Prüfungsfragen KS 2006

KS, NetSec
Falco Dressler
März 2006

Bemerkungen zu Prüfung und Prüfer

- Ergebnis: 1,0
- sehr lockere Atmoshäre, Dressler absolut freundlich und hilfsbereit, lacht immer! :-) Beisitzer (Jochen Kaiser) schweigt.
- Fragen eher allgemeiner Art, meiner Ansicht nach war das genaue Lernen von ATM, Protokollen, Modellierungstechniken, etc. umsonst, da Zeit viel zu kurz um sowas zu fragen.
- Zusammenhänge, die das Grundverständnis zeigen sind viel wichtiger als Details.
- Bei einer Frage kam ich etwas ins Straucheln und Rumstöpseln. Dass ich dann aber selber durch Nachdenken auf die Lösung gekommen bin, hat ihm gut gefallen.
- Keine Themensprünge innerhalb eines Vorlesungsstoffes, sondern schön konsequent aufeinander aufgebaute Fragen.
- Gewichtung (zeitlich, inhaltlich und notentechnisch) KS:NetSec 50:50
- habe das Skript gelernt, wobei der Schäfer - Netzsicherheit das Buch zur Vorlesung ist und da natürlich alles schön ausformuliert ist.
- Zeit verging wie im Flug, die halbe Stunde ist unglaublich schnell vorbei!

Fragen

KS

- Er malt ein Bild auf: ein Host, dann drei Router, dann ein Host, jeweils durch eine Leitung verbunden. VoIP-Traffic zwischen den beiden Hosts.
  F: Woher kommt der Delay und Jitter, was kann man gegen ihn machen?
  A: Jitter: Kommt von zusätzlichem Verkehr durch die Router, wenn nur VoIP-Traffic (mit konstanter Rate) zwischen den Hosts unterwegs wäre, dann gäbe es keinen Jitter. Der Delay kommt vom Store-And-Forward in den Routern, und der Ausbreitungsgeschwindigkeit der Pakete.
  Gegen Jitter kann man Playout-Buffer einbauen, der um das maximale Delay der Pakete verzögert. Gegen Delay kann man mehrere Queues in den Routern aufbauen, den VoIP-Traffic in eine hoch-priore Queue stecken und bevorzugt behandeln.

- F: Erkläre Weighted-Fair-Queuing, das man ja im obigen Beispiel einsetzen könnte.
  A: Da kam ich ins Straucheln. Er hat mir dann aber geholfen und ich bin durch bissl nachdenken draufgekommen. Antwort steht wohl besser im Skript, als ich das jetzt hier erklären kann.

- F: Was machen, wenn die Hosts die abgemachte Datenrate nicht einhalten?
  A: Policing, Beschränkung der Rate durch Token-Buckets. Entweder Shaper (verzögern der Pakete, die nicht passen), Marker oder Dropper.

NetSec

- Er malt das übliche Bild, Alice, Eve, Bob
  F: Entwickle ein Protokoll, dass Datenintegrität und Vertraulichkeit sicherstellt.
  A: Ich habe zuerst gefragt, was denn vorausgesetzt ist, ob PSK, Zertifikate, gemeinsamer Schlüssel, etc. Er sagt: egal, denk dir was aus. Hab dann gesagt, beide haben ein Zertifikat über ihren jweiligen public-Key.
  Aushandlung eines Session Keys: Erste Nachricht: A nach B: Nonce + von A erzeugter Key K, beides verschlüsselt mit Public-Key von B. Zweite Nachricht: B nach A: Nonce+1, verschlüsselt mit K.
  Senden von Nachricht m: Verschlüsselung von m mit K (Vertraulichkeit), zusätzlich HMAC-Berechnung über K und m (Datenintegrität).

- F: Erkläre Needham-Schröder-Protokoll.
  A: Siehe Skript! Außerdem wichtig: Wie Eve das ganze per Replay-Attacke umgehen kann, wenn er einen alten Session-Key kennt.

Damit wir auch in Zukunft aktuelle Prüfungsfragen haben, sind wir auf Deine Mithilfe angewiesen.
Bitte maile uns die Fragen Deiner Prüfung, ein Formular dazu findest Du auf unserer Homepage.