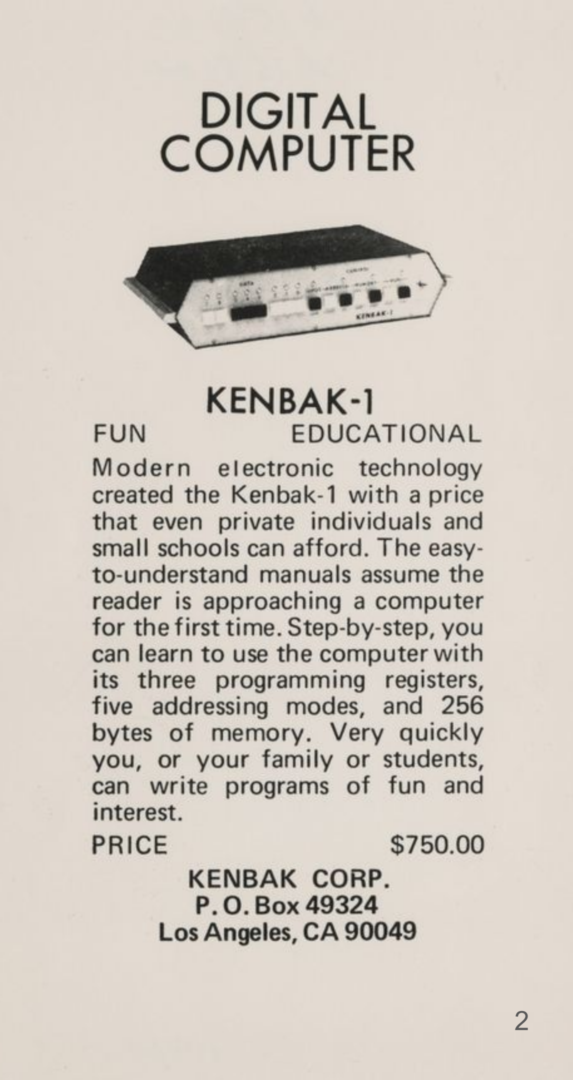
Secure Software Development

Course Plan

CSC 6585 ◇ Fall 2024 ◇ Dr. Stacy Prowell ◇ sprowell@tntech.edu

Course Parts

- Part 0: Preliminaries – Class structure
- Part 1: Motivation – What is security and why is it hard
- Part 2: Basics – Weaknesses, vulnerabilities, and exploits
- Part 3: Security – Physical vs cyber
- Part 4: Models – Historical security models and properties
- Part 5: Threats – Threat modeling and attack trees
- Part 6: Advanced Models – Capability systems and zero trust
- Part 7: Privacy – Understanding differential privacy
- Part 8: Development – Develop secure software
- Aside: Case study of a secure system
- Part 9: Ethics – The ethical crisis in computing



DIGITAL COMPUTER

KENBAK-1

FUN EDUCATIONAL

Modern electronic technology created the Kenbak-1 with a price that even private individuals and small schools can afford. The easy-to-understand manuals assume the reader is approaching a computer for the first time. Step-by-step, you can learn to use the computer with its three programming registers, five addressing modes, and 256 bytes of memory. Very quickly you, or your family or students, can write programs of fun and interest.

PRICE $750.00

KENBAK CORP.
P. O. Box 49324
Los Angeles, CA 90049

Advertisement for the Kenbak-1, arguably the first personal computer

CSC 6585

Preliminaries

Part 0: Preliminaries

Purpose

Understand the class structure, goals, and expectations.

Key Ideas

- Homework focuses on practical application, exams focus on theory
- Collaboration on homework is acceptable, but not on exams
- You are solely responsible for your work
- Grades are what they are; you are not in competition with your classmates
- Security is hard; come to class, review the slides, and do the homework

CSC 6585

MOTIVATION

Part 1: Motivation (1)

Purpose

Start to develop a security mindset. What is security and why is it so hard to define, achieve, and measure? What are some ways people have tried to understand security?

Key Ideas

- Security is a property of systems, and the definition of a system can be (almost) arbitrary
- Security is highly contextual; a system that is secure in one context may not be in another
- Insecurity often arises at interfaces, tacit assumptions, and unenforced standards

Part 1: Motivation (2)

Understand
Why is security hard? What do we mean when we say something is secure or insecure, and why is that so hard to pin down?

- Example of a system and its security in context (mag lock)
- Security is contextual and a property of a system
- Eisenhower: If a problem cannot be solved, enlarge it (expand the system or context)
- Given a goal, think about how to accomplish that goal by attacking a system

Know
Explain a skill and have the students practice it in the homework. Motivate it: Why is this worth knowing?

- No homework for this part; in class collaborative exercise on system exploitation (avoiding an F in this class)
- Start thinking about risk-reward

CSC 6585

Basics

Part 2: Basics (1)

Purpose

Understand how weaknesses become vulnerabilities that can be exploited. Understand the MITRE models

Key Ideas

- Weaknesses often arise when assumptions can be violated
- Weaknesses can give rise to a vulnerability
- A vulnerability exists when there is an exploit
- There are lists of common weaknesses and vulnerabilities

Part 2: Basics (2)

Understand
Where does insecurity come from?

- Security is different from other "ilities."
- All systems are systems-of-systems
- Insecurity arises at the "edges"
- A system can become insecure because of insecurity in other systems
- Adding a feature to a secure system can make it insecure
- CVE and CWE

Know
Start thinking about what security means in different contexts.

- Defining security
- Properties of a definition of security

CSC 6585

security

Part 3: Security (1)

Purpose

Understand physical vs. cyber security and how threats can interact

Key Ideas

- We can learn from physical security models
- Think about blended threats

Part 3: Security (2)

Understand
How a common model for physical protection compares to a common model for cyber security

- DoD & DOE protection model: Deter, Detect, Delay, Respond, Neutralize
- Failure is anticipated
- NIST Five Functions: Identify, Protect, Detect, Respond, Recover
- Scoping security

Know
Begin thinking adversarially about goals, consequences, risk, and protection

- Informally model the security of a system
- What value could the system provide to an attacker?
- What are acceptable failure modes?
- What are the consequences of a security failure?

CSC 6585

MODELS

Part 4: Models (1)

Purpose

Understand historical security models

Key Ideas

- Simple security models provide a way to think about the bare-minimum requirements for a secure system
- Properties of secure systems can be in conflict and have to be balanced based on mission

Part 4: Models (2)

Understand
Historical models for security and security properties

- The CIA triad
- The Parkerian hexad
- The Four Step model
- The Bell-LaPadula model
- The Biba model
- The Clark-Wilson model

Know
Understand historical views of security, security properties, security models, and how properties can come into conflict

- Evaluate a system with respect to security models
- Understand what a violation of each property entails

CSC 6585

threats

Part 5: Threats (1)

Purpose

Understand threat modeling

Key Ideas

- Threat modeling helps identify risks and consequences, and can organize security efforts

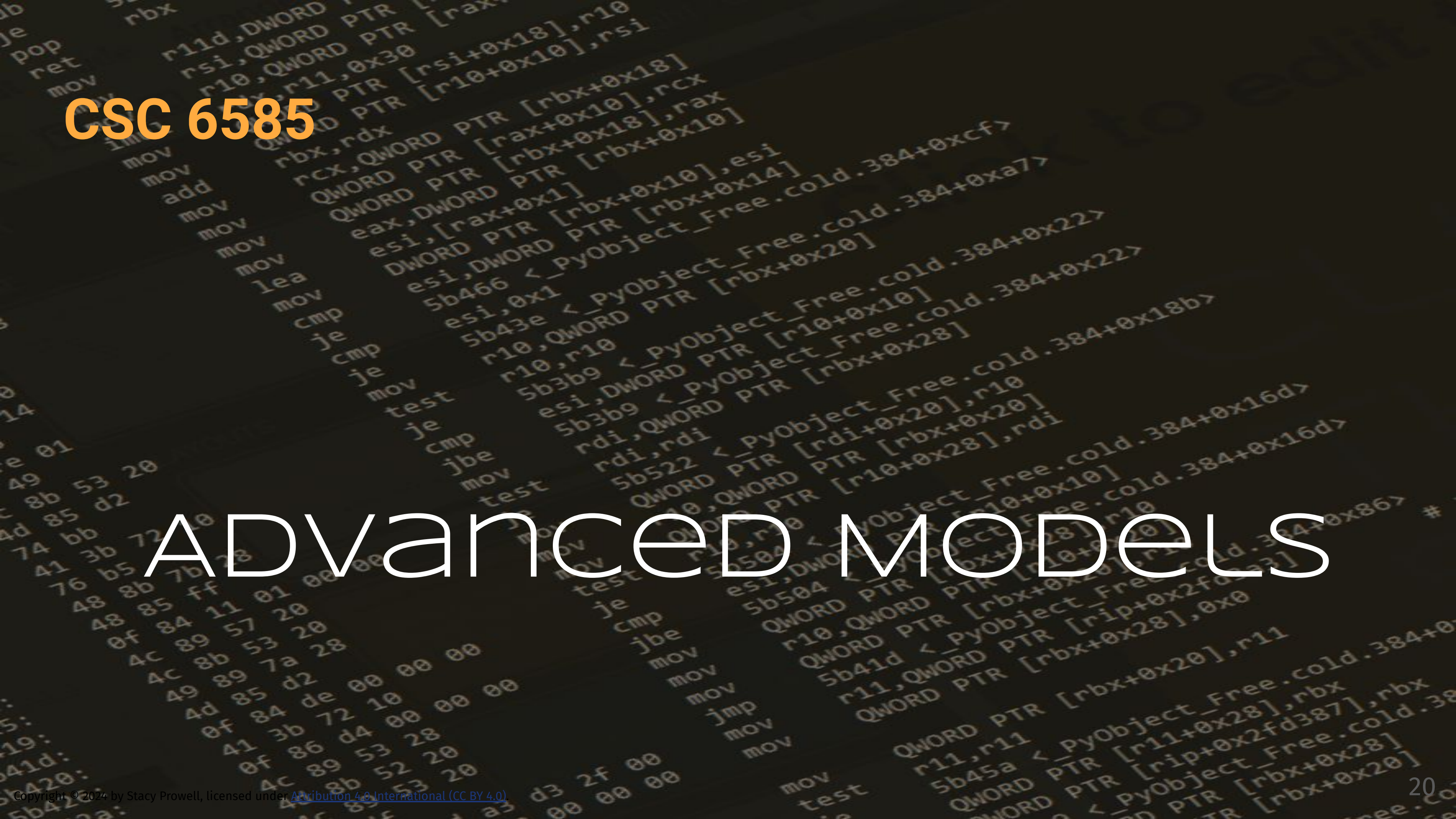
Part 5: Threats (2)

Understand
Understand basic threat modeling

- System diagrams
- Interaction diagrams
- Ad-hoc modeling
- Threat lists (OWASP and MITRE)
- STRIDE
- The "Sterile Field" and trust boundaries
- The attack surface
- CAPEC
- Attack trees
- Attack graphs

Know
Understand basic threat modeling

- Identify system interactions and assumptions
- Identify the attack surface for a system
- Apply basic threat modeling with STRIDE
- Create attack trees for a scenario



CSC 6585

Advanced Models

Part 6: Advanced Models (1)

Purpose

Understand some modern approaches to security

Key Ideas

- Understand capability systems and "zero trust"

Part 6: Advanced Models (2)

Understand
Understand more advanced threats and models

- The confused deputy problem
- CSRF, clickjacking, and symlink race
- Access control systems
- RBAC, ABAC, MAC/DAC, RAdAC
- Capability systems
- The perimeter problem
- Zero trust initiatives
- Zero trust architecture(s)

Know
Recognize more advanced (interaction) threats

- Identify potential risk from system interactions
- Identify issues with zero trust implementations
- Understand the comparative benefits and weaknesses of modern security models

CSC 6585

privacy

Part 7: Privacy (1)

Purpose

Understand data privacy

Key Ideas

- Data privacy versus data security
- Simple privacy models
- Differential privacy

Part 7: Privacy (2)

Understand
Understand the need for and implementation of data privacy

- Why privacy is important/relevant
- Data privacy versus data security
- Individual privacy and population data
- Statistical concepts for privacy
- The spinner model and deniability
- Indistinguishability and group identifiers
- k-Anonymity
- Introduction to differential privacy

Know
Recognize more advanced (interaction) threats

- Recognize privacy threats
- Apply basic differential privacy

Development

Part 8: Development (1)

Purpose

Understand application-level security

Key Ideas

- Understand what security means for your application
- Develop a security plan for your application
- Apply everything learned to application development

Part 8: Development (2)

Understand

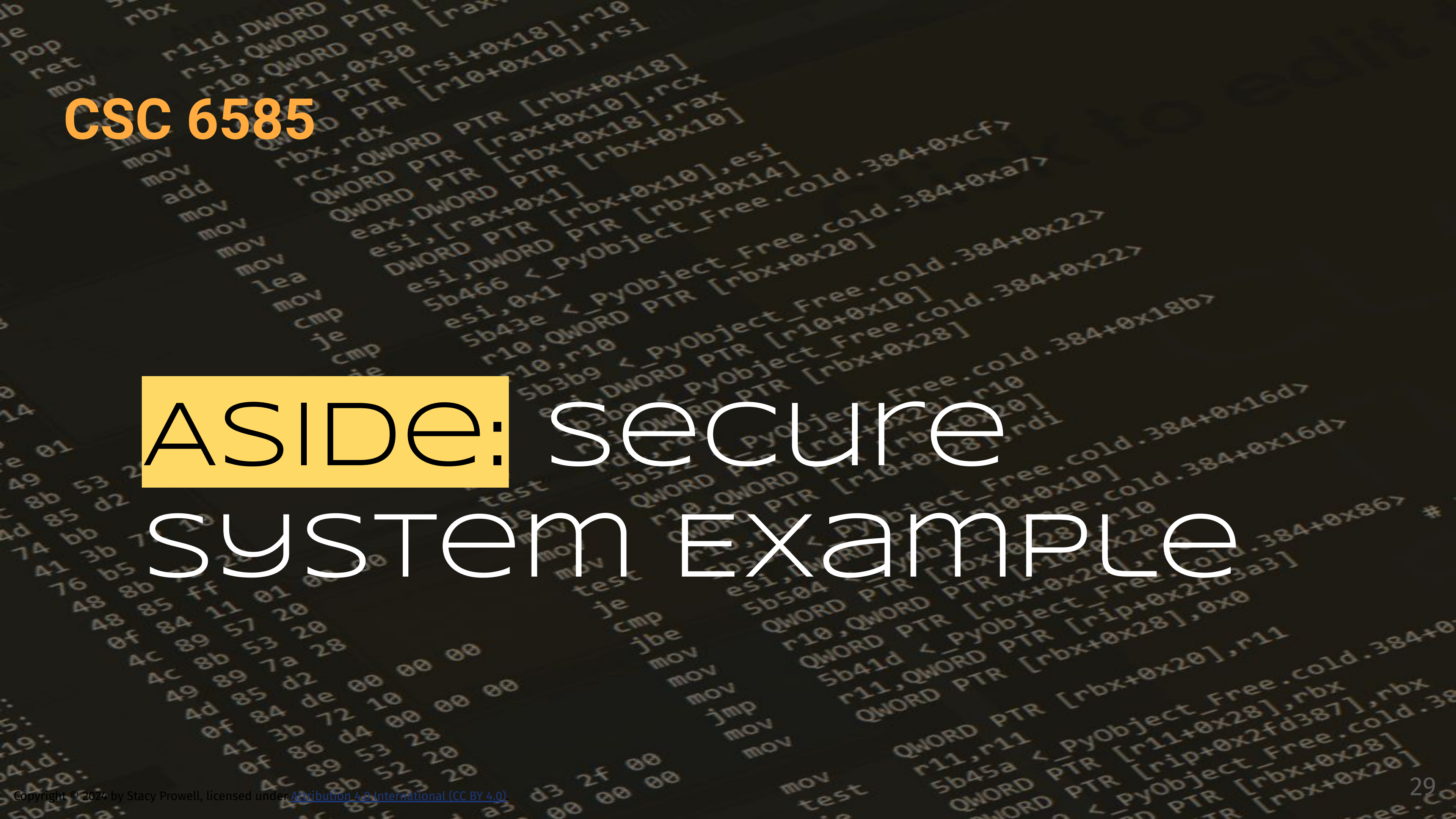
Understand security concepts in application development and maintenance

- Identify security issues early and develop a security plan
- Apply security-oriented thinking to application development
- Least information principle
- Secure coding guidelines
- SEI/CERT Coding Guide
- MISRA Coding Guide
- AuthN and AuthZ
- Successful applications must be maintained
- Security always decays

Know

Apply security lessons to software development

- Identify information leakage
- Identify interface concerns
- Implement data validation
- Develop an application-level security plan
- Understand the role of documentation in maintaining security



ASIDE: secure system example

Aside: Secure System Example (1)

Purpose

Present a case study of a highly-secure system from architecture to design and implementation

Key Ideas

- Understand the role of each concept we have discussed and how the fit into the case study

CSC 6585

ETHICS

Part 9: Ethics (1)

Purpose

Understand ethical and legal issues in secure software

Key Ideas

- Cover legal issues not already covered elsewhere in the lectures
- Recent developments in security and privacy legislation and litigation
- Ethical concerns in software security and data privacy

Part 9: Ethics (2)

Understand
The legal landscape for security and privacy

- Liability laws and litigation
- Identity and privacy protection laws and litigation
- EU and US privacy protection
- Ethical concerns and the "ethics crisis" in computing

Know
Understand some of the legal and ethical landscape of security and privacy and how it affects software development

- Recognize ethical concerns in software development and apply ethical decision making
- Recognize privacy concerns and suggest mitigations
- Understand when you need a security or privacy review