Malicious Code Analysis: more appropriately System and Network Security Research

Dr. Yeonjoon Lee

General Information

- **Instructor: Assistant Professor Yeonjoon Lee**
  - Office: Room 504, Engineering Building 3
  - Email: yeonjoonlee@hanyang.ac.kr
  - Web: yeonjoonlee.com
  - Office hour: before class or by appointment

- **Time**
  - Friday, 9:00 – 12:00, Engineering Building 1, Daehakwon Lecture Room 1

Tell me what you want from the class

- Your name
- Your department
- What are your research interests?
- What do you expect from the class?
  - Credits only?
  - Help your research?
  - For funs?

Course Objective: a Journey to Innovate

- Expose you to some most recent innovations in System and Network security
- Encourage you to do the same
- Help you try

What you are supposed to do

- Learn: what's the technical proposals people appreciate
  - Read research papers and criticize them
  - Try to sense the difference between good work/mediocre work/bad work
- Do: come up with your own idea, comparable with others' good work, and make it happen
  - Propose your project
  - Make a preliminary step to materialize it

Common questions

Q1: I just want to get some knowledge for becoming a security professional. Can I get it here?

- A: Yes, you can get knowledge from the lectures and paper reading, but the focus here is learning to innovate.

- Innovation and imagination is important not only to the security researchers but also to security practitioners
  - Hackers are innovative
  - New computing systems (cloud, smartphone, web services, etc.) keep coming out
  - So we need to continuously do something new

Common questions (cont'd)

Q2: How is the course different from a Security Reading Group?

- A: Simply put, you have to do a lot more homework ☺
- For the reading group, you read research papers
- Here, you learn how to evaluate others' innovations, and come up with your own
  - How to appreciate brilliant mind, being critical but also fair
    This won't work; it is just incremental; this is promising; it is indeed a surprise!
  - Is your own idea up to the par?

Paper reading

Let's organize a conference for fun!

***The Security Research Review Workshop* (SySecR)**

- We will run a conference management system HotCRP
- I will first "submit" 16 to 20 suggested papers
- You are also welcome to do that

Paper reading (cont'd)

1. Everyone needs to read every paper.
2. Everyone needs to present one paper.
3. Everyone needs to write technical reviews for 5 papers.
4. The reviewers must submit reviews 2 days before a class
5. You are required to read all the reviews before the class
6. We discuss the paper and all its reviews on the class
7. You could vote for the best review
8. Reviews will be graded
9. We plan to rank these papers and "accept" some of them

Paper Reading (cont'd)

- Where the papers come from?
  - Leading security venues: Oakland, CCS, NDSS, USENIX Security and others
  - I will provide a list and you are also welcome to recommend those related to Cloud, Web and Smartphone security and privacy

Course projects

- Individual or two-person projects
  - Inspired by what you learn from the research papers
  - Materialized through our discussion
- You are encouraged to participate in real research projects

How to work on course projects

- Discuss your initial idea on the class
- Give a formal proposal talk to get feedbacks
- Execute your research plan
- Demonstrate your achievement in the final presentation
- Give me a formal report

How will you be graded

- Paper reading (30%)
- Presentation (5%)
- Class participation and discussion (15%)
- Course projects (50%)
  - Proposal talk (5%)
  - Proposal (10%)
  - Project report (25%)
  - Final presentation (10%)

- This is subject to change

Policies for missing classes

- The points that are subtracted from the total points for the semester associated for non-attendance will commence ONLY after two unexplained absences.
- Besides that class, you can ask for medical leave if you can provide proper evidence.
- Otherwise, you will lose 2 points whenever you miss one class

Arrangement

- Introduction, paper posting/assignment
- Paper presentation, review and discussion
- project proposal due (1 week of Oct)
- proposal talks
- Paper presentation, review and discussion
- Paper presentation, review and discussion
- Final report due
- Final project talks

Let's begin with 5 papers (Pick one)

1. Finding Unknown Malice in 10 Seconds: Mass Vetting for New Threats at the Google-Play Scale (오지강)
2. It's Free for a Reason: Exploring the Ecosystem of Free Live Streaming Services (김예은)
3. IOTGUARD: Dynamic Enforcement of Security and Safety Policy in Commodity IoT (유동민)
4. *Following Devil's Footprints: Cross-Platform Analysis of Potentially Harmful Libraries on Android and iOS* (proposal instructions and examples) (이석원)
5. WHYPER: Towards Automating Risk Assessment of Mobile Applications (Martin)

As there are only 5 students…

1. Pick a topic
   - Mobile Security
   - Cloud Security
   - IoT Security
   - Web Security
   - etc
2. Present and share what you studied
   - You can directly use your research topic for this course

How often?

- Paper Reading - every week
  - One student should present the selected paper.
  - All students should read and review the selected paper.
    - The presenter is not required to write a formal review.
- Research Project - Share what you have studied
  - The presenter of the paper is not required to share what he has studied.
- Grading will be based on the paper reviews and the final report of the research project

How does a review look like?

- Summary
- Strength
- Weakness
- Comments

Let’s see a real-world example

Demos..

5 papers (Pick one)

1. Skill Squatting Attacks on Amazon Alexa (유동민)
2. Understanding Craigslist Rental Scams (Marton)
3. The Dropper Effect: Insights into Malware Distribution with Downloader Graph Analytics (김예은)
4. Mass Discovery of Android Traffic Imprints through Instantiated Partial Execution (이석원)
5. Finding Clues for Your Secrets: Semantics-Driven, Learning-Based Privacy Discovery in Mobile Apps (오지강)

Other Papers..

Understanding and Securing Device Vulnerabilities through Automated Bug Report Analysis

Devils in the Guidance: Predicting Logic Vulnerabilities in Payment Syndication Services through Automated Documentation Analysis