Saal: Project 22:30 01:00 Day: 4 Track: Security & Hacking nA 2501

Title: **TLS interception considered harmful**

Subtitle: How Man-in-the-Middle filtering solutions harm the security of HTTPS

Speaker: **hanno**

Short: *With the more widespread use of encrypted HTTPS connections many software vendors intercept these connections by installing a certificate into the user's browser. This is widely done by Antivirus applications, parental filter software or ad injection software. This can go horribly wrong, as the examples of Superfish and Privdog have shown. But even if implemented properly these solutions almost always decrease the security of HTTPS.*

Long: In February a software called Superfish was detected preinstalled on Lenovo laptops that would intercept HTTPS connections by installing a certificate into the user's browser. This certificate was shared amongst different installations and therefore an extraction of the certificate allowed creating rogue certificates that would be accepted by many Lenovo laptops. Shortly after Superfish many other software products with the same or similar vulnerabilities were found. The speaker of this talk discovered that the software Privdog, advertised by the certificate authority Comodo, had an even worse vulnerability. Superfish and Privdog were extreme examples, but the technology of intercepting HTTPS connections by installing X.509 root certificates into the browser is widespread. These solutions are often part of software that is supposed to bring more security to the user - like Antivirus applications - but they lower the user's security. For example Kaspersky Antivirus users were still affected by the FREAK vulnerability months after the issue was found and fixed. The talk will first give an introduction into some problems in the TLS protocol that were found in recent years (BEAST, CRIME, FREAK, CA failures) and show some technologies that were invented to prevent common problems of TLS (e. g. HPKP). After that the speaker will give some examples of TLS interception software and how it endangers the security of the user.