Sommersemester 2005
Übung zur Vorlesung

Hasso-Plattner-Institut, Universität Potsdam
Fachgebiet Internet-Technologien und -Systeme
Meinel / Kutzner

Aufgabenblatt 1

Abgabe: Mo, 25.04.2005, bis 12 Uhr
(per E-Mail an mathias.kutzner@hpi.uni-potsdam.de)

Thema: Sicherheitsanforderungen, Krypto-Protokolle

Erreichbare Punkte: 19

Aufgabe 1: 5 Punkte

Wichtige Sicherheitsanforderungen an die Datenkommunikation sind z.B.:

1. Vertraulichkeit
2. Integrität
3. Authentifikation
4. Zugriffskontrolle
5. Verbindlichkeit

Erklären Sie kurz mit eigenen Worten, was diese Sicherheitsanforderungen jeweils beinhalten.

Aufgabe 2: 5 Punkte

Online-Banking mit dem PIN-/TAN-Verfahren ist eine unter Privatanwendern weit verbreitete Möglichkeit, die eigenen Bankgeschäfte zu Hause am PC zu erledigen. Machen Sie sich mit diesem Verfahren vertraut und beschreiben Sie, wie die in der vorherigen Aufgabe genannten Sicherheitsanforderungen gewährleistet werden sollen.

Aufgabe 3: 5 Punkte

Überlegen Sie sich eine Strategie, wie ein Angriff auf das PIN-/TAN-Verfahren aussehen könnte und erläutern Sie diese Strategie. Erklären Sie, welche Sicherheitsanforderungen Ihrer Meinung nach dadurch verletzt werden. Begründen Sie ihre Entscheidung.

Aufgabe 4: 4 Punkte

In der Vorlesung wurden unter anderen folgende Angriffsmöglichkeiten auf Krypto-Protokolle behandelt:

- Denial-of-Service-Attacke
- Spoofing-Attacke

Erklären Sie diese beiden Methoden genauer. Finden Sie für jede Methode ein konkretes Beispiel für eine Attacke, durch die eine größere Institution bzw. zahlreiche Internetnutzer angegriffen wurden. Erläutern Sie ihre Beispiele kurz und geben Sie die Quellen an.