Security analysis of existing and new Web standards

Subject

To provide an even richer online experience, the web evolves at a frantic pace, introducing new functionalities every year. Recently, this translated to better usage of the hardware through low-level APIs like WebAssembly and WebGPU that take full advantage of the CPU and GPU, respectively. Other recent drafts look to extend access to connected hardware like WebUSB for USB devices, Web Bluetooth for Bluetooth ones, and WebXR for AR/VR reality headsets. Despite all the best efforts to consider security and privacy from the design phase, adding new APIs widens the browser's attack surface and can harm user's privacy.

The aim of this thesis is to measure the impact of these new web standards on the user's privacy and design generic defense techniques to increase privacy in case their security is lacking.

Profile and skills required

Master degree or equivalent is required. Knowledge of JavaScript is highly recommended while knowledge of fuzzers and the inner-workings of web browsers is optional but desirable.

Bibliography

- Schwarz, M., Lackner, F., Gruss, D., "JavaScript Template Attacks: Automatically Inferring Host Information for Targeted Exploits". In: NDSS. 2019.
- Olejnik, L., Acar, G., Castelluccia, C., Diaz, C., "The Leaking Battery - A Privacy Analysis of the HTML5 Battery Status API". In: DPM and QASA. 2015.
- Konoth, R. K., Vineti, E., Moonsamy, V., Lindorfer, M., Kruegel, C., Bos, H., Vigna, G., "MineSweeper: An In-Depth Look into Drive-by Cryptocurrency Mining and Its Defense". In: CCS. 2018.
- Reis, C., Moshchuk, A., Oskov, N., "Site Isolation: Process Separation for Web Sites within the Browser". In: USENIX Security Symposium, 2019

Contact

The PhD will take place in the Spirals team at Inria Lille from September 2022 to August 2025. To apply, send your CV and all your questions to Pierre Laperdrix, Clémentine Maurice, Romain Rouvoy and Walter Rudametkin.