

The **updated course outline** is at: <https://people.scs.carleton.ca/~paulv/5407/jan2022.html>

The project involves detailed technical explanation and discussion of two software security incidents:

1. Log4Shell (CVE-2021-44228) from Nov 2021; and
2. the “supply chain” attack on the SolarWinds’ Orion product from Dec 2020.

Students are to independently find source materials (this typically involves considering a large number of candidate sources), cross-check these for consistency and to gain a solid understanding, and then produce an **original, in-depth** technical report.

The report should be **between 15 and 20 pages** (excluding cover page, which is unnecessary).

It should include a detailed technical summary of each incident in your own words; explain if **violation of any security principles** were enabling factors; discuss the societal impact; and suggest remedies or defenses that could prevent similar incidents in the future.

The form should roughly resemble a survey paper (look at those we are reading in class).

The exact structure is left open to allow a variety of styles—but you should begin with an abstract, and formally list your references (properly formatted) in a separate end-of-report section.

Provide your own insights and opinions—supported by convincing reasoning and explanations.

Use figures and diagrams to improve explanations, but they must all be of your own creation (no cut-and-paste or screen-captures in this course). If you redraw or modify existing diagrams, you must cite the source in the caption and explain this (otherwise plagiarism issues arise).

CAREFULLY re-read the instructions at “**DETAILS for all WRITTEN DELIVERABLES**” in the course outline (URL at top of page), for a reminder of the specific requirements regarding:

- **Font size and layout.** 11-pt font, single column, single spacing, no excessive white space.
- **No cutting-and-pasting or screen captures.** Neither is allowed in this project. All tables and images used must be self-created, while still citing sources for ideas.
- **Formal references.** See the URL for explicit details specifying the required style.
- **Grammar and clarity.** Beware the **deduction up to 20%** for failing to meet expectations.
- **Individual work.** Re-read the ACADEMIC INTEGRITY policy; **never plagiarize or copy.**
- **Strict deadline.** Due **11:59pm**, Friday Feb 25, 2022. The **late deduction** is 2/20 (10%) **per day** (including part days).
- **Submission mode:** through Brightspace.

Additional advice:

- ❖ **Start early.** *No additional material will be provided in class, beyond these instructions.* You should have sufficient knowledge for this project from your pre-requisite courses.
- ❖ **Provide context and overviews.** Keep your reader in mind as you write and proof-read.
- ❖ Aim to be **self-contained**. Avoid jargon. Define all special notation and terminology used.
- ❖ Be sure to **explain the technical details** underlying each incident, and the **societal impact**.

Grading scheme: 20 marks. See above regarding **deductions**.

- 5 marks: **context** and being **self-contained**; explain or cite background where it is helpful.
- 5 marks: inclusion of technical **details** that **convey a technical understanding** to the reader.
- 5 marks: **clarity** and **accuracy** of technical discussion (correctness in details).
- 5 marks: **insights, original observations, and overall quality** of the report.