Side Channel Attacks in the Browser

Case for Support

a six-page (maximum) Case for Support: an account of the motivation for the work, the approach being taken, and a breakdown of the work to be carried out (often in terms of ”workpackages”), plus a management plan (how will the project be managed such that it delivers what you have promised to do) and any other information that usefully describes the nature of the project being proposed)

Background

Side-Channel Attacks (SCA) are an important class of cryptanalytic techniques which target unintentional information leakage in order to disclose private data. In general, Side-Channel attacks monitor a device performing an interesting operation and try to find a correlation between the side-channel information and the internal state of the processing device which is related to the secret parameters involved in the computation. Side-channel information can be obtained by monitoring variations in the execution time (*Timing Attacks*), the power consumption (*Power Analysis*), the electro-magnetic emission (*Electromagnetic Analysis - EMA*), or the state of the cache memory (*Cache Attacks*) [1]. The goal of an attacker in side-channel attacks is to either recover the secret parameters involved in the computation by targeting faults in the implementation of some cryptographic algorithm, or disclose private information about a user, such as location or browsing history. Side-channel exploit vulnerabilities in a specific implementation rather than targeting an abstract algorithm, making them less generic but more powerful [1].

The expansion of the Internet determined browser vendors to add more and more features to their software in order to offer a richer, dynamic and more interactive web pages. The evolution of browser software not only improved the overall user experience but also opened the way for a new category of side-channel attacks known as browser attacks. These types of attacks target vulnerabilities in the browser software. Browser attack fall into two categories: traditional timing attacks which measure the time it takes the server to respond, and cache timing attacks which measure how long it takes to retrieve a resource from the browser’s cache memory.

Browser attacks are a very powerful category of side-channel attacks, which require minimal set up and affect a wide range of users. In general, these types of attacks require a user to navigate to an untrusted website, which contains attacker-controlled content. The web page has a background script which collects information about the victim which can be used by the attacker to infer a user’s location, browsing history, or even current browsing activity.

References

[1] François-Xavier Standaert. Introduction to side-channel attacks. In *Secure Integrated Circuits and Systems*, pages 27–42. Springer, 2010.

Budget

a one-page (maximum) Budget: a table/spreadsheet of expenditure

Justification For Resources

a one-page (maximum) Justification For Resources: essentially a written narrative on why you need the expenditure on each line-item in your budget

Impact Statement

a one-page (maximum) Impact Statement: a description of how you intend to ensure that your work makes a difference in the world, rather than sitting on a shelf gathering dust)

Workplan

and also a one-page (maximum) Workplan:typically a GANTT chart or similar diagram indicating the order in which workpackages are carried out)