Praktische Informatik (Vertiefung)

Gedächtnisprotokoll zur mündlichen Diplomprüfung

17. März 2010 (WS09/10, RWTH Aachen University)

Johannes Gilger <heipei ät hackvalue.de>

Inhalt:

- IT Security I + II (V3 + V3, nach Folien von Prof. Meyer aus SS09 bzw. WS09/10)
- Communication Systems Engineering I (V3, nach Folien von Prof. Wehrle aus SS09)
- Massively Distributed Systems I (V3, nach Folien von Prof. Wehrle aus WS09/10)

Prüfer:

- Prof. Dr. Klaus Wehrle (Lehr- und Forschungsgebiet für verteilte Systeme, Lehrstuhl für Informatik IV)
- Prof. Dr. Ulrike Meyer (Lehr- und Forschungsgebiet für IT-Sicherheit, UMIC Research Centre)

Prüfungsdauer: 50 Minuten

Prüfungsnote: 1.3

Hinweis: Bei diesem Prüfungsprotokoll handelt es sich *nicht* um ein offizielles Prüfungsprotokoll der RWTH sondern um ein privates Gedächtnissprotokoll, das ca. zwei Stunden nach der eigentlichen Prüfung angefertigt wurde. Fragen und Antworten sind also nur sinngemäß zu verstehen und es wird kein Anspruch auf Vollständigkeit erhoben. Fehler und Verbesserungsvorschläge nehme ich gerne per E-Mail entgegen.

Die Reihenfolge der Themen habe ich die Prüfer wählen lassen.

IT Security I

- Welche Sicherheitsziele gibt es? (Confidentiality, Integrity, Non-Repudiation, Availability etc.)
- Wie kann man Non-Repudiation erreichen? (Public-Key Signaturen, kurz anhand RSA erklärt)
- Wie verifiziert man Signaturen? (CAs, Web of Trust, Cross-Certification, Zertifikatskette verifizieren)
- Was ist in einer Signatur alles drin? (Felder)
- Hinweis auf den MD5-Rouge-CA Angriff mittels Kollision der Hashfunktion.
- Was ist Replay Protection und wie kann man das erreichen? (Stichwort Timestamps / Nonces)
- Wie funktionieren IPSec Security Associations? Wie wird ein Key-Exchange vollzogen?

IT Security II

- Warum benutzt man Biometrie? (Identifikation / Authentifikation)
  - Was ist Negative Recognition?
  - Was für Vorteile gegenüber normalen Systemen gibt es?
  - Wie funktioniert Key Revocation bei biometrischen Systemen?
  - Welche Bedenken sollte man haben wenn man sich anhand biometrischer Merkmale identifiziert? (Privacy Concerns)
  - Welche Angriffe auf biometrische Systeme gibt es? (Spoofen, Replay, Datenbasis verwässern)
- E-Voting
  - Welche Sicherheitsanforderungen ans E-Voting gibt es? (Unterschied herkömmliche Wahl zu E-Voting)
  - Wie funktioniert Three Ballot? (Kurze Erklärung, Frage warum es in Deutschland nicht zulässig wäre)
  - Welche Probleme hat E-Voting im Allgemeinen? (Zu kompliziert um es dem Durchschnittsbürger zu erklären)

Massively Distributed Systems I

- Was für Netzwerkmodelle wurden behandelt, warum untersucht man solche Modelle? (Haben gute Eigenschaften die man evtl. in P2P-Systemen verwenden will)
- Was sind Small-World Netzwerke, wie entstehen die, was zeichnet sie aus?
- Was ist Flexibility und an welchen Stellen braucht man Flexibility? (für Static Resilience und PNS bzw. PRS)
- Wie könnte man Multicast auf einem P2P-System aufsetzen? (er wollte Scribe hoeren, kannte ich nicht, ist aber das gleiche Prinzip wie bei i3)

Communication Systems Engineering I

- Wir haben auf OSI Layer 3 angefangen, ich habe erst einen kurzen Überblick über die Layer 1-3 gegeben und klar gemacht wen man da jeweils addressiert.
- Was ist der Unterschied zwischen Circuit-Vermittlung und Paketvermittlung, welche Eigenschaften und Anforderungen ergeben sich daraus (z.B. Reihenfolgetreue, gesicherte Bandbreite)
- Kann man Circuit-Vermittlung und Paket-Vermittlung auf einem Layer kombinieren?
- Was für Dinge braucht man auf Layer 3? (Adressierung und Routingprotokolle)
- Ahand des Beispiels vom Routing von Prof. Wehrle's Rechner nach New York die Schritte im Routingprozess erklärt:
  1. Nachgucken ob Rechner im lokalen Segment ist, falls ja ARP verwenden um die MAC zu finden und dann das Paket ohne Router schicken
  2. Wie funktioniert ARP? (Paketformat, Broadcast-Adresse für Layer-2)
  3. Falls die Adresse nicht lokal ist, dann wird ein Gateway benutzt. (Muss das Paket vorher noch verändert werden?)
- OSI Layer 4: UDP bietet ja eigentlich gar nichts, deswegen war die Frage welchen Service TCP bereitstellt.
- Erklärung dass TCP einen bestätigten Byte-Stream zur Verfügung stellt.
- Wie funktioniert die Fehlerkontrolle? (Stop-and-Wait, Go-Back-N, NAKs)
- Wie werden Flow-Control und Congestion-Control realisiert? (Sliding Window, Congestion Window, Congestion Algorithmus)
- Hinweis dass alles allgemeingültige Algorithmen sind die auch auf anderen Layern funktionieren
- Paket-Fragmentierung bei IPv4 erklärt (anhand eines zu großen UDP-Pakets und Byte-Offsets und Last-Paket-Bit)
- Unterschiede IPv6-Header zu IPv4 (Extensions, keine Standard-Felder für Fragmentation, keine Checksum)

Fazit

Die Prüfung mit Prof. Wehrle und Prof. Meyer hatte eine sehr angenehme Prüfungsatmosphäre. Prof. Meyer hat Karten mit Punkten von denen sie sich jeweils ein paar aussucht, Prof. Wehrle geht eher fliessend von einem Thema zum Nächsten über weil es sich z.B. bei den OSI-Layern super anbietet. Ein paar mal bin ich ins Stocken geraten und musste die Sachen nach und nach aufbauen, z.B. bei dem Last-Fragment-Bit oder den IPv6-Headern, dabei hilft Prof. Wehrle allerdings. Bei Prof. Meyer ist man sich manchmal nicht ganz sicher ob man grade etwas Falsches gesagt hat oder ob sie nur kurz überlegt ob das wirklich alles so stimmte, deswegen einfach kurz warten anstatt wild Stoff hinterherzuschaufeln. Die Note habe ich wahrscheinlich wegen ein paar kleinen Aussetzern gekriegt da ich ansonsten den Eindruck hatte dass ich immer relativ schnell auf den Punkt gekommen bin und den beiden sagen konnte was sie hören wollten.

Ich hatte mich über einen Zeitraum von etwa fünf Wochen vorbereitet, wobei ich kurz vor der eigentlichen Lernphase noch Scheinklausuren in den Fächern ITSec 1 und MDS 1 geschrieben hatte (inkl. Übungsblättern während des Semesters), und somit eine gewisse Grundlage hatte (und somit ein paar Wochen mehr gelernt hatte). Gelernt habe ich in einer Gruppe von vier Leuten mit denen wir uns täglich getroffen haben um uns gegenseitig auszutauschen. Wichtig ist, wie immer, erst einen Überblick über die Liste der Themen zu kriegen und dann nach und die Folien durchzuarbeiten.

Lernbegleitend ist für die CSE-Vorlesung das Buch "Computer Networks" (Tanenbaum) zu empfehlen. Wikipedia ist auch manchmal hilfreich. Bei MDS 1 kann ich eigentlich nur empfehlen die ursprünglichen Paper die die verschiedenen DHTs beschreiben komplett zu lesen bevor man versucht die Details der Algorithmen anhand der Folien zu verstehen. Für den Stoff aus IT Security kann man versuchen in Büchern wie "Applied Cryptography" (Schneier) noch zusätzliche Informationen zu finden. Auch hier wird man nicht umhin kommen gelegentlich ein Paper zu lesen wenn man wirklich sicher stellen will dass man ein System verstanden hat.

Aufruf

Noch eine Sache die ich persönlich sehr wichtig finde: **Schreibt Prüfungsprotokolle!** Am besten nicht länger als ein paar Stunden nach der Prüfung. Ich habe bisher zu allen meinen Prüfungen Protokolle geschrieben, nicht zuletzt weil ich selber von einigen Protokollen profitiert habe während des Lernens. Die Arbeit für euch ist minimal und es werden euch Generationen von Studenten danken.

Wenn ihr meint nicht die gesamte Unterhaltung im Kopf zu haben schreibt ihr halt nur das hin was ihr noch wisst, und wenn euch eure Note zu peinlich ist könnt ihr ein anonymes Protokoll schreiben, das ist besser als eins ohne Note. Ob ihr euer Protokoll nur an die Fachschaft gebt oder auch auf Seiten wie s-inf.de hochladet bleibt euch überlassen.