8 ZeroKnowlege

Das Secure Remote Password (SRP)-Protokoll ist nicht unbedingt ein Zero-Knowledge-Proof-Protokoll, es enthält jedoch Elemente von Zero-Knowledge-Proofs, um eine sichere Authentifizierung zu erreichen. SRP ist ein passwortbasiertes Authentifizierungsprotokoll, das es einem Client und einem Server ermöglicht, einen gemeinsamen geheimen Schlüssel zu erstellen, ohne das eigentliche Passwort über das Netzwerk zu übertragen.

SRP verwendet eine Form des Zero-Knowledge-Proofs namens Zero-Knowledge-Passwort-Proof (ZKPP), um die Kenntnis des Passworts nachzuweisen, ohne es preiszugeben. Während der Protokollausführung nehmen Client und Server an einer Reihe von Interaktionen und Berechnungen teil, bei denen der Client dem Server nachweist, dass er das Passwort kennt, ohne es explizit preiszugeben.

Das ZKPP in SRP verwendet eine kryptografische Technik, die als sichere Hash-Funktion bezeichnet wird, beispielsweise SHA-256. Der Client sendet einen vom Passwort abgeleiteten Commitment-Wert an den Server, und der Server fordert den Client auf, zusätzliche, vom Passwort abgeleitete Informationen bereitzustellen. Der Client führt Berechnungen auf Grundlage des Passworts durch und sendet die Antwort zurück an den Server, der die Antwort dann überprüft. Wenn die Antwort gültig ist, bedeutet dies, dass der Kunde nachgewiesen hat, dass er das Passwort kennt, ohne es preiszugeben.

Auf diese Weise kombiniert SRP wissensfreie Beweise mit kryptografischen Techniken, um eine sichere Passwortauthentifizierung zu erreichen, ohne dass das Passwort während der Übertragung offengelegt wird. Es ist jedoch wichtig zu beachten, dass es sich bei SRP nicht um ein reines Zero-Knowledge-Proof-Protokoll handelt, da es eher der sicheren Authentifizierung als dem Nachweis allgemeiner Aussagen dient.

- SRP enhält Elemnte von Zero-Knowledge-Proofs, um eine sichere Authentifizierung zu erreichen
- es verwendet ein Form von Zero-Knowledge-Passwort-Proof (ZKPP) um die Kenntnis des Passworts nachzuweisen, ohne es preiszugeben.

- Während der Protokollausführung werden gerade Präsentierte Interaktionen und Berechnungen zwischen Client und Server ausgeführt
- Hier weist der Client dem Server nach das er das Passwort kennt ohne es explizit preiszugeben.
- Das ZKPP in SRP verwendet eine kryptografische Technik, die als sichere Hash-Funktion bezeichnet wird
- Auf diese Weise kombiniert SRP wissensfreie Beweise mit kryptografischen Techniken, um eine sichere Passwortauthentifizierung zu erreichen, ohne dass das Passwort während der Übertragung offengelegt wird

Die Korrektheit im SRP (Secure Remote Password) bezieht sich auf die Eigenschaft des Protokolls, dass der Client und der Server korrekt miteinander interagieren und die gewünschte Authentifizierung erfolgreich durchgeführt wird. Im SRP gibt es verschiedene Schritte, die von beiden Parteien durchgeführt werden, um den gemeinsamen Geheimschlüssel zu etablieren, und die Korrektheit stellt sicher, dass das Protokoll wie beabsichtigt funktioniert.

Die Korrektheit im SRP umfasst:

1. Der Client und der Server halten sich an das SRP-Protokoll und führen die erforderlichen Schritte in der richtigen Reihenfolge aus.
2. Der Client sendet den richtigen Benutzernamen und das Passwort an den Server.
3. Der Server verifiziert die Identität des Clients und stellt sicher, dass der berechnete gemeinsame Geheimschlüssel mit dem des Clients übereinstimmt.
4. Der Client und der Server können nach der erfolgreichen Authentifizierung den gemeinsamen Geheimschlüssel verwenden, um weitere sichere Kommunikation durchzuführen.

Die Korrektheit im SRP ist entscheidend, um sicherzustellen, dass die Authentifizierung zuverlässig und fehlerfrei ist, sodass kein unbefugter Zugriff auf das System oder die Kommunikation ermöglicht wird. Durch die Einhaltung des SRP-Protokolls und die korrekte Umsetzung der einzelnen Schritte

können sowohl der Client als auch der Server die Korrektheit sicherstellen.

Im Zusammenhang mit dem Secure Remote Password (SRP)-Protokoll bezieht sich Soundness auf die Eigenschaft, die Widerstandsfähigkeit gegen betrügerisches oder bösartiges Verhalten der beteiligten Parteien sicherstellt. Es gewährleistet, dass ein Angreifer, selbst mit erheblichen Rechenressourcen, sich nicht erfolgreich als legitimer Benutzer ausgeben kann oder das Passwort des Benutzers aufgrund der Ausführung des Protokolls ableiten kann.

Im SRP wird Soundness durch kryptografische Techniken und den Einsatz starker Hash-Funktionen erreicht. Es stellt sicher, dass ein Angreifer das Protokoll nicht manipulieren kann, um unberechtigten Zugriff zu erlangen oder vertrauliche Informationen zu erhalten.

Konkret bedeutet Soundness im SRP Folgendes:

1. Geheimhaltung des Passworts: Das Passwort wird während des Authentifizierungsprozesses nicht offengelegt oder preisgegeben. Selbst wenn ein Angreifer die Kommunikation zwischen dem Client und dem Server abfängt, kann er das Passwort nicht extrahieren.

2. Integrität der Authentifizierung: Das Protokoll gewährleistet, dass der Client tatsächlich der legitime Benutzer ist und kein Betrüger. Der Server überprüft die Identität des Clients, indem er ihn mit zufälligen Werten herausfordert und die erhaltenen Antworten überprüft.

3. Widerstandsfähigkeit gegen Offline-Angriffe: SRP ist darauf ausgelegt, sich gegen Offline-Angriffe zu schützen, bei denen ein Angreifer auf die vom Server gespeicherten Daten zugreift (wie den Passwort-Verifier) und versucht, das Passwort durch erschöpfende Suche oder andere rechnerische Methoden abzuleiten. Der Einsatz starker Hash-Funktionen und kryptografischer Techniken macht es für einen Angreifer rechnerisch unmöglich, das Passwort aus den gespeicherten Daten zu erhalten.

Durch die Gewährleistung von Soundness bietet das SRP-Protokoll ein hohes Maß an Sicherheit, schützt Benutzerpasswörter und verhindert unberechtigten Zugriff auf sensible Systeme oder Informationen.