Übung zur Vorlesung „Sicherheit“
30.06.2014 – Übungsblatt 5

Jessica Koch
jessica.koch@kit.edu

Sicherheit – Übungsblatt 5 – Aufgabe 1

Aufgabe 1.

(a) Wir betrachten das Lehrbuch RSA-Signaturverfahren und folgendes Sicherheitsspiel: Ein Angreifer mit Zugriff auf ein Signaturorakel ist erfolgreich, falls er zu einer vorgegebenen Nachricht m^* eine gültige Signatur σ^* ausgeben kann, für die er keine Anfrage gestellt hat. Wird dieser Sicherheitsbegriff vom Lehrbuch RSA-Signaturverfahren erfüllt?

Sicherheit – Übungsblatt 5 – Aufgabe 1

Aufgabe 1.

(b) Schnorr-Verfahren:

$\text{Gen}(1^k)$: wähle $x \xleftarrow{\$} \mathbb{Z}_p$, berechne $y := g^x$.
$pk = (g, y)$, $sk = (g, x)$.

$\text{Sig}(sk, m)$: $m \in \{0,1\}^*$, ziehe $r \xleftarrow{\$} \mathbb{Z}_p$:
$t := g^r \in \mathbb{G}$, $c := H(t||m) \in \mathbb{Z}_p$, $s := cx + r \in \mathbb{Z}_p$
$\sigma := (t, s) \in \mathbb{G} \times \mathbb{Z}_p$.

$\text{Ver}(pk, m, \sigma)$: $g^s \stackrel{?}{=} y^{H(t||m)} \cdot t$

Aufgrund von schlechten Zufallszahlengeneratoren oder Implementierungsfehlern kann es vorkommen, dass der gleiche Zufall r mehrmals verwendet wird für verschiedene Signaturen. Was kann ein Angreifer dadurch lernen?

Sicherheit – Übungsblatt 5 – Aufgabe 1

Fazit:

- Homomorphie ermöglicht leicht zu fälschen.
  Gegenmaßnahme: Hash-then-Sign
- Zufall sollte immer frisch gewählt werden.

Sicherheit – Übungsblatt 5 – Aufgabe 2

Wir betrachten den Digital-Signature-Algorithmus (DSA) über der Gruppe $\mathbb{G} = Q(\mathbb{Z}_p^*)$, für ungerades primes $p \in \mathbb{N}$. Dabei sei $Q(\mathbb{Z}_p^*) := \{x^2 : x \in \mathbb{Z}_p^*\}$ die Menge der Quadrate in $\mathbb{Z}_p^*$.

(a) Erstellen Sie einen (DSA-)Public-Key/ Secret-Key
$pk := (\mathbb{G}, g, g^x, (\mathrm{H}, h_1, h_2))$, $sk := (\mathbb{G}, g, x, (\mathrm{H}, h_1, h_2))$.
$p := 2q + 1$, $q := 11$,
$\mathrm{H} : \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{Z}_q^*$, $(x_1, x_2) \mapsto h_1^{x_1} h_2^{x_2} \bmod q$

(b) Signieren Sie damit die Nachricht $M = (7, 3)$

(c) Verifizieren Sie die Signatur zur Nachricht M aus (b).

Sicherheit – Übungsblatt 5 – Aufgabe 3

Aufgabe 3. Sei ein 2-Parteien-2-Nachrichten-Schlüsselaustausch-verfahren $\mathsf{KE} = (\mathsf{KE.Gen}, \mathsf{KE.Encap}, \mathsf{KE.Decap})$ gegeben:

- $\mathsf{KE.Gen}(1^k)$ erhält den Sicherheitsparameter $k \in \mathbb{N}$ und gibt State s und Nachricht X aus. ($X \mathrel{\hat{=}}$ erste Nachricht im Schlüsselaustauschverfahren.)
- $\mathsf{KE.Encap}(X)$ erhält Nachricht X, gibt Nachricht Y und Schlüssel K aus. ($Y \mathrel{\hat{=}}$ zweite ausgetauschte Nachricht im Schlüsselaustauschverfahren.)
- $\mathsf{KE.Decap}(s, Y)$ erhält einen State s, Nachricht Y und gibt einen Schlüssel K' aus.

Konstruieren Sie ein Public-Key-Verschlüsselungssystem $\mathsf{PKE} = (\mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ aus KE.

Sicherheit – Übungsblatt 5 – Aufgabe 4

Aufgabe 4

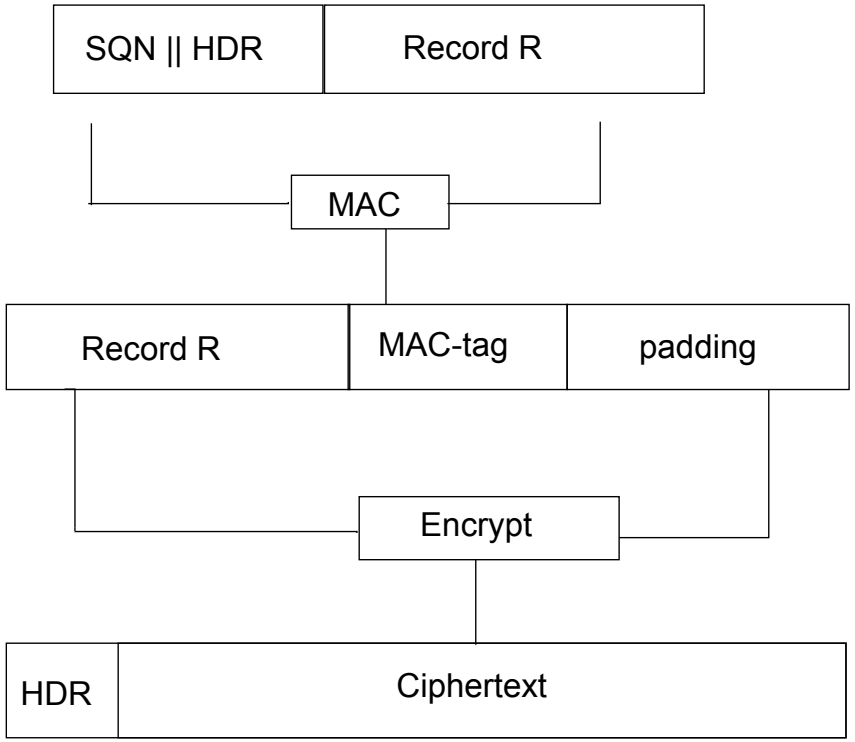

Abbildung : TLS Record Protocol

Überlegen Sie, wie ein aktiver Angreifer das hier verwendete Design MAC-then-encrypt mithilfe von einem Seitenkanalangriff (timing attack) ausnutzen könnte.

Sicherheit – Übungsblatt 5 – Aufgabe 4

Lucky 13 Angriff:

- Es gibt aufgrund des CBC-Modus zusätzlich noch die Möglichkeit von einem Chiffrat C alle Klartextbits zu berechnen.

Fazit:

- Erst Integrität überprüfen, dann entschlüsseln. (Encrypt-then-MAC)

Organisatorisches

- Nächste Übung am Mo, 14.07.14
- Nächstes Übungsblatt am Mo, 30.06.14
- An- und Abmeldung zur Hauptklausur bis Mo, 14.07.14
- Fragen per Mail an jessica.koch@kit.edu