Prüfungs Rekonstruktion
NICHT DEM PROF ZEIGEN!

Datum	27.01.2014
Semester	WS 13/14
Dozent	Prof Dr. Skornia
Standort	Regensburg
Studiengang	Allgemeine Informatik
Gesamtpunktzahl	??? Punkte
Prüfungszeit	90 Minuten
Zugel. Hilfsmittel	Taschenrechner

1. Aufgab: Es wurden vor kurzem viele Millionen Emailkonten gehackt. Welche Schutzziele sind durch diesen Emailhack bedroht (3 Stück reichen)?

2. Aufgabe
   a) Nennen Sie zwei Regeln des Bella-Lapadula Modells?
   b) Welche dieser Regeln steht im widerspruch zu einem hirarchischen rollenbasierten Modell.

3. Jemand ist auf die Administrationsoberfläche eines Routers eingelogged und surft im gleichen Browser.
   a) Welches Risiko ergibt sich dadurch?
   b) Erläutern Sie anhang einem Beispiel den Unterschied zwischen Reflected XSS und Stored XSS.

4. Fia-Feige-Schamir-Verfahren: Es sind gegeben: N, s_1, s_2 und s_3
   a) Welche Informationen müssen an den Lizenzierungsserver weitergeleitet werden.
   b) Welche weiteren Nummern werden benötigt um ein vollständiges Feige Fiat Schamir Verfahren durchzuführen?

5. Es ist ein C-Programm gegegeben. Darin enthalten war ein strcpy. Erläutern Sie, wie durch folgende Techniken der Angriff erschwert werden kann:
   a) Address-Space-Layer-Randomisation
   b) Canaries
   c) Non-Executable-Bit

6. SSL verwendet eine Kombination aus asymetrischen und symetrischen Verfahren.
   a) Warum wird dies so verwendet?
   b) Warum ist es wichtig einen guten Zufallsgenerator zu verwenden (SSL-Handshake)

7. Snowden schreit Ihnen durchs Telefon: $p = 19$, $g = 5$ und $A = 4$
   a) Welches Verfahren kommt hier zum Einsatz?
   b) Welche Antwort müssen Sie zurück schicken und auf welchen Key haben Sie sich geeinigt?
   c) Warum ist es wichtig, dass Sie Snowden an seiner Stimme erkennen?

8. In den letzen zwei Jahren vermehrten sich die Angriffe auf Root-CAs. Welche Gefahr entsteht hierbei für eine Trusted Computing Plattform wenn diese Angriffe erfolgreich sind.

9. IPSec: Zeichnen Sie eine Skizze in der der Unterschied zwischen Tunneled-Mode und Transport-Mode klar werden. Zeigen Sie jeweils einen Anwendungsfall.