CS 4910
Intro to Computer Security

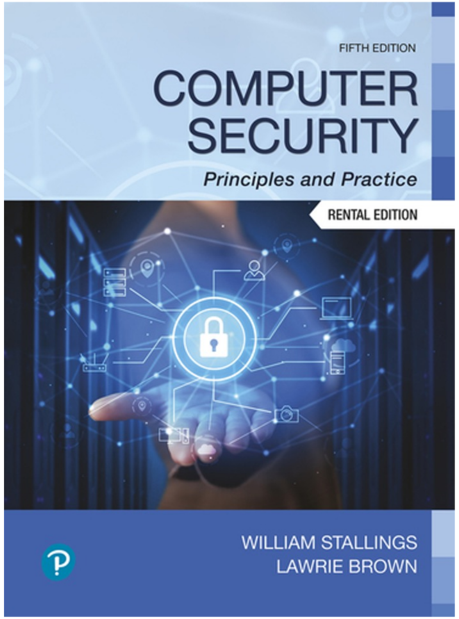
Instructor: Xi Tan

Today’s Agenda

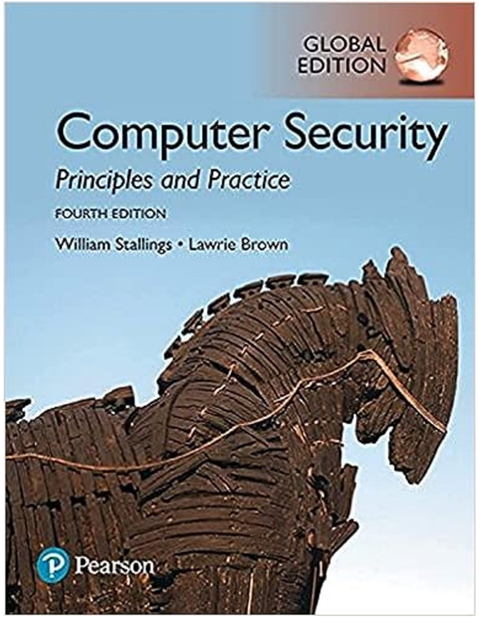
- Class Logistics
- Introduction to This Course
- Computer Security Attacks

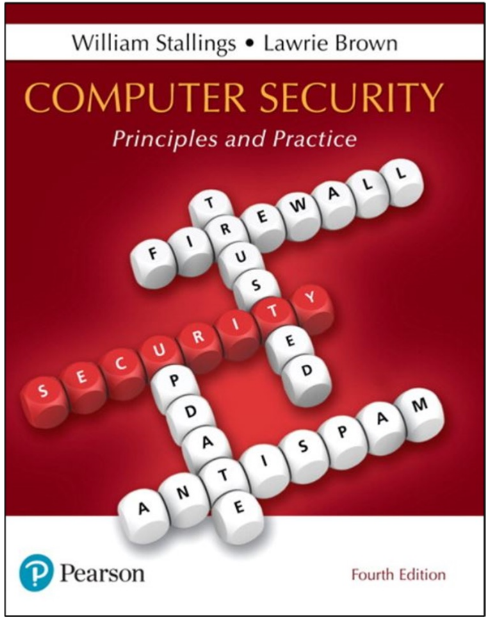
Textbooks

William Stallings and Lawrie Brown, Computer Security: Principles and Practice, **4th edition, Pearson, 2017**.



5th Edition, 2024





4th Edition, 2017

Additional Resources

- Michael T. Goodrich and Roberto Tamassia, **Introduction to Computer Security**, Addison-Wesley, 2011
- Charles Pfleeger and Shari Pfleeger, **Security in Computing**.
- Charlie Kaufman, Radia Perlman, and Mike Speciner, **Network Security: Private Communication in a Public World**.
- Edward Skoudis and Tom Liston, Counter Hack Reloaded: **A Step-by-Step Guide to Computer Attacks and Effective Defenses**.
- Ross Anderson, **Security Engineering: A Guide to Building Dependable Distributed Systems**.

Course Learning Objectives

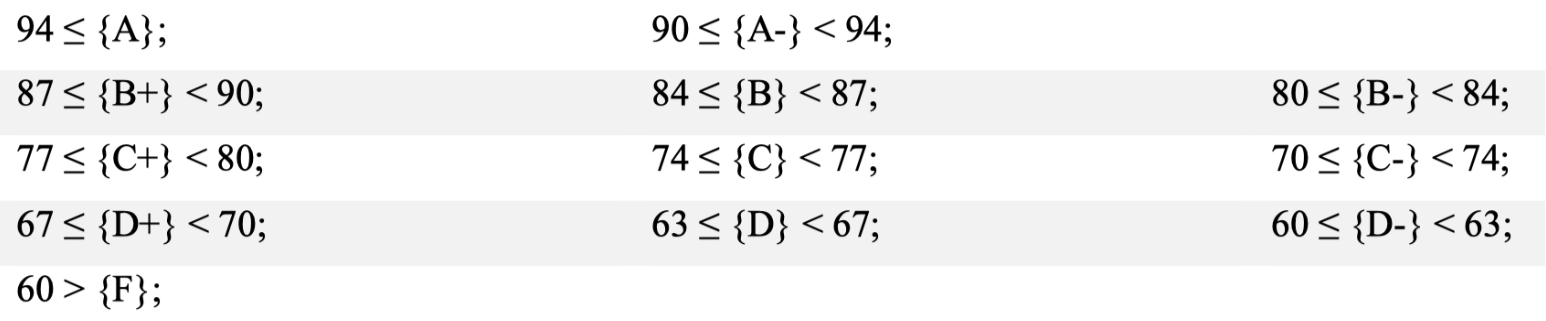
1. Understand fundamental principles of the security field
2. Build knowledge of tools and mechanisms to safeguard a wide range of software and computing systems
3. A tentative list of the covered topics:
   - Cryptographic background and tools
   - Access control
   - Authentication
   - Software and system security
   - Network security
   - Database security
   - Microarchitectural attacks
   - Legal and ethical aspects
   - …

First Month: See syllabus on Canvas for full schedule

Date	Topic	Notes
01/22	Overview I	Chapter 1
01/27	Overview II	
01/29	Crypto tools I (chap 2, 20)	Assignment 1 Release
02/03	Crypto tools II (chap 2, 21)	
02/05	Crypto tools III (chap 2.4, 2.5)	
02/10	Authentication (chap 3)	
02/12	Access control I (chap 4)	Assignment 1 Due
02/17	Access control II (chap 4)	Assignment 2 Release
02/19	Database security (chap 5)	
02/24	Malicious software (chap 6)	Lab 1 Due (Secret-Key Encryption)

Grading Scheme

Letter grades are received by earning points



$94 \leq \{A\}$;	$90 \leq \{A\text{-}\} < 94$;	
$87 \leq \{B+\} < 90$;	$84 \leq \{B\} < 87$;	$80 \leq \{B\text{-}\} < 84$;
$77 \leq \{C+\} < 80$;	$74 \leq \{C\} < 77$;	$70 \leq \{C\text{-}\} < 74$;
$67 \leq \{D+\} < 70$;	$63 \leq \{D\} < 67$;	$60 \leq \{D\text{-}\} < 63$;
$60 > \{F\}$;		

Grading

- Assignment (4): 20%
- Hands-on Labs (3): 30%
- Research Paper (1): 10%
- Midterm Exam (1): 20%
- Final Exam non-cumulative (1): 20%
- Pop Quizzes: bonus points

- Homework/Projects should be done individually. The exam will contain several questions from the projects.
- Homeworks will be submitted via Canvas; they must be typed (diagrams can be hand-drawn) and normally would need to be submitted as a PDF.
    - 0 points for homework if plagiarising is found. No exceptions.

Hands-on Labs (Individual)

SEED Lab: https://seedsecuritylabs.org/Labs_20.04/

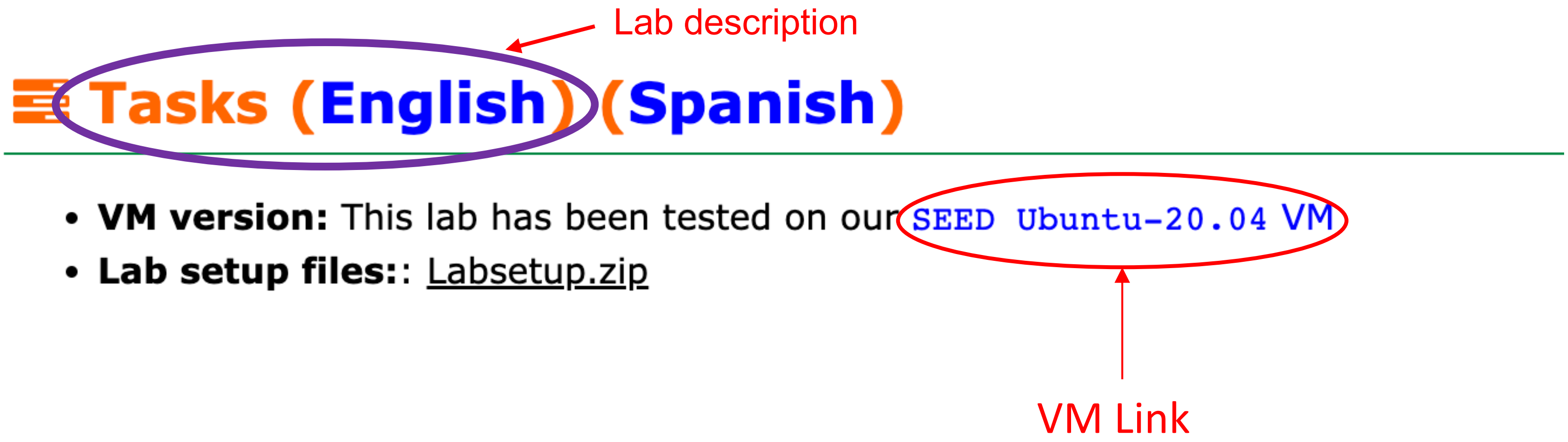
To setup the environment, please follow the instructions:

https://seedsecuritylabs.org/labsetup.html

Labs include:

- Cryptography: Secret-Key Encryption
- Network security: Packet Sniffing and Spoofing Lab
- System security: Buffer-Overflow Attack Lab (Set-UID Version)

Hands-on Labs



Tasks (English) (Spanish)

- **VM version:** This lab has been tested on our SEED Ubuntu-20.04 VM
- **Lab setup files:**: Labsetup.zip

Lab description

VM Link

Research Paper (Individual)

- Topic should be:
  - Interesting to you
  - Relatively specific
    - E.g., encryption of vehicle communications, not just encryption
  - State-of-the-art
- IEEE double column format, 4 pages of actual text
- Contains:
  - Survey/summarization of 8 or more scholarly references
  - Anyone currently applying such research?
  - How would you build on this research if you had to?
  - I will have you submit your topic and the 8 or more references first

Late Policy

All assignments are due on the day and time posted.

- You can submit an assignment up to 7 days late with a fixed **daily penalty** of 10% out of total points. Latest submission (7 days late) will receive at most 30% of max points even if it’s all correct; 0 points if more than 7 days late.
- **The workload is heavy, you should start the assignments early!** Excuses that you did not have enough time for an assignment will not be considered. Extraordinary circumstances will be considered at the discretion of the instructor (not the TAs!), contact the instructor via E-mails if you think these apply to you.

Regrading requests

- Homework or exam regrade requests need to be submitted within two weeks of releasing the graded material to the class
- The request needs to be in writing clearly describing the error in grading

Lectures

- Will mostly follow the textbook + additional resources
  - Read the lecture notes
  - Read relevant chapters if needed

How to do well?

- Preview the textbook, attend lectures and review notes
- Start early on assignments
- Do homework, labs and projects yourself
- Ask TAs (and us) questions during office hours

ADA, Military, Etc.

If you have any accommodations or special requests please make them known to me during office hours

Instructor and Teaching Assistant

Dr. Xi Tan

Assistant Professor

Secure and Reliable System Research Lab (SRUNRISE)

Email: xtan4@uccs.edu

Homepage: http://mintancy.github.io

Course page: https://mintancy.github.io/teaching/uccs/cs4910/spring2025.html

Office hours: M/W 3:00 PM - 4:30 PM or by appointment

Loc: Cybersecurity Building (3650 N Nevada Ave) A-120J or online

Teaching assistant: Aryan Padiyal

TA office hours: By appointment

I will try to post an announcement if I have to cancel office hours.

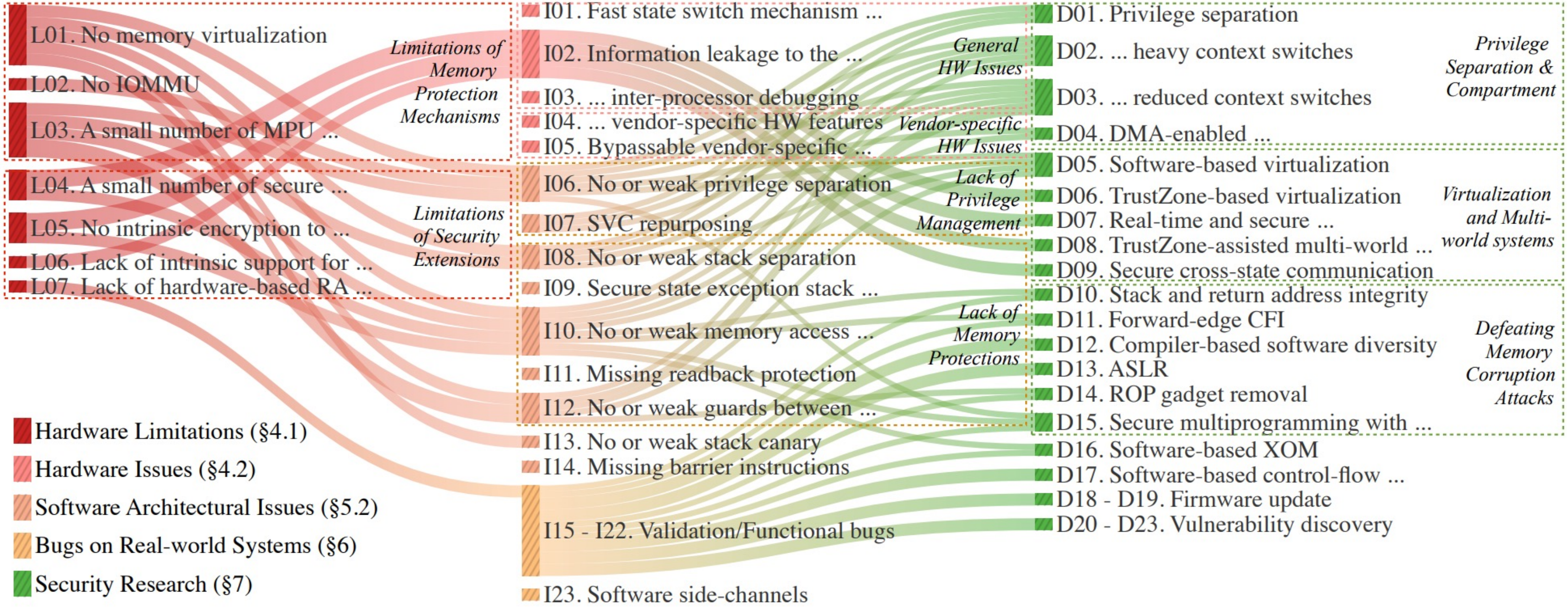
About Secure and Reliable System Research Lab

Director: Dr. Xi Tan

Research areas:

- (Embedded) System Security (Arm Cortex-M, Cortex-A, RISC-V, FPGA, etc.)
- Software Security
- Program Analysis and Compiler
- Vulnerability Discovery
- Network security
- IoT hacking/CTF platforms
- CTF competitions
- …

Research: embedded system security

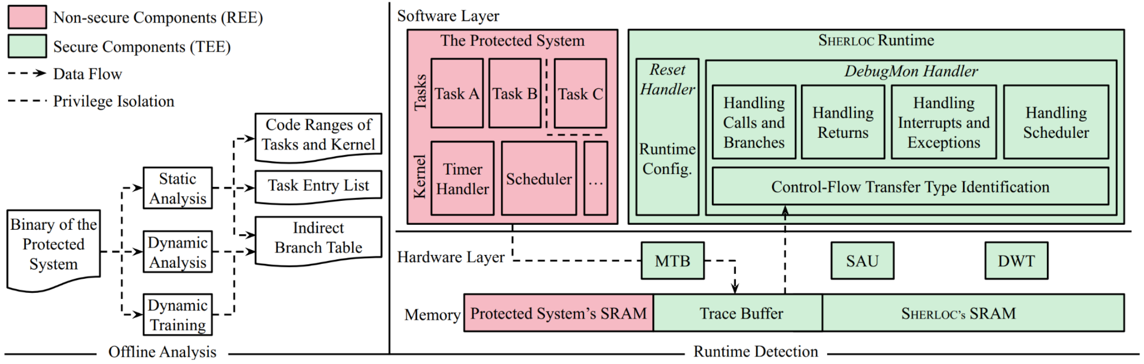

L01. No memory virtualization
L02. No IOMMU
L03. A small number of MPU ...
Limitations of Memory Protection Mechanisms
L04. A small number of secure ...
L05. No intrinsic encryption to ...
L06. Lack of intrinsic support for ...
L07. Lack of hardware-based RA ...
Limitations of Security Extensions
I01. Fast state switch mechanism ...
I02. Information leakage to the ...
I03. ... inter-processor debugging
General HW Issues
I04. ... vendor-specific HW features
I05. Bypassable vendor-specific ...
Vendor-specific HW Issues
I06. No or weak privilege separation
I07. SVC repurposing
Lack of Privilege Management
I08. No or weak stack separation
I09. Secure state exception stack ...
I10. No or weak memory access ...
I11. Missing readback protection
I12. No or weak guards between ...
Lack of Memory Protections
I13. No or weak stack canary
I14. Missing barrier instructions
I15 - I22. Validation/Functional bugs
I23. Software side-channels
D01. Privilege separation
D02. ... heavy context switches
D03. ... reduced context switches
D04. DMA-enabled ...
Privilege Separation & Compartment
D05. Software-based virtualization
D06. TrustZone-based virtualization
D07. Real-time and secure ...
D08. TrustZone-assisted multi-world ...
D09. Secure cross-state communication
Virtualization and Multi-world systems
D10. Stack and return address integrity
D11. Forward-edge CFI
D12. Compiler-based software diversity
D13. ASLR
D14. ROP gadget removal
D15. Secure multiprogramming with ...
Defeating Memory Corruption Attacks
D16. Software-based XOM
D17. Software-based control-flow ...
D18 - D19. Firmware update
D20 - D23. Vulnerability discovery
Hardware Limitations (§4.1)
Hardware Issues (§4.2)
Software Architectural Issues (§5.2)
Bugs on Real-world Systems (§6)
Security Research (§7)

Existing Hardware/Software Issues/Limitations and Defenses on Embedded Systems

Tan, X., Ma, Z., Pinto, S., Guan, L., Zhang, N., Xu, J., Lin, Z., Hu, H. and Zhao, Z., 2024. {SoK}:{Where's} the {"up"?}! A Comprehensive (bottom-up) Study on the Security of Arm {Cortex-M} Systems. In 18th USENIX WOOT Conference on Offensive Technologies (WOOT 24)

Research: control-flow integrity

Control-flow violation detection [1]:

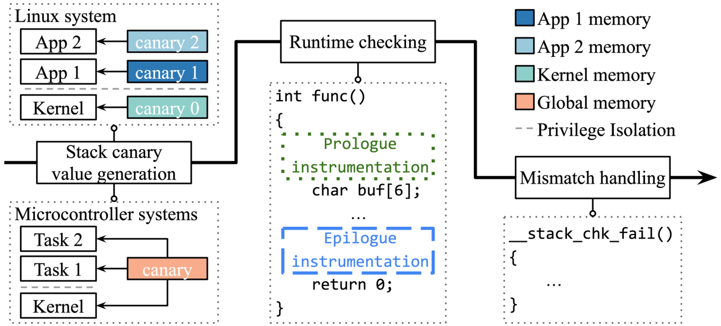


🟥 Non-secure Components (REE)
🟩 Secure Components (TEE)
Data Flow
Privilege Isolation

Binary of the Protected System
Static Analysis
Dynamic Analysis
Dynamic Training
Code Ranges of Tasks and Kernel
Task Entry List
Indirect Branch Table
Offline Analysis

Software Layer
The Protected System
Tasks
Task A
Task B
Task C
Kernel
Timer Handler
Scheduler
...
SHERLOC Runtime
Reset Handler
Runtime Config.
DebugMon Handler
Handling Calls and Branches
Handling Returns
Handling Interrupts and Exceptions
Handling Scheduler
Control-Flow Transfer Type Identification
Hardware Layer
MTB
SAU
DWT
Memory
Protected System's SRAM
Trace Buffer
SHERLOC's SRAM
Runtime Detection

Stack canaries [2]:



Linux system
App 2 ← canary 2
App 1 ← canary 1
Kernel ← canary 0
Stack canary value generation
Microcontroller systems
Task 2
Task 1
Kernel
canary
Runtime checking

```
int func()
{
   Prologue
 instrumentation
    char buf[6];
        ...
   Epilogue
 instrumentation
    return 0;
}
```

Mismatch handling

```
__stack_chk_fail()
{
    ...
}
```

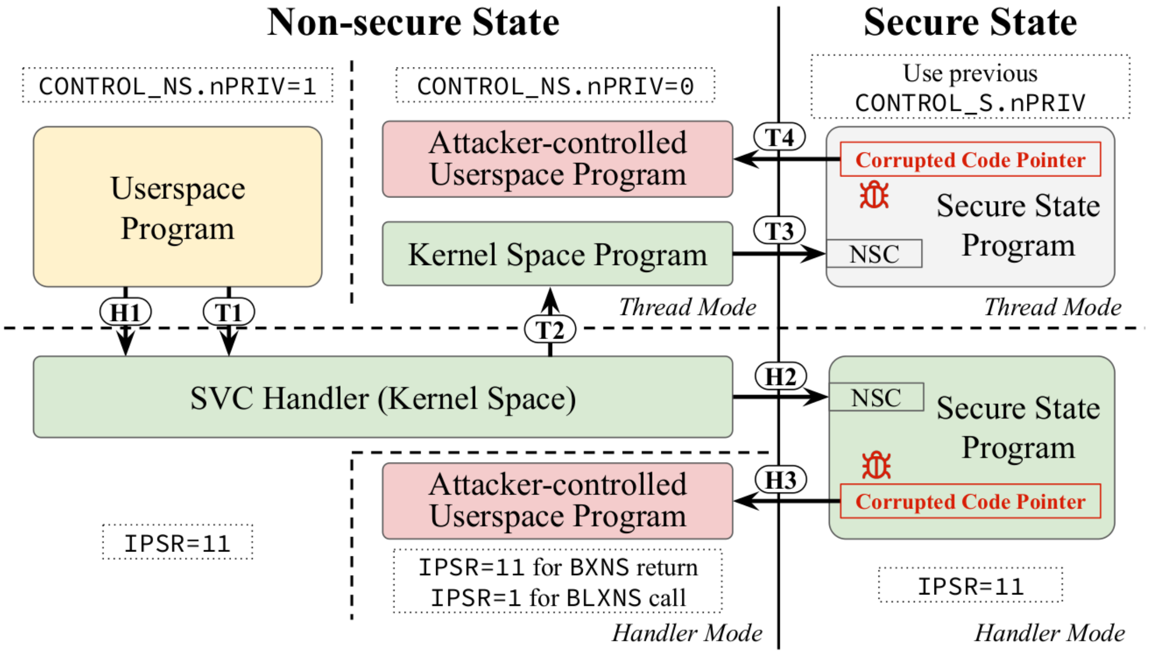
🟦 App 1 memory
🟦 App 2 memory
🟩 Kernel memory
🟧 Global memory
Privilege Isolation

[1] Tan, X. and Zhao, Z., 2023, November. Sherloc: Secure and holistic control-flow violation detection on embedded systems. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (pp. 1332-1346).

[2] Tan, X., Mohan, S., Armanuzzaman, M., Ma, Z., Liu, G., Eastman, A., Hu, H. and Zhao, Z., 2024, April. Is the Canary Dead? On the Effectiveness of Stack Canaries on Microcontroller Systems. In Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing (pp. 1350-1357).

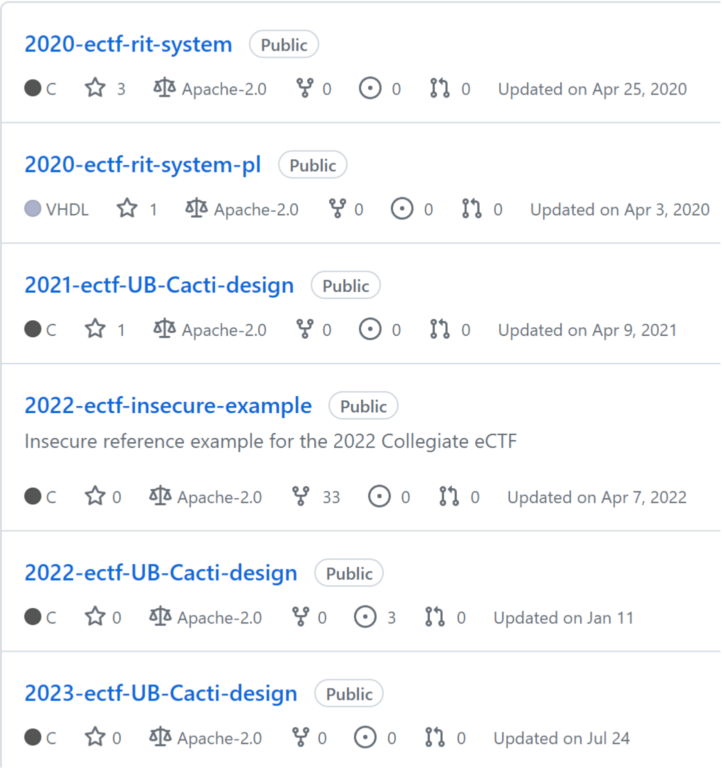
Research: vulnerability discovery

Return-to-Non-Secure vulnerabilities [1]:



[1] Ma, Z., Tan, X., Ziarek, L., Zhang, N., Hu, H. and Zhao, Z., 2023, July. Return-to-Non-Secure Vulnerabilities on ARM Cortex-M TrustZone: Attack and Defense. In 2023 60th ACM/IEEE Design Automation Conference (DAC) (pp. 1-6). IEEE.

eCTF participations



2020-ectf-rit-system Public
● C ☆ 3 Apache-2.0 0 0 0 Updated on Apr 25, 2020

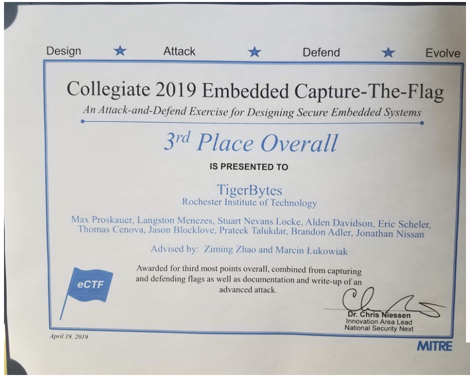
2020-ectf-rit-system-pl Public
● VHDL ☆ 1 Apache-2.0 0 0 0 Updated on Apr 3, 2020

2021-ectf-UB-Cacti-design Public
● C ☆ 1 Apache-2.0 0 0 0 Updated on Apr 9, 2021

2022-ectf-insecure-example Public
Insecure reference example for the 2022 Collegiate eCTF
● C ☆ 0 Apache-2.0 33 0 0 Updated on Apr 7, 2022

2022-ectf-UB-Cacti-design Public
● C ☆ 0 Apache-2.0 0 3 0 Updated on Jan 11

2023-ectf-UB-Cacti-design Public
● C ☆ 0 Apache-2.0 0 0 0 Updated on Jul 24



Design ★ Attack ★ Defend ★ Evolve

Collegiate 2019 Embedded Capture-The-Flag

An Attack-and-Defend Exercise for Designing Secure Embedded Systems

3rd Place Overall

IS PRESENTED TO

TigerBytes
Rochester Institute of Technology

Max Proskauer, Langston Menezes, Stuart Nevans Locke, Alden Davidson, Eric Scheler, Thomas Cenova, Jason Blocklove, Prateek Talukdar, Brandon Adler, Jonathan Nissan

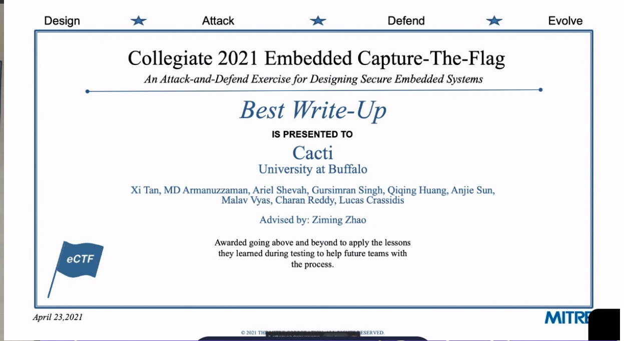
Advised by: Ziming Zhao and Marcin Łukowiak

Awarded for third most points overall, combined from capturing and defending flags as well as documentation and write-up of an advanced attack.

Dr. Chris Niessen
Innovation Area Lead
National Security Next

April 19, 2019

MITRE



Design ★ Attack ★ Defend ★ Evolve

Collegiate 2021 Embedded Capture-The-Flag

An Attack-and-Defend Exercise for Designing Secure Embedded Systems

Best Write-Up

IS PRESENTED TO

Cacti
University at Buffalo

Xi Tan, MD Armanuzzaman, Ariel Shevah, Gursimran Singh, Qiqing Huang, Anjie Sun, Malav Vyas, Charan Reddy, Lucas Crassidis

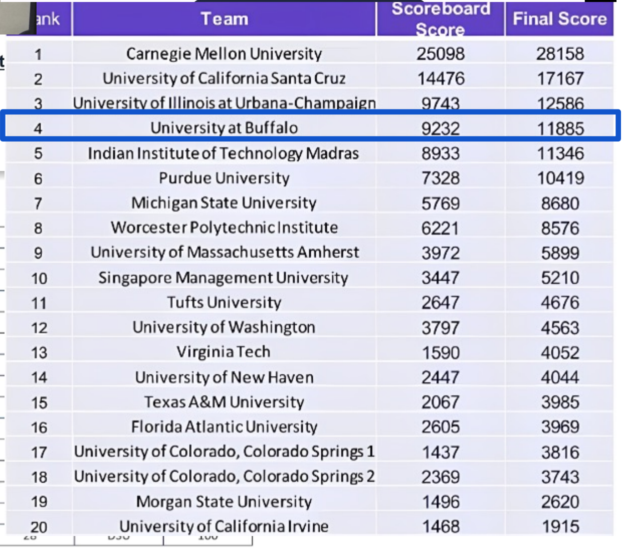
Advised by: Ziming Zhao

Awarded going above and beyond to apply the lessons they learned during testing to help future teams with the process.

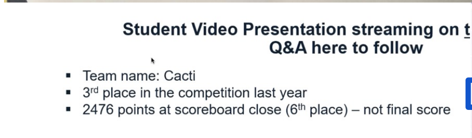
April 23,2021

MITRE

© 2021 TH[illegible]ESERVED.

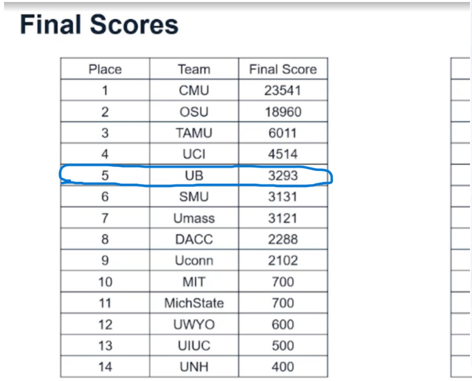


ank	Team	Scoreboard Score	Final Score
1	Carnegie Mellon University	25098	28158
2	University of California Santa Cruz	14476	17167
3	University of Illinois at Urbana-Champaign	9743	12586
4	University at Buffalo	9232	11885
5	Indian Institute of Technology Madras	8933	11346
6	Purdue University	7328	10419
7	Michigan State University	5769	8680
8	Worcester Polytechnic Institute	6221	8576
9	University of Massachusetts Amherst	3972	5899
10	Singapore Management University	3447	5210
11	Tufts University	2647	4676
12	University of Washington	3797	4563
13	Virginia Tech	1590	4052
14	University of New Haven	2447	4044
15	Texas A&M University	2067	3985
16	Florida Atlantic University	2605	3969
17	University of Colorado, Colorado Springs 1	1437	3816
18	University of Colorado, Colorado Springs 2	2369	3743
19	Morgan State University	1496	2620
20	University of California Irvine	1468	1915



Student Video Presentation streaming on t
Q&A here to follow

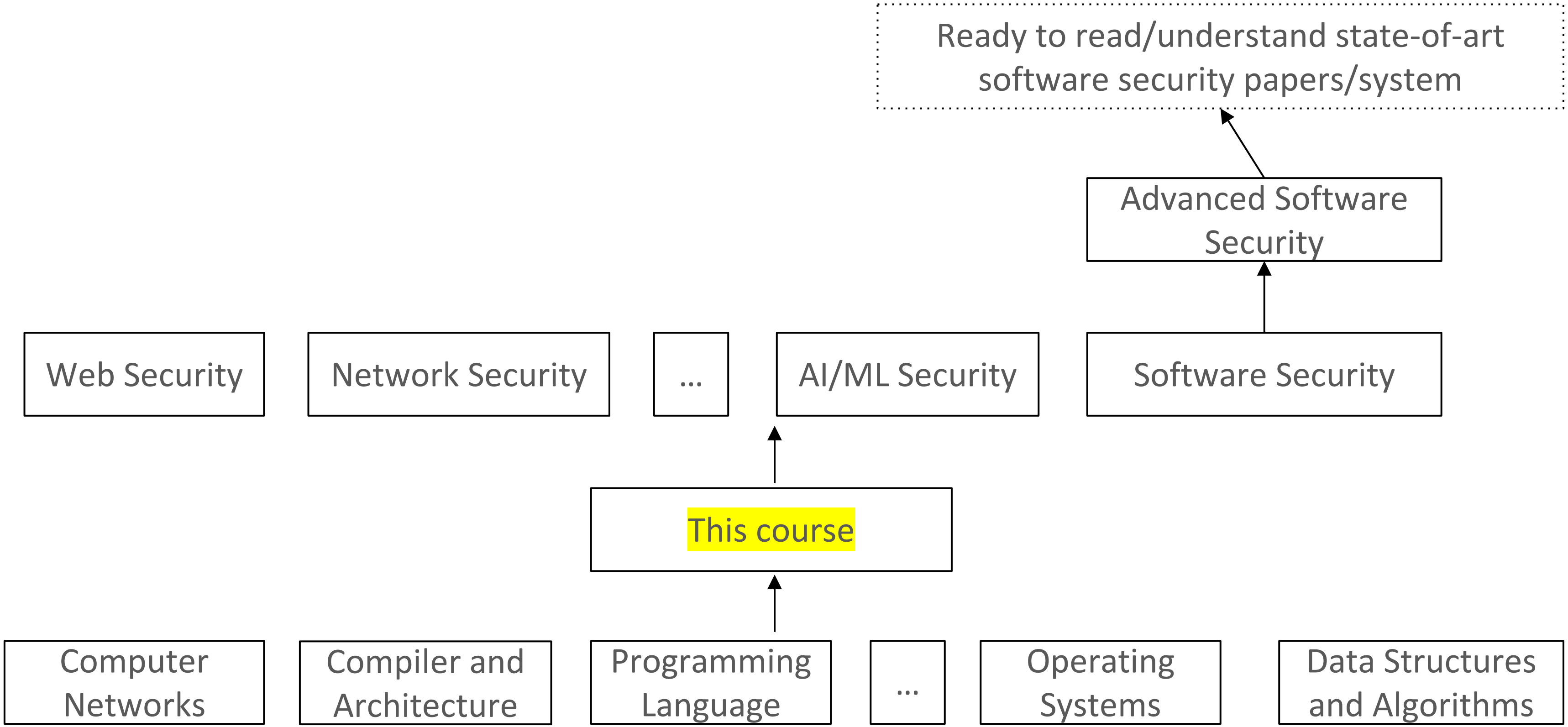
- Team name: Cacti
- 3rd place in the competition last year
- 2476 points at scoreboard close (6th place) – not final score



Final Scores

Place	Team	Final Score
1	CMU	23541
2	OSU	18960
3	TAMU	6011
4	UCI	4514
5	UB	3293
6	SMU	3131
7	Umass	3121
8	DACC	2288
9	Uconn	2102
10	MIT	700
11	MichState	700
12	UWYO	600
13	UIUC	500
14	UNH	400

If you want to be a security researcher …



Ready to read/understand state-of-art software security papers/system

Advanced Software Security

Web Security

Network Security

…

AI/ML Security

Software Security

This course

Computer Networks

Compiler and Architecture

Programming Language

…

Operating Systems

Data Structures and Algorithms

Why is Computer Security as a field?

Computer security is very broad as a field

It covers many areas:

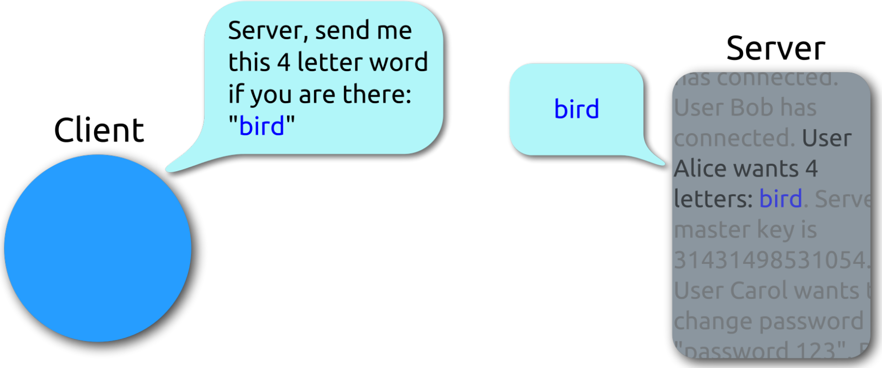
- Network security
- Software security
- System security
- Web security
- Safety in programming language
- Database security
- Usable security
- Access control
- Privacy
- Cybercrime
- …

Protocol Flaws: Heartbleed (2014)

https://github.com/adamalston/Heartbleed

Protocol Flaws: Heartbleed (2014)

Heartbeat – Normal usage

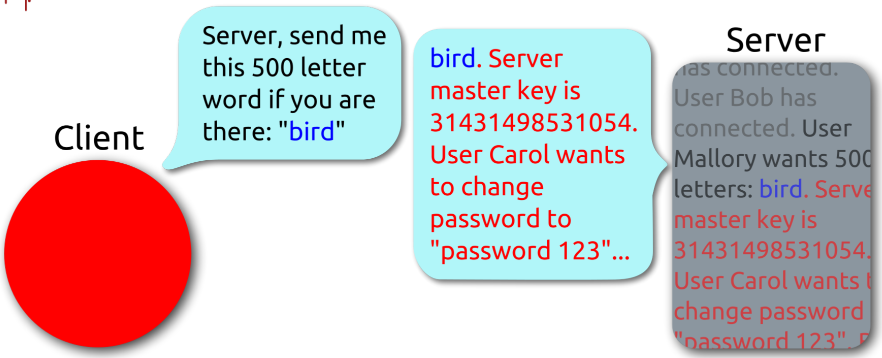


Server, send me this 4 letter word if you are there: "bird"

bird

as connected. User Bob has connected. User Alice wants 4 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P

Heartbeat – Malicious usage



Server, send me this 500 letter word if you are there: "bird"

bird. Server master key is 31431498531054. User Carol wants to change password to "password 123"...

as connected. User Bob has connected. User Mallory wants 500 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P

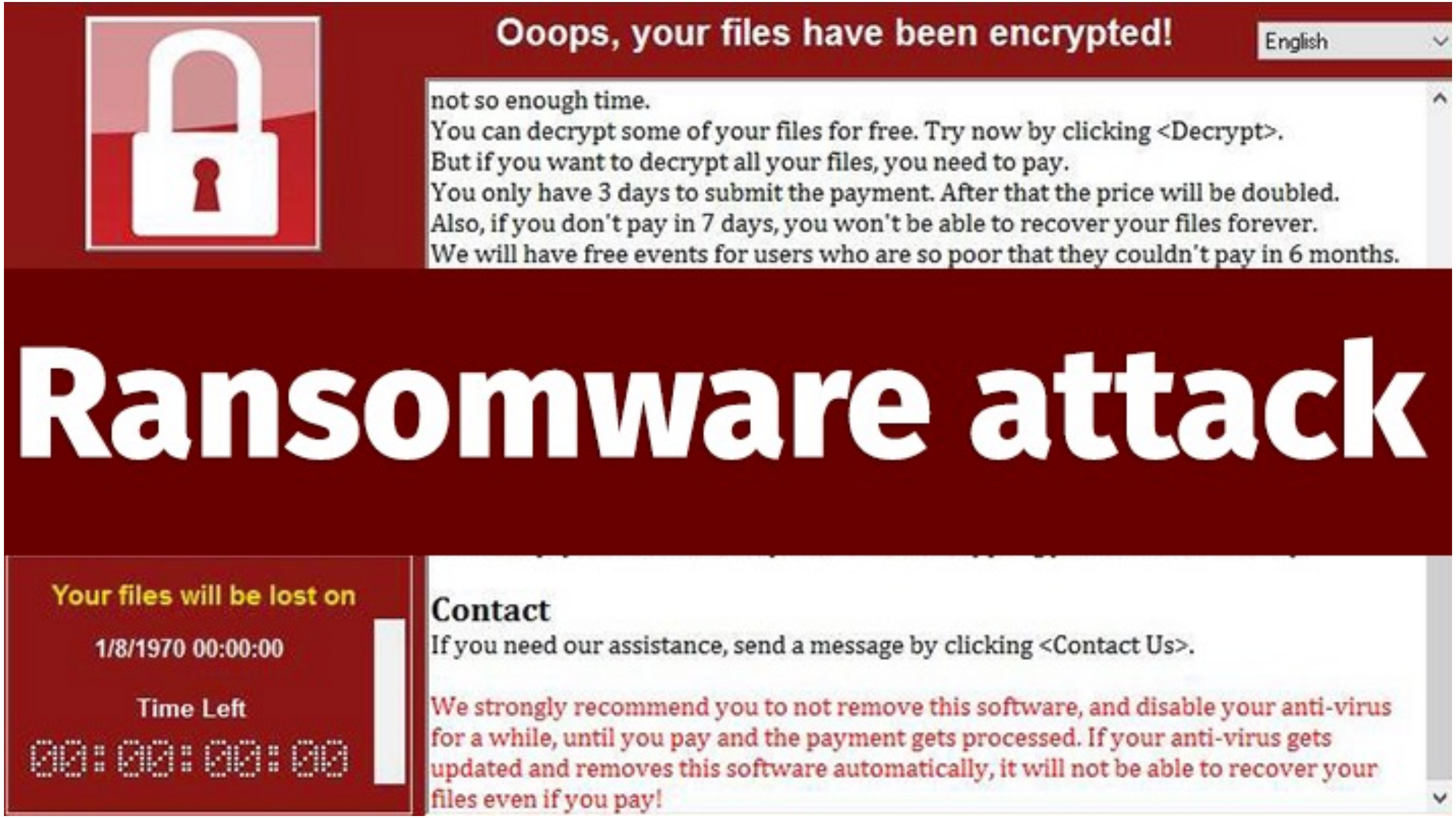
CPU Flows (Intel, AMD, and ARM) (2017)

https://meltdownattack.com/

CPU Flows (Intel, AMD, and ARM) (2017)

- Meltdown:
  - Affected CPU Types: Intel, Apple
  - Attack Vector: execution code on the system
  - Method: Intel privilege escalation & speculative execution
  - Exploit Path: read kernel memory from user space
  - Remediation: software patches
- Spectre
  - Affected CPU Types: Intel, ARM, Apple, AMD
  - Attack vector: execute code on the system
  - Method: branch prediction & speculative execution
  - Exploit path: read memory contents from other applications
  - Remediation: software patches

WannaCry Ransomware (2017)



Ooops, your files have been encrypted!

not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

Your files will be lost on

1/8/1970 00:00:00

Time Left

00:00:00:00

Contact

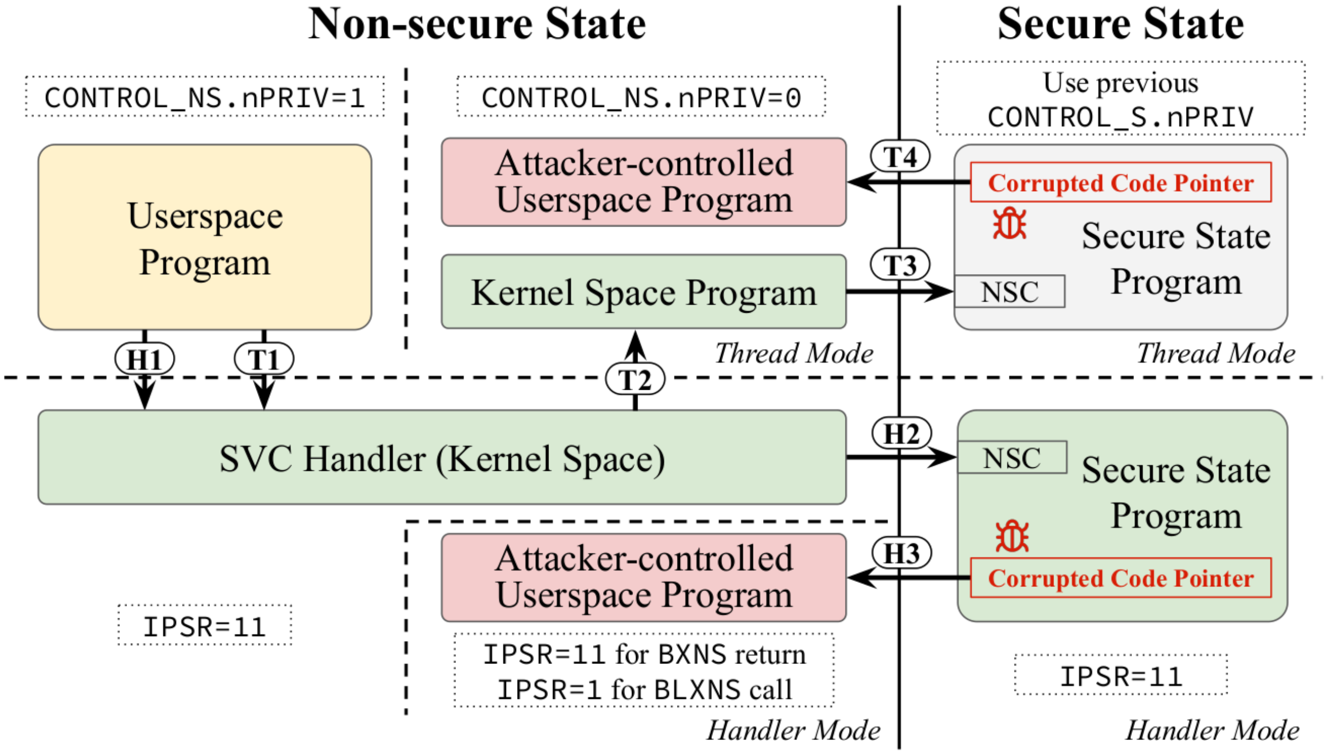
If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

Colonial Pipeline Ransomware (2021)

Protocol Flaws: Stealing Cars (2023)

Return-to-Non-Secure Attack (2023)



https://github.com/CactiLab/ret2ns-Cortex-M-TrustZone

Attacks on Large Language Models (2024)

- **LLMjacking: link**
  Attackers exploited stolen cloud credentials to abuse LLMs, such as Anthropic's Claude, causing financial losses (e.g., $46,000/day).
- **Prompt Injection: link**
  Techniques like BEAST bypassed LLM safety, creating harmful outputs in under a minute with minimal resources.
- **Data Extraction: link**
  The "Imprompter" attack covertly extracted sensitive data from LLMs, with up to an 80% success rate.
- **Backdoor and Supply Chain Attacks: link**
  Hackers implanted backdoors during LLM training, triggering malicious behavior with specific inputs, posing supply chain risks.
- …

Next Class

- Chapter 1