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

Chef: 2433 Lindworm: 5463 Emergency: 112 Security: 110 Heaven: 1023 Speakers Desk: 1020 Info Desk: 1111

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.