# Secure Software Development

## Course Plan

CSC 6585 ◇ Fall 2024 ◇ Dr. Stacy Prowell ◇ <u>sprowell@tntech.edu</u>

Copyright © 2024 by Stacy Prowell, licensed under Attribution 4.0 International (CC BY 4.0)

### **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

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

## DIGITAL



### KENBAK-1

EDUCATIONAL

Modern electronic technology created the Kenbak-1 with a price that even private individuals and small schools can afford. The easyto-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

FUN

\$750.00

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

#### 0 P110.DAU rsi, QNORD PTR [rat PTR 1/10+0×101,151 pop rox, OHORD PTR [nbx+0x18] Fat ONORD PTR [ratiox10].rcx mos ENURD PTR interestants in rax ONORD PTR PTR Interestants eax, DNORD AND AND AND INTEREST est-unuru Prin Iroxtoxia Jold.384+0xcf7 50466 4\_Pyobject\_Free.cold.384+0xcf7 est.ext 00 Pozaroz EDWORD PTR LIDX+0X101,esi est,0X1 & PyObject\_Free.cold.384+0x377 5043e 19.00000 PTR [nbx+0x20] nov Protocologic Presidente Control 1 nov esi, fraxtox1) 300 sologo and a problect free.cold.384+0x227 100 mos r10,00000 PTR (rbx+0x20) est. 04000 prin interester cold.384+0x227 50309 < Pyobject Free.cold.384+0x227 rdi.04000 prin [rbx+0x28] 100 nov rdi-indi & Pyobject Free.cold.384+0x1807 50522 PTR [rdi-toy28].rdi 50522 PTR [rdi-toy28].rdi 123 e51,0x1 mon CMP r10,r10 CMP CONTRACTOR AND A CONTRACT AND A CONT mon 1255 200 cnp 502 mos Unont PATA Nobject Free.cold.384+8x867 = 56416 04080 PTR [ree.cold.333] 80 ONO 40 35 60 7 70 65 00 CHORD PTR LIDX+07281,0x9 30 14 35 20 50453 PTR Inthe Ar2 Firee. cold. 384+0 84 ONORD PTR [rbx+0x20],r11 05 300 89 100 30 101 de 00 mos 35 09 500 84 12 00 04 mov 12,123 195 100 86 4205 25 00 89 05 GA20: 20 80 00 ion 4.6 InterNational (CC BY 4.0) 511Sh-02024 00 er <u>Attrib</u>

### **Part 0: Preliminaries**

#### Purpose

Understand the class structure, goals, and expectations.

- 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



### 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?

- 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



### Part 2: Basics (1)

#### Purpose

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

- 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



### Part 3: Security (1)

#### **Purpose**

Understand physical vs. cyber security and how threats can interact

- 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?



### Part 4: Models (1)

#### Purpose

Understand historical security models

- 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



### 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

#### est. 04000 prin interester cold.384+0x227 50309 4 pyobject free.cold.384+0x227 rdi.04000 prin [rbx+0x28] 191-rat pyobject\_free.cold.384+0x18b> 50522 probject\_free.cold.384+0x18b> 00000 pro frai+0x201,0001 00000 pro frai+0x2021 pri Nobject Free cold. 384+0x16d> Pol. rol 502 100 advanc East C0X867 85 82 60 Ebatic & Pyobject Freeorer Ebatic Onono Free Linipronorer Fritzon oron Free Linipronorer 852,010 Quono PTR (roxyour -10,0H0R0 FTT QUORD PTR 50584 CHORD PTR [nbx+9/28], 9/9 80

300

00

25

100

100

1103

500

mov

most

est-unuru Prin Iroxtoxia Jold.384+0xcf7 50466 4\_Pyobject\_Free.cold.384+0xcf7 est.ext

r10,00000 PTR (rbx+0x20)

estate A pyobject Free.cold.384+0x377 5043e A pro pre Inbytexpail

esi onono pin [riotoxio]

sologo and a problect free.cold.384+0x227

50453 PTR Inthe Ar2 Firee. cold. 384+0

ONORD PTR [rbx+0x20],r11

123,123

0

2 De

30 40

192

4205

GA20:

7191-02024

pop

Fat

mos

101

35

08

84

09

30

35

as-

05

84

MON

300

mov mov

NOV mos

123

103 cmp

COP

00

64

80

12

86

er <u>Attrib</u>

39

20

00

ion 4.6 InterNational (CC BY 4.0)

now 1255

P110.DAUGO

rsi, QNORD PTR [rat

00 POXATOS

585 Prestox181,011

PTR [n10+0x10],nsi

rcx, OHORD PTR [nbx+0x18]

esi, (rax+0x1)

COD

ONORD PTR [ratiox10].rcx

e51,0x1

ENURD PTR interestants in rax ONORD PTR PTR Interestants eax, DNORD AND AND AND INTEREST

EDWORD PTR LIDX+0X10], esi DWORD PTR LIDX+0X10], esi DWORD PTR LIDX For MANA

r10,r10

Pronto hono promono xtoxtoxtal

### 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



### Part 7: Privacy (1)

#### Purpose

Understand data privacy

- 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

#### 0 P110.DAUGO rsi, QNORD PTR [rat 585 Prestox181,011 PTR [n10+0x10].nsi pop rcx, OHORD PTR [nbx+0x18] ret ONORD PTR [ratiox10].rcx mon ENURD PTR interestants in rax ONORD PTR PTR Interestants eax, DNORD AND AND AND INTEREST est-unuru Prin Iroxtoxia Jold.384+0xcf7 50466 4-Pyobject\_Free.cold.384+0xcf7 est.ext 00 POX.rdx EDWORD PTR LIDX+0X101,esi estate A pyobject Free.cold.384+0xa77 5043e A pro pre Inbreaxal nov Protocologic Proston (noxtoxtoxta) nov esi, (rax+0x1) 300 sologo and a problect free.cold.384+0x227 mov mos r10,00000 PTR (rbx+0x20) est. 04000 prin interester cold.384+0x227 50309 4 pyobject Inbx+0x281 rdi.04000 prin Inbx+0x281 NOV 100 123 ratingi a pyobject Free.cold.384+0x18b7 5b522 a FTR [rdi+0x20],n10 5w0RD PTR [rdi+0x20],n01 2w0RD PTR [rde+0x28] rdi esi onono pin [riotoxio] e51,0x1 most cmp r10,r10 COP 2025 Free cold. 384+0x16d> 1103 1255 2- cold. 384+0×1607 2 De 101,101 COD 502 103 UNOND PTR POSTON 20 ... 10 ... 384+0x867 ; 50414 CHODIECT Free. cold.384+0x867 ; 50414 CHORD PTR [riptox2f038] or 511.0NORD PTR [ribtox28] or 01020 PTR [ribtox28] or 02020 PT East 80 40 35 60 50584 CA OHORD PTR PTR 65 00 653 11 01 20 123 CHORD PTR [rbx+9728], 9x9 58 35 50453 PTR Inthe Ar2 Firee. cold. 384+0 ONORD PTR [rbx+0x20],r11 84 300 05 89 100 30 100 Dec 1103 35 09 20 500 84 00 mov 64 12,123 192 100 86 4205 05 89 GA20: 28 Yon 4.0 International (CC BY 4.0) 88 20 Pyright 02024 er <u>Attrib</u> <u>((C BY 4.0)</u>

### Part 8: Development (1)

#### Purpose

Understand application-level security

- 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

#### ONORD PTR [[axtox10].rcx Envirue print internet and in nax ONORD print internet and interaction eax, DNORD print interaction est-sumuru prin troxtox141\_Ja84+0xcf7 50466 4\_pyobject\_Free.cold.384+0xcf7 est\_8x1 EDHORD PTR [rbx+0x10], esi DHORD PTR PTR [rbx+0x10], esi, onord production (rbx+0x10]) est. 0x4 x pyobject Free. cold.384+0xa77 5043e x pyobject free. cold.384+0xa77 10,0NORD pTR [rbx+0x20] 10309 Convolter Free.cold.384+0x227 est, (rax+0x1) mov more Jun pyobject noxtexte loid .384+0x227 NOV 103 123 e51,0x1 most cno 10,010 50309 2222 Free Cold - 384+0x16d> See.cold.384+0x16d7 ASIDE: PIR Interest 505 12.04080 PTR OIORD 09 test ·384+0x867 30 85 STQ Anoraba Indiana Indian 60 OHORD PTR LIDSHOSSE F10, OHORD FTR QUORD PTR 50504 QUORD PTR [rbx+0)28],000 853 30 111 23 50453 PTR Inthe Ar2 Firee. cold. 384+0

300

00

25

100

100 mos

500

mov

mos

ONORD PTR [rbx+0x201,r11

P12,011

#### rsi, Qiono PTA rst, anono pra tra 585 Prestox181,011 rox ouono pre [nox+ox18] more 00 POXATON mos

300

mon

8Ar

09

30

35

05

00

Yon 4.0 International (CC BY 4.0) 20

84

80

86

ARC

89

05

1110.00000

PTR [r10+0x10],r51

0

2 De

40

192

4105

6428:

pop

rat

### 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



### Part 9: Ethics (1)

#### Purpose

Understand ethical and legal issues in secure software

- 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