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.*

($?_2$) May a same topic be chosen by two teams? *Yes but only if there is no substantial overlap (e.g., one team deals with one aspect, the other team with another). Please coordinate yourselves.*

($?_3$) 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 research-oriented.*

($?_4$) I do not understand something, may I ask questions? *Yes, in fact, you should.*

($?_5$) 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 solid 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. *SoK: Make JIT-Spray Great Again*, Gawlik and Holz, USENIX 2018
   New Trends in Browser Exploitation: Attacking Client-Side JIT Compilers, Groß, BlackHat USA 2018
   memory exploitation, browsers

2. *ROBOT: Return of Bleichenbacher's oracle threat*, Böck, Somorovsky and Young, USENIX 2018
   website security, crypto, side-channel

3. *Synesthesia*, Genkin, Pattani, Schuster, Tromer, (on arXiv) 2018
   Screaming Channels, Francillon et al., BlackHat USA 2018
   exfiltration, side-channel, signal processing

4. *Off-Path TCP Exploit*, Chen and Qian, USENIX 2018
   exfiltration, side-channel, network security

5. *The Air-Gap Jumpers*, Guri, BlackHat USA 2018
   exfiltration, side-channel

6. *OATmeal on the Universal Cereal Bus: Exploiting Android phones over USB*, Horn, Google Project Zero 2018
   Universal Serial aBUSe, Dawes and White, Defcon 2018
   exfiltration, phone security

7. *TLBleed: When Protecting Your CPU Caches is Not Enough*, Gras, BlackHat USA 2018
   Translation Leak-aside Buffer, Gras et al., USENIX 2018
   CPU, side-channel

8. *Foreshadow* and *Foreshadow-ng*, van Bulck et al., USENIX 2018
   CPU, side-channel

9. *Physical Adversarial Examples for Object Detectors*, Eykholt et al., WOOT 2018
   Machine Duping 101: Pwning Deep Learning Systems, Clarence Chio, Defcon 2018
   machine learning, self-driving cars

10. *Skill Squatting Attacks on Amazon Alexa*, Kumar et al., USENIX 2018
    machine learning

11. *Fast Message Franking*, Dodis et al., Crypto 2018
    facebook security, crypto

12. *Efail: Breaking S/MIME and OpenPGP Email Encryption*, Poddebniak, Dresen and Müller, USENIX 2018
    e-mail security, crypto

13. *Who Left Open the Cookie Jar?*, Franken, van Goethem and Joosen, USENIX 2018
    privacy, browsers, website security

14. *WebAssembly: A New World of Native Exploits on the Browser*, Engler and Lukasiewicz, BlackHat USA 2018
    exploitation, browsers

15. *Abusing Bleeding Edge Web Standards for AppSec Glory*, Zadegan and Lester, Defcon 2018
    website security

16. *A Geometric Approach for Real-time Monitoring of Dynamic Large Scale Graphs*, Salamatian, Kaafar and Salamatian, ACM IMC 2018
Cartographier les routes de l'Internet grâce à la commande Traceroute : l'exemple du Caucase du sud, Limonier, 2018
internet security, maths, geopolitics

17. *Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets*, van Wegberg et al., USENIX 2018
Reading Thieves' Cant, Yuan et al., USENIX 2018
economics, cybercrime

18. *Is the Mafia Taking Over Cybercrime?*, Lusthaus, BlackHat USA 2018
cybercrime