Lec 1: Introduction

CS220: Programming Principles

Sang Kil Cha
Who am I?
Sang Kil Cha

• Researcher, Engineer, and Hacker.
Sang Kil Cha

- Researcher, Engineer, and Hacker.
- Leader of SoftSec. Lab.
Sang Kil Cha

- Researcher, Engineer, and Hacker.
- Leader of SoftSec. Lab.
- Research Keywords:
  - Binary Analysis
  - Vulnerability Discovery
  - Exploit Verification
  - Malware Analysis
Contact

- Office: N5, #2319
- Office hour: by appointment.
  - 🏠 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

Team A  Team B

Team C
Normal CTFs

Team A → Team B
Team B → Team C
Team C → Team A

Vulnerable App

Team A
Team B
Team C
Normal CTFs
CGC

Team A → Team B → Team C

Vulnerable App

Who am I?

My Research Development Environment Conclusion Question?
Winner = Mayhem

ForAllSecure (Carnegie Mellon University)

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

K-CGC (Korean CGC)

- Officially called “KISA Data Challenge”.
K-CGC (Korean CGC)

- Officially called “KISA Data Challenge”.
- Started in 2018.
K-CGC (Korean CGC)

- Officially called “KISA Data Challenge”.
- Started in 2018.
- SoftSec. Lab. won the challenge twice in a row (2018 and 2019).
K-CGC (Korean CGC)

• 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](https://goo.gl/PLekyZ)
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.
A vulnerability was found in Apple iOS up to 12.1. It has been classified as critical. This affects code of the component WebKit. 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 $25k-$100k at the moment (estimation calculated on 12/06/2018). It expected to see the exploit prices for this product increasing in the near future. The advisory points out:
My Research: Binary Analysis

Idea

Source Code

Intermediate Representation

Assembly

Binary Code

Compile

Reversing
My Research: B2R2

• The fastest binary analysis frontend.
• The basis of our system for K-CGC.
My Research: Testing Binary IR

Let me thank you for the great work you did!

Carnegie Mellon University

UCSB

Thank you for doing this research!

Thanks for the hard work and the help in making better binary platforms.
Q: But how were all these possible?
Q: But how were all these possible?

A: Right language and right engineering principles.
You will learn fundamental *principles* for programming, and how to apply such concepts to build real-world programs using a state-of-the-art and practical language called *F#*. 
Q: Is F# used in practice?

A: Yes!
An Anecdote: MSRD

The engineering team, consisting of **three developers** at the time, was given the ambitious goal to build an entirely new service from scratch and ship it to external customers in just **three months**¹.

¹See: https://goo.gl/CJvmdq
Another Anecdote: KCGC

Mission: build a fully automated system for exploit generation for *three months* with 3 Master students and 3 Ph.D. students who take 2–3 courses during the semester.
### What Languages Are Associated with the Highest Salaries Worldwide?

<table>
<thead>
<tr>
<th>Language</th>
<th>Global</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>F#</td>
<td>$74,000</td>
<td></td>
</tr>
<tr>
<td>Ocaml</td>
<td>$73,000</td>
<td></td>
</tr>
<tr>
<td>Clojure</td>
<td>$72,000</td>
<td></td>
</tr>
<tr>
<td>Groovy</td>
<td>$72,000</td>
<td></td>
</tr>
<tr>
<td>Perl</td>
<td>$69,000</td>
<td></td>
</tr>
<tr>
<td>Rust</td>
<td>$69,000</td>
<td></td>
</tr>
<tr>
<td>Erlang</td>
<td>$67,000</td>
<td></td>
</tr>
</tbody>
</table>

¹Developer survey result in 2018 by stackoverflow.com.
What Languages Are Associated with the Highest Salaries Worldwide?

<table>
<thead>
<tr>
<th>Global</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clojure</td>
<td>$90k</td>
</tr>
<tr>
<td>F#</td>
<td>$80k</td>
</tr>
<tr>
<td>Go</td>
<td>$80k</td>
</tr>
<tr>
<td>Scala</td>
<td>$78k</td>
</tr>
<tr>
<td>Elixir</td>
<td>$76k</td>
</tr>
</tbody>
</table>

1Developer survey result in 2019 by stackoverflow.com.
Most Loved, Dreaded, and Wanted Other Frameworks, Libraries, and Tools

<table>
<thead>
<tr>
<th>Loved</th>
<th>Dreaded</th>
<th>Wanted</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NET Core 77.2%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Torch/PyTorch 77.1%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flutter 75.4%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pandas 74.7%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TensorFlow 73.0%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹Developer survey result in 2019 by stackoverflow.com.
Course Overview

• **Approach:** learn fundamental programming principles.
• **Target Audience:**
  - One who has basic understanding of programming.
  - Students who have *taken CS101*, or have equivalent knowledge/skills.
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.
Honor Code

To take this course, you **must** sign the Google form.
https://forms.gle/2sxMFD5FHBb3cShFA
Course Attendance

We will check your course attendance in the middle of each class.

• Check every class.
• Three days of freedom: you can safely be absent for up to three lectures without affecting your grade.
• We will *ignore* any request about course attendance. We are not asking you something crazy here: we are just asking you to attend at least 89% (= 25/28) of the lectures.
• If you miss four or more classes, you will get an ‘F’.

No excuse, no compromise.
I understand, but what if I have a personal occasion?

That is exactly why we give the three-day of freedom. Use your time *wisely*.

Q: What if I really have a serious problem, e.g., a significant health problem, etc.? Can this be an excuse?

A: Still no. The general rule here is to always be sincere about attending lectures, so that you can safely use your options when something serious happens. If you have really a serious problem, and cannot attend lectures for long, then you should really consider taking a break.
Our Agreement

During the course, if you did not attend 89% of the lectures, you get an ‘F’ no matter what reasons you may have. No excuse. No compromise.
Questions in Korean

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

- **Basic Communication**: Classum (https://classum.com/).
  - You can use Hangul in Classum, but we will answer in English.

- **Syllabus & Slides**: https://softsec.kaist.ac.kr/courses/2020s-cs220/.
TA Office Hour?

- No physical meeting except midterm and final.
- We will always use Classum, an online Q&A platform.
- We do not accept emails asking questions about homework: Use Classum.
  - 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 to attend the midterm exam due to a critical reason.
Text Book?

You are recommended to refer to the **Wizard book**:

“Structure and Interpretation of Computer Programs (2nd Edition)” by Harold Abelson and Gerald Jay Sussman.
Course Load

• Heavy hands-on in-class exercises.
• No homework.
• Three midterms and one final.
Course Logistics

- 30% Participation (attendance and in-class activities).
- 20% Midterm 1 and 3
- 20% Midterm 2
- 30% Final
I’ve taken CS320 (Programming Language). Can I still take this course?

We recommend you to take this course first, and then take CS320. However, this course has its own value, so it is totally up to you.
Development Environment
You are free to use any OS you want including *Linux*, *macOS*, and *Windows*, because we are going to use OS-independent tools and languages. Regardless of the OS, we assume that you are working on a terminal (a.k.a. console or shell) with a proper editor, such as Emacs, Vim, Visual Studio Code, etc.
Environmental Setup

1. Install latest .NET Core on your machine. You should be able to run the command ‘dotnet’ in your terminal.

2. Make sure you install .NET Core version 3.0 or higher. If you already have a lower version of .NET Core installed on your machine, you should remove it first, and then install a latest version.

3. Install Git on your machine. You should be able to run the command ‘git’ in your terminal.
## Check Your Installation

### On Windows (from `cmd.exe`)

C:\Users\sangkilc> dotnet --version
3.0.100

C:\Users\sangkilc> git --version
git version 2.21.0.windows.1
Check Your F# REPL

- Open a terminal (e.g., cmd.exe on Windows).
- Type `dotnet fsi` in the prompt.
Check Your F# REPL (cont’d)

$ dotnet fsi

Microsoft (R) F# Interactive version 10.6.0.0 for F# 4.7
Copyright (c) Microsoft Corporation. All Rights Reserved.

For help type #help;;

>
Conclusion
Notes

• From the next class, we will assume that you have successfully configured your development environment.
• Check our course web site, and read references.
• “The first and the last homework” is due by the next class.
  - Install .NET Core 3.0 or above on your machine.
  - Install Git on your machine.
  - Make sure you can successfully run `dotnet --version` and `git --version` in a terminal.
Question?