CMPS 485 - Computer Security
Review Paper and Presentation
Fall 2018

Each group of 3 students will select a specific computer security-related topic, do some research based on recent papers, book chapters or industry reports. Then present the findings in class and lead the discussion. This assignment is worth 20% of your course grade.

You need to prepare a literature review paper to survey state-of-the-art results presented in major Computer Security conferences, journals or industry reports. Then you will present and discuss your findings in class using effective presentation techniques. Each presentation will be given 20 minutes including questions and answers. The paper and presentation must be the student's original work. The written paper should be at 10-12 pages. The key objective of this assignment is that you gain experience researching an advanced topic by gathering **multiple authoritative** references and integrating your findings **into a well-structured paper and presentation** with the highest possible academic standards. In addition to learning about advanced security topics, this assignment will also give you the opportunity to gain experience reading and critically evaluating papers. You will practice communicating complex technical material, both orally and in writing.

Submitted review papers and presentations will be made available to all students. This will enable everyone to learn from the efforts of all the other students.

1. Review Paper Components

The goal for this assignment is to let you explore, in more detail, an area of security that interests you. You should work in teams of 3 students. There are three components that you need to address:

1. *Breadth*. Reading a variety of related work to an area and summarizing all of it while showing how it is related.
2. *Depth*. Deeply researching some aspects of your topic and distilling the information down to make it accessible to your classmates.
3. *Demo*. Present a demo showing a practical aspect of your selected topic (e.g., demo a product implementing some of the security techniques you have presented).

If you are taking this class for honor's credit, your work must include implementation and testing components.

Besides sections specific to the selected topic, the review paper should include:

- Abstract
- Introduction: describe the topic being addressed and discuss its importance. Introduce the solution.
- Background: describe all key related concepts, and define any terms, especially technical terms and technical background, that are necessary to understand the problem.
- Solution: How is it solved? Architecture, concepts, algorithms and applications. Illustrate key technical points (Examples are a great way to do this.)
- Evaluation: strengths and weaknesses.
- Discussions: your own views and thoughts (e.g., is the solution(s) technically sound and why?)
- Conclusions
- Bibliography

Overall, your review paper should give a good idea of the content of the reviewed papers and the advantages and disadvantages to someone who has not read them.

2. Possible Topics

I recommend you choose a topic that interests you. You may choose and propose your own. The selected topic must be specific enough. Students are encouraged to focus on topics that complement the material covered in the course,

but you need to go significantly deeper. Each group is required to select **at least 3 academic papers and/or industry reports** relevant to their topic, summarize, analyze and ***synthesize*** them and present them to the class.

Suggested topics:

- Blockchain
- Crypto-currency
- Studying particular attacks: the how, the impact, detection mechanisms, prevention mechanisms
- Network Intrusion Detection and Prevention Systems (e.g., SNORT)
- Host Intrusion Detection and Prevention Systems (e.g., OSSEC)
- Cloud security
- Digital forensics
- Malware analysis
- IoT Security (Securing Cyber-Physical Devices)
- Situational awareness (Log analysis)
- Social Engineering
- Penetration Testing
- Big data log analysis for improved security
- Cybersecurity risk assessment
- Secure software design
- Honeypots
- Security of Mobile Applications
- Elliptic Curve Cryptosystems
- Machine Learning Applications to Information Security
- Implementation of a crypto system using FPGA
- Multifactor Authentication
- Steganography (i.e., concealing messages typically within other messages/files/ images/videos)
- Smart Cards Security
- Critical Infrastructure Protection
- Securing messaging apps
- Other. Your own idea! (I recommend this.)

3. Deliverables

Pre-Proposal

You need to sit with your team and brainstorm potential review paper ideas and what sub-topics/aspects you will focus on. You need to present a written brief summary of your discussions during office hours to get feedback during the week of 16th September 2018.

Proposal

Each team must submit a 1 page formal proposal containing an abstract, report draft structure and the references to be used. These must be submitted to your group GitHub repository.

Your proposals are due by **Thursday, September 27th 2018** at 11:59pm.

Report

You should produce a 10-12 pages report with your findings. It should be A4, 12 point Times New Roman font with 1 inch margins. 10-12 pages is not very long, so you need to be strategic about what you present.

Note: When writing your report, you may be tempted to cut and paste pieces of various online sources together into a report or even just parts of your report. This would be unwise, as I will fail you and report you for cheating. For a project like this you are NOT permitted to reuse material from ANY other source in ANY quantity. (No, not even just a sentence or picture.) Brief quotations (1-2 sentences each) properly quoted and cited are acceptable only if they do not constitute a major portion of any section. Write it yourself! (I take this REALLY seriously...) and I will

detect copying using http://www.ithenticate.com/

Presentation

Your presentations should be 20 minutes long and will be used by you to present your findings and demo to the class. All team members must be part of the presentation.

What should you submit?

You should submit to GitHub:

- PDF copy of the reviewed papers / technical reports.
- Your review paper as a Word document.
- Your PowerPoint presentation.

On the day of the presentation, you should also submit a hardcopy of your review paper and a hardcopy of your presentation.

4. Grading schema

Beside the above guidelines, this is what I will focus on during grading:

- Depth of literature review and adequate level of detail. The more in-depth and specific the better.
- Avoid vague generalities.
- Referring to concepts or points made in our course content is a plus.
- Do not plagiarize. Quote and cite sources where necessary.
- Emphasis computer security related issues
- Paper and presentation organization, i.e., logical order and transitions
- Clear, concise and accurate writing
- Conclusion justified and logically sound
- Well Prepared presentation and high level of confidence during the presentation delivery
- Quality of PowerPoint slides
- **Presenting NOT reading** – student just reading their presentation will have lower grade
- Time management during the presentation
- Adequately answering the questions during/after the presentation

Grading

Your report and presentation will be used to determine your grade as follows:

Evaluation criteria	%
Pre-proposal and proposal	5
Depth of literature review and adequate level of detail: the more in-depth and specific the better. Emphasis on security related issues. Clear, concise and accurate reporting of findings.	40
Paper organization, i.e., logical order and transitions	5
Evaluation: strengths and weaknesses.	5
Discussions: your own views and thoughts.	5
Conclusion justified and logically sound	5
Presentation Organization: - Presentation well-organized: information presented in logical and interesting sequence that the audience can easily follow - Good quality and neat visual aids	6

Presentation Content: - Presentation provides pertinent, concise and clearly explained information - Material is covered with adequate depth	6
Presentation Delivery: - Engaging talk with high level of confidence and enthusiasm - Speaks clearly and uses appropriate language - Meets time limit (20 minutes) - Adequately answering the questions	8
Demo	10
Peer evaluations (both performing and receiving)	5
Total	100

Deadlines

The report and presentation are due on **Thursday, November 1st 2018** at 11:59pm. These must be submitted to your group GitHub repository (included the cited papers/reports).

The presentations will be during the week of 4th November 2018.

How to locate academic papers?

- QU Library Online Databases http://library.qu.edu.qa/
- Google Scholar http://scholar.google.com/ - it works best if you use within QU campus because you can go straight to the full text via QU library.
- *Email me if need any further guidance or help*.

Useful links

- Tips for Writing Technical Papers, by Prof. Jennifer Widom
- Tips for a Good Conference Talk, by Prof. Jennifer Widom