Handout – Menezes Qu Vanstone (MQV)

Gruppe: Lorenzo Haidinger, Samuel Kominek, Stefan Ohnewith, Ernst Schwaiger

Überblick

- MQV ist ein sicheres Schlüsselaustauschprotokoll basierend auf Diffie-Hellman + Authentifizierung.
- Entwickelt von Menezes, Qu und Vanstone (1998), optimiert für Elliptische Kurven.
- Ziel: Authentifizierter Austausch mit Forward Secrecy ohne Signaturen.

Wie funktioniert MQV?

- Beide Parteien haben:
  - Längerfristigen Public Key X und Y – Längerfristigen Private Key x und y
  - Temporäre Public Key A und B pro Sitzung
  - Temporäre Private Key a und b pro Sitzung
- Gemeinsamer Schlüssel basiert auf beiden Paaren, z.B. für Alice: K = $(B \times Y^B)^{(a+x \cdot A)}$

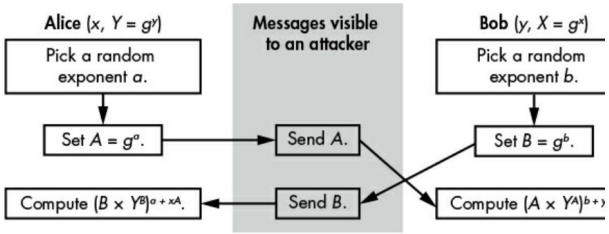

Figure 11-6: The MQV protocol

Abbildung: MQV-Protokoll – übernommen aus [1]

Stärken & Schwächen

- Stärken:
  - Authentifizierung durch kombinierte Schlüssel
  - Sicherer als Authenticated DH
  - Man muss kein zusätzliches Signatur Schema zusätzlich zur DH-Funktion verwenden. – Forward Secrecy (bedingt)
- Schwächen:
  - Komplexer als z.B Diffie-Hellman
  - Implementierungsanfällig (bei falscher Verwendung)
  - War früher durch Patente belastet, was den weit verbreiteten Einsatz behinderte.

Angriffsmöglichkeiten

- Invalid-Curve/Small-Subgroup-Attack
  - Wenn Kurvenpunkte nicht validiert werden kann der Sessionkey rekonstruiert werden
- Weak Forward Secrecy:
  - Erstellung des Sessionkeys nicht nur von ephemeren Parametern abhängig.
- UKS (Unknown Key Share)
  - Alice und Bob teilen sich einen Schlüssel, glauben aber diesen mit unterschiedlichen Parteien zu teilen

Implementierungsidee (Java)

- Nutzung von:
  - Zufallszahlengenerator für temporäre Schlüssel
- Ablauf:
  1. Long-Term Keys generieren
  2. Ephemeral Keys erzeugen
  3. MQV-Berechnung auf Basis der Formel
  4. Schlüsselvergleich

Möglicher Angriff in der Implementierung

- Aktiver MitM

- Wenn die PublicKeys nicht verifziert werden und keine Key Confirmation durchgeführt wird.
- Eve erzeugt je einen Key mit Alice und einen mit Bob
- Kann dann den Traffic mitlesen und entschlüsseln, da sie alle Sessionkeys hat

Credits

Template by John Smith, 2015 http://johnsmith.com/

Referenzen

[1] Jean-Philippe Aumasson: *Serious Cryptography – A Practical Introduction to Modern Encryption*, No Starch Press, 2024.