

Cybersecurity goals

- **Primary goals: CIA**
  - Confidentiality
  - Integrity
  - Availability
- **Secondary goals**
  - Assurance
  - Authenticity
  - Anonymity

Confidentiality, Integrity, Availability

- The C.I.A. Triad.
- These are the primary goals of information security.



Confidentiality

Definition (Confidentiality)

Avoidance of unauthorized disclosure of information or resources.

- You're authorized to read the data ⇒ you get to read it.
- You're unauthorized ⇒ you get to know nothing about the data.
- Reading, viewing, printing, knowing existance of, ...

Confidentiality: Who needs it?

- Who needs confidentiality?
  - Government
  - Military
  - Industry
- Originated in the military — information needs to be restricted to those with a need to know.
- Industry — Personnel records, designs, . . .
- Industrial espionage is a huge problem.

Integrity — Concepts

Definition (Integrity)

Ensure that information hasn't been modified in an unauthorized way.

- Example: whispering game (pass a message from child-to-child, sitting in a circle). Whispering doesn't preserve integrity!
- Benign compromise: a bit gets flipped on disk, the disk crashes, ...
- Malicious compromise: virus infects our system and destroys files, ...
- Writing, changing, deleting, creating, ...

Integrity

- Confidentiality originated in the military arena.
- Integrity originated with corporations (banks) that needed to ensure records (accounts) to be unmodified.

Availability

Definition (Availability)

Ensure that information/ systems/ . . . are accessible by those who are authorized in a timely manner.

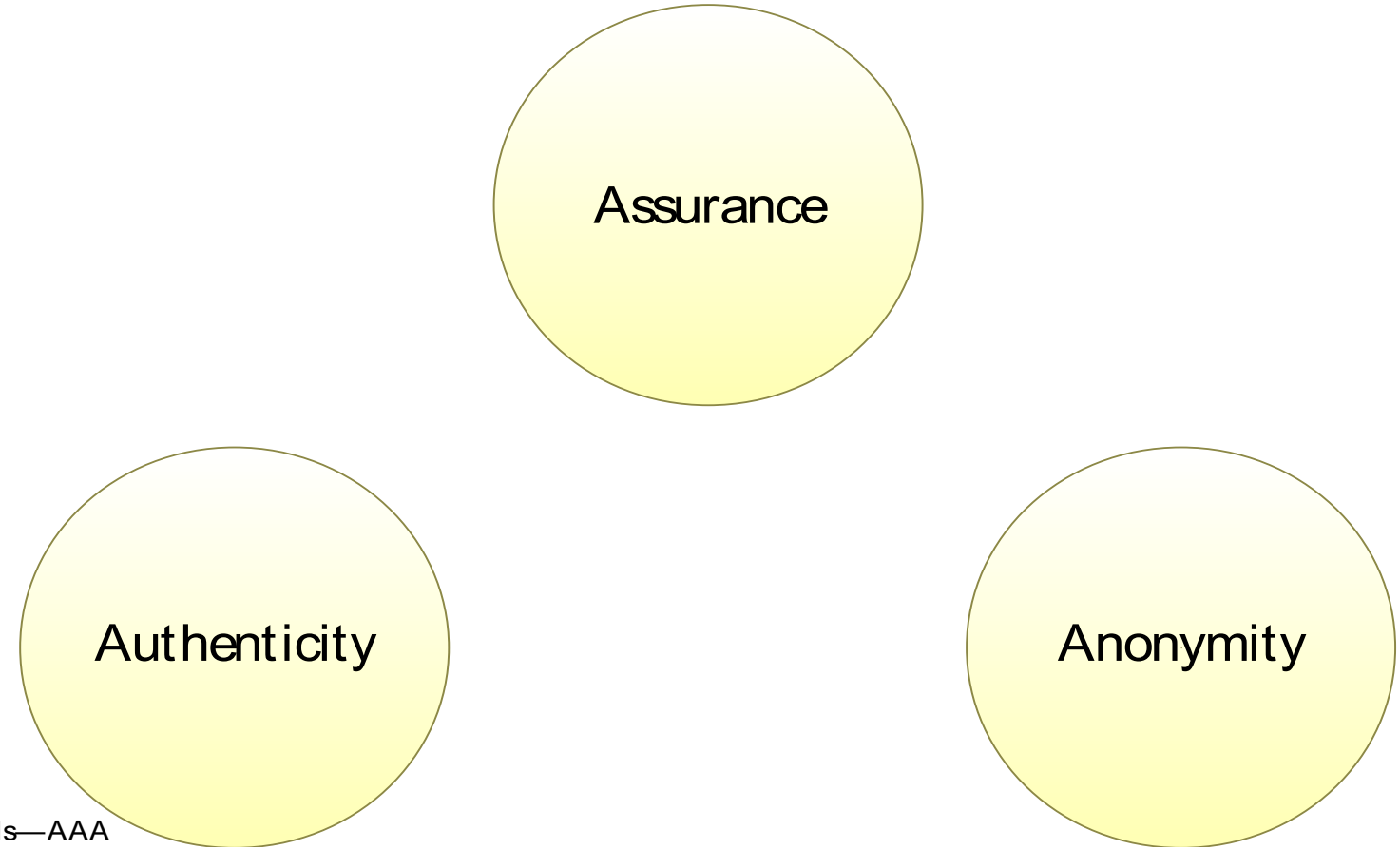
- Some information is time sensitive — it's only valuable if we can get to it when we need it:
  - Stock quotes
  - Credit card number black lists

Cybersecurity goals

- **Primary goals: CIA**
  - Confidentiality
  - Integrity
  - Availability
- **Secondary goals**
  - Assurance
  - Authenticity
  - Anonymity

Assurance, Authenticity, Anonymity

- In addition to the C.I.A. triad we also have the A.A.A. triad of secondary security goals.



Assurance, Authenticity, Anonymity

- Assurance — can we trust systems/people to behave as expected?
- Authenticity — is an issued statement/permission/policy/... genuine?
- Anonymity — can records/transactions not be tied to a particular individual?

Assurance

Definition (Assurance)

The way in which trust is provided and managed in a computer system.

- Trust — the degree to which we expect people and systems to behave as expected. (Many other definitions of trust!)

Assurance: Concepts

- To ensure trust, we first specify
  1. policies — Specifications of how people/ systems are expected to behave;
  2. permissions — Descriptions of actions that people/ systems are allowed to perform.
- Then we put in place
  1. Protections — Mechanisms that enforce policies and permissions.

Authenticity

Definition (Authenticity)

The ability to determine that statements, policies, permissions issued by persons or systems are genuine.

- We need to be able to enforce contracts.
- We cannot enfore the contract unless we know it's genuine.

Authenticity: Nonrepudiation

Definition (Nonrepudiation)

The property that authentic statements issued by a person or system cannot be denied.

- A person could claim they didn't sign a contract, or say it was signed by someone else.

Anonymity

Definition (Anonymity)

Records or transactions cannot be attributed to any individual.

- Our identity is tied to the online transactions we perform:
  - medical records
  - purchases
  - legal records
  - email
  - browsing history

Anonymity: Examples — U.S. Census

- The Census publishes data (race, ethnicity, gender, age, salary) by zip-code.
- They won't publish the information if it would expose details about an individual.

Science of cybersecurity

What is science?

- Science is the intellectual and practical activity encompassing the systematic study of the structure and behavior of the physical and natural world through observation and experiment

- Science is also a systematically organized body of knowledge on a particular subject
  - Physics
  - Chemistry
  - Biology
  - Computer science: theory of computation and design of computational systems

Is science equivalent to theory?

Is science equivalent to theory?

Basic scientific method

- Form hypotheses from what is observed
- Formulate falsifiable predictions from those hypotheses
- If new observations agree with the predictions, a hypothesis is supported (but not proved); if they disagree, it is rejected

Why science of cybersecurity?

- **Transcend specific technologies and attacks**, yet **still be applicable in real settings**
- Introduce **new models and abstractions**, thereby **bringing pedagogical value besides predictive power**
- **Facilitate discovery of new defenses** as well as describe non-obvious connections between attacks, defenses, and policies, thus providing a better understanding of the cybersecurity landscape.

Fred B. Schneider, "Blueprint for a science of cybersecurity", The Next Wave, Vol. 19 No. 2, 2012

Challenges for science of cybersecurity

- The "universe" of cyber-security is an artificially constructed environment that is only weakly tied to the physical universe.
  - Computer hardware and software are **human-made artifacts**, part of what Simon called **sciences of the artificial** – activities that involve making artifacts with desired properties

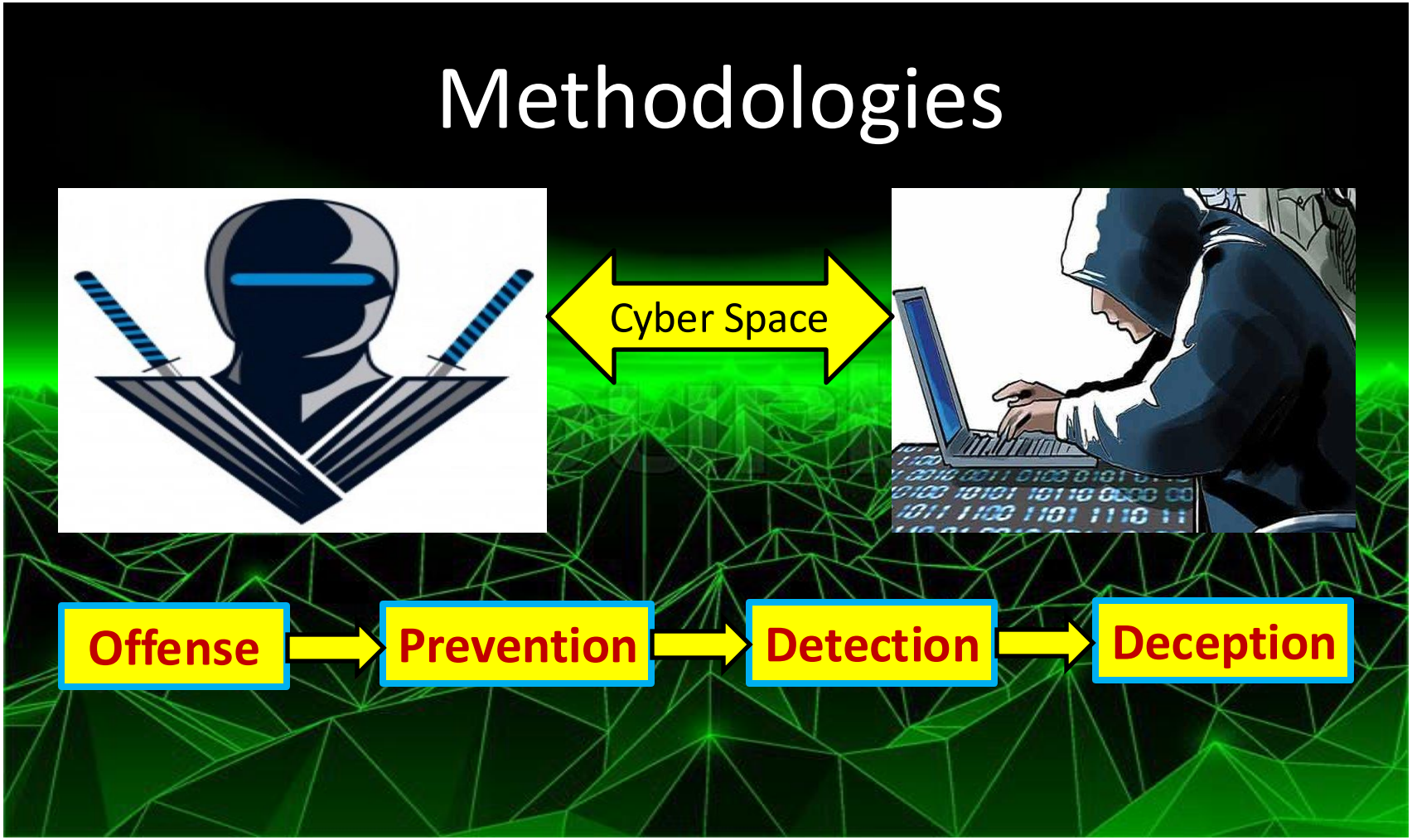
- The threats associated with cyber-security are dynamic in that the nature and agenda of adversaries is continually changing and the type of attacks encountered evolve over time, partly in response to defensive actions.

Cryptography in science of cybersecurity

- Shamir, in accepting the 2002 Turing award, described that non-crypto security is "a mess."
- Peter Neumann, "If you think cryptography is the answer to your problem, then you don't know what your problem is."
- Despite many pointing to crypto as role-model for a Science of Security, its methods are less suitable for numerous areas, e.g., systems security and others involving empirical research. Simply wishing for systems security to be as neat and tidy as mathematically-based crypto does not make it so.

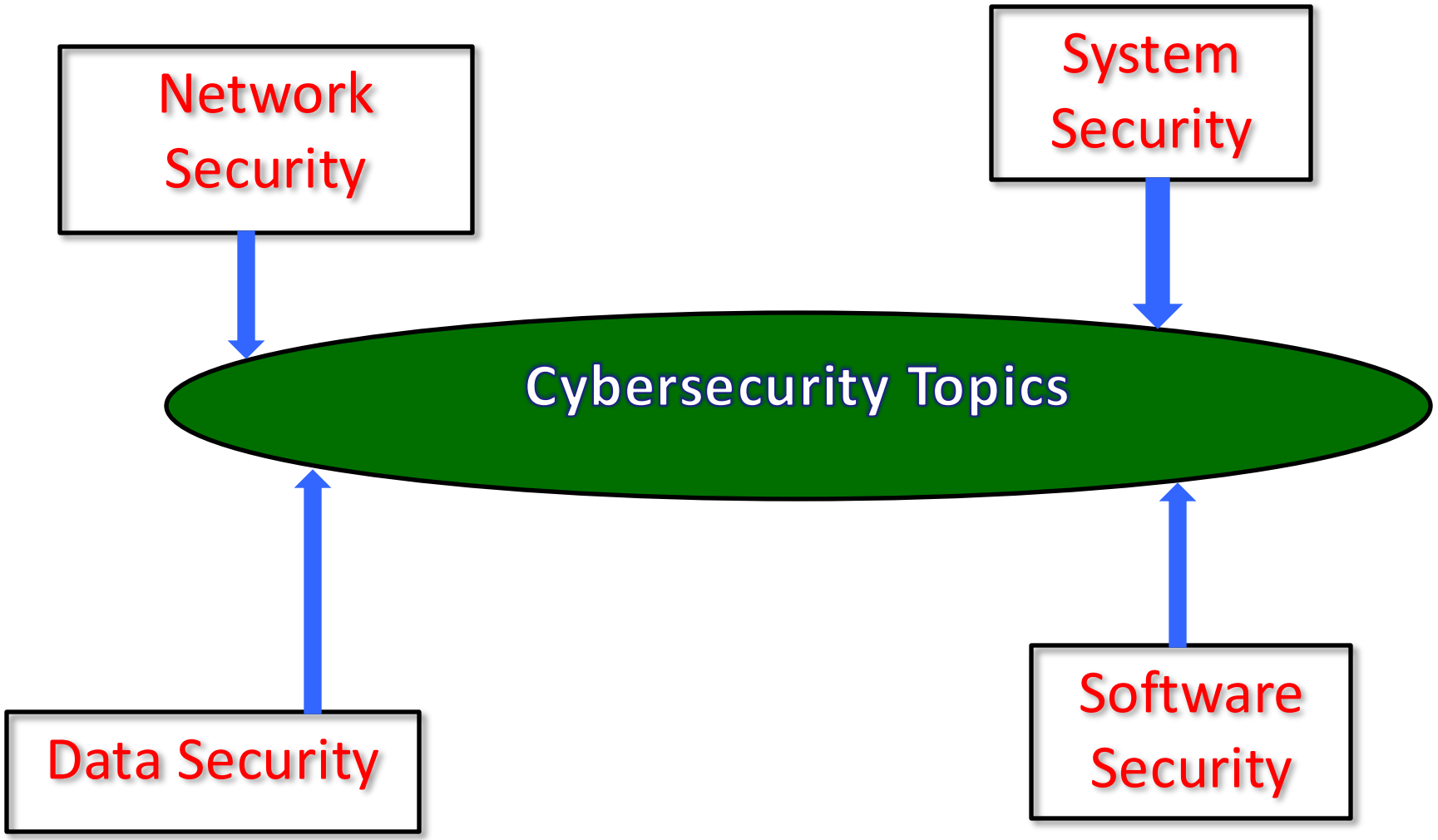
Cryptography will NOT be covered in this course.

Main theme of this course

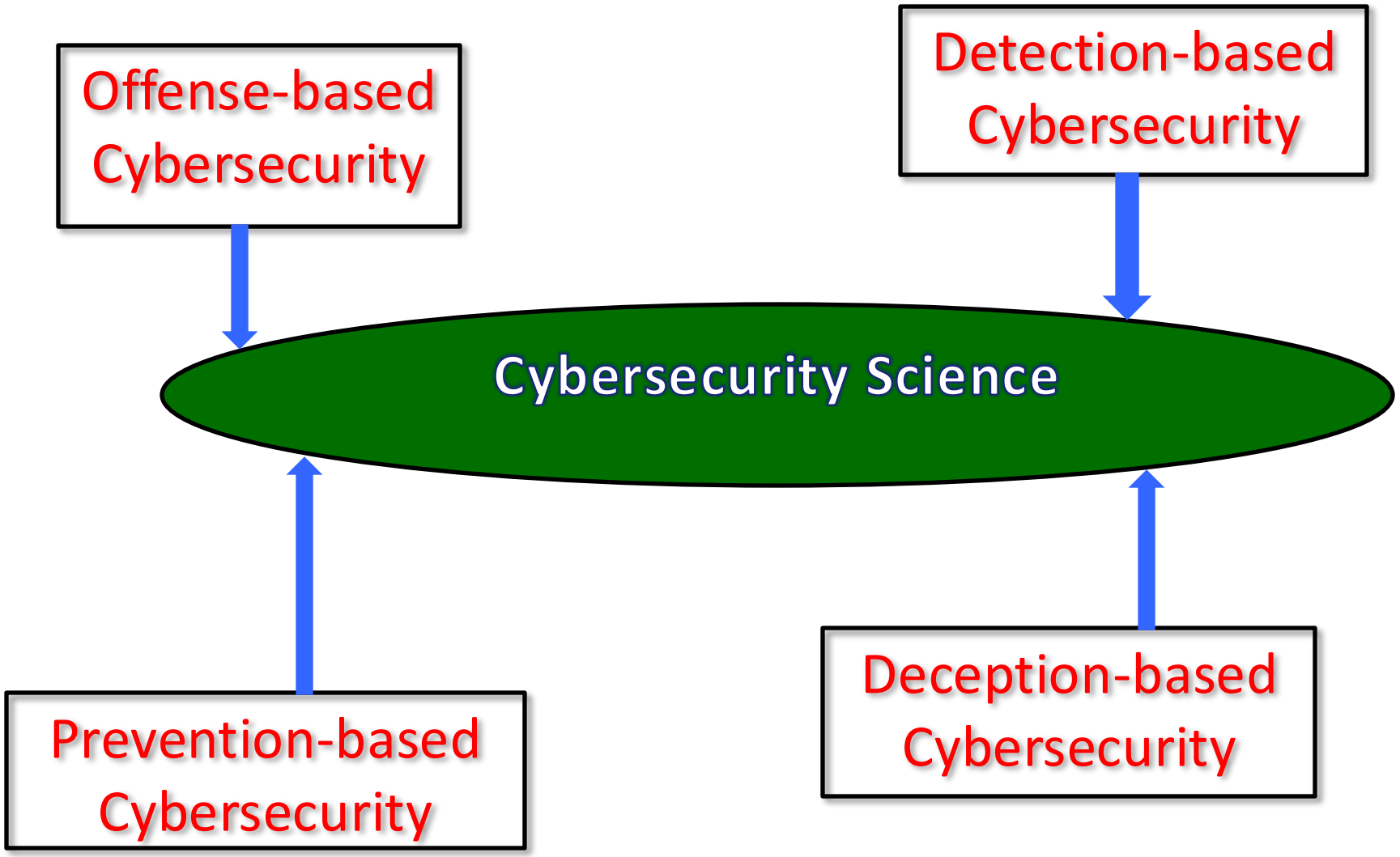


Syllabus

Overview of cybersecurity topics



Overview of cybersecurity science



Course contents (tentative)

- Introduction
- Taxonomy of cybersecurity
- Chapter 1: **offense-based** cybersecurity
- Chapter 2: **prevention-based** cybersecurity
- Chapter 3: **detection-based** cybersecurity
- Chapter 4: **deception-based** cybersecurity
- Conclusions
- Presentations

Chapter 1: offense-based cybersecurity

- (1) Reconnaissance and scanning
- (2) Exploitation of software vulnerabilities
- (3) Exploitation of network vulnerabilities
- (4) Exploitation of system vulnerabilities
- (5) Exploitation of hardware vulnerabilities
- (6) Exploitation of human vulnerabilities

Chapter 2: prevention-based cybersecurity

- **Goal: prevent bad things from happening**
- Secure input handling
- Program testing
- Reference monitor
- Formal methods

Chapter 3: detection-based cybersecurity

- **Goal: catch the bad guys before they do bad things!**
- Signature-based detection
- Anomaly-based detection
- Specification-based detection
- Robustness of detection

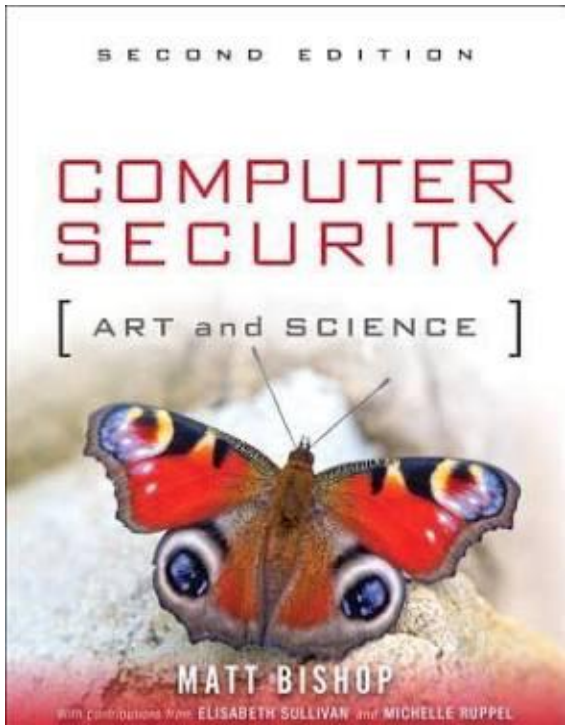
Chapter 4: deception-based cybersecurity

- **Goal: deceive the bad guys into doing something!**
- Art of deception
- Honeypots
- Honeytokens
- Moving target defense

Course material

- Recommended:

Computer Security: Art and Science, Matt Bishop, Addison-Wesley



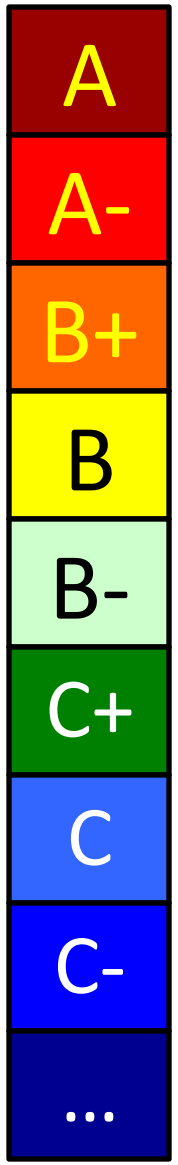
Teaching staff

- **Instructor: Guanhua Yan**
  - Best way to reach me is by email: ghyan@binghamton.edu
  - Office: Q-11 Engineering building
  - Office hours: 1-3PM Monday

- **TA: Srinidhi Shetty**
  - Office: https://binghamton.zoom.us/j/96458469415
  - Office hours: Thursday 10am to noon on Zoom
  - Email: sshetty8@binghamton.edu

Grading (preliminary)

- **Attendance: 10%**
- **Quiz 1: 10%**
- **Quiz 2: 10%**
- **Projects: 20% (TA-graded)**
  - Cyber attacks (demo & report, 10%)
  - Cyber defenses (demo & report, 10%)
- **Presentation: 10% (peer-review)**
- **Capture-the-Flag competition: 10%**
- **Final project report: 30% (Instructor-graded)**
  - At least 15 pages long



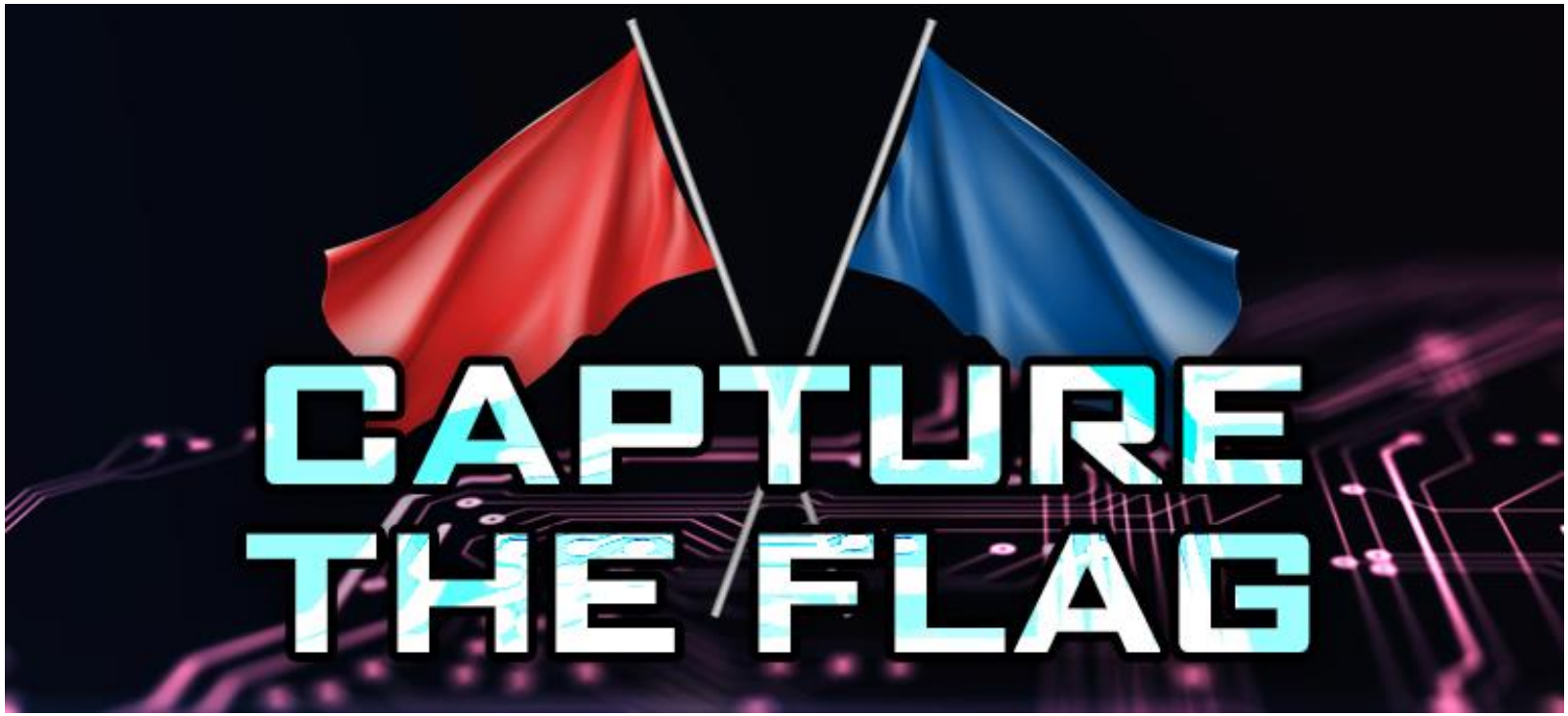
Grading

- Individual projects: graded by the TA
- Final project report: graded by the instructor
- Presentations: graded by peer classmates
- Capture-The-Flag: graded by the TA

Attendance

- Sign-up sheet in each class

Capture-The-Flag



Creativity --> publication?

Have fun from this course!

Getting Help

- **Office hours: will be announced soon**

- **1:1 Appointments**
  - You can schedule 1:1 appointments with any of the teaching staff

- **BrightSpace**
  - Class communication and for handing in projects

Policies: Assignments

- **Unless specified, you must work alone on all assignments**
- **Handins**
  - Assignments due at 11:59pm on due date
- **Appealing grades**
  - Within 7 days of completion of grading

Timeliness

- **Lateness penalties**
  - Get penalized **2.5% per half day**
  - No handins later than **4 days after due date**

- **Catastrophic events**
  - Major illness, death in family, …
  - Let us know as early as possible
  - Will be dealt with on a case-by-case basis

Cheating

- **What is cheating?**
  - **Copying literally the same sentences from other sources (0 tolerance)**
  - **Write your own report**
    - **Cite your sources if you use existing tools**
- **What is NOT cheating?**
  - Explaining how to use systems or tools
  - Helping others with high-level design issues
- **Penalty for cheating:**
  - Look at the Watson School Honesty Code
- **Detection of cheating:**
  - We do check
  - Tools for doing this are much better than most cheaters think!

Violations in a previous year (Spring 2019)

- **Project 1**
  - **Violations: 7**
  - Penalty: 1/4 on presentation category
- **Project 2:**
  - **Violations: 2**
  - Penalty: 10 points on the project
- **Project 3:**
  - **Violations: 3**
  - Penalty: -50 points on the project
- **Project 4:**
  - Violations: 0
  - Penalty: F on the course?

Use of generative AI: Principles from Provost

- Without clear and explicit permission from the course instructor, using generative AI tools for any course assignment or exam (e.g., by entering exam or assignment questions) will be considered analogous to unauthorized collaboration and/or plagiarism.

- In courses that allow the use of generative AI, students should acknowledge and properly cite the use and default to disclosing such assistance when in doubt.

Course policy:

- **Generative AI should be cautiously used in this course. If you use it, please cite it as a reference.**

- **Evaluation:**
  - Presentation: 1-4
  - Difficulty: 1-4
  - Novelty: 1-4
  - Results: 1-4

Final word: This is your class!

- Constant feedback will be greatly appreciated!

Reading list

- JASON, the MITRE Corporation. (2010). Science of cyber-security.

- Herley, C., & van Oorschot, P. C. (2017). SoK: Science, security and the elusive goal of security as a scientific pursuit. In Proceedings of IEEE Symposium on Security and Privacy (S&P), (pp. 99-120). IEEE.

End of Lecture 1