Musteraufgaben

31. August 2013

Name: _____ Matrikelnr.: _____

Aufgabe	1	2	3	4	5	6	Übung	**Summe**
Punkte								

Studiengang: _____

Bearbeitungszeit der Klausur: 120 min
Zugelassene Hilfsmittel:

- Ein *nichtprogrammierbarer* Taschenrechner

Hinweise: Bitte schreiben Sie Ihre Lösungen immer direkt unter die jeweiligen Aufgaben. Sollte Sie trotz der zusätzlichen Leerseite zu jeder Aufgabe noch weiteren Platz benötigen, können Sie ebenfalls die Nebenrechnungen am Ende der Klausur für Lösungsangaben verwenden. Bitte verwenden Sie für Ihre (endgültigen) Lösungen keinen Bleistift.

1. *Grundlagen (xx Pkte.)*

   (a) Welche drei Grundlegenden Arten der (Benutzer-)Authentifizierung unterscheidet man im Allgemeinen?

   (b) Nennen Sie Vor- und Nachteile der folgenden drei Arten von Protokollen für Authentifizierungs-Tokens und vergleichen Sie die Sicherheit und Benutzbarkeit derselben: (1) Challenge-Response, (2) Counter-basiert, (3) Zeitstempel-basiert.

2. *Salt (xx Pkte.)*

   Beschreiben Sie einen Passwort Hash mit Salz. Was sind Vor- und Nachteile dieser Konstruktion? Wie wirkt sich dies auf die Berechnungs-)Komplexität des Servers und des Angreifers aus?

3. *Offline guessing attack gegen Passwort Protokoll (xx Pkte.)*

   Betrachten Sie folgendes Protokoll zur (hoffentlich sicheren) Authentisierung mit Passwort, bei dem (im Vergleich zu EKE) zusätzlich c_1 in die zweite Verschlüsselung eingebunden wird.

Alice (mit pwd)		Bob (mit pwd')
$a \leftarrow^R \{1,\ldots,p\}$	$\xrightarrow{c_1 := E_{pwd}(g^a)}$	
	$\xleftarrow{c_2 := E_{pwd'}(g^b \parallel c_1)}$	$b \leftarrow^R \{1,\ldots,p\}$
$B = E^{-1}_{pwd}(c_2)$		$A = E^{-1}_{pwd'}(c_1)$
$K = B^a$		$K' = A^b$

   Beschreiben Sie einen offline guessing Angriff gegen dieses Protokoll.

4. *(xx Pkte.)*

   Nennen und erklären Sie fünf wichtige Kriterien für den Vergleich von Authentifizierungsverfahren.

   Benutzen Sie diese Kriterien, um klassische (textbasierte) Passwörter und Authentifizierung mittels P300-basierter Passworteingabe (BCI) zu vergleichen.