Team:

Weronika Buras

Radosław Motyka

Mateusz Konar

Opis protokołu SRP

Protokół SRP to tak zwany zero-knowledge proof protocol co w dosłownym tłumaczeniu oznacza “zero wiedzący”. O co więc chodzi? Mianowicie serwer nie przechowuje hasła i klient może pewnie i śmiało się uwierzytelnić. Ataki typu man-in-the-middle czy eavesdropper nie mogą uzyskać istotnych wiadomości do przeprowadzeni ataku. Zalety SRP:

* Uwierzytelniania bez wysyłania hasła do sieci
* Chroni przed atakami man-in-the-middle czy eavesdroppe
* Daje pewność identyfikacji serwera do klienta i na odwrót, daje pewność, że nie grozi nam towarzystwo osoby niepożądanej
* Dodatkowo generuje zaszyfrowany klucz, tak więc klient &serwer mogą przesyłać zaszyfrowane dane na poziomie bezpieczeństwa TLS

Podsumowując SRP jednym zdaniem “Nie wykradniesz hasła, jeśli go nie przechowujesz”