SWE3009: Computer Security

Lecture 0x00: Course Overview and Introduction

Hojoon Lee

Systems Security Lab

SUNGKYUNKWAN UNIVERSITY 1398 성균관대학교

Instructor: Hojoon Lee (이호준)

- Joined SKKU since Sept. 2019
- Research Areas
  - Software Security
    - Vulnerability analysis
    - Attacks and Defenses
  - Systems Security
    - Trusted Computing
    - Secure Computation for AI
- Leader of Systems Security Lab @ SKKU
  - `https://sslab.skku.edu`
  - Hiring MS/PhD students and undergraduate interns

Systems Security Lab

SUNGKYUNKWAN UNIVERSITY 1398 성균관대학교

시스템 보안 연구실

Systems Security Lab (SSLab)

@Sungkyunkwan University (SKKU)
https://sslab.skku.edu

Welcome to SSLab

시스템 보안 연구실 (SSLab)은 열정 있고, 뭔가를 망가뜨리고 고치는걸 좋아하는 해커기질을 가진 학생들을 찾고 있습니다. 다음과 같은 관심사를 가지고 있다면 더욱 더 환영합니다.

- 로우레벨 (어셈블리 등)
- 운영체제 및 아키텍처
- 공격기술에 대한 흥미

신입생 교육과정 (SSLab 훈련소)

신입생 (학부과정) 들은 체계화된 교육과정을 통해 기초적인 소프트웨어 공격부터 보안 연구를 수행할 수 있게 하는 지식과 기술들을 배우게 됩니다.

- 리눅스 및 어셈블리 분석
- 해킹대회 기출문제
- 시스템프로그래밍/컴파일러 등

핵심 연구 분야

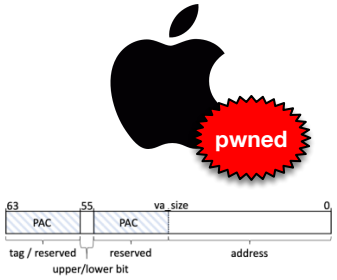
운영체제/클라우드 보안
- 보안전담 프로세서
- 운영체제 공격/방어
- 소프트웨어 격리기술

소프트웨어 보안
- 공격 기법 연구
- 취약점 발견/분석

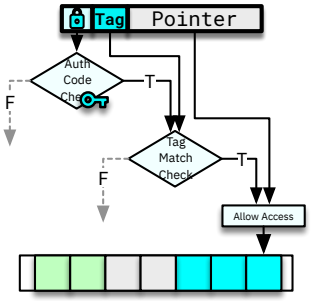
AI 보안
- 신뢰실행기반 AI 연산
- AI 시스템 취약점

진행중인 연구 분야

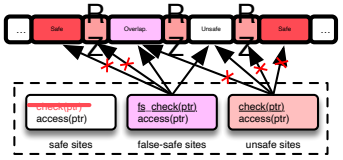
iOS/macOS 최신보안기술 우회 공격



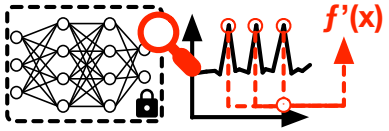
Capability기반 보안 적용 운영체제



메모리 취약점 탐지 컴파일러 기술 개발



AI 연산에 대한 부채널공격 및 보호



Syste
Secur
Lab

SUNGKYUNKWAN UNIVERSITY
1398
성균관대학교

Syllabus Walkthrough

Syllabus Walkthrough: Grading

Grading

- Attendance 10%
- Assignments 30%
- Exams 60%

Syllabus Walkthrough: Attendance

- Yes. Attendance is required
- And it makes up 10% of course grade

Syllabus Walkthrough: Academic Integrity

Any form of academic dishonesty is strictly prohibited in this course.

- Cheating on Exams
- Copying your friend's code
- etc …

Consequence: A grade of "0" will be given to the {Exam/Assignment} grade

Syllabus Walkthrough: Assignments

- Capture-The-Flag Competition (We'll get to this soon)

Syllabus Walkthrough: Helpful (but not required) Books

- *Security Engineering* by Ross Anderson
- *Information Security: Principles and Practice* by Mark Stamp
- *Introduction to Computer Security* by Michael Goodrich and Roberto Tamassia
- *Computer & Internet Security: A Hands-on Approach* by Wenliang Du

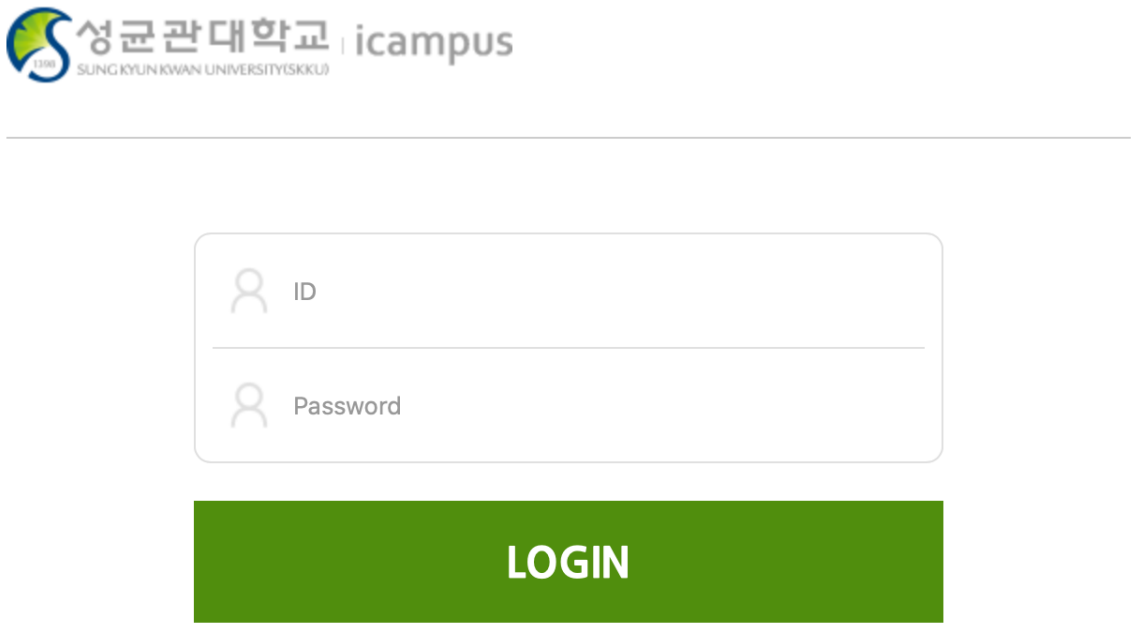
Course Objectives

- Learn foundational concepts in security through lectures and readings
- Learn how computer security problems *really work* through assignments

Course Coverage

- Weeks 1~5 : Foundations of Computer Security
  - Authentication
  - Access Control
  - Cryptography
- Weeks 6~15: Computer and Internet Security
  - Network Security
  - Software Security
  - Systems Security

Authentication



Access Control

```
crw-rw---- 1 root kvm 10, 232 Mar 27 22:29 /dev/kvm
```

Group ACL Owner Group

- Users who belong in group "kvm" can "rw-" to "/dev/kvm"
- Only I and your TA can create/delete virtual machines on the server

ME ME Your TA

```
kvm:x:108:hjlee,sslab-admin,khadinh
```

Cryptography

- Ciphertext:

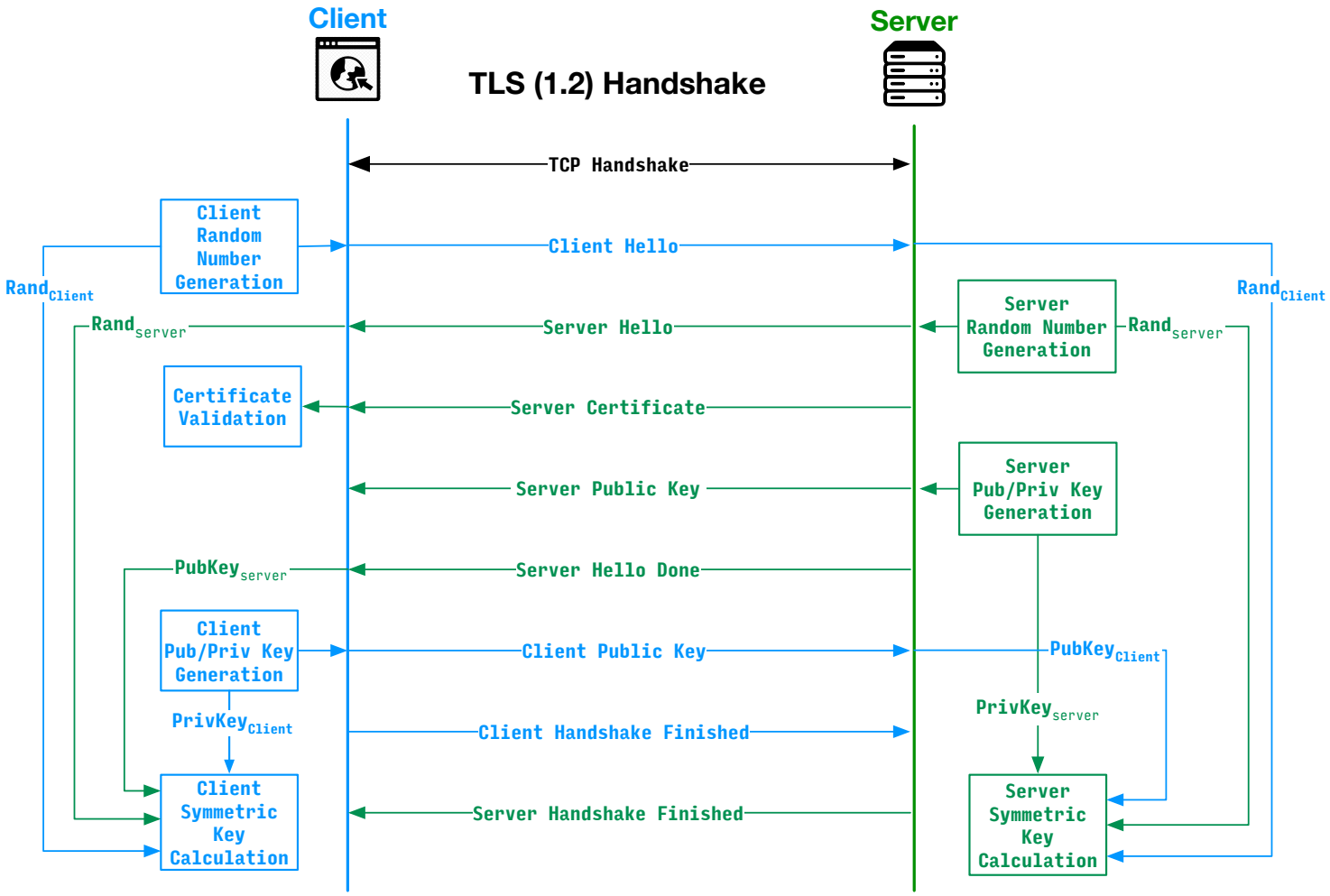
PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFXQWAXBVCXQWAXFQJVWLEQNTOZQGGQLFX
QWAKVWLXQWAEBIPBFXFQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFEVWLXGDPEQVPQGVPPBFTIXPFHXZHVFAG
FOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQPBQWAQJJTODXQHFOQPWTBDHHIXQVAPBFZQHCFWP
FHPBFIPBQWKFABVYYDZBOTHPBQPQJTQOTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVFOJIWFFACFCCFHQWAUV
WFLQHGFXVAFXQHFUFHILTTAVWAFFAWTEVOITDHFHFQAITIXPFHXAFQHEFZQWGFLVWPTOFFA

Ciphertext frequency counts:

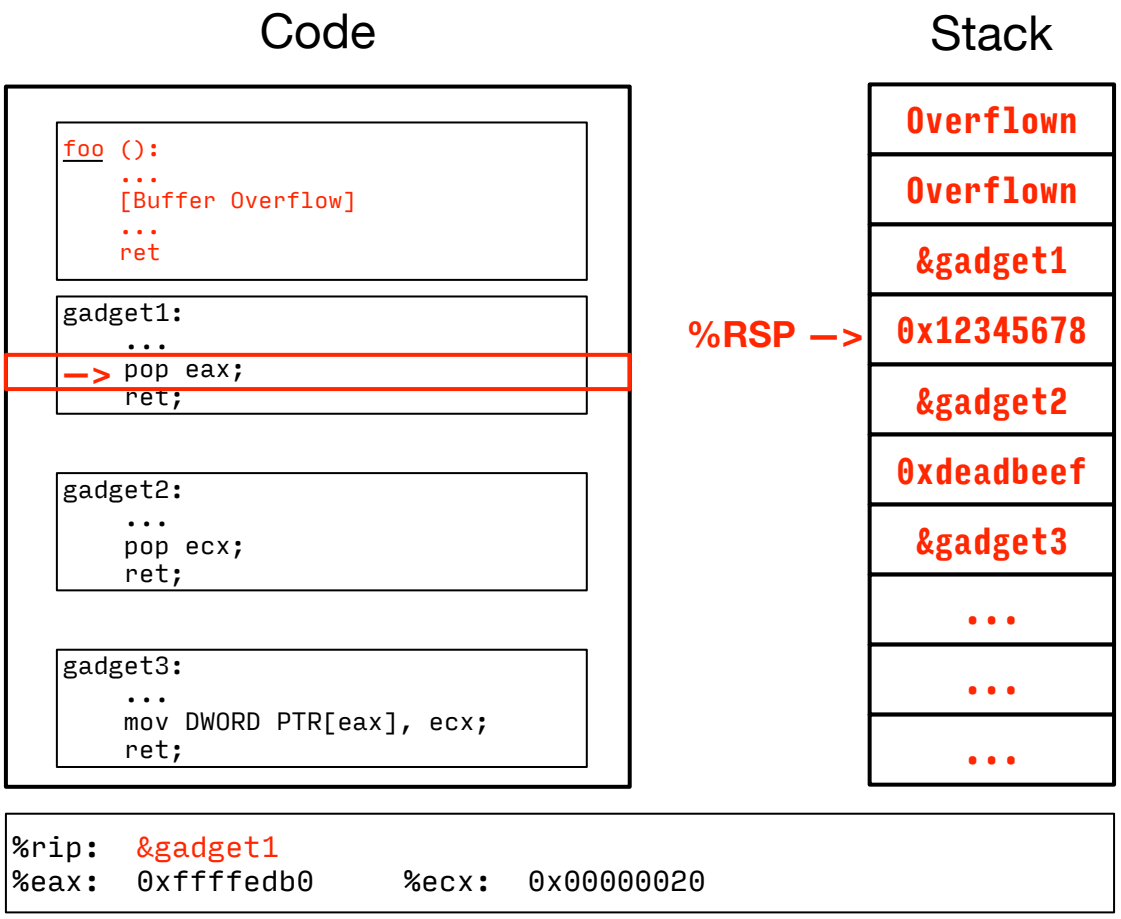
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
21	26	6	10	12	51	10	25	10	9	3	10	0	1	15	28	42	0	0	27	4	24	22	28	6	8

This is probably 'e' ???

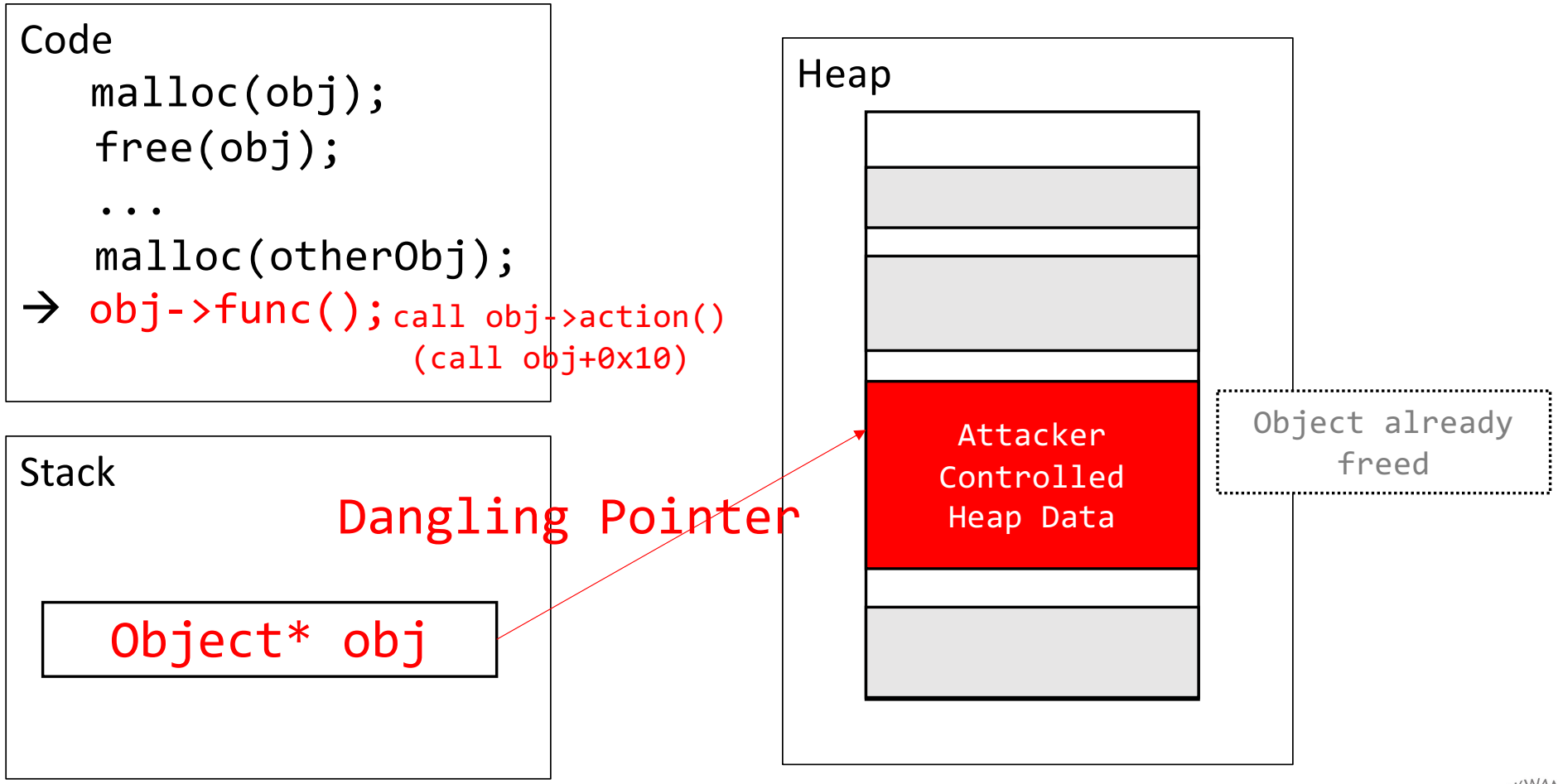
TLS and Secure Communication



Software Security



Software Security



CTF as Security Education

- CTF stands for Capture-The-Flag
- CTF refers to a form of simulated cyber wargame
- By exploiting the vulnerability of the given {program,website, etc ..}, you will extract the "flag" hidden inside
- We will have CTF assignments in this course

Capture-The-Flag as Security Education

- There are many Team-based CTF competitions around the world
- The most well-known one is called "Defcon" held in Las Vegas every year
- Many universities have a CTF team that actively participates in CTF competitions
  - e.g., CMU's PPP,
- SKKU CTF Team anyone?

Systems Security Lab

CTF as a Security Education

- Security from attacker's perspectives
- Learning by doing (hacking)

Systems Security Lab

SUNGKYUNKWAN UNIVERSITY 1398 성균관대학교

SSLab CTF Website

Systems Security Lab

SUNG KYUN KWAN UNIVERSITY 1398 성균관대학교

SSLab CTF Challenges

Hard

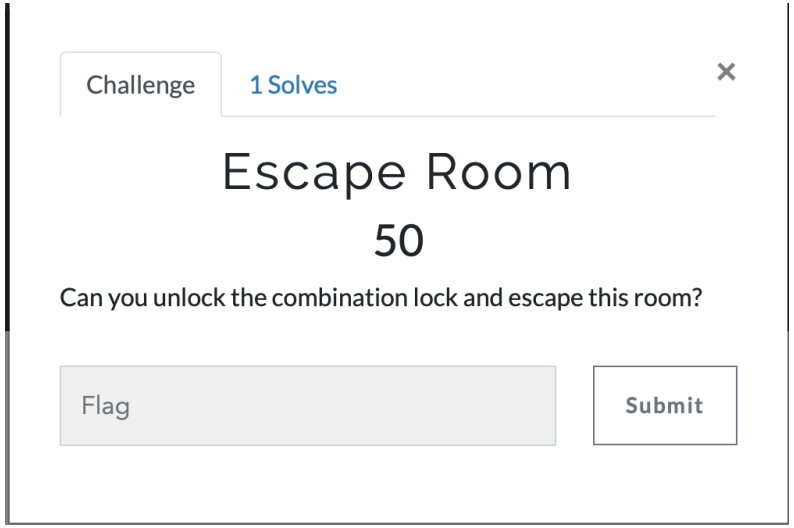
- Canary Bypass — 100

Medium

- Escape Room — 50
- Escape Room 2 — 50
- Use-After-Free — 75

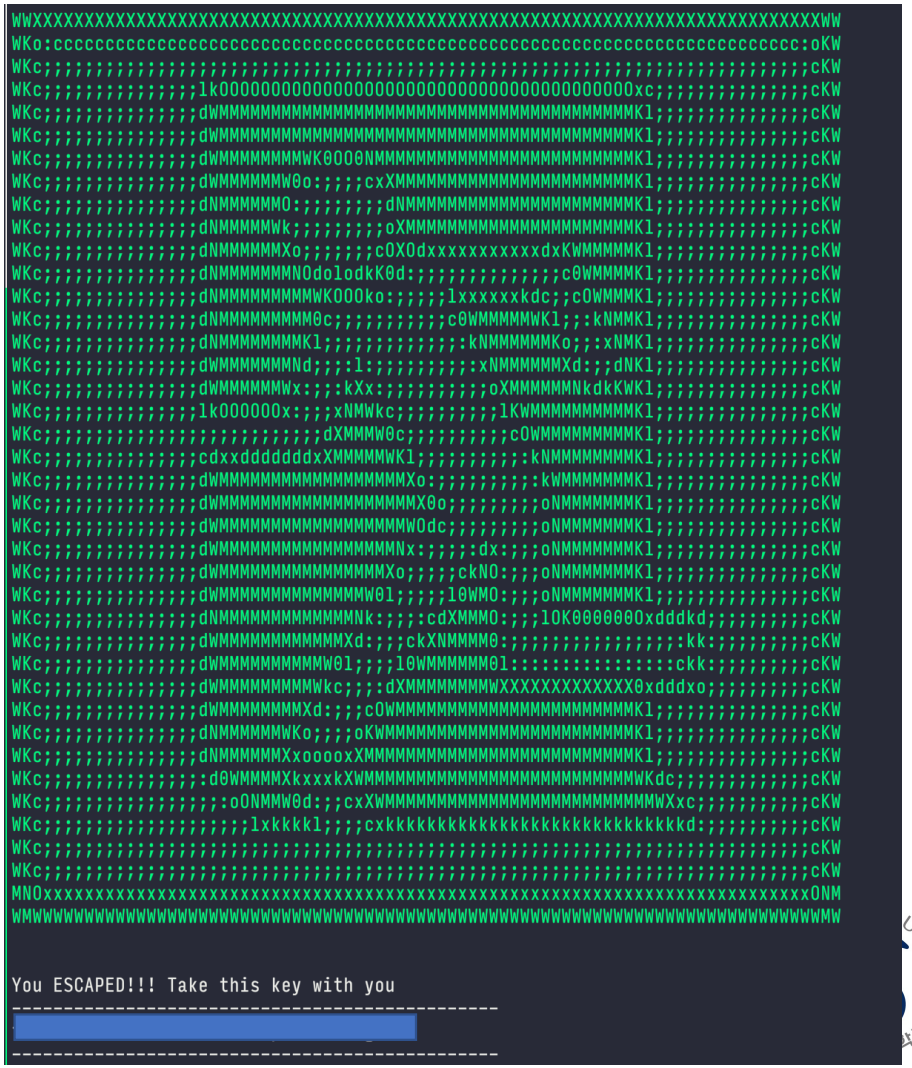
Easy

- Easy Buffer Overflow — 33
- Rock! Scissor! Paper! — 33



SSLab CTF Challenges

Exploit



Systems Can be Hacked

Case Study 0x1:Hacking Prison Monitoring System

Systems Can be Hacked

Case Study 0x1:Hacking Prison Monitoring System

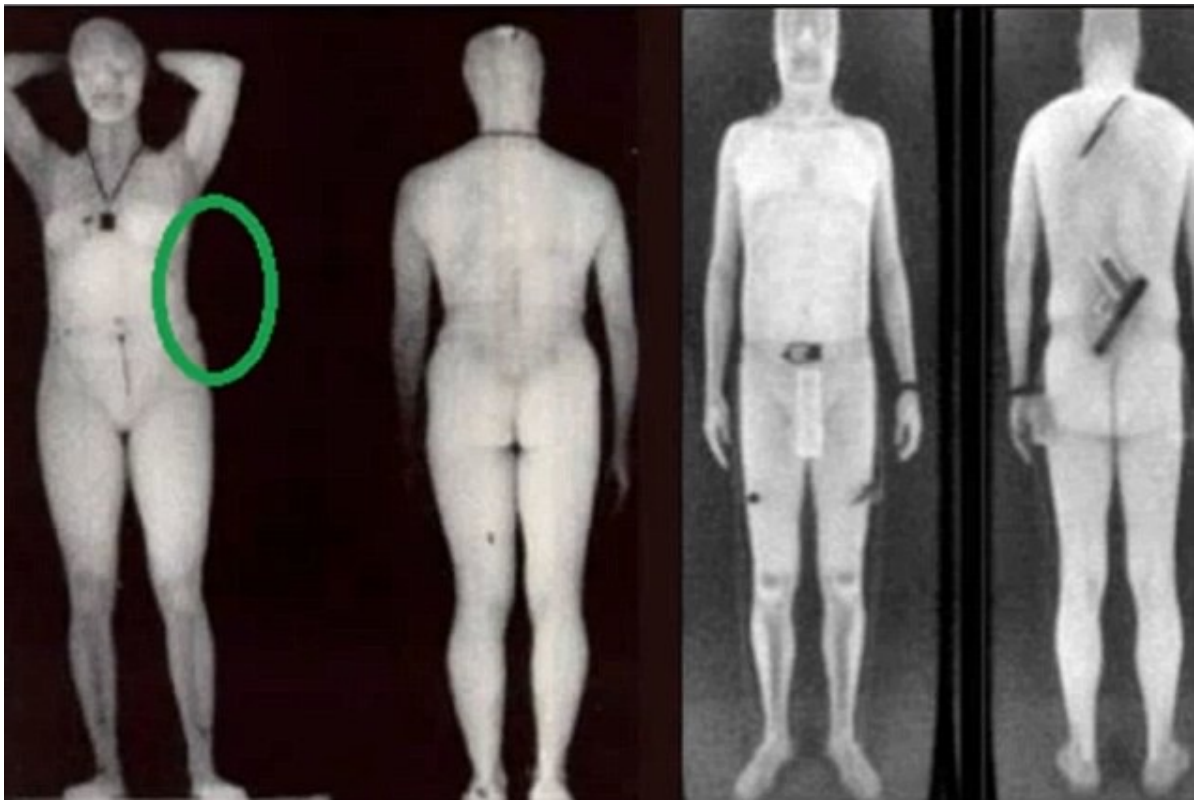
+

Systems Can be Hacked

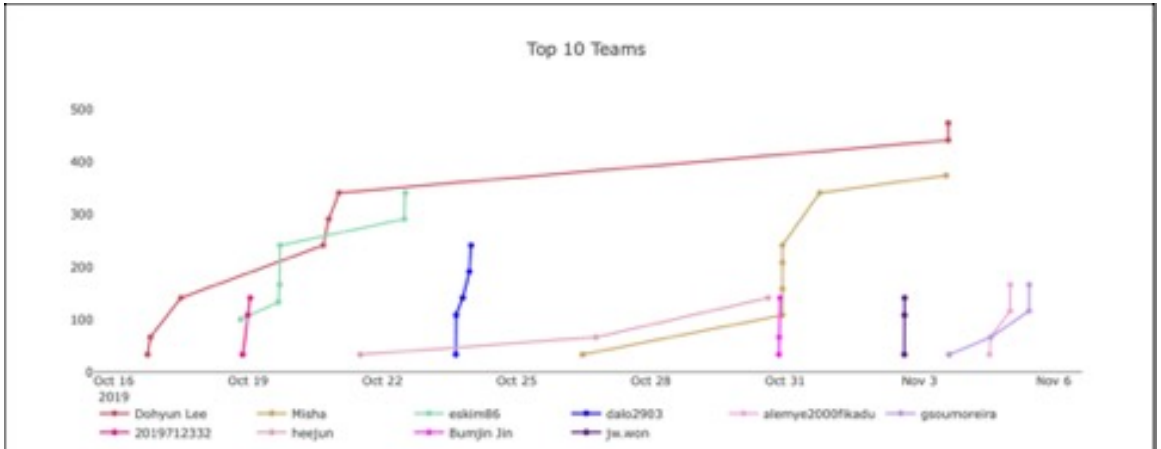
Case Study 0x2: Hacking Airport Security Scanner

Systems Can be Hacked

Case Study 0x2: Hacking Airport Security Scanner



SSLab CTF Challenges



Place	Team	Score
1	Dohyun Lee	474
2	Misha	374
3	eskim86	341
4	dalo2903	241
5	alemye2000fikadu	166
6	gsoumoreira	166
7	2019712332	141

Class poll

- I know how to program in C
  - YES: [ ]
  - NO: [ ]

Class poll

- My confidence level in C is ..
  - Very confident: [ ]
  - Fairly confident: [ ]
  - Not so confident: [ ]
  - Hello world??: [ ]

Class poll

- I have used Linux before
  - YES: [ ]
  - NO: [ ]

Class poll

- (If no Linux experience) I know what virtualization is and how to make a virtual machine
  - YES: [ ]
  - NO: [ ]

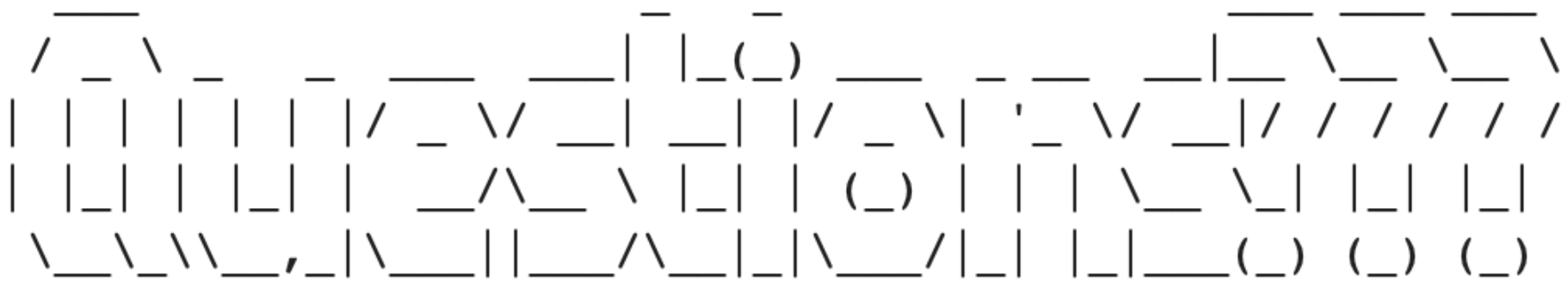
Class poll

- I can reverse engineer x86 assembly code (SWE2001-시스템 프로그램)
  - YES: [ ]
  - NO: [ ]

Class poll

- I do not have a x86-based computer (I only have a M1/M2 macbook)
  - YES: [ ]
  - NO: [ ]

Any Questions?



- If you have any questions about the course
- Please feel free to drop me an email
- hojoon.lee@skku.edu
- Please title the email such that it begins with “[SWE3025]” to have a high priority in my mailbox.