technische universität dortmund

Prof. Dr. Jan Jürjens, Thomas Ruhroth
Lehrstuhl 14 – Software Engineering
Fakultät für Informatik
SFL – Deadline 7.1.2015

Sicherheit: Fragen und Lösungsansätze – Übung 5

AUFGABE 1(Fiat-Shamir) (3LP):

I Alice ist im Besitz des Geheimnisses $s = 1337$ und sie möchte Bob davon überzeugen, ohne ihm das Geheimnis verraten zu müssen. Da fällt ihr ein, dass sie ein entsprechendes Verfahren in der SFL-Vorlesung kennengelernt hat. Zur Vorbereitung hat sie die Zahlen $p = 19$ und $q = 29$ erzeugt.

a) Welche Werte muss Alice jetzt öffentlich machen?

b) Alice wählt die Werte $r_1 = 7,\ r_2 = 23,\ r_3 = 30,\ r_4 = 550$ aus. Welche Werte muss sie an Bob senden?

c) Bob sendet jeweils ein Bit $b = 1$ aus. Womit antwortet Alice?

II Auch Bob behauptet nun, ein Geheimnis $\tilde{s}$ zu kennen. Er veröffentlicht dazu $v = 653$ und $n = 1111$.

a) Bob nennt $x = 900$ und auf das Bit $b = 1$ antworter er mit $y = 149$. Kennt er das Geheimnis $\tilde{s}$?

b) Alice misstraut Bob ein wenig und fragt nochmal nach. Diesmal nennt er $x = 529$ und auf $b = 0$ antwortet er $y = 78$. Was lernt Alice daraus?

c) Alice ist überzeugt, dass Bob das Geheimnis $\tilde{s}$ kennt. Als sie Bob schon anbieten will, s gegen $\tilde{s}$ auszutauschen, nennt Bob ihr gerade $x = 308$, in der Annahme, Alice zögere noch. Anstatt ihn über das Missverständnis aufzuklären, fragt Alice mit $b = 1$ noch ein letztes Mal nach. Bob antwortet darauf $y = 808$. Wie reagiert Alice?

AUFGABE 2(CR-Verfahren) (3BP):

Bob hat Alice erklärt, dass es sich lediglich um einen Zahlendreher gehandelt hat, er wollte eigentlich $y = 880$ nennen.
Daraufhin ist Alice einverstanden, die Geheimnisse auszutauschen, muss aber aus Zeitmangel bitten, dies an einem späteren Zeitpunkt zu erledigen.
Damit sie und Bob sich auch wieder erkennen schlägt sie vor, mithilfe eines CR-Verfahrens, welches sie aus der Vorlesung kennt, das Wiedererkennen zu vereinfachen.
Bob allerdings hält nicht viel von symmetrischen Verfahren und will deshalb die assymetrische Abwandlung nutzen.
Wie müsste ein entsprechendes assymetrische CR-Verfahren aussehen?

AUFGABE 3(Kerberos) (2BP + 2LP):

Zum vereinbarten Zeitpunkt bekommt Alice eine Nachricht von Bob, dass er Aufgrund eines Datenverlustes nicht in der Lage wäre, seine Identität mithilfe des vereinbarten CR-Verfahrens zu beweisen.
Alice bietet ihm daraufhin an, sich mithilfe des Kerberos-Protokolls zu authentifizieren.

1. Wie läuft diese Authentifizierung ab?
2. Der Absender der Nachricht sei nicht Bob, sondern Eva gewesen, und diese versucht nun, sich gemäß Alices Angebot als Bob zu authentifizieren.
   Überlegen Sie sich mögliche Versuche Evas und welche Folgen diese haben. (2BP)