Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
PD Dr. Helmut Reiser, PD Dr. Wolfgang Hommel

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2012/2013
Übungsblatt 8

Abgabetermin: 16.01.2013 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per Email an die Adresse **uebung-itsec_AT_lrz.de** oder schriftlich vor der Übung). Während des Semesters werden vier Übungsblätter korrigiert. Bei vier richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei nur drei oder zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

Aufgabe 19: (H) Authentisierung & One-Time Passwords

a. Zur Authentisierung von Benutzern werden bekanntlich verschiedene Verfahren eingesetzt, die sich unterschiedlichen Kategorien zuordnen lassen. Passwörter beispielsweise werden der Kategorie *Wissen* zugeordnet. Nennen Sie mindestens drei weitere geeignete Kategorien und geben Beispielverfahren aus der Praxis an. Benennen Sie auch Vor-/Nachteile der jeweiligen Kategorie oder des konkreten Verfahrens.

b. Bei der Authentisierung von Nutzern findet eine 1:1-Verifikation statt. Nennen Sie ein Beispiel, bei dem eine 1:N-Verifikation erforderlich ist/sein könnte? (Tip: Fingerabdruck)

c. Sie sind ein Sicherheitsverantwortlicher in einem Unternehmen. Ihre Mitarbeiter benötigen auf Dienstreisen, auch aus Internet-Cafes heraus, Zugriff auf interne Ressourcen. Welchen Mechanismus zu einer möglichst sicheren Benutzerauthentisierung schlagen Sie der Unternehmensleitung vor? Begründen Sie ihre Antwort und zeigen Sie dabei Angriffsmöglichkeiten auf andere Mechanismen auf.

d. One-Time-Pad gilt derzeit als die sicherste Verschlüsselungsmethode. Wie lautet das Chiffrat, wenn die Eingabe HALLOWELT und das Pad MISTGABEL lautet?

e. Welchen Vorteil bieten zur Absicherung von Remote-Zugängen Smartcard- und OTP-Token-basierte Lösungen? Welche(n) große(n) Nachteil(e) haben diese?

f. Betrachten Sie eine Web-Applikation. Zur Nutzerauthentisierung werden Passwörter eingesetzt, die unverschlüsselt übertragen werden. Mallet snifft den kompletten Netztraffic mit und möchte die Zugangsdaten später wiederverwenden? Um welche Art von Angriff handelt es sich dabei am ehesten: Brute-Force-, Wörterbuch-, Social-Engineering- oder Replay-Angriff? Begründen Sie ihre Antwort und erläutern Sie die drei verbleibenden Antwortmöglichkeiten.

Aufgabe 20: (H) Biometrie

Analysten erwarten ein starkes Wachstum im Bereich Biometrie innerhalb der nächsten Jahre. Die Nutzer erwarten in erster Linie Bequemlichkeit, während die Sicherheitsverantwortlichen auf eine höhere Sicherheit bei Finanztransaktionen und Bezahlvorgängen abzielen. Doch wo Chancen sind, sind meist auch Risiken.

a. Nennen Sie mindestens 5 Eigenschaften eines zur Authentisierung geeigneten biometrischen Merkmals?

b. Beschreiben Sie kurz in eigenen Worten die allgemeine Vorgehensweise bei Verwendung eines biometrischen Systems.

c. An welchen Stellen des in der vorherigen Aufgabe beschriebenen Ablaufs ist ein Angriff möglich? Geben Sie auch Beispiele für konkrete Gegenmaßnahmen an.