Binary Code Analysis and Secure Software Systems

01 – Introduction to Software Security

Sang Kil Cha
Who Am I?

• Sang Kil Cha
• Researcher, Engineer, and Hacker
Software Security

- Binary Analysis
- Program Analysis
- Exploit Verification
- Vulnerability Discovery
- Bug Detection & Classification
- Mawalre Analysis
- …

IS893: Advanced Software Security
Software Security
What is the difference between science and engineering?
SCIENCE

ENGINEERING
Where there is an engineering, (chances are) there are security issues.
Why?

Human $\Rightarrow$ Error
Software Engineering is No Exception!

Lenovo, Dell, Toshiba PC Vulnerability Exposes Millions to Attack: Report

NEWS ANALYSIS

Vulnerability in Samsung Galaxy phones put over 600 million Samsung phone users at risk

Russian hackers have scraped over $790 million in three years

By: Chris Smith | Hacking & Security News | Posted: Nov
Software Engineering is No Exception!

Because software engineers make mistakes
(Software Bugs)
Software Bug is the Root of Evil

Attackers

Exploit

Malicious input that triggers bug(s)

- Stealing private data
- Executing arbitrary commands
- ...
Software Engineering
Software Engineering vs. Software Security

Software Engineering
Let’s build secure and reliable software systems.

Software Security
Building a perfect system is impossible, so let’s minimize the impact of software bugs.

Same Goal: secure and safe computing
Goal of This Course

Software Security
Building a perfect system is impossible, so let’s minimize the impact of software bugs.

1. Understand how attackers (hackers) exploit bugs
2. Learn current defense techniques
3. Understand general principles of secure software system design and analysis
Course Overview

• **Approach**: learn how to secure software systems by learning both attacks and defenses

• **Target Audience**
  - Possess *system programming* skills (C/C++) (prerequisite)
  - Possess knowledge about *computer architecture* and *compiler* (not necessarily a prerequisite though)
Course Resources

• Course Mailing List
  - is561-staff@softsec.kaist.ac.kr
  - This sends emails to all instructors

• Course Web
  - http://softsec.kaist.ac.kr/courses/2017f-is561/: slides and schedule
  - KLMS: Q&A and Homework

• Faculty: Sang Kil Cha (sangkilc@kaist.ac.kr)
Logistics

• 5% Reading critique
  - No more than 2~3 paragraphs for each critique
  - Brief summary, things you learned, and things that can be improved

• 20% Homework
• 40% Project
• 15% Midterm
• 20% Final Exam
Reading Critique (2~3 paragraphs)

Answer questions below:
• What kind of problem does this paper try to solve?
• Do you think the problem is important to tackle?
• Why do you think previous work is insufficient?
• Why do you think the proposed solution in the paper is good (or bad)?
• Do you think the evaluation is reasonable?
• What did you learn from the paper?
• How would you improve upon this work?
CTF (Capture The Flag) = Hacking Competition

- Mainly two types
  - Attack & Defense style: real-time attack and defense
  - Jeopardy style: problem solving

- Homeworks are mostly jeopardy-style CTF problems
  - Solve problems (You will get instant feedback)
  - Write reports
Projects

• Write a research proposal by 10/03/2017
  – Max. 3 people in a group
  – Any topics in software security
  – To get an idea, read papers from good conferences
  – Clearly set your milestones and schedule

• Final presentation: 12/05/2017
What are Good Papers?

• Top 4 Security Conf.
  − IEEE S&P
  − CCS
  − NDSS
  − USENIX Security

• Top Systems Conf.
  − SOSP
  − OSDI
  − NSDI
  − ASPLOS

• Top S/W Engineering Conf.
  − ICSE
  − FSE
  − ASE

• Top P/L Conf.
  − PLDI
  − POPL
  − OOPSLA
  − ICFP
Success Stories

• A course project from the previous IS-561 (last year) has accepted in CCS 2017

• Another course project is getting ready to be submitted to Oakland 2018

• Another course project got the best student paper award in CISC 2016
How to Choose Your Project Topic?

• Must be related to software security

• Try to find ideas by looking at the latest papers

• We give several example topics in the proposal document

• Iterate with instructors often!
KaisHack

• Graduate hacking team @ KAIST
  (Undergrad hacking team is GoN)

• Join us today!
  – Send an email to 김동관: dkay@kaist.ac.kr
Question?