Project

INSE 6150: Security Evaluation Methodologies

Due: Last Class. Hand in during class.

The project will consist of a written report. The subject of the report may be either a novel research topic relating to security evaluation methodologies or a systemization of knowledge. Research papers should contain an element of *security evaluation*, and not merely demonstrate an attack, vulnerability or tool for improving security. Systemization of knowledge papers should survey a methodology or set of methodologies for security evaluation, while offering a useful perspective.

Requirements:

1) You may work individually or in groups up to 4 people.

2) The report should be no more than 12 pages. This is a maximum and for projects by an individual, a shorter paper may be more appropriate.

3) You can use any template with normal margins and font sizes.

4) Review and understand how to avoid plagiarism: https://www.concordia.ca/encs/students/sas/expectation-originality.html

Tips:

1) Avoid writing a survey which merely reports on a number of results. If you are describing the work of others, you should do it critically: having looked at all the results, compare and contrast them. Evaluate it them critically—authors may miss or leave out important criteria in evaluating their own results.

2) If you are having difficulty selecting a topic, thumb through the proceedings of a security conference to see the types of things being explored in the research literature: *IEEE Symposium on Security & Privacy*, *USENIX Security*, *ACM CCS*, and *NDSS* are good places to start. You can also look at the "Related Work" section included in most papers to see a summary of the research in the area.

3) I am here to help. You are not required to submit anything to me other than the final report but I am happy to discuss your topic and progress during office hours.

4) Ineffective projects string together some arbitrary results about a general topic. Effective projects (and it is not strictly necessary to do this) answer a specific security question, pulling all results and only results that are relevant to answering the question.

5) Security is a broad field. Quoted below is the list of topics suggested for works submitted to *USENIX Security* to provide some sense of the breadth of research possible:

- Systems security
    - Mobile systems security
    - Web security
    - Cloud computing security
    - Distributed systems security
    - Operating systems security
    - Storage security
- Cryptographic implementation analysis and construction, applied cryptography
- Language-based security
- Hardware security
    - Embedded systems security
    - Methods for detection of malicious or counterfeit hardware
    - Randomness
    - Secure computer architectures
    - Side channels
- Network security
    - Intrusion and anomaly detection and prevention
    - Network infrastructure security
    - Denial-of-service attacks and countermeasures
    - Wireless network security
- Privacy-enhancing technologies, anonymity
    - Research on surveillance and censorship
- Human-computer interaction, security, and privacy
- Social issues and security
    - Research on computer security law and policy
    - Ethics of computer security research
    - Research on security education and training
- Security analysis
    - Malware analysis
    - Analysis of network and security protocols
    - Attacks with novel insights, techniques, or results
    - Forensics and diagnostics for security
    - Automated security analysis of hardware designs and implementation
    - Automated security analysis of source code and binaries, program analysis
- Security measurement studies
    - Measurements of fraud, malware, spam
    - Measurements of human behavior and security
- Others
    - Security in critical infrastructures
    - Security in electronic voting
    - Security in health care and medicine
    - Security in ubiquitous computing, sensors, actuators
    - Security in electronic commerce

Above list taken from:
https://www.usenix.org/conference/usenixsecurity15/symposium-topics

Grading:

Grading Scheme	
3	Scope
5	Interpretation
2	Technicality
10	**Total**

Scope

A good project will have a clearly define scope: what is on-topic for the project and what is off-topic. Of the items that are on-topic, they should be a complete and comprehensive set for addressing the issue of the paper. The paper should have a logical flow through that links its material together and there should be a reason that each portion of the paper exists. I recommend phrasing your project topic as a question and the project itself answers the question.

Interpretation

It is easy to read other research or technical documents and repeat what it says. A good project will explain the other research in way that makes it clear that the writer really understood it. It is also very quick to repeat the results of other research — a good project will demonstrate an adequate level of work went into it (it is a project that is meant to be worked on for the whole term).

Technicality

A good project will include technical details that appropriate for a graduate-level course in security.