2BPR

Blind Password Registration for Two-Server Password
Authenticated Key Exchange and Secret Sharing Protocols

Nach dem gleichnamigen Paper von Franziskus Kiefer und Mark Manulis

1. Hintergrund

2PAKE = Two-Server Password Authenticated Key Exchange
2PASS = Two-Server Password Authenticated Secret Sharing
Auf mehreren Servern (meist 2) wird jeweils ein Passwortteil (Share genannt) gespeichert. Beim Userlogin arbeiten die Server ähnlich wie bei Diffie-Hellman zusammen, um den User anzumelden.

\+ Man kann beiden Servern zu 100% vertrauen
\+ Sicher gegen Brutforce + Sicher gegen Man-in-the-Middle

2. Motivation

Die Kontrolle der Passwortrichtlinie ist bisher unmöglich
Kein Server darf genügend Informationen erlangen, um das Passwort zu rekonstruieren
\+ Wir erhalten als Ergebnis ein festdefiniertes Protokoll, an das man sich halten kann

3. Begriffe

COMMITMENTS

Binding = Man legt sich auf eine Wahl bindend fest (Münzwurf → Kopf / Zahl)
Hiding = Meine Wahl bleibt solange geheim, bis ich erlaube sie aufzudecken

ZERO KNOWLEDGE PROOF

Ziel: Ich beweise einem Verifizierer V mit einer hohen Wahrscheinlichkeit, dass ich als Beweiser P ein Geheimnis Kenne, ohne diese Geheimnis konkret zu enthüllen

PASSWÖRTER

Passwortrichtline f = (ulld,8)
Passwort Sharing $\pi = s_0 + s_1$
Passwort Wörterbuch enthält alle gültigen Pwds.
Passwortumwandlung String wird in Integer umgewandelt

4. Protokoll

1. CLIENT VORBEREITUNG

Der Client bereitet Primzahlen, Passwort und Commitments vor.

2. PASSWORT REGISTRIERUNG

Der Client bestätigt die Konformität des Passworts gegenüber den Servern mit Proof of Correctness, Proof of Membership und Proof of Shuffle.

3. SHARE VERIFIKATION

Die Server testen ob der Client mit beiden Servern dasselbe Passwort und dieselben Shares verwendet hat.

6. Fazit

Sichere Registrierung von Passwörtern in 2PAKE und 2PASS Systemen mit Kontrolle der Passwortrichtlinien ist ein Erfolg durch Two-Server Blin Password Registration Protokoll.
VERWENDET VERDAMMT NOCHMAL GUTE PASSWÖRTER UND EINEN PASSWORTSAFE!!!

\+ Performance + Sicherheit
\- Pedersen Commitments nur „computational binding“