Privacy and Security in Mozilla Firefox

Marc Kaeser

Master thesis in Computer Science

As a master thesis, this work was intended to give an overview about a specific topic, to allow deepening of a chosen matter in order to learn, understand, and finally modify the code in order to achieve a defined goal. This thesis was written in the scope of the FDS (Foundations of Dependability and Security) Research Group of the Departement of Computer Science at the University of Fribourg (Switzerland), and deals with privacy and security in the Mozilla Foundation's well known web browser Firefox. The main objectives were to find a way to increase both privacy and security by using a Trusted Platform Module (TPM) in order to hide and protect stored credentials for web pages, and cookies in a further step. The difficulty and the challenge of the work turned out to lay in the understanding of the many existing lines of code. In a long work of reverse engineering, the way to put pieces of a large puzzle together by modifiying them in a very precise way had to be learned. The result is a Firefox built that connects to a TPM to protect the symmetric key used by Firefox to encrypt logins and passwords for web sites. It also uses the MD5 message digest algorithm to hide private information contained in HTTP cookies. This work provides a view into the XPCOM framework of the Mozilla Foundation which had to be modified in order to achieve the changes just mentioned. Unfortunately, the implemented changes are not advanced enough to be checked into the source code at Mozilla Foundation, but manage to prove the viability of the concept.

The following chapters show how it is proven, starts with a large scope that becomes precise in the end, and after having explained several facets of the work done and the different technologies used, gives an overview of what had to and what still could be done.

Prof. Ulrich Ultes-Nitsche