Nutzerauthentifizierung

Dozent: Prof. Dr. Michael Eichberg

Kontakt: michael.eichberg@dhbw.de

Version: 1.0

Folien: [HTML] https://delors.github.io/sec-nutzerauthentifizierung/folien.de.rst.html
[PDF] https://delors.github.io/sec-nutzerauthentifizierung/folien.de.rst.html.pdf

Fehler melden: https://github.com/Delors/delors.github.io/issues

1. Grundlagen

Challenge-Response Authentifizierung

Beobachtung

Die Verwendung einer (kryptographischen) Hashfunktion alleine ist nicht ausreichend zur sicheren Benutzerauthentifizierung über eine nicht-sichere Verbindung. Eine einfache Replay-Attacke ist möglich.

Ein einfaches Challenge-Response Protokoll (*Herausforderung- und Antwortprotokoll*) basierende auf einer Hashfunktion f wäre:

Alice	unsicherer Kanal	Bob
Gibt Benutzerkennung ein: ID	→ sendet ID	sucht zu ID Schlüssel K in der Datenbank
		↓
Gibt Passwort K' ein	sendet r ←	wählt zufällige Zahl r
		↓
berechnet: $Res' = f(K', r)$	→ sendet Res'	$f(K, r) \stackrel{?}{=} Res'$

? Frage

Wie bewerten Sie die Sicherheit (dieses Protokolls)?

Zero-Knowledge Protokolle

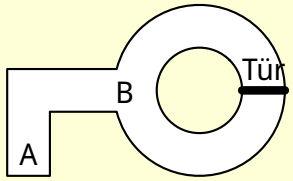
Die Idee ist, dass man jemanden davon überzeugen möchte, dass man eine bestimmte Information hat, ohne diese Information zu offenbaren.

Beispiel

Der geheimnisvolle Geheimgang

Peggy möchte Victor überzeugen, dass Sie den Code zur Tür kennt, ohne ihn zu offenbaren.

- Peggy wählt einen der Wege zur Tür, während Victor an der Stelle A steht und darauf wartet, dass Sie bei der Tür ist.
- Sobald Peggy bescheid gibt, dass Sie an der Tür angekommen ist, geht Victor zu Punkt B und sagt Peggy auf welchem Weg sie zurückkommen soll.
- Kommt Sie auf dem falschen Weg zurück, dann kennt sie den Code der Tür (offensichtlich) nicht. Kommt Sie auf dem richtigen Weg zurück, könnte es noch immer Zufall gewesen sein mit Wahrscheinlichkeit $\frac{1}{2}$.



Wird das Spiel jedoch n mal gespielt und Peggy kommt immer auf dem richtigen Weg zurück, dann ist die Wahrscheinlichkeit, dass Peggy immer zufällig den richtigen Weg genommen hat $\frac{1}{2^n}$.

Viele Zero-Knowledge Protokolle basieren darauf, dass man im Prinzip ein Spiel spielt, das man auch zufällig gewinnen kann. Durch die Wiederholung des Spiels wird die Wahrscheinlichkeit jedoch für permanentes zufälliges gewinnen sehr schnell sehr klein (exponentiell). Somit kann man für praktische Zwecke hinreichend sicher sein, dass der Beweisführende (im Beispiel Peggy) über das Wissen verfügt, dass er vorgibt zu besitzen, wenn er immer gewinnt.

Nach 20 Runden ist die Wahreinschlichkeit nur noch $1/2^{20} = 1/1\,048\,576$.

Mit 128 Runden erreicht man ein Sicherheitsniveau, dass vergleichbar ist mit anderen kryptographischen Verfahren (AES-128, SHA-256, ...).