Wie wird mein Online-Banking wieder sicher? Die Folgen von SSL/TLS Interception und was uns davor schützen kann

---

Zusammenfassung:

Die Methoden für Sicherheit beim Online-Banking entwickeln sich mit der Zeit stetig weiter. Damit nehmen auch die Methoden zu, welche Angreifer nutzen, um Sicherheitsbarrieren zu durchbrechen.

Neben Fehlern in der Implementierung seitens der SSL Entwickler, gefälschten Zertifikaten oder gebrochenen Verschlüsselungen, bildet TLS Interception einer der größten Gefahren für SSL/TLS. Dafür genügt ein man in the middle Angriff mit einem interception Proxy.

Diese Präsentation hat sich das Ziel gesetzt, die aktuelle Situation hinsichtlich der Verwundbarkeit von SSL/TLS beim Online-Banking zu analysieren, sowie potenzielle Lösungen vorzustellen, um sich davor zu schützen. Es wird auf die Funktionsweise von TLS, den bekannten Schwachstellen und insbesondere auf TLS Interception eingegangen.

Abstract:

The methods for secure online banking evolve continuously over time. But not only security measures increase. At the same time online banking is also facing new methods to break the security systems.

In addition to implementation errors, written by the SSL developers, faked certificates or broken encryptions, TLS Interception is a much higher risk for online banking. All you need is an interception proxy and a man in the middle attack.

The goal of this presentation is to analyze the current situation, regarding the vulnerability of SSL/TLS while online banking, as well as showing possible solutions to stay secure. The presentation covers the functionality of TLS, known issues regarding the security and especially TLS Interception.

Überblick:

1. Geschichte von SSL/TLS
2. Funktionsweise von einem TLS Handshake
3. Bekannte Schwachstellen von TLS
4. Wieso sind diese Schwachstellen heute noch problematisch?
5. Sicherheitscheck von der Haspa und der Postbank
6. Wie funktioniert TLS Interception?
7. Wozu TLS Interception?
8. Schwachstellen von TLS Interception
9. Was kann man dagegen machen?
10. Fazit
11. Quellen

Quellen:

- https://www.ibm.com/developerworks/library/ws-ssl-security/
- https://tools.ietf.org/html/rfc5246
- https://blog.qualys.com/ssllabs/2013/09/10/is-beast-still-a-threat
- https://upload.wikimedia.org/wikipedia/commons/8/80/CBC_encryption.svg
- https://tools.ietf.org/html/rfc7507
- https://media.blackhat.com/bh-eu-12/Jarmoc/bh-eu-12-Jarmoc-SSL_TLS_Interception-Slides.pdf
- https://www.globalsign.com/de-de/blog/was-ist-certificate-transparency/
- http://www.elektronik-kompendium.de/sites/net/1906251.htm