

## IT-Sicherheit im Wintersemester 2020/2021

### Übungsblatt 10

Abgabetermin: 02.02.2021 bis 12:00 Uhr

#### Aufgabe 21: (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.

- In der symmetrischen Variante von Needham-Schröder kommt ein sogenannter Nonce zum Einsatz. Erklären Sie, wozu dieser im Protokoll verwendet wird.
- 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!
- 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 22: (K) Kerberos

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

- 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?
- 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?