CS-676 Adv. Topics in Systems Security

Instructor: Georgios Portokalidis

Spring 2019

Course Goals

Learn about research in the area of systems and security

Learn how to read research papers

- And practice reviewing them

Learn how to give technical presentations

Tackle open problems by designing, implementing, and evaluating a solution

- Practice writing a research paper on the developed solution

Format

Studying and presenting papers

Research project

Studying Papers

3 papers have been assigned to each course meeting

The entire class must study the papers the week leading to the meeting

Each student needs to submit a critical review of the papers before the meeting

- 1 or 2 paragraphs are sufficient
- Discuss the pros and cons
- Include two thought-provoking questions
- Briefly point to future directions

Presentations

A student will be assigned to give a 40-minute presentation of each paper

- ~3 presentations/student

Each presentation will be followed by a 10-minute Q&A session

- I will go around the classroom giving the opportunity to each student to ask a question about the paper to the presenter

Evaluation of Presentations

Understanding: Does the presenter understand the material?

Thoughtfulness: Does the presented have insights and opinions beyond what is in the paper?

Clarity: Can the audience understand the presentation? Are there useful examples?

Materials: Do the slides (or use of whiteboard) illustrate and support the talk? Are there diagrams to help convey the technicalities?

Delivery: Has the presenter practiced?

Non-regurgitation: Did the presenter do something beyond simply typing sections of the paper as bullet points? Did the presenter motivate the ideas in their own words?

Answering questions: Can the presenter handle questions from the audience?

Research Project

Students must work in a semester-long research project

- Students should come up with the topic
  - Feel free to arrange a meeting with me to discuss your ideas
- Topic should be approved by me
- Project should include significant software development or experimentation

Milestones

- Literature survey and proposal presentation, March 11, 2019
- Project presentation and demo, May 6, 2019

Start immediately!

Studying for the Project

It is important to read various papers and skim even more before deciding what to work on

- Hence the literature survey

Consult …

- The papers in the course schedule
- The optional papers in the syllabus
- Other papers cited in the papers you are reviewing
- Use https://scholar.google.com

Use the proposal presentation as an opportunity to get feedback from your classmates

Project Evaluation

Project should result in short research paper

Two approaches

Replicate existing papers

- a more thorough analysis of the original work's strengths and weaknesses must be undertaken

Investigate a new idea

- Awesome!

Grading

Project software and report	45%
Project presentation	5%
Project proposal and literature survey	15%
Proposal presentation	5%
Weekly presentations	20%
Weekly reviews	5%
Attendance	5%

Giving a Technical Presentation

How?

Giving a good talk is many times a matter of experience

- This is why it is important to give talks

You can learn from the talks of others

- Attend seminars
- Identify both strong an weak points of the speaker, adopt the first, avoid the latter

It is similar in structure to writing a technical paper

- But also different
  - Live audiences tend to wonder off
  - You can have interaction
  - Stage presence matters

Structure

Problem statement

Importance of the problem

How did previous approaches try to solve the problem

How does the approach described in the paper solve the problem (aka the technical details)

How is the approach evaluated in the paper

Conclude

Problem Statement

Make sure you understand the problem tackled in the paper

Concisely present the problem

Do not be afraid to use examples

Sometime the problem statement starts as a broad statement, but quickly focuses on a very specific problem

If you define the problem too broadly, it will be hard to explain how the described solution solves it

Importance of the Problem

Some problems may be more important than others

- **More important:** Software bugs in cyberphysical systems, like cars, can lead to loss of human life
- **Less important:** Software bugs in Call of Duty II can cause players to lose their equipment

Important problems tend to keep audiences more interested

- Different audiences may have different priorities

It is always fun to show articles that quantify the importance of the problem

- For example, the cost of bug overflows is estimated to $100B

Experts working with Homeland Security hacked into Boeing 757

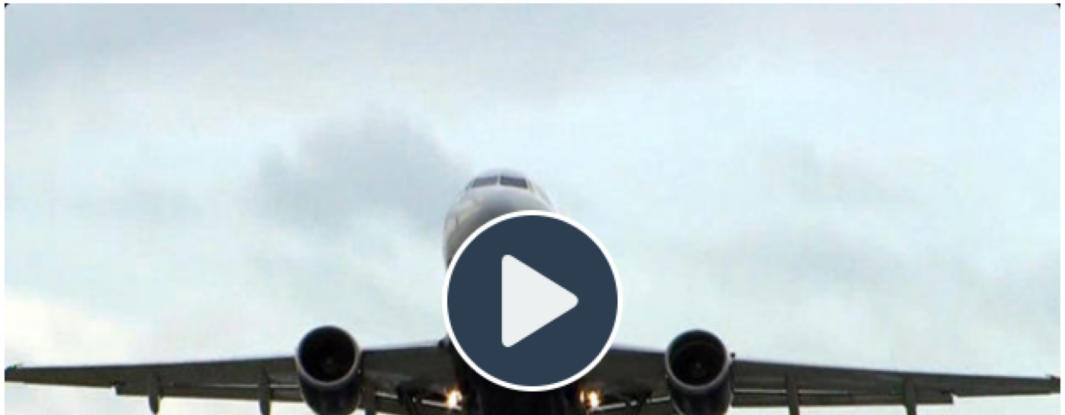
There's some unsettling news about one of America's most widely-used jetliners.

In a test, experts working with Homeland Security hacked into a Boeing 757. The team of researchers needed only two days in September 2016 to remotely hack into a 757 parked at the airport in Atlantic City, New Jersey.

Speaking at a conference this week, Robert Hickey of the Department of Homeland Security said his team used "typical stuff that could get through security" and hacked into the aircraft systems using "radio frequency communications."

"The 757 hasn't been in production since 2004, but the aging workhorse is still flown by major airlines like United, Delta and American," said Mark Rosenker, the former chair of the National Transportation Safety Board.

President Trump's personal jet is a 757. So is the plane Vice President Pence often uses -- including on his recent trip to Texas.



Previous Approaches

Describe how have others attacked the problem

- References can be found all around the paper
- Mostly discussed in related work section

Compare the paper with previous works

- What is this paper doing that other's didn't
- This is important but hard to do
  - Carefully read the paper to see how they compare/place their work compared with that of others
  - I would be super-excited to see you compare it with stuff you know of

Technical Details

The main body of the presentation

Start by describing the approach of the paper at a high level

- What are its main contributions
- How does it solve the problem without going into the gritty details

Then dive into the details

- How are particular challenges overcome?
- How do things work?

Papers are dense so pick the key details to focus on

- But make sure you comprehend how all aspects work
- Prepare back up slides for details that didn't make the cut

Evaluation

How is the presented solution evaluated

Include:

- Experimental setup
- Key measurements
- How are the measurements interpreted

Include graphs or tables where appropriate

- Make sure they are visible
- Understand what exactly is shown and what is the point of the graph/table

Conclusions

What is the take away message of the paper

What have we learned from this work

- Summarize contributions

Has this paper lead to follow up works that supersede it or confirm its findings?

More Advice

Slides also matter

- Pick a clean design
- Avoid dark backgrounds
- Don’t clutter your slides
- Use animations only when necessary

Read: https://homes.cs.washington.edu/~mernst/advice/giving-talk.html

Consult the syllabus

Look at the schedule today and signup for papers

Signing Up to Give a Talk

Go to the following link and add your name next to three papers

- Login with your Stevens account
- You cannot edit the paper, stay in suggesting changes mode

Deadline: end of day Wednesday!

- I will randomly assign students to papers on Thursday

Group Sign up Before Proposal