

Seminar

# Side-channel leaks in web applications

Unlike a desktop application, a web application is split into browser-side and server-side components. Between both sides typically a lot of information needs to be exchanged. In order to secure this traffic, encryption methods are applied. Side-channel leakage often goes hand in hand with encryption and it has been shown, that it can be exploited even in web applications.

The goal of this topic is to exemplary state different threat models and the information an attacker can gain from exploiting them. Furthermore, the opportunities and limitations compared to classical side-channel analysis on non-web applications should be evaluated.

## References:

- Chen, Shuo, et al. "Side-channel leaks in web applications: A reality today, a challenge tomorrow." 2010 IEEE Symposium on Security and Privacy. IEEE, 2010

## Contact

[Request Topic](#)

## Advisors

Matthias Probst