COMP 5407 **Grading Rubric for Project 2 (Bluetooth Security)** **23 Feb 2022**
30% of term mark

Project 2 is to deliver an **in-depth, original, up-to-date** technical survey on Bluetooth security, beyond the older material covered in class. Class material may be included as background to position your main content. Some other early Bluetooth documents that might help include those listed below Class 12 on the course outline at: https://people.scs.carleton.ca/~paulv/5407jan2022.html

Students should independently find reference materials from a wide variety of sources, use them to gain a solid understanding, and then create an original report from the most useful of these sources. *Provide your own insights*. **Support opinions** with convincing reasoning and explanations.

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

Its 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 it must begin with an abstract, and formally list your references (properly formatted) in a separate end-of-report section.

Use figures and diagrams to improve explanations, but they must all be of your own creation. If you redraw or modify existing diagrams, cite the source in a caption (to avoid plagiarism issues).

CAREFULLY re-read the "**DETAILS for all WRITTEN DELIVERABLES"** from the course outline, 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 April 15, 2022. Submit through Brightspace.
  The late deduction is 3/30 (10%) **per day** (including part days).

Additional advice:

- **Start early.** *No further instructions are needed, beyond this page and the course outline.*
- Clearly **declare your scope** at the outset of the report.
- Include **recent material** from major security conferences if possible, especially any "big four" venues (ACM CCS, IEEE Symp. Security and Privacy, USENIX Security, NDSS).
- Focus on **security aspects**, especially related to our curriculum on **authentication** (e.g., provisioning of initial keying material, device pairing, session key establishment). Draw on your knowledge from background courses on security and applied cryptography.
- Provide **context and background.** 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.
- **Include and explain technical details**. This helps demonstrate your own understanding.
- Reports judged to have potential for progression to a peer-reviewed publication get A+.

Grading scheme: 30 marks. See above regarding **deductions**.

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