Einführung Kryptographie und IT-Sicherheit

Sommersemester 2020

Andreas Uhl

Department of Computer Sciences
University of Salzburg

June 15th, 2020

Montag 15. Juni, 13:15

Fragen zum Skriptum - Abschnitt 4.2.1

1. Warum kann man in einem offenen verteilten System nicht darauf vertrauen, dass eine Workstation ihre Benutzer geg. Netzwerk Sevices korrekt identifiziert ?
2. Was ist ein besonderes (und überraschendes) Merkmal von Kerberos bzgl. der im Einsatz stehenden kryptographischen Methoden ?
3. Warum wurde bei Kerberos der TGS eingeführt und was ist seine Aufgabe ?
4. Welche Bedeutung (pos. wie neg.) haben Ticket timestamp und Lebensdauer ?
5. Was ist ein Kerberos Realm (und welche Daten werden dafür benötigt ?
6. Wie funktioniert Inter-Realm Autnetifizierung ?
7. Kritik an Kerberos ?

Fragen zum Skriptum - Abschnitt 4.2.2. - 4.2.3

8. Beschreiben sie den Authentifizierungsvorgang in GSM Netzen.
9. Welche Rollen spielen die Algorithmen A3, A5 und A8 ?
10. Mit welchem Argument werden im Ausland Gespräche ins dortige Festnetz zum Auslandstarif berechnet ?
11. Welche Probleme wurden bei GSM nicht gelöst ? Inwieweit brachte UMTS Verbesserungen ?
12. Welche beiden Schichten können bei SSL unterschieden werden ?
13. Was ist deren jeweilige Aufgabe ?
14. Welche Analogien sehen sie zu IPSEC ?

Fragen zum Skriptum - Abschnitt 4.2.3

15. Wie wird bei SSL die Zugehörigkeit eines Keys zu einem bestimmten Server festgestellt ?
16. Was ist https ?
17. *** Was ist der Unterschied zwischen SSL und TLS ? Erklären sie die Funktionsweise von “Fallback” und “Downgrade” Angriffen. ***
18. Was ist shttp ?
19. Was ist das Ziel von SET ?
20. Welche Entitäten arbeiten bei SET zusammen ?
21. Beschreiben sie die Idee der Dualen Signatur (inklusive ihrer Motivation).

Fragen zum Skriptum - Abschnitt

22 Welche Möglichkeiten des Keymanagements stehen bei sicherer e-Mail zur Verfügung ?

23 Erklären sie das Konzept des Web-of-Trust.

24 Was ist das “Geheimnis des Erfolgs” von PGP ?

25 Welche Funktionalitäten stellt PGP zur Verfügung ?

26 Beschreiben sie die PGP Key-rings !

27 Welche Funktionen stellt S/MIME zur Verfügung ?

28 Welche Bedeutung hat due S/MIME MUST/SHOULD Struktur ?

29 Skizzieren sie Gemeinsamkeiten und Unterschiede von PGP, S/MIME, PEM und MOSS.