

Ergebniss: 2.0

Prüfer: Dr. Dressler

Sehr lockere Atmosphäre, Dressler war absolut nett, freundlich und hilfsbereit, :) Besitzer (Limmer) auch freundlich und lacht immer!

Fair Bewertung

(Ich schreibe die genau Frage, aber Antworten nur in Stichwort.)

NetSec;

F: Welche Sicherheitsziele haben wir in die Vorlesung kennengelernt?

A: Vertraulichkeit, Dataintegrität, Authentifizierung

F: Er malt das Bild: A-----E-----B, wie kannst du ein Sicherheitsprotokoll gegen Angreifer Eve entwerfen, um die oben genannte Sicherheitsdienst zu realisieren

Austausch von CA um jeweils öffentliche Schlüssel zu erhalten,

Berechnung der MD5, Symmetrische Verfahren Signierung / oder einfach MAC hier verwenden

F: Erzähl mal IPsec

A: Realisierte Sicherheitsdienst: Nachrichtenauthentifizierung, Vertraulichkeit über Nutzdaten, Schutz vor Replay von IP-Packet

SA, AH/ESP, Tunnel/Transportmode

F: wie funktioniert SSL-Sitzung zwischen Web-client und Web-server, um welche Sicherheitsdienst zu realisieren

Handshake phase (CA-basierte Authentifizierung)

Mastersecret dient zur Erzeugung Sitzungsschlüsseln

Record processing

KS

F: Er hat Netzwerktopologie mit 4 Hosts, 2 Routern, die jeweils paarweise an einem Router verbunden sind. Zwischen den oberen Host ist VoIP-Verkehr und zwischen den unteren Hosts ist ein beliebiger Datenverkehr, was für Probleme auftreten könnten

A: VoIP Pakete könnten verzögert werden unter default FIFO Warteschlange das erschwert die Gesprächsqualität,

F: Wie kann man dagegen machen

A: PQ, WFQ

F: Erzähl mal WFQ

A: Steht besser in Skript

F: Was kann man machen, wenn Host 1 die vereinbarte Verbindungsleitung übersteigert.

A: Policing

F: Erzähl mal ausführliche verfahren

A: Leaky/token Bucket

F: was sind reguliert damit,

A: mittlerer Rate,Spitzrate, Max.burst groesse

F: Regulierung die mittlerer Rate,Spitzrate gleichzeitig

A: (2 token bucket hintereinander)Steht besser in Skript

Mfg

Sitomtom