Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2016/2017
Übungsblatt 8

Termin: 17.01.2017 um 12:00 Uhr

Aufgabe 17: (K) 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. Welchen Vorteil bieten zur Absicherung von Remote-Zugängen Smartcard- und OTP-Token-basierte Lösungen? Welche(n) große(n) Nachteil(e) haben diese?

e. 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 18: (K) 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.

Aufgabe 19: (K) Authentisierung & Needham-Schröder

In der Vorlesung wurden verschiedene Varianten zur Authentisierung bei Verwendung symmetrischer, asymmetrischer Verschlüsselungsverfahren und Hash-Funktionen diskutiert. Außerdem wurde das Authentisierungsprotokoll Needham-Schröder unter Verwendung eines symmetrischen Verschlüsselungsverfahrens erläutert.

a. Skizzieren Sie den Nachrichtenfluss der zum Verbindungsaufbau im Rahmen des Needham-Schröder-Verfahrens benötigten Pakete zwischen Alice und Bob bei Verwendung asymmetrischer Verschlüsselung. Den Kommunikationspartnern sei der öffentliche Schlüssel K_T von Trent T bekannt. Trent kennt andererseits die öffentlichen Schlüssel aller Beteiligten (K_A für Alice, K_B für Bob).

b. Die symmetrische Protokollvariante von Needham-Schröder besitzt eine bekannte Schwäche für Replay-Attacken bei bekanntem Session-Key. Erläutern Sie das Problem und beheben Sie dessen Ursache!