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

Vortrag von Nikolaus Khaled
24.05.2016

Inhalt dieses Vortrags:

- Geschichte von SSL/TLS
- Funktionsweise von einem TLS Handshake
- Bekannte Schwachstellen von TLS
- Wieso sind diese Schwachstellen heute noch problematisch?
- Sicherheitscheck von der Haspa und der Postbank
- Wie funktioniert TLS Interception?
- Wozu TLS Interception?
- Schwachstellen von TLS Interception
- Was kann man dagegen machen?
- Fazit
- Quellen

Geschichte von SSL/TLS

- Gegründet von Netscape Communications im Jahr 1990
- Ziel ist es eine sichere Kommunikation zwischen Client und Server, über einem ungeschütztem Netzwerk zu gewähren
- Bis heute Standard für kryptographische Protokolle
- Bietet Datenschutz, Integrität der Daten und Authentifizierung von einem oder beiden Kommunikationsendpunkten
- SSL trägt zur Sicherheit von Emails, Telefonate, Datenübertragungen, HTTP und viele mehr bei
- 1999 verabschiedet die IETF eine verbesserte Version von SSL v3, genannt TLS 1.0, aktuellste Version momentan TLS 1.2

TLS Handshake

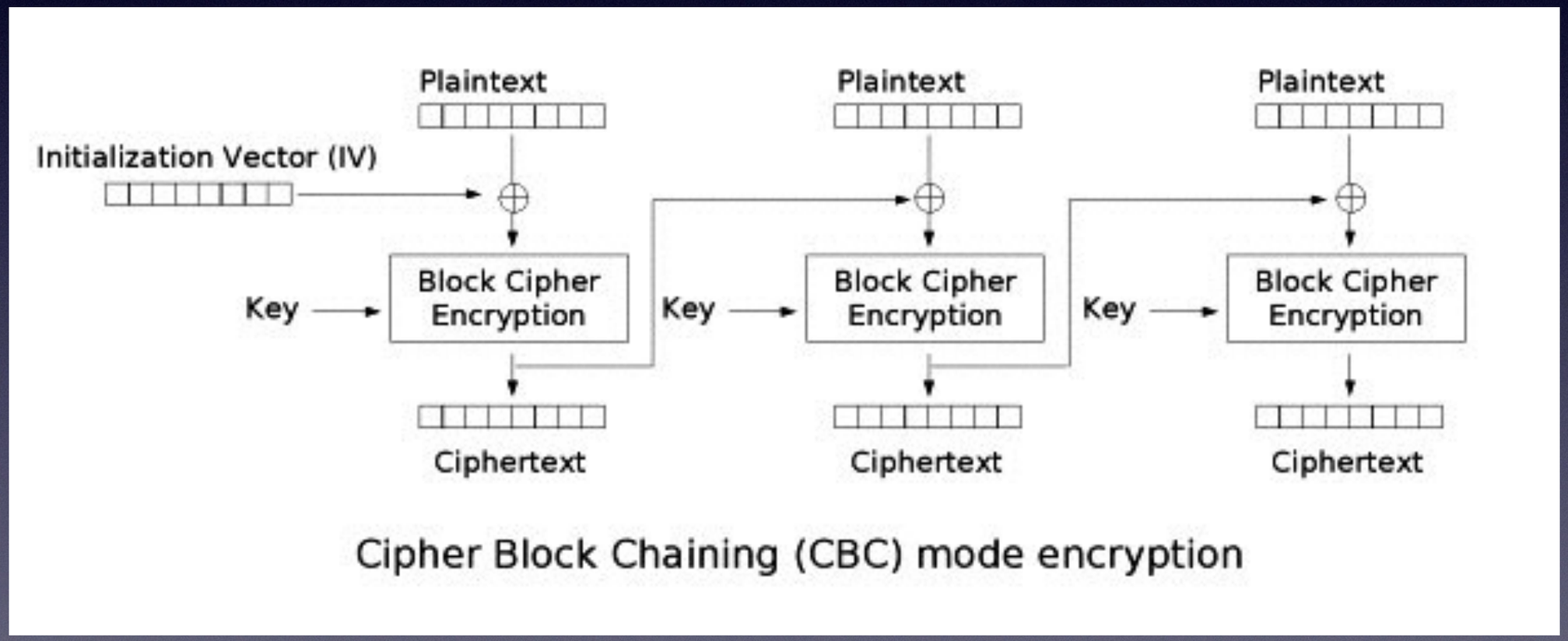
Client		Server
ClientHello	——>	
		ServerHello Certificate + Public Key ServerKeyExchange CertificateRequest ServerHelloDone
	<——	
Certificate Symmetric Session Key ClientKeyExchange CertificateVerify [ChangeCipherSpec] Finished	——>	
		[ChangeCipherSpec] Finished
	<——	
Application Data	<——>	Application Data

Bekannte Schwachstellen von SSL/TLS

- BEAST (Browser Exploit against SSL/TLS)
  - Anwendbar auf TLS 1.0 und älter
  - Angriff auf den Operationsmodus CBC (Cipher Block Chaining)
  - Durch MITM Angriffe können Initialisierungsvektoren, bevor sie mit Cipher Blöcken verschlüsselt werden, vorhergesagt werden und auf Richtigkeit geprüft werden

Bekannte Schwachstellen von SSL/TLS

BEAST CBC Funktionsweise



https://upload.wikimedia.org/wikipedia/commons/8/80/CBC_encryption.svg

Wieso sind solche Schwachstellen heute noch problematisch?

- Online-Banking Seiten unterstützen meistens TLS 1.0 bis TLS 1.2, im schlimmsten Fall auch SSL v3

- Grund hierfür ist die Kompatibilität für ältere Browser zu gewähren, die kein TLS 1.2 implementiert haben

- Selbst wenn Client und Server TLS 1.2 implementiert haben, können Downgrade Angriffe dafür sorgen, dass man über das unsichere und 17 Jahre alte TLS 1.0 kommuniziert

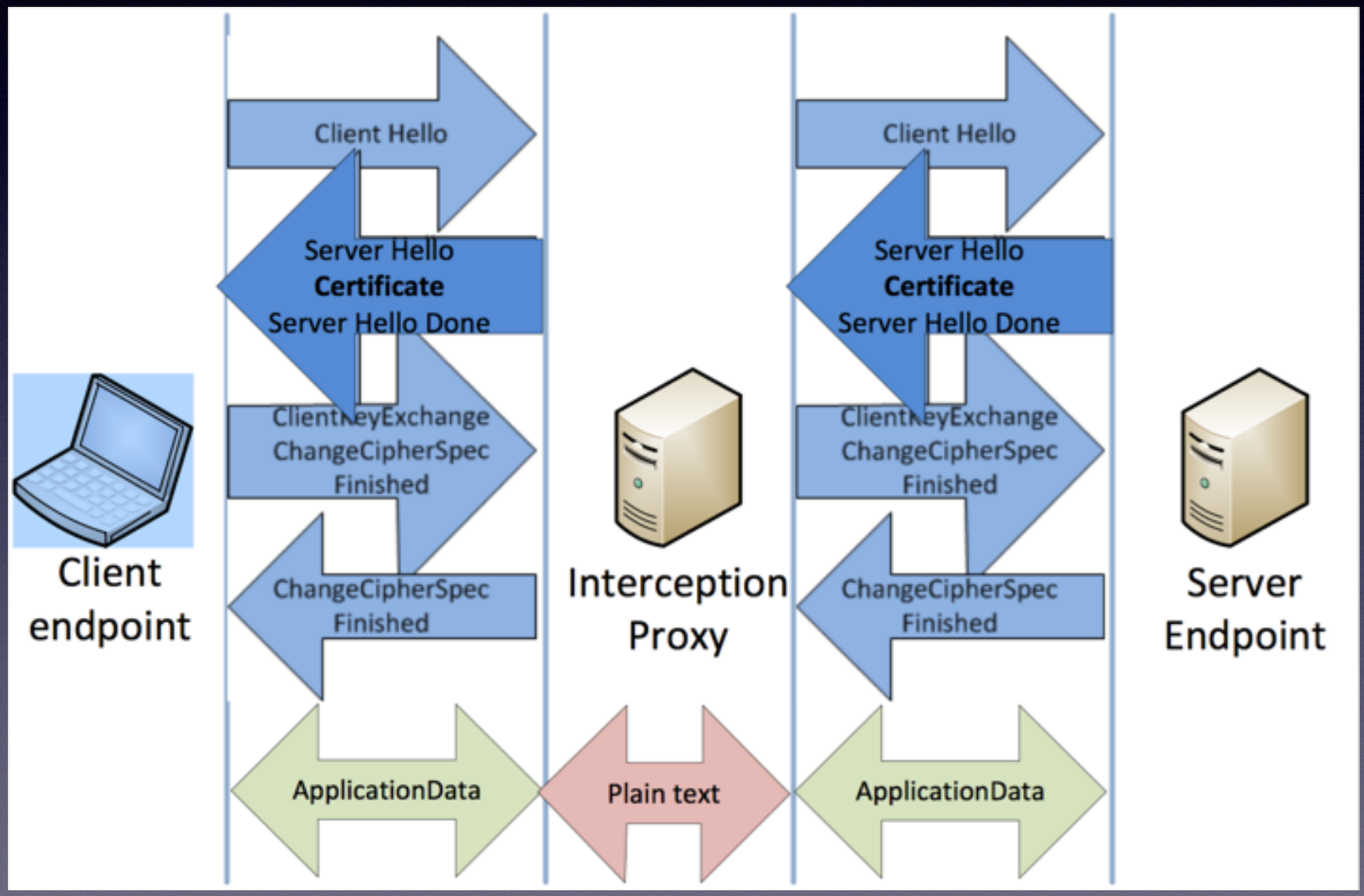
- TLS Fallback Signaling Cipher Suite Value ist eine TLS Erweiterung, welche den Client warnt,

Sicherheitscheck von Haspa und Postbank

- Um die Sicherheit zu überprüfen, wird auf ssllabs.com/ssltest/index.html ein Sicherheitscheck ausgeführt

- Ziel ist es zu schauen, welche Protokolle unterstützt werden und wie die Verwundbarkeit zu einigen TLS Angriffen aussieht

Wie funktioniert TLS Interception?



https://media.blackhat.com/bh-eu-12/Jarmoc/bh-eu-12-Jarmoc-SSL_TLS_Interception-Slides.pdf

Wozu TLS Interception?

- Durch TLS Interception kann der Datenverkehr zwischen Client und Server überwacht werden

- Firmen nutzen dies, um das Surfverhalten Ihrer Mitarbeiter beispielsweise auszuspähen und somit prüfen zu können, ob Firmeninterne Geheimnisse weitergegeben werden, ohne das die Mitarbeiter das merken

- Dadurch kann auch die Wahrscheinlichkeit minimiert werden, dass Malware seinen Weg auf einen Client PC findet, indem HTTP Verbindungen zu bestimmten Servern blockiert werden

Schwachstellen von TLS Interception

- Angreifer können, agierend als TLS Proxy den Datenverkehr auslesen
- Durch gezielte MITM (man in the middle) Angriffe kann der Angreifer die Kommunikation vom Client abfangen und anschließend manipuliert an den Server weiter schicken. Die Antwort vom Server wird ebenfalls abgefangen und manipuliert an den Client gesendet
- Client ist auf den Proxy angewiesen, welcher entscheidet, ob ein Server seitiges Zertifikat valide ist oder nicht
- Server Identität kann nicht mehr unabhängig vom Client verifiziert werden
- 2 verschiedene Cipher Suite Verhandlungen, welche dazu führen können, dass schwächere kryptographische Verfahren angewendet werden, als eigentlich unterstützt
- Proxy ist somit ein hochwertiges Ziel für einen Angreifer

Was kann man dagegen machen?

- Die Benutzung von Certificate Transparency, welche die Zertifikatsausstellung einer CA für Überwachung und Überprüfung offen macht

- Transparenz dadurch, dass CA Zertifikate auf öffentlich zugänglichen qualifizierten CT-logs registriert werden

- Verhindert keinen Angriff, macht ihn jedoch transparent und ersichtlich, sodass sich Angriffe nicht mehr verstecken lassen

Was kann man dagegen machen?

- Verwendung von DANE (DNS-Based Authentication of Named Entities) und DNSSEC (Domain Name System Security Extensions)
- DANE verhindert Angriffe, welche auf unrechtmäßig ausgestellten Zertifikaten basieren
- Unrechtmäßig erstellte Zertifikate sind zwar aus technischer Sicht einwandfrei, haben jedoch einen unterschiedlichen Fingerabdruck
- Um DANE zu nutzen, hinterlegt der Server Betreiber den Fingerabdruck seines TLS Zertifikats zusammen mit dem Public Key als TLSA Eintrag im DNS
- DANE kontaktiert mit Hilfe von DNSSEC den DNS des Hosts, um das Zertifikat zu prüfen und nicht wie üblich die CA, dabei bekommt der Client gleichzeitig den Public Key
- DNSSEC gewährleistet Authentizität vom Client und macht DNS Manipulation sichtbar
- Client berechnet mit dem Public Key vom Host einen Hash, den er mit dem Fingerabdruck aus der DNS vergleicht. Sind beide gleich, kann der Verbindung vertraut werden

Fazit

- In den letzten Monaten werden immer mehr Techniken entwickelt, welche sehr viel versprechend sind und viel zur Sicherheit im Internet und beim Online Banking beitragen

- Es gilt sich langsam von 17 Jahre alten Protokollen zu verabschieden und neue sicherere Protokolle als Standard für den Datenaustausch zu erzwingen

- Immer auf dem neuesten Stand bleiben und die Entwicklung im Auge behalten

- DANE zusammen mit DNSSEC könnten einen erheblichen Beitrag zur Cybersecurity beitragen, sind jedoch noch nicht weit verbreitet, obwohl das Vertrauen in Zertifikate von CA in den letzten Jahren sich nicht immer als gut erwiesen hat

- Certificate Transparency verspricht ebenfalls mehr Sicherheit, wird jedoch wie DANE und DNSSEC noch nicht häufig verwendet

Vielen Dank

Quellenangaben

- Folie 3: https://www.ibm.com/developerworks/library/ws-ssl-security/
- Folie 4: https://tools.ietf.org/html/rfc5246
- Folie 5: https://blog.qualys.com/ssllabs/2013/09/10/is-beast-still-a-threat
- Folie 6: https://upload.wikimedia.org/wikipedia/commons/8/80/CBC_encryption.svg
- Folie 7: https://tools.ietf.org/html/rfc7507
- Folie 9 - 11: https://media.blackhat.com/bh-eu-12/Jarmoc/bh-eu-12-Jarmoc-SSL_TLS_Interception-Slides.pdf
- Folie 12: https://www.globalsign.com/de-de/blog/was-ist-certificate-transparency/
- Folie 13: http://www.elektronik-kompendium.de/sites/net/1906251.htm