LU06d - Asymmetrisch verschlüsseln

Einleitung

Eine normale Email kann mit einfachen Mitteln von jedem Angreifer gelesen werden. Um die Information einer Email geheim zu halten, wollen wir den Text, Anhänge und teilweise sogar den Betreff verschlüsseln.

Anwendung

Das Verschlüsseln einer Nachricht basiert auf einem Verschlüsselungsverfahren mit zwei unterschiedlichen Schlüsseln.

- Ein geheimer Schlüssel (Private Key) dient zum Entschlüsseln der Nachricht. Diesen Schlüssel darf nur der Empfänger kennen.
- Ein öffentlicher Schlüssel (Public Key) dient zum Verschlüsseln der Nachricht. Der Absenden muss den Empfänger und dessen Public Key kennen.

Ein solches Verfahren nennt man asymmetrisch, da beim Verschlüsseln und Entschlüsseln zwei verschiedene Schlüssel verwendet werden.

Ablauf

In diesem Beispiel möchte Anna eine geheime Nachricht an Ernst senden. Die Emailprogramme von Anna und Ernst verfügen über die notwendigen Funktionen zum Ver- und Entschlüsseln von Nachrichten.

1. Public Key senden

Damit Anna die Nachricht verschlüsseln kann, benötigt sie den Public Key von Ernst. Diesen Schlüssel kann Anna auf verschiedene Art erhalten:

- Ernst sendet ein eMail mit dem Verfikationsschlüssel als Anhang.
- Ernst stellt den Verifikationsschlüssel auf Ihre Homepage, wo Anna den Schlüssel kopieren kann.
- Ernst übergibt Anna den Verifikationsschlüssel auf einem USB-Stick.

Anna muss lediglich sicher sein, dass der Schlüssel wirklich von Ernst stammt. Danach speichert Anna diesen Public Key in Ihrem Schlüsselbund.

2. Email verschlüsseln

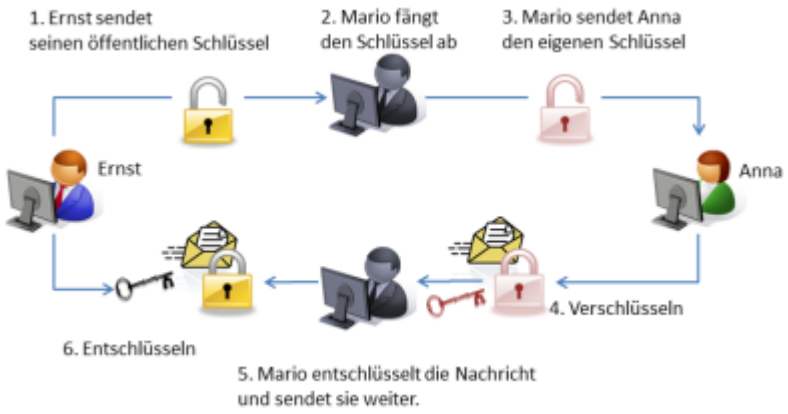
Anna schreibt die Email an Ernst. Vor dem Absenden wählt Sie aus, dass die E-Mail verschlüsselt wird. Für die Verschlüsselung wird nun der Public Key von Ernst verwendet.

3. Email entschlüsseln

Ernst empfängt die verschlüsselte Email von Anna. Sein Emailprogramm erkennt die Verschlüsselung und fragt Ernst nach seiner Passphrase für den Private Key. Danach wird die Nachricht automatisch entschlüsselt.

Man-in-the-middle Attacke

Bei dieser Attacke versucht ein Angreifer (Mario) dem Absender (Anna) einen falschen Public Key zu übergeben. Wenn ihm dies gelingt, kann er künftig die verschlüsselten Nachrichten von Anna an Ernst mitlesen.



1. Ernst sendet eine Email mit seinem Public Key an Anna.
2. Mario fängt diese Email ab und speichert den Public Key von Ernst.
3. Mario sendet eine gefälschte Email mit seinem eigenen Public Key an Anna.
   Anna speichert diesen Public Key in Ihrem Schlüsselbund.

4. Anna schickt eine verschlüsselte Email an Ernst.
5. Mario fängt die Email ab und entschlüsselt die Nachricht.
   Anschliessend verschlüsselt Mario die Nachricht mit dem Public Key von Ernst und schickt sie weiter.
6. Ernst empfängt die Nachricht und entschlüsselt sie.

Weder Anna noch Ernst merken, dass ihre Nachrichten abgefangen und mitgelesen werden. Darum ist es sehr wichtig, die Herkunft eines Public Keys genau zu prüfen. Zum Beispiel kann der Fingerprint des Public Keys auf einem separaten Kanal übermittelt werden. Dieser Fingerprint ist ein eindeutiger Code, der aus dem Inhalt des Keys berechnet wird. Vergleicht Anna den Fingerprint des erhaltenen Keys mit dem Fingerprint den Ernst ihr per WhatsApp mitteilt, kann sie einen gefälschten Schlüssel erkennen.

---

m114-A0G