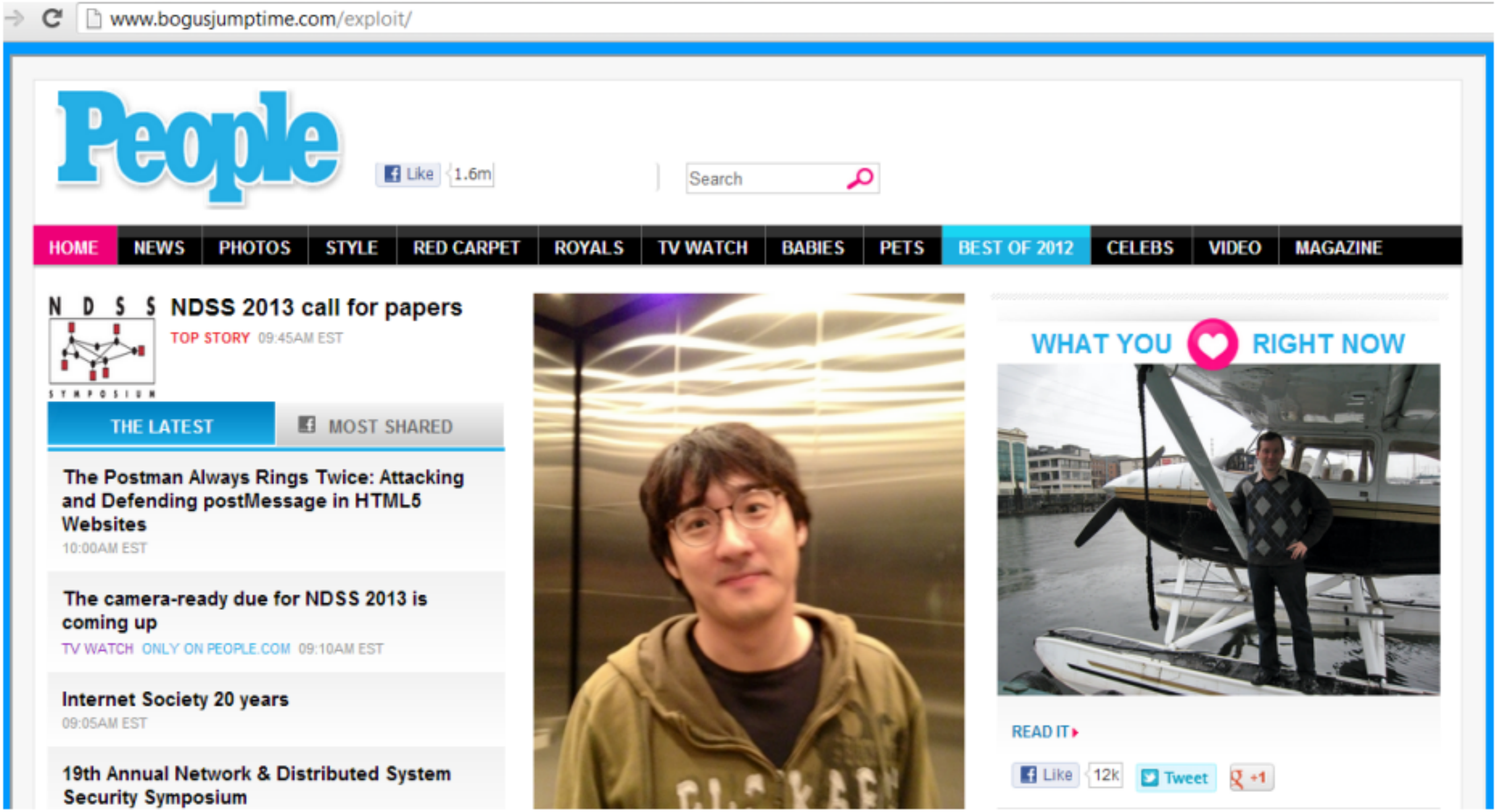
Course Introduction

Machine Learning Application
Trends in Information Security

Sooel Son
CS492

KAIST

Who Am I?



www.bogusjumptime.com/exploit/

NDSS 2013 call for papers

TOP STORY 09:45AM EST

The Postman Always Rings Twice: Attacking and Defending postMessage in HTML5 Websites

10:00AM EST

The camera-ready due for NDSS 2013 is coming up

TV WATCH ONLY ON PEOPLE.COM 09:10AM EST

Internet Society 20 years

09:05AM EST

19th Annual Network & Distributed System Security Symposium

Machine Learning Application Trends in Information Security

- Class Homepage: [https://spostman.github.io/cs492]

- We will study together the latest published papers that address machine learning topics in information security

- What will you learn from this course ?
  - The ML application trends in information security
  - The ideas and topics for your future research
  - Manifesting technical challenges and methods of applying ML algorithms t o real-world problems

- This is NOT a lecture-driven class by the professor!
  - Require your participations

Evaluation

- Attendance & Class participation: 15%
- Paper critiques: 20%
- Paper presentation #1: 10%
- Paper presentation #2: 10%
- Paper presentation #3: 10%
- Project proposal & Midpoint evaluation: 5%
  - Submit your proposal by 9/26/2018 (One page)
  - Prepare a 10-minutes presentation for the midpoint evaluation
- Final group project: 30%
  - 20 minute presentation for the final presentation
- Office Hour:
  - Every Tuesday 11:00 AM to 12:30 PM

Attendance & Participations

- Don’t be late!
  - If you are late at the class two times, it is same as one absent
- If you are absent 3 times without any notice, there is no score for the attendance and participations
- Discussions
  - Ask questions!
  - The presenter should summarize the questions that he/she did not addressed.

How to Write a Critique?

- Summary
  - Describe the paper.
- Pros
  - At least 2 pros or more
- Cons
  - At least 2 cons or more
- Meaning of the paper
  - What are the key contributions of the paper?
  - Why do they matter?
  - If this is an attack paper, how critical is the described attack?
  - If this is a defense paper, how robust is the described defense? How effectiv e are they?
  - Is this the first paper to address the topic?

How to Present a Paper?

- Please present your paper in the following order
- 1. Present the title and authors' affiliations
- 2. Summarize the paper with 1 or 2 slides
  - Problem, Contribution, Result, Meaning
- 3. Motive
  - Why this research is helpful for what purpose?
- 4. Background
  - Consider your audiences as undergraduate students who did not take a ML course.
- 5. Content
  - It is up to you! But remember that the presentation should cover at least 45 minutes.
- 6. Evaluations
  - Please describe in detail the experiment setups
- 7. Summary

Things to Remember

- If your presentation is on the next Tuesday, submit your slides by Tuesday 11:59PM to your TA and me!
  - sevendays37@kaist.ac.kr, son.sooel@gmail.com
- For the Thursday, submit your slides by Thursday 11:59PM

- If the presenter has questions or topics to discuss, please add those at the last slide to have discussions! [Mandatory]
- If the presenter has a list of points that he/she does not understand, please add those as well
- The goal of the class is to study together and to learn from each other
- Your participation is important

Project Ideas

- Each one should pick his/her own project!
- Submit your proposal by 9/26/2018 (One page)
- The earlier is the better because the projects should have no overlap!
- It is ok to reproduce the result of the covered papers.
- It is totally up to you what topics to choose.