Lec 1: Introduction

CS492E: Introduction to Software Security



Who am I?





• Researcher and Software Engineer.





- Researcher and Software Engineer.
- · Leader of SoftSec. Lab.





- Researcher and Software Engineer.
- · Leader of SoftSec. Lab.
- Director of CSRC (Cyber Security Research Center)





- · Researcher and Software Engineer.
- · Leader of SoftSec. Lab.
- Director of CSRC (Cyber Security Research Center)
- Research Keywords:
 - Binary Analysis
 - Vulnerability Discovery
 - Exploit Verification
 - Malware Analysis



Contact

- Office: N5, #2319
- Office hour: by appointment.
 - A Homepage: https://softsec.kaist.ac.kr/~sangkilc/
 - 🖂 Email: sangkilc@kaist.ac.kr



My Research



My research is all about building *large* and *complex* systems that automatically analyze programs to resolve security problems.



My Research: Automatic Exploit Generation

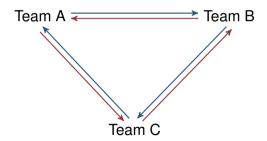
Fully automated hacking and defense (e.g., DARPA's Cyber Grand Challenge)





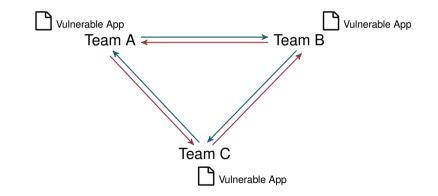


Normal CTFs



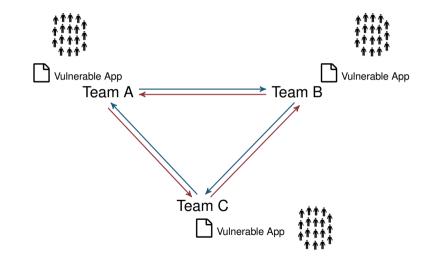


Normal CTFs



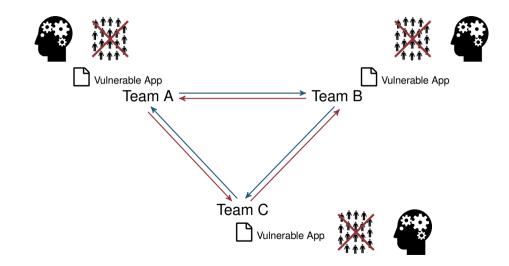


Normal CTFs





CGC





Winner = Mayhem



ForAllSecure (Carnegie Mellon University)

Question?

Image from https://forallsecure.com/wp-content/uploads/2016/08/mayhem-crs.jpg

000



Winner = Mayhem



ForAllSecure (Carnegie Mellon University)

2012 IEEE Symposium on Security and Privacy

Unleashing MAYHEM on Binary Code

Sang Kil Cha, Thanassis Avgerinos, Alexandre Rebert and David Brumley Carnegie Mellon University Pittsburgh, PA {sangkilc, thanassis, alexandre.rebert, dbrumley}@cmu.edu

Image from https://forallsecure.com/wp-content/uploads/2016/08/mayhem-crs.jpg



• Officially called "KISA Data Challenge".



- Officially called "KISA Data Challenge".
- · Started in 2018.



- Officially called "KISA Data Challenge".
- Started in 2018.
- SoftSec. Lab. won the challenge twice in a row (2018 and 2019).



- Officially called "KISA Data Challenge".
- Started in 2018.
- SoftSec. Lab. won the challenge twice in a row (2018 and 2019).
- · Built our own system from scratch!



My Research: Windows Error Reporting

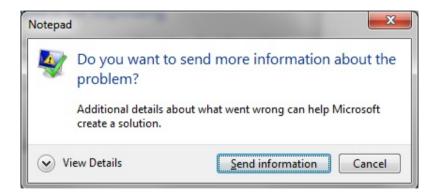


Image from https://goo.gl/PLekyZ



My Research: macOS Kernel Vulnerabilities



About the security content of macOS High Sierra 10.13.2, Security Update 2017-002 Sierra, and Security Update 2017-005 El Capitan

This document describes the security content of macOS High Sierra 10.13.2, Security Update 2017-002 Sierra, and Security Update 2017-005 El Capitan.



My Research: Windows Kernel Vulnerabilities

• Published in 2021 IEEE Security & Privacy.

• Earned 25,000 USD bounty for finding zero days.



My Research: Browser Vulnerabilities

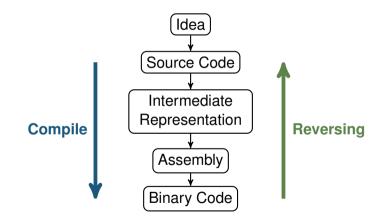


A vulnerability was found in Apple IOS up to 12.1 -. It has been classified as critical. This affects code of the component WebVit. The manipulation with an unknown input leads to a memory corruption vulnerability. CWE is classifying the issue as CWE-119 -. This is going to have an impact on confidentiality, integrity, and availability.

The weakness was released 12/05/2018 by HyungSeok Han, DongHyeon Oh and Sang Kil Cha with KAIST Softsec Lab as *HT209340* as confirmed advisory (Website). The advisory is shared at support.apple.com ... This vulnerability is uniquely identified as CVE-2018-4437 ... It is possible to initiate the attack remotely. No form of authentication is needed for exploitation. Neither technical details nor an exploit are publicly available. The price for an exploit might be around USD \$256.\$100k at the moment (estimation calculated on 12/05/2018). It expected to see the exploit prices for this product increasing in the near future. The advisory points out:



My Research: Binary Analysis





My Research: B2R2

- The fastest binary analysis frontend.
- The basis of our system for K-CGC.





This Course



Question

Why do you want to learn *software* security?





Why do you want to learn *software* security?

A: because software is everywhere.



Software is Pervasive

Nearly everything (services, communication, products, entertainment, etc.) is dependent on *software*.



Software vs. Hardware

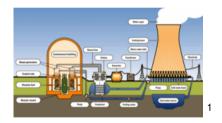
The boundary is becoming largely blurred.

¹Image from https://www.foronuclear.org/en/updates/in-depth/what-are-the-different-components-of-a-nuclear-power-plant/



Software vs. Hardware

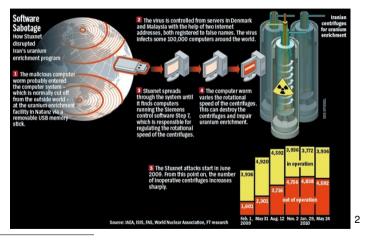
The boundary is becoming largely blurred.



¹Image from https://www.foronuclear.org/en/updates/in-depth/what-are-the-different-components-of-a-nuclear-power-plant/



Example: Stuxnet



²Image from https://cyberhoot.com/cybrary/stuxnet/



Cybersecurity?

"Cyber" attacks no longer remain in the cyber world!



Al is Software

Al is a program that takes in an input and returns an output.



Al is Software

Al is a program that takes in an input and returns an output.

Al is also not free from security threats.



Software Security is the Key

Software is everywhere and most security problems stem from software issues.



Software Security is the Key

Software is everywhere and most security problems stem from software issues.

So you need to learn software security!



Key Takeaway

Not every programmer needs to become a security expert, but every programmer should know software security principles.



Common Misconception about Security

Many people think that security researchers are like a *hacker*. But what is a hacker?



Hackers?



3

³Image from

https://www.theguardian.com/technology/2017/jun/23/russian-hackers-stole-passwords-of-british-mps-and-public-servants



Hacking Simulation!?

https://hackertyper.net/



Magical Things?

Computer security (or hacking) is *not* a magic.



Principles Matter

This course is not about teaching hacking skills. All you need to do is to learn the basic principles.



Course Overview

- Approach: learn fundamental security principles with an emphasis on software.
- Target Audience:
 - One who has basic understanding of programming.
 - Students who have taken CS230, or have equivalent knowledge/skills.
- Topics:
 - Why software is insecure?
 - How attackers can exploit insecure programs?
 - How does malware work? and how to combat it?
 - How should we protect software systems?
 - And etc.



Introductory Course

This is an introductory course, if you want get more advanced knowledge, you should take *IS-561*: Binary Code Analysis and Secure Software Systems.



The Most Important Thing: Academic Integrity

Any solution you submit (quiz, exam, etc.) must be your *own* work.

No cheating, no plagiarism.

If you violate this rule, you will immediately get an F, and possibly get expelled from the university.



Students enrolled at all courses provided by KAIST School of Computing are expected to respect personal honor and the rights of others, as well as to do their best to uphold personal integrity and honesty. The students will neither give nor receive any unauthorized aid in class work that is to be graded by the instructor. The following acts are regarded as violations of academic integrity and honesty.



- 1. Reusing, or referring to other students/publisher's solutions, assignments, program source code, and reports.
- 2. Using solution-sharing online services such as chegg.com for exams and assignments.
- 3. Sharing your own solution to code repositories such as GitHub, or referring to code from such repositories.
- 4. Allowing another student to refer from one's own work.
- 5. Submitting another student's work as his or her own.
- 6. Sitting for someone else's exam.
- 7. Unpermitted collaboration or aid on take-home examinations and class assignments.
- 8. Plagiarism: the use of another person's original work, regardless of lengths, without giving reasonable and appropriate credit to or acknowledging the author or source.



The professor will determine whether any violation has occurred and the appropriate penalty for the violation. All violations will be reported to head professor of student affairs as well as the head of School of Computing. Internally, those who reported will receive the following penalty.

- 1. Exclusion from any awards or scholarship consideration/recommendation for two following semesters.
- 2. (If the major is not CS) Exclusion from change of major to School of Computing for two folowing semesters.



Depending on the seriousness of violation, the student can also reported to the institution-wide disciplinary committee. To see the maximum possible penalty for academic misconduct, please refer to the attached penalty guideline below (taken from the English version KAIST Student Handbook 2021, page 79, available from https://www.kaist.ac.kr/html/kr/campus/campus_0508.html)



Academic Integrity is Crucial for Security

You will learn several security principles that can possibly be misused to harm or threat others. Therefore, academic integrity is especially more important for this course.



Questions in Korean

I love questions. You can ask questions in *Korean* during the class. I will try to interpret your question to English for other students.



Course Resources

- Basic Communication: KLMS.
 - Feel free to write in Hangul to ask questions, but we will answer in English.

Syllabus & Slides:

https://softsec.kaist.ac.kr/courses/2022s-cs492e/.



TA Office Hour?

- No physical meeting except midterm and final.
- We will always use KLMS (Q&A Board).
- We do *not* accept emails asking questions about homework: Use KLMS.
 - TAs have a right to ignore your personal email if it is about the coursework.
 - We do accept emails for *administrative* issues only, e.g., when you were not able attend the midterm exam due to a critical reason.



Course Logistics

- 20% Participation (assignments and in-class activities).
- 40% Midterm
- 40% Final



Good News

This course will be rarely offered by me. So you are very lucky! ③



Question?

