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 2024/2025
Übungsblatt 10

Besprechung: Do, 16.01.2025 um 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.

Aufgabe 1: (T) Post Quantum Cryptography

a. Mosca's inequality – what's the problem?

b. Welche Bedrohung stellen Quantencomputer für Kryptosysteme dar? Sind symmetrische, asymmetrische und Hash-Funktionen gleichermaßen betroffen? Gilt das für alle Algorithmen/Kryptosysteme dieser Klassen?
Tipp: Shor, Grover, ...

c. Manche staatlichen Institutionen speichern Ciphertexte im großen Stil – zur späteren Entschlüsselung, sobald die nötige Rechenleistung dafür verfügbar sein wird. Ist das ein Problem?

Aufgabe 2: (T) 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. In der symmetrischen Variante von Needham-Schröder kommt ein sogenannter Nonce zum Einsatz. Erklären Sie, wozu dieser im Protokoll verwendet wird.

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!

c. 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).

Aufgabe 3: (T) Kerberos

Ein weitverbreitetes Protokoll zur Benutzerauthentisierung ist Kerberos. Beschreiben Sie den Ablauf sowie den konkreten Aufbau der ausgetauschten Nachrichten anhand des folgenden Beispiel-Szenarios:

a. Sie kommen um 08:00 Uhr in die Arbeit und loggen sich mit Ihrem Nutzernamen *bsp26395* und zugehörigem Passwort *3z!fG7qiT* ein. An welche an Kerberos-beteiligte Komponente werden diese Informationen übermittelt? Wie sieht die zugehörige Nachricht aus?

b. Die Antwort, die Sie auf Ihre erste Nachricht in Teilaufgabe a) erhalten ist verschlüsselt. Welcher Schlüssel wurde hierzu verwendet? Welche Informationen werden in dieser Antwort-Nachricht übertragen?

c. Sie arbeiten gerade an einem Text-Dokument, welches Sie nun ausdrucken wollen. Die Steuerung des Druckers erfolgt über einen dedizierten Print-Server. An welche Kerberos-Komponente müssen Sie Ihre Druck-Anfrage übermitteln und welche Informationen enthält diese? Welchen Inhalt hat die entsprechende Antwortnachricht?

d. Welche Schritte sind abschließend zu durchlaufen, damit Ihr Dokument ausgedruckt wird?

Aufgabe 4: (H) Biometrie

Biometrie wird heute immer häufiger zur Authentisierung verwendet. 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 5: (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. Betrachten Sie eine Web-Applikation, die Passwörter zur Nutzerauthentisierung einsetzt. Diese werden 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.