SER335 Engineering Secure Software Systems (Sp. 2024-Session B): Case Study Topics and Guidelines

Outcomes:

1. Practice a case study assessment methodology
2. Gain awareness of real-world security problems
3. Apply the fundamental principles in the course to a real-world context

Background

You will submit a short case study paper (4-5 single-spaced pages, plus references) on a real-world cybersecurity situation – an exploit or near-exploit. You will be provided a template for the paper with formatting guidelines. You will also be given a choice from a list of recent high profile cybersecurity cases. To write the case study, you will follow a methodology and paper outline given here.

Topics:

Though we have covered a broad range of security topics, these topics have been gleaned from software-specific incidents, so exploits or "hacks" involving the compromising of private information are not included (unless they involve a specific security component). All hyperlinks below go to the corresponding Wikipedia page, which you may use as one reference, but you are expected to go to primary and other secondary references as well (more below).

1. **United States federal government data breach** – *This is the famed "SolarWinds" exploit of late 2020. The broader attack also included Microsoft and VMWare.*
2. **Zoom software vulnerabilities** – *Zoom has become pervasive since the advent of the COVID-19 pandemic. But even before the pandemic started, it has experienced software-related exploits. The Wikipedia page link to the security section includes exploits from the past 3 years (2018, 19, and 20). Delve into the details of these attacks and actions taken.*
3. **CryptoLocker Ransomware attack** – *While ransomware has been around for a while, this attack from 2013 seems to have set off a wave of ransomware attacks in recent years.*
4. **Idaho National Laboratory Data Breach** – *Hacktivists breach U.S. nuclear research lab and steal employee data. The attackers openly leaked stolen data on hacker forums and a Telegram channel run by them, not caring to negotiate with the victim or demand ransom.*
5. **Attacks on critical infrastructure** – *A significant risk are vulnerabilities in a nation's infrastructure, including the power grid, water supply, or fuel supply. Some example attacks include the Ukraine Power Grid attack in 2015,the Florida water supply (2021), and the Colonial Pipeline ransomware attack of 2021.*
6. **Toyota Financial Services (TFS) Ransomware Arrack** – *A Toyota Financial Services (TFS), a subsidiary of the popular automaker, has confirmed suffering a ransomware attack. The company stated that Toyota Financial Services Europe & Africa "recently identified unauthorized activity on systems in a limited number of its locations."*
7. **Slack's Github Account Hack**– *On December 29, 2022, Slack, one of the most popular business communication tools has become victim to a hacker. The threat actor had also downloaded private code repositories on December 27, but neither Slack's primary codebase nor were any customer data included in the downloaded repositories*.
8. **Kubernetes Cluster Hack** – *Kinsing malware targeting Kubernetes Clusters. Two paths of exploitation utilized: vulnerable images and misconfigured PostgreSQL servers.*
9. **The Social Engineering Twitter Hack of 2020** – *Twitter's influence on public discourse was undeniably at its peak in 2020, but so was its vulnerability to its largest exploit – a social engineering attack where several high-profile accounts were compromised. Teams looking into this attack should also explore ramifications for other high-profile social media platforms.*
10. **The Log4j attack of 2021** – Log4j is an open-source (Apache Foundation) logging platform widely used in all forms of web server deployments. This vulnerability led to a slew of sudden attacks across corporate networks.

Your team will vote on topics and then assigned a topic by Dr. Gary based on "best-fit" voting across all teams.

Critical Inquiry Guidelines:

Your case should address questions including but not limited to:

1. What exactly is the attack? Where did it come from? Trace its evolution (did it originate from prior attacks? how has it evolved over time [with examples]?) What other high-profile attacks are from a similar type of exploit in recent years? Are there ongoing risks from this type of attack?
2. Provide the particulars in the security fundamentals (Module 1) you learned – What was the asset? What was the threat? Who was the threat agent? What was the vulnerability? What was the exploit? Was CIA compromised?

3. In your opinion, was there a software engineering related process flaw? That is, a flaw in system security requirements? Design? Architecture? V&V? Construction? Indicate and provide a justification based on your supporting readings and any other evidence available.
4. Summarize the human dimension – were there secondary impacts to citizens? Were black and/or white hat hackers involved? Did engineers working in security face consequences? What was the financial impact?
5. What are the active questions related to this topic (what has happened since? Has it evolved in a new form? Has it been "closed off"?). How has it impacted the broader field of cybersecurity? Has it impacted government policy and regulations?

Process:

This is a discovery-based assignment. That is, I have given you cases and an initial set of questions, but you should use these as a starting point, not as a "checklist" to complete the assignment. You may use some or all of these activities.

- Find primary sources of evidence. *Primary* sources of evidence are those that present direct facts and observations of the incident, not hearsay or secondary analysis of the event. Primary sources tell you exactly what happened.
- Find opposing secondary sources. *Secondary* sources analyze the situation and provide subjective interpretation (often an expert viewpoint). Seek to find more than one interpretation. Consider the strength of the information and the interpreter.
- Use "valid" primary and secondary sources. You should find both scholarly and "gray" literature for your references. "Gray" literature are sources such as blogs, magazine articles, newspapers. These are often written with little to no peer review (having an editor does not make it peer-reviewed). These can be useful to capture expert opinion or "in-the-moment" interpretation, but are questionable for scientific validity. Scholarly literature items are in scientific venues (mostly journal and conferences) where experts and scientists peer-review the findings and conclusions for validity, and this process makes them more trustworthy.

Grading Criteria:

1. (10%) Does the paper cover the topic appropriately (proper level of depth and breadth)?
2. (15%) Does the paper explain the incident's origins, evolution, impact, and potential future impact?
3. (15%) Does the paper appropriately apply and identify the security concepts using the terminology taught in this course?
4. (20%) Does the paper provide a critical analysis of the incident in the context of software engineering with supporting evidence?
5. (15%) Is the paper based on appropriate sources (see Process)?
6. (15%) Is the paper properly formatted, and has correct spelling, punctuation, and grammar?
7. (10%) Is the paper well-written with a proper flow?

As you can interpret from these 7 criteria, items 1-4 are qualitative based on the content of the paper itself and how well you apply the concepts in this class and in software engineering. Criteria 5-7 are assessed based on proper references and citations, proper writing format, and proper writing structure.

I do understand that you are not asked to write many analytical style papers with evidence as references. I am happy to do a preliminary "brief" review of a draft of your paper to provide tips. This is not a preliminary grade, it is an opportunity to gain formative feedback on how one interprets your written communication. You would have to email the draft to me with Subject Line "DRAFT 335 Case Study) at kgary@asu.edu no later than one week before the deadline to get feedback in time to help you.

Submission and Paper Style Guidelines

- Submissions of a Microsoft Word document (not PDF) will be made on Canvas.
  - Late submissions are not accepted.
  - If you wish to use an alternative word processing program please ask me first.
- Your paper must have at least 6 references (in addition to the Wikipedia or other pages I give you!)
  - At least 2 additional reference (other than Wikipedia) to provide factual descriptions (primary evidence)
  - At least 2 additional gray literature sources – trade magazines, industry white papers or reports, bogs – not peer-reviewed
  - At least 2 scholarly literature sources – papers appearing in peer-reviewed conferences or academic journals
    - Use Google Scholar or ASU's Library "OneSearch" to find such references
    - In your references be sure to list properly, not just give a URL to somewhere.
- Your paper should be 4-5 pages single column single-spaced in the ACM format template provided. No modifications to page margins, spacing, fonts, and font sizes are allowed. Images, figures, charts, or tables will only count for a maximum of 1-page of the overall page length. References are not included in the page requirement.
- Your paper must use proper spelling, punctuation, and grammar.
- Your paper should follow a logical flow, with clearly-defined sections, section introductions and conclusions, and transitions between sections that make the paper flow properly. You are working in a team but I expect the paper to look and read like it was written by one person!

Plagiarism:

Plagiarism is a form of cheating and is not allowed. I consider it cheating and will give you a zero and subject you to the additional terms in the syllabus under Academic Integrity Violations. Plagiarism can take many forms:

- Using someone else's written work without proper attribution. This includes things you find on the Internet, your classmates work, or your Mom's handwritten notes.
- It also includes quotes from the papers you reference – if you use a direct quote then it must be properly presented (an inline quote or a blockquote) with a proper citation format. No more than 1-page of length should be direct quotes.
- When you take an idea or evidence, even paraphrased from a paper, the paper should be cited.
- Rearranging words of a sentence/paragraph from someone else's work and calling it yours is plagiarism (you must cite the work).
- You are not allowed to use Generative AI tools like ChatGPT, CoPilot , etc. You may use AI-powered spelling and grammar checkers (e.g. Grammarly).

There is zero tolerance for plagiarism. If you don't know what it is or have any concern, come see me about it. It is your responsibility to prevent this on your paper, work with your partner! If one person of the team plagiarizes the entire team fails!

A significant part of your grade is the ability to demonstrate skills required for critical inquiry. These skills include finding and citing proper evidence. They also include framing an argument, supporting viewpoints with evidence, presenting opposing viewpoints, analyzing technology, and putting forward a professional presentation. Consider these requirements for your paper.

Finally, I want to emphasize that this is a team project. You and your partner share equal responsibility for ALL aspects of the paper. This means (for example, but not limited to) the paper should read as if it were written by one person, all are responsible for all content and aspects listed in the grading criteria, and plagiarism is a shared penalty (to be clear, I will give a zero and invoke the AIP against all team members for such an incident, not just an individual).