Security Engineering Coursework 2: Operating Systems Security

Ross Anderson & Yuvraj Patel

Deadline 22/03/24 12:00 (Noon)

This coursework asks you to write a short (1250 words maximum, excluding references) review of three papers on the above topic.

1. *Linux Security Modules: General Security Support for the Linux Kernel*, Chris Wright, Crispin Cowan, Stephen Smalley, James Morris, and Greg Kroah-Hartman, USENIX Security 2002 (link).
2. *seL4: Formal Verification of an OS Kernel*, Gerwin Klein, Kevin Elphinstone, Gernot Heiser, June Andronick, David Cock, Philip Derrin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harvey Tuch, and Simon Winwood, SOSP 2009 (link).
3. *CURE: A Security Architecture with Customizable and Resilient Enclaves*, Raad Bahmani, Ferdinand Brasser, Ghada Dessouky, Patrick Jauernig, Matthias Klimmek, Ahmad-Reza Sadeghi, and Emmanuel Stapf, USENIX Security 2021 (link)

The format should be as follows (same as CW1):

- Summary: 1–3 paragraphs per paper describing each paper's key insights and results.
- Key Themes: Approximately 400 words discussing similarities and contrasts between the three works. Do they use similar methodologies? Do they come to similar conclusions?
- Legacy: Approximately 400 words. Here you should explore the citations within the papers and influential papers that cite these works (using, e.g., Google Scholar) to discuss how these papers have been interpreted over time and how they relate to other works. In addition, we expect you to reference at least ten other papers, describe their relevance, and back up or refute the arguments made in the original three papers.

This coursework is worth **25%** of your total mark – unlike the first, it will be marked summatively. You will submit your essay as a PDF file via Learn on the "Assessment" page. Word counts should be provided on your submission. Word counts significantly above the 1250-word limit will be penalized.

Scholarship

While we encourage you to discuss the papers on, e.g., Piazza, all text within essays must be **your independent work**, and you must not send text from your essay to anyone else other than the markers via Learn. Essays will be checked for similarity using automated tools and manual checking. Students are reminded of the school's policy on poor scholarship linked here.

Use of Large Language Models

We would like to remind students that essays must be your own work. You are not allowed to use LLMs such as GPT, Gemini, and Bard to generate summaries. We will be able to detect the superficial summaries that LLMs may generate and initiate disciplinary actions.

You are allowed to use LLMs with the initial brainstorming and identifying relevant related work to cite. You can also use LLMs for grammar and spell check.

You must write all the text yourself. Please do not cut and paste the text from elsewhere as it may be wrong or infringe copyright, which may trip a plagiarism detection alarm if the copyrighted material isn't properly cited.

Extensions

Extensions are permitted, and Extra Time Adjustments (ETA) for extensions are permitted **up to 6 days**.

Extensions, Extra Time Adjustment (ETA) for Extra Time, and Extra Time for Proofreader/Interpreter are permitted but cannot be combined. The maximum extension is up to 6 days or fewer if specified.

Penalty: If assessed coursework is submitted late without an approved ETA extension, it will be recorded as late and a penalty of 5% per calendar day will be applied for up to the specified number of calendar days (≤ 6), after which a mark of zero will be given.

For electronic submissions, the last version that has been submitted by the deadline will be the one that is marked (late submission will only be accepted if no submission in time has been made). If a student with an extension or either type of ETA submitted late beyond the specified extended deadline, a mark of zero will be given.