https://brown-csci1660.github.io

CS1660: Intro to Computer Systems Security
Spring 2025

Lecture 1: Introduction

Co-Instructor: **Nikos Triandopoulos**

January 23, 2025

BROWN

Instructor: Nikos Triandopoulos

Associate Professor (of the Practice) in CS, Brown University, 2024 – current

- Co-director of Graduate Studies (Master’s Program)

Preparation

- Diploma in Computer Engineering & Informatics, University of Patras (Greece), 1999
- Graduate studies in Logic, Algorithms & Computation, University of Athens (Greece) 2000
- Sc.M & Ph.D. in Computer Science, Brown University, 2002 & 2006

Prior experience

- Postdoctoral Researcher at Dartmouth College, 2006-7 & Aarhus University (Denmark), 2007-8
- Research & Adjust Faculty at Boston University, 2008-16 & Brown University, 2008-10
- Principal Research Scientist at RSA Laboratories (Cambridge, MA), 2010-16
- Associate Professor in CS at Stevens Institute of Technology, 2016-24

Instructor: Nikos Triandopoulos

Researcher & Educator

- Interests & experience, as a professional & scholar, in Information Security, Privacy & Cryptography

Research

- Trustworthy computing – e.g., private & verifiable outsourced & distributed computation
- Broad & applied, principled & interdisciplinary, academic & industrial
- Enterprise security & Secure Machine Learning (ML) – e.g., intrusion resilience, self-defense security analytics, crypto-enhanced learning, trustworthy, fair & private collaborative learning

Teaching

- Intro to IT Security, Beginner/Advance Cybersecurity, Security, Privacy & Society, Foundations of Cryptography
- Intro to Scientific Comp. & Problem Solving, Seminar/Research & Entrepreneurship in CS
- This Spring: **CSCI1640: AI & Computer Security** & **CSCI1660: Intro to Computer Systems Security**

CSCI1640

AI & Security

How

Artificial Intelligence

& Computer Security

intersect, affect or

contradict each other?

New course for Spring 2025 **Now Open for Enrollment in CAB**

Class meetings: M 3-5:30pm, CIT 368

Instructor: Nikos Triandopoulos

Today

- Course logistics
- Introduction to the Computer Systems Security
  - motivation
  - in-class discussion with real-world examples
    - secure computation outsourcing

1.1 Course logistics

CS1660: Intro to Computer Systems Security

Computer System Security [= Information Security, Computer Security, Cybersecurity]

- Protection of information systems from theft or damage to the hardware, software, or information stored on them, and from disruption or misdirection of the services they provide

CS1660 [= CSCI1660, CSCI1260, CSCI2660]

- 3 course codes, 6 sections (1 in-person & 1 remote per course), but essentially one course…
- Same topics, learning goals, materials, structure, assignments, just difference workload

Disclaimer

CSCI1660 will share course components (e.g., class meetings, Web page and other online learning resources) with CSCI1620 and CSCI2660. Students in these 3 courses (in any section) will be able to see the roster of the other courses or sections. If you have concerns about this, please e-mail the CSCI1660 instructors as soon as possible to discuss your options.

CS1660: Catalog Description

Introduction to Computer System Security

1660

- Computer security from an applied viewpoint
- Hands-on experience on security threats & countermeasures
- Principles & skills for making informed decisions & understanding how security interacts

Topics

- code execution vulnerabilities (buffer overflow, sandboxing), malware (trojans, viruses, worms)
- access control (users, roles, policies), cryptosystems (encryption, hashing, signatures, certs),
- web & network security (password, firewalls, TLS, IDS, VPN), human & social issues (ethics, privacy)

CS1260/2660: Catalog Description (cont.)

1660

- Computer security from an applied viewpoint
- Hands-on experience on security threats & countermeasures
- Principles & skills for making informed decisions & understanding how security interacts

1620/2660

- Via more advanced work on projects, **a half-credit concurrent lab** or **2000-level course version**
- Deeper understanding of materials, focusing on real-world skills, e.g.,
  - performing attacks against systems that are harder to launch or carry out under realistic constraints, rely on less serious vulnerabilities, and achieve higher quality standards than a mere "proof of concept."

CS1660

- 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"

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…	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)

CS1660: 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)

CS1660: The waitlist

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

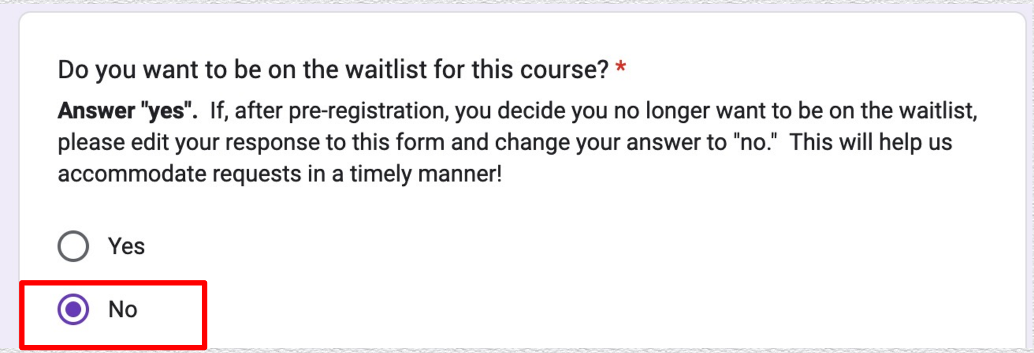
- Were unable to preregister due to CAB issues
- Cannot take the course again or have strict program req’s
- More admissions soon (within the next few days) -- watch your email!

CS1660: 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

CS1660: Learning Goals

Develop a security mindset

- Learn how to understand & communicate about security principles
  - How to assess security threats, identify ways to defend
- Learn by implementing (and breaking) real systems
  - How attacks work in practice
- Learn about historical examples that have shaped modern security
  - Best practices & many examples of what not to do!
- Learn about tradeoffs and impact of security mechanisms, policies, enforcement, …
  - Securing computer systems is a “war,” not a “battle”

CS1660: Topics

- 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, …)

CS1660: Staff

Co-instructors

- **Nikos Triandopoulos** & **Bernardo Palazzi** (to take over after Spring break)
- Course organization/management, lectures, assignments, grades, …
  - all mistakes will be mine ☺
- Office hours: Tuesdays/Thursdays, 1 – 2pm or by appointment
- Office location: CIT 223

Teaching assistants

- Calvin Will, Siming Feng (HTAs),
- Jamie Gabbay, Dan Healey, Ahad Bashir, Shobhit Patel, Patrick Mccann (UTAs or UTA/STAs)
- Assistance w/ labs, projects, assignments, help sessions, grading, demos, as needed
- Office hours: TBA

CS1660: 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

CS1660: Clicker Questions

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

CS1660: 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

CS1660: 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…

CS1660: 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

CS1660: 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!

CS1660: 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…

CS1660: 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!

CS1660: Asking for help (cont.)

- 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 <u>it’s up to you to pieces together</u>

CS1660: Asking for help (cont.)

- 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

CS1660: 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)
- We want you to rest => take time to think about things

CS1660: 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

CS1660: Setup Homework 0

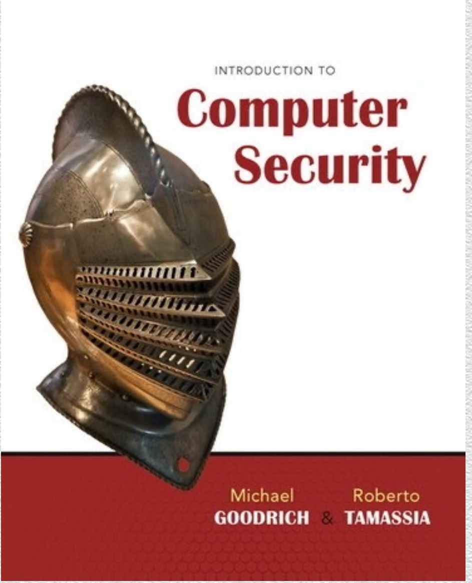
- Ensure you have access to course resources
- Helps us to gauge your comfort level with various topics and concepts covered in this course
- We will use this to determine how to scope lectures and provide other resources
- Complete by next lecture

CS1660: 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)

CS1660: (Optional) Textbook

- The textbook for the course is
  - Introduction to Computer Security by Michael T. Goodrich and Roberto Tamassia, 1st Edition.
- The lecture schedule includes supplementary readings from the textbook, which is available in the Brown University Library.
- Students are not required to purchase this textbook to participate in the course.



Questions?

- Please ask questions during class!

Today

- Course logistics
    - topic of study, enrollment eligibility, sessions
    - staff, learning materials, course organization
    - expectations, grading, policies, announcements
    - syllabus overview, course objectives/outcomes
- Introduction to Computer Systems Security
    - motivation
    - in-class discussion with real-world examples
        - secure computation outsourcing

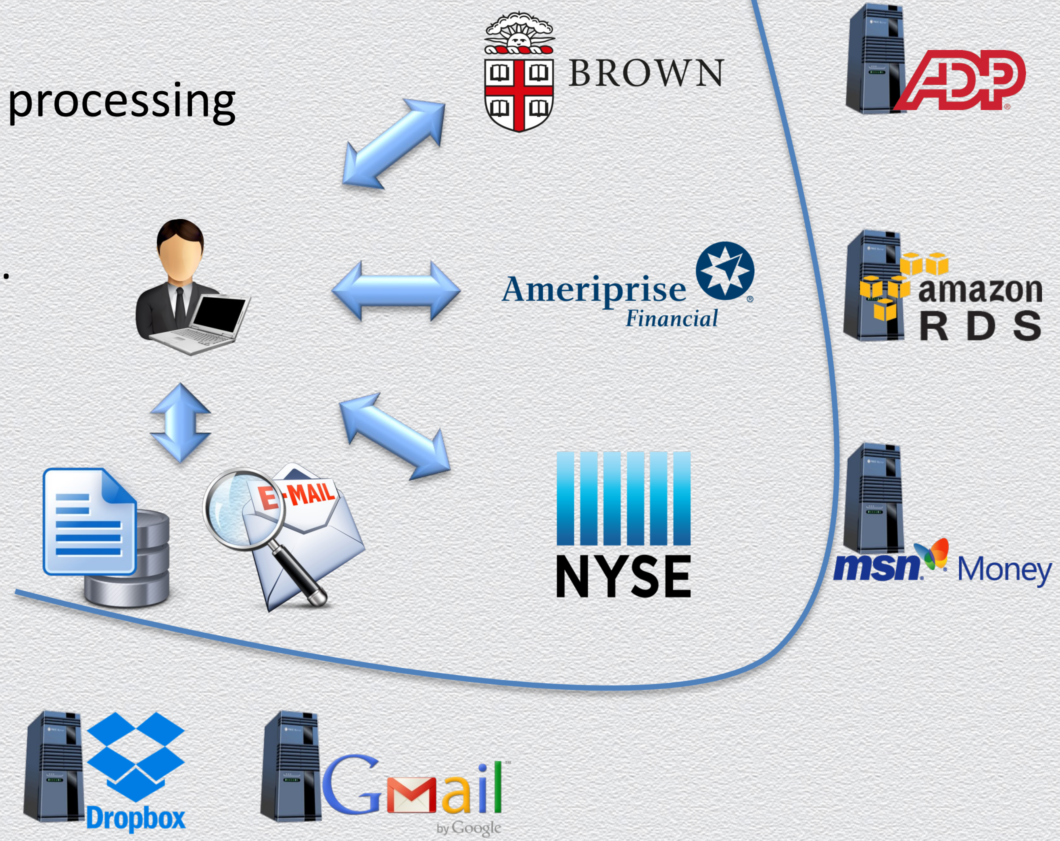
1.2 Secure outsourced computation

Another example: Tax return preparation…

Involves information collection & processing

- calculate financial data
  - payroll, profits, stock quotes, …
- manage data
  - search emails, store records, …
- submit – done!

⇨ **… by many unknown machines!**



Data & computation outsourcing

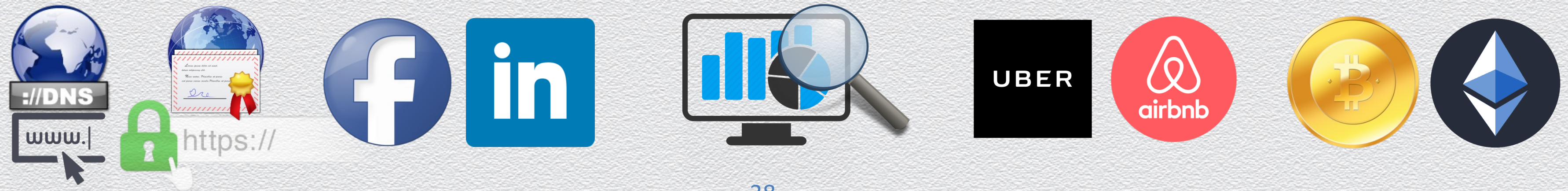
Cloud-based services

- hardware, OS, software, apps, …
- storage, computation, databases, analytics, …

Transformative multi-platform technology

- businesses, organizations or individuals
- client-server, distributed, P2P, Web-based, …

Internet protocols **social networks** **big-data analytics** **sharing economy** **FinTech**



Security consequences

Fact: Untrusted interactions

- information is processed outside one’s administration control or “trust perimeter”

Risk: Falsified / leaked information

- information may (un)intentionally altered by or shared with unauthorized entities

Goal: Integrity / privacy safeguards for outsourced assets

- need to protect information against change, damage / unauthorized access

What can go wrong?

Fact: Untrusted interactions

- information is processed outside one's administration control or "trust perimeter"

Risk: Falsified / leaked information

- information may (un)intentionally altered by or shared with unauthorized entities

Goal: Integrity / privacy safeguards for outsourced assets

- need to protect information against change, damage / unauthorized access

Threats:

- misconfigurations, erroneous failures, limited liability
- economic incentives of cost-cutting providers
- compromises, attacks, advanced persistent threats (APTs)

The C-I-A triad

Captures the three fundamental properties that make any system valuable

- **C**onfidentiality **+ I**ntegrity **+ A**vailability

⇨ Computer security seeks to prevent unauthorized viewing (confidentiality) or modification (integrity) of data while preserving access (availability)