Instructions

The final exam consists in a *short, dynamic 10-15 min team oral presentation*, with 1 to 5 students per team, followed by questions aiming at establishing proper understanding of key notions and testing each student's personal involvement in the project. Students are expected to:

- *Provide precise context* (be it technological, economical, political...) so that their topic can be understood by fellow students.
- *Summarize their understanding* of the topic, including new skills acquired thanks to this course, articles provided and personal research.
- *Provide a live demo* that helps visualising the methods, breadth or impact of their topic in a concrete way.
- *Discuss critically and scientifically* the documents used for their preparation (including source identity, reliability and ties).
- *Provide all documents and source code* (slides, demos) prior to the defence.
- *Provide a 5–10 lines short abstract* of their topic.

The final grade will account for consistency and thoroughness, relevance, originality and depth; clarity and correctness of provided answers.

Note: Oral presentation may be in French or English, but *please avoid mixing the two*. Klingon is not an option.

About topics

Topics revolve around a recent research or press article. As such this article *is maybe not enough, or maybe too much* for your presentation, you should combine it with other sources (articles, research, discussion with other teams...) and decide where to cut and where to emphasise. In particular, especially for older sources, **make sure to update them if necessary**.

There is no obligation to discuss the whole article *but* you must present correct, clear notions; the overarching idea of your talk must be understood by layman audiences. **Do not merely summarise the paper you choose.**

Each article in the list can be accessed online for free, sometimes with additional resources (videos, code, etc.). Preparation time is estimated around 3 full days, interaction with other teams (including for setting up demos or during presentations) is very strongly encouraged.

Some of the topics are harder than others, you are welcome to ask questions (including to the authors!) early to avoid going in the wrong direction or to get a head start, and you will not be penalised for enquiring. That being said, I expect you to be honest about it, and **you will be graded on *your* work**.

Q & A

($?_1$) Can we choose freely our topic from the list? *Yes, you can.*

($?_2$) I do not understand something, may I ask questions? *Yes, in fact, you should.*

($?_3$) May the same topic be chosen by two teams? *Yes but only is there is no substantial overlap (e.g., one team deals with one aspect, the other team with another). Please coordinate yourselves..*

($?_4$) I would like to address a topic not in the list, is it possible? *We can talk about it. At the very least it should be based off a recent research or press article, or be original. In any case the teacher's approval is mandatory.*

($?_5$) I disagree with the article / I want to articulate my talk in a radically different way! *A critical approach is strongly encouraged, just make sure to have good arguments for your claims.*

($?_6$) That wasn't discussed in the lectures! *This is not a question. Welcome to the real world.*

Improving this course

This course was build for and by students, and will improve from your comments. If you wish to contribute (typos, ideas, remarks, wishes, or even teach), just send me a mail!

List of topics

1. *Attacking Electric Motors for Fun and Profit*, Jablonski and Wijesekera, 2019.
2. *Dragonblood: Attacking the Dragonfly Handshake of WPA3*, Mathy Vanhoef, 2019.
3. *All the 4G Modules Could be Hacked*, Gao–Xie–Huang–Ye, 2019.
   New Vulnerabilities in 5G Networks, Altaf Shaik, 2019.
4. *A Billion Open Interfaces for Eve and Mallory*, Stute et al., 2019.
5. *Why do Adversarial Attacks Transfer?*, Demontis et al., 2019.
   Seeing is Not Believing: Camouflage Attacks on Image Scaling Algorithms, Xiao et al., 2019.
6. *Wireless Attacks on Aircraft Instrument Landing Systems*, Sathaye et al., 2019.
7. *The Spies Hacking our Phones are Going Dark, and We're All in Trouble*, Scott-Railton and Marczak, 2019.
8. *50 Ways to Leak Your Data*, Reardon et al., 2019.
9. *The Tor Censorship Arms Race: The Next Chapter*, Dingledine, 2019.
10. *Harnessing Weapons of Mac Destruction*, Wardle, 2019
11. *GSM: We Can Hear Everyone Now!*, Murray and Kulikowski, 2019
12. *SSO Wars: The Token Menace*, Muñoz and Mirosh, 2019
13. *SELECT code_execution FROM * USING SQLite*, Gull, 2019
14. *State of DNS Rebinding*, Doussot and Meyer , 2019
15. *Confessions of an Nespresso Money Mule*, Kollars, 2019
16. *ZombieLoad: Cross-Privilege-Boundary Data Sampling*, Schwartz et al., 2019.
    Meltdown: Reading Kernel Memory from User Space, Lipp et al., 2018.
17. *RISC-V: #AlphanumericShellcoding*, Barral et al., 2019