Security News Research Project

CS357, Fall 2022
Boston University

November 14, 2022

Students will work in **groups of four** to prepare and create a poster about a news-worthy topic related to security and privacy that has recently appeared in the tech popular press (*e.g.,* arstechnica, slashdot, `bits.blogs.nytimes.com`, `www.washingtonpost.com/blogs/the-switch/`, `https://www.theregister.com/security/`, `https://www.csmonitor.com/Technology`, etc) or advocacy websites (*e.g.,* the EFF, etc). If you are looking for good topics, you can also look through some cybersecurity researcher blogs and "trace back" the stories they are writing about to news articles in the popular press. See for example `https://onlinedegrees.sandiego.edu/top-cyber-security-blogs-websites/`.

Ground rules:

- Your topic was first reported in the news no earlier than March 1, 2021.
- Your group must pick its own **unique** topic.
- To keep the project exciting, you are strongly encouraged to pick an topic that has received a reasonable amount of media attention. Do not present recently published research results that have not been covered in the media.
- Pick a topic that allows you to properly answer all the of the questions in the "project contents" detailed below.

Project Contents

Each group's research should consider the following:

1. The way the event was presented in the mainstream press. What was the "story" here? Why did the press bother to pick up this story?
2. The underlying technical issues. For instance, a story about a hacker using ransomware to shut down a hospital should also explain how the ransonware works, what vulnerabilities it exploited in the hospital system, what specific technology or network protocol was exploited, what could be been done to make the hospital IT more secure and less likely to be compromised, etc. Just telling a story about a hospital that was shut down is NOT sufficient for this project.
   - Bonus points are available if the group points 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)

3. How could the attack could have been prevented? Were there any bad security practices the enabled the attack? Do you have any thoughts about why the entity that was breached failed to put these security measures in place?

4. Discussion of incentives.

   - What motivated the attacker?
   - What harm was caused to the entity that the attack compromised? (e.g. the hospital)
   - What other parties were affected/harmed by the attack? (e.g. patients at the hospital)
   - Was there a misalignment of incentives that lead to the attack happening? (For instance, consider the Equifax breach of 2017, where hackers stole credit-record information about the majority of Americans from Equifax. Was Equifax sufficiently incentivized to protect this information? Probably not, because these Americans are not actually Equifax's customers - Equifax customers are the entities that REQUEST credit information, e.g. landlords, banks, mortgage brokers, etc, but not the people who Equifax is actually storing information about!)

5. What ethical issues are raised by the incident?

6. What legal issues are raised by the incident (if any)? If there was a misalignment of incentives, what laws, rules, regulations or norms could be put in place to better align incentives? Do such laws, rules, regulations or norms exist in other countries? Why don't these exist in the country where the breach happened?

7. List of references you used in your research (including news articles, wikipedia, blogs, textbooks, *etc.*), and an "Acknowledgements" section listing any collaborators your worked when preparing your project. If you did not collaborate or discuss this project with anyone outside of your group, you can instead include the sentence "This work was done without any outside collaboration." at the end of your blog post.

Notice that obtaining all this information will require you to dig deeper than just what was presented in the popular press. In particular, understanding the underlying technical issues will likely require you to read blog posts by experts, product documentation, protocol documentation, and other stuff outside of the mainstream media. Your grade will NOT be good if you rely only on the mainstream media.

Project Deliverables.

Topic approval. [Get your topic approved by Professor and listed on the signup sheet by Tuesday November 15, 2022.]

To get your topic approved, your group should prepare these references and submit on the course signup sheet to get feedback on your topic choice before Tuesday November 15, 2022. You can reach out during office hours (for a synchronous conversation) or via Piazza at any time (for an asynchronous conversation).

- Article about the topic in the popular press

- At least one source of information you will use to understand the technical details behind the attack, *e.g.,* a blog post by a security researcher, a product datasheet, a technical report, etc.

- At least one source of information you will use to discuss the legal or ethical or incentive issues related to your topic

Content check-in.

Your group should prepare an outline of your report and the content that will be on the poster as a google doc. Make sure that the google doc is shared with goldbe@bu.edu and ivani@bu.edu and that we have the ability to make comments on the doc. You should submit it via the signup sheet AND on Gradescope to get feedback before Tuesday November 22, 2022. This is just a check-in to make sure your group is on the right track, and it will not be graded. You can reach out during office hours (for a synchronous conversation) or via Piazza at any time (for an asynchronous conversation).

Group deliverable

Each group should prepare the following:

1. **Blog post.** One single blog post on your topic, covering all the points above, authored by all of the group members. In your post, you are expected to hyperlink to source documents that support the points that you are making, as well as provide academic citations to your reference information. Your post should be between 1,500 to 3,000 words long, excluding references (item 7).
2. **Poster.** A poster that summarize the incident. Details about how to prepare the poster will be provided on Piazza in a separate post.
3. **Poster session!** Your will present your poster **in person!** at our class poster session on **Friday December 2, 2022 from 4:00-7:30pm at GSU Alley**. Be prepared to answer questions from your classmates and instructors about your poster. You grade will be based in part on how well you answer these questions. [If one of your groupmates need leave early, please let the instructors know in advance via a private post on piazza and we will make a best effort to grade you early before you have to go.]
4. Submit your group deliverable as follows.
    - Your blog post will be made available to the entire class on the class signup sheet.
    - Each student should also submit a copy of your poster and blogpost to gradescope.
    - Each member of the group submits the same information.
    - Blog and poster are all due at **11:59PM on Friday December 2, 2022**

Individual Wrap-up Report.

As a final deliverable, each individual student in CS357 will be required to a submit a **300-500** word report due at **11:59PM on Friday December 9, 2022**. The (imagined) recipient of the report is the US National Cyber Security Division (NCSD). Your goal is to advise the division on the most important "cybersecurity" issues of the year. Your report should:

- Discuss the system / industry that you believe is most vulnerable to attacks, along with a justification of why you believe this systems/industries/devices/etc is the most vulnerable.

- Describe the three most important cybersecurity events of the year, including a justification of why you believe these events were the most important. These incidents MUST have been presented by groups in the class.
- Provide two recommendations that the NCSD can use to improve the nation's security. These recommendations can be of any type, including suggesting increased (or decreased) regulation, modifications to laws, recommendations to fund research in certain areas or development in certain industries, recommendations to train users, engineers, politicians, *etc.* in certain topics, or whatever else you can think of. You must justify why your believe your recommendation will improve the nation's security, and explicitly reference incidents that were presented in other group's projects that lead you to arrive at these recommendations.

Grading scheme.

This project is worth 25% of your final grade, broken down as:

- 22% for the group project, broken down as: 15% for technical depth (judged both from poster, report and poster session), 4% for poster presentation and ability to answer questions at the poster session, and 3% for report style (clarity, completeness).
- 3% for the wrap-up report, broken down as 2.5% for content and 0.5% for style and clarity.