

# Final Project

ISA 656: Network Security, Spring 2018  
George Mason University

The goal of this project is to understand, explore, question, explain/demonstrate a recent network attack or a recent security/privacy protocol.

The research you will do should consider the following:

1. Why the topic is interesting. In case of an attack: how did it affect users/public? In case of a new protocol: what is the problem being solved, why is it interesting? Real world scenarios and applications.
2. What is the related work? I.e. Similar attacks, similar protocols. In your report you have to be thorough.
3. In case there was news coverage, where there any superficial/sensational issues when the topic was presented in the press (incorrect statements etc)?
  - Up to 5% bonus points are available if you point out where and how a media report on the incident made a technical error. (Exact quotes or a screen shot from the relevant media are required.)
4. The underlying technical issues. For instance, a story about a hacker compromising a certificate authority and then issuing fake SSL certificates should also include an explanation of what an SSL certificate is, why issuing fake SSL certificates compromises web security, and details about how the certificate authority was compromised. **This is the core goal of your project. You need to have a clear understanding of the attack/problem or new protocol.**
5. Possible demonstration of attack or implementation/demo of protocol.
6. Thoughts/suggestions on how the attack/vulnerability could: (a) could be strengthen. Are there better ways to attack that specific vulnerability? Could you come up with one? and (b) how could the attack have been prevented? Where there any bad security practices the enabled the attack? Similarly for new protocol: could efficiency be improved, could the solution be tweaked to solve a similar problem?
  - Up to 15% bonus points if you go beyond the attack/solution! I.e. propose a modification/improvement of a protocol, find another way to attack a system, implement a protocol/ attack that was only theoretical before.
7. In case of an attack: discussion of incentives. (a) What motivated the attacker? (b) What harm was caused to the entity that the attack compromised? (c) What other parties were affected/harmed by the attack? If your topic is not a specific attack that has happened build a hypothetical scenario: why would an adversary attack the system?

8. Any interesting legal or ethical issues raised by the incident or the use of the new protocol.
9. List of references you used in your research (including academic publications in conferences and journals, news articles, wikipedia, blogs, textbooks, *etc.* )

Notice that you absolutely *have* to study and include academic references (try looking at google scholar for academic papers related to the topic or talk to the instructor).

## Deliverables and dates.

You should prepare the following:

1. **March. 22nd, midnight:** Preliminary report. After spending enough time researching your topic you have to provide a summary of your proposal. Describe the main idea of the attack or protocol you will be presenting in 1-2 paragraphs. Include the main resources you are using (academic papers, white papers, new articles, blog posts etc). Finally, provide a list of items that you plan to include in your final report and presentation. I.e. Related work, specific background that you plan to cover, technical details, demo etc (think of this as the outline/sections of your report and presentation). The list you will provide is a commitment to what the instructor should expect in your final report and presentation. You will receive comments in your preliminary report and might need to re-adjust your goals.
2. **April. 26th, midnight:** Prepare a 15 minute presentation. Submit a draft of your slides **in PDF format**. In case you need to make adjustments you will receive feedback by April 29th.
3. **May 3rd, in class:** Give a 15 minute presentation in class. Presentations will be open to the public (you may invite friends, classmates, etc) - so it is important to be prepared! Right before class, email the instructor with your slides and current version of final report **in PDF format**.
4. **May 10th, midnight:** Submit your final report *in PDF format*. It should be between 10-15 pages (excluding references). It should also include an extra title page that will consist of Title, Names of team members and a short abstract of your report. The report should cover all of the issues enumerated above and should address any interesting comments that were discussed during the group's presentation. Note that your final reports and slides will be posted in the class website.

**No late policy accepted for any of the final project deliverables.**

## Templates

You *have* to use the LNCS templates for your report. <https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines> I highly recommend to use Latex to write your report.

## Grading scheme.

This presentation and report is worth 25% of your final grade, broken down as: 2% for proposal and preliminary report, 5% for presentation style (clarity, ability to answer questions, slides), 2% for report style (clarity, references format), and 15% for technical depth (judged both from presentation and report). Note that all team members will receive the same grade. Also, all team members should be able to answer to technical questions during presentation.