Project 2501 12:45 01:00 Day: 5 Track: Security & Hacking en

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

Translation (check if available): 8011 Technical Coordinator: 1611

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 soft-

browser. This is widely done by Antivirus applications, parental filter software or

ware vendors intercept these connections by installing a certificate into the user's

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.