Rasmus Diederichsen
Lisa Goerke
Sebastian Höffner

Sven Kleine-Albers
Kristin Schmidt

Lösungen zu Übungsblatt 5
Kryptographische Verfahren

Besprechung 4. Dezember 2015

Aufgabe 5.1. Der Geburtstagsangriff mit konstantem Speicher terminiert

Es sei mit $P(n, k)$ die Wahrscheinlichkeit bezeichnet, bei n Versuchen (n verschiedenen Eingaben) bei einer Hashlänge von 2^k Bits keine Kollision zu erhalten.

$$\begin{aligned} P(n,k) &= 1 \cdot \frac{2^k - 1}{2^k} \cdot \ldots \cdot \frac{2^k - n + 1}{2^k} \\ P(n,k) &= \prod_{i=0}^{n-1} \frac{2^k - i}{2^k} \\ &= \prod_{i=1}^{n-1} (1 - \frac{i}{2^k}) \end{aligned}$$

Da $(1 - x)$ durch e^{-x} nach oben abgeschätzt werden kann, gilt

$$\begin{aligned} &\leqslant \prod_{i=1}^{n-1} e^{-\frac{i}{2^k}} \\ &= e^{\sum_{i=1}^{n-1} -\frac{i}{2^k}} \\ &= e^{-\frac{1}{2^k} \sum_{i=1}^{n-1} i} \\ &= e^{-\frac{1}{2^k} \frac{n(n-1)}{2}} \\ &\leqslant e^{-\frac{(n-1)^2}{2 \cdot 2^k}} \end{aligned}$$

Gesucht ist nun n, sodass $P(n, 128) \leqslant \frac{1}{4}$.

$$\begin{aligned} e^{-\frac{(n-1)^2}{2 \cdot 2^k}} &\leqslant \frac{1}{4} \\ -\frac{(n-1)^2}{2 \cdot 2^k} &\leqslant \ln \frac{1}{4} \\ -(n-1)^2 &\leqslant 2 \cdot 2^k \cdot \ln \frac{1}{4} \\ -n^2 + 2n - 1 &\leqslant 2 \cdot 2^k \cdot \ln \frac{1}{4} \\ n^2 - 2n + 1 &\geqslant -2 \cdot 2^k \cdot \ln \frac{1}{4} \end{aligned}$$

Mit den üblichen Verfahren, z.B. pq-Formel und Computerunterstützung lässt dies als positive Lösung zu

$$n_{128} \gtrapprox 30.715.843.678.825.642.450 \approx 3.0716 \cdot 10^{19}$$

Man müsste also mehr also über dreißig Trillionen Versuche machen. Analog gelangt man für $k = 160$ zu dem Ergebnis

$$n_{160} \gtrapprox 2.012.993.531.335.517.303.552.701 \approx 2.013 \cdot 10^{24}$$

oder etwa 2 Quadrillionen Versuche.

Aufgabe 5.2. Der Geburtstagsangriff mit konstantem Speicher findet Kollisionen

Falls es $1 \leqslant I < J$ mit $x_I = x_J$ und damit $H(x_{I-1}) = H(x_{J-1})$ gibt, so hat die Folge $x_1, \ldots, x_q$ offenbar eine Periode von $J - I$. Der $(J + i)$-te Wert ist also gleich dem $(I + i)$-ten. Falls man die Periodizität schon für $i < I$ annehmen kann, gilt $x_{J-I} = x_{J-I+J-I} = x_{2(J-I)}$.
Allgemein stimmt die Aussage aber nicht!
Gilt zum Beispiel $x_7 = x_{12}$, so ist $x_8 = x_{13}, x_9 = x_{14}, x_{10} = x_{15}, x_{11} = x_{16}$ und kein $i < J$ erfüllt die Bedingung.

Aufgabe 5.3. Schlüsseltauschprotokolle

a)

Der Breitmaulfrosch ist nicht einmal gegen Angriffe ohne bekannten Schlüssel sicher, wenn es keinen Zeitstempel gibt. Fängt der Angreifer eine Nachricht ab, deren Inhalt er kennt (hierfür könnte er den bekannten Schlüssel vielleicht verwenden), so könnte er diese erneut senden und erneut eine Reaktion auslösen (z.B. eine Überweisung o.Ä.).

Ein Problem ist auch, dass vor allem ohne Zeitstempel (aber potenziell auch mit, wenn der Angriff innerhalb eines Zeitfensters durchgeführt wird, das nicht verdächtig ist) ein Angreifer die Validität eines Schlüssels erhalten kann, indem er abwechseln Alice und Bob vertritt und die Nachricht $E_{K_{BC}}(t_Z, A, K_{AB})$ an Charlie sendet, die dieser zuvor an Bob geschickt hatte. Charlie sendet dann $E_{K_{AC}}(t'_Z, B, K_{AB})$ an Alice und der Schlüssel K_{AB} bleibt aktiv. Sendet man die Nachricht immer schnell genug zurück an Charlie, kann der Schlüssel so am Leben erhalten werden.

b)

Das Needham-Schroeder-Protokoll ist **nicht** sicher gegen Angriffe mit bekanntem Sitzungsschlüssel mit Zusatzinformation. Angenommen, Everett kennt einen alten Sitzungsschlüssel k_{AB} und hat die dritte Nachricht $E_{k_{SB}}(A, k_{AB})$ (also die Nachricht, in der Charlie ein für Bob bestimmtes Chiffrat an Alice sendet) aufgezeichnet. Er kann nun die Nachricht erneut an Bob senden, welcher mit seiner verschlüsselten Zufallszahl $E_{k_{AB}}(r_B)$ antwortet. Diese kann Everett entschlüsseln, ändern, verschlüsseln und wieder an Bob schicken, sodass dieser dann denkt, er würde mit Alice kommuizieren.

Ist allerdings **nur** der Sitzungsschlüssel bekannt, kann ein Angreifer damit nichts anfangen, denn die Nonce r_A garantiert Alice dass der erhaltene Schlüssel aktuell ist und die Schlüssel werden von Charlie unabhängig generiert.

Bei Otway-Rees existiert das Problem mit der fehlenden Authentizität nicht (s.o.). Bob kann also nicht so einfach über die Identität seines Kommunikationspartners getäuscht werden. Auch hier generiert Charlie unabhängig die Sitzungsschlüssel k_{AB} und Alice und Bob werden durch die Noncen r_A und r_B von der Aktualität überzeugt.

Für den Diffie-Hellman-Schlüsseltausch werden in jeder Sitzung die Exponenten a und b neu zufällig generiert. Wenn ein Angreifer einen Schlüssel $(g^a \mod p)^b \mod p$ kennt, kann er nicht einfach a oder b berechnen oder auch bloß $(g^a \mod p)$. Mit der letzen Information könnte er eine MITM-Attacke durchführen, kennt er aber nur den alten Schlüssel, geht dies nicht.

c)

Da Alice A und den Sessionkey aus $E_{kA}(r_A, k_{AB}, B, E_{kB(A,k_{AB})})$ weiß, kann sie aus $E_{kB}(A, k_{AB})$, A und k_{AB} auf k_B schließen, je nach Verschlüsselungsverfahren (z.B. Rainbow Tables). Der Angriff funktioniert auch, wenn das Protokoll um einen Timestamp erweitert wird.

Aufgabe 5.4. Ein sicheres Protokoll?

a)

$$\begin{aligned} w \oplus t &= u \oplus r \oplus t \\ &= s \oplus t \oplus r \oplus t \\ &= k \oplus r \oplus t \oplus r \oplus t \\ &= k \oplus r \oplus r \oplus t \oplus t \\ &= k \oplus 0 \oplus 0 \\ &= k \end{aligned}$$

b)

1. Erste Nachricht von Alice abfangen $\rightarrow s := k \oplus r$
2. Erste Nachricht von Bob abfangen $\rightarrow u := s \oplus t$
3. Zweite Nachricht von Alice abfangen $\rightarrow w := u \oplus r$
4. Berechnen:

$$\begin{aligned} r &= w \oplus u \quad (u \oplus r \oplus u) \\ k &= s \oplus r \quad (k \oplus r \oplus r) \end{aligned}$$

Damit hat der Angreifer den Schlüssel, der von Alice und Bob verwendet wird.