Zürcher Hochschule
für Angewandte Wissenschaften

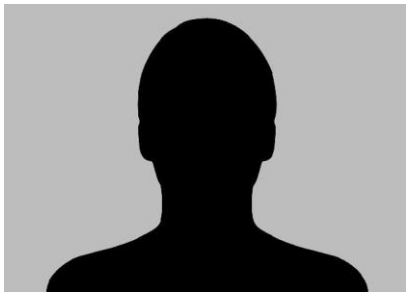
School of
Engineering

InIT Institut für angewandte
Informationstechnologie

Eine Implementierung von OPAQUE für Web Apps

OPAQUE ist eine neuartige Technik für Passwortauthentifizierung, die Vorteile in folgenden Punkten mit sich bringt: Erstens kann sie in einer Konfiguration verwendet werden, in der der Server nie das Passwort lernt. Zweitens ist sie nicht rechenintensiv. Und drittens gibt es für den Angreifer keine bessere Strategie als die «Dictionary Attacke», wenn ein Server kompromittiert wurde.

OPAUQE-EA war ein technischer Prototyp, um zu demonstrieren, dass OPAQUE im «Browser/Web Server»-Umfeld funktioniert. Da OPAQUE-EA in Go geschrieben ist, musste der «Client»-Quelltext zu WebAssembly kompiliert werden. Ich untersuche, ob ein «Client» in TypeScript geschrieben werden kann und schreibe einen Einführungsartikel zu OPAQUE und dessen wichtigste Primitive ORPF.



Diplomand
Ryan Steiger

Dozent
Stephan Neuhaus

Bild klein 1.

Bild klein 2.