SVS Bachelor-Projekt Network Security

Blatt 6: Kryptographie

Louis Kobras
6658699

Utz Pöhlmann
6663579

1 Absicherung des TCP-Chats mit SSL

2 CAs und Webserver-Zertifikate

2.2 Selbstsignierte Zertifikate

Es wurde in mehreren Läufen die Fallstudie durchgearbeitet. Und zwar mehrmals und sowohl zusammen als auch einzeln und unabhängig voneinander. Mit dem Ergebnis, dass der Apache2-Server nicht funktioniert. Die Gruppe neben uns, denen wir inzwsichen bestimmt mega auf den Keks gehen und denen ich als Wiedergutmachung ein Eis mitgebracht habe, konnte uns leider auch nicht helfen. Unsere certs und pems und reqs und keys und csrs wurden alle ordnungsgemäß erstellt und Schritt für Schritt, Wort für Wort nach der Fallstudie erzeugt und bearbeitet. Es ist kaputt. Selbst Reboots und Reinstallationen helfen nicht. Folglich funktionieren Aufgabe 2.1ff nicht. Mal wieder. Sind wir echt so blöd oder liegt vielleicht ein Fehler auf unserer Maschine vor?

2.3 HTTPS-Weiterleitung

.

2.4 sslstrip

sslstrip wurde nach [1] installiert und gestartet.
Die Verbindung wurde am "svs.informatik.uni-hamburg.de" erkannt. (IP: 134.100.15.55)
Die Browsereinstellungen wurde unter `Edit` → `Preferences` → `Advanced` → `Network` → `Connection` → `Settings...` auf `localhost` und Port `8080` gesetzt. Zudem wurden die `No Proxy for`-Einstellungen entfernt.
Der Inhalt der Datei: vgl. [ssllog (S. 3)] Die Lösung aus Aufgabe 2.3 ist somit definitiv ein Plus an Sicherheit. Der Sinn von HSTS ist, sich vor sog. "downgrade Attacks" zu schützen. Hierbei wird der Client dazu gewzungen statt einer "modernen" sicheren Verbindung eine "alte" unsichere Verbindung aufzubauen. (Bsp.: HTTP statt HTTPS) Ein weiterer Nutzen ist, "Session Hijacking" zu unterbinden. Hier wird ein Authentifikationscookie abgefangen und so ein Man-In-The-Middle-Angriff gestartet. Da HSTS Webservern erlaubt, auf Browser den Zwang einer sicheren Verbindung (via HTTPS) auszuüben, sind alle Server, die diese Möglichkeit nutzen, auch sicher vor SSL-Stripping-Angriffen.

3 Unsichere selbstentwickelte Verschlüsselungsalgorithmen

3.1 BaziCrypt

.

3.2 AdvaziCrypt - Denksport

.

3.3 AdvaziCrypt - Angriff implementieren

.

4 EasyAES

5 Timing-Angriff auf Passwörter (Bonusaufgabe)

Literatur

[1] https://moxie.org/software/sslstrip/

ANHANG

ssllog