Praktische Informatik

Gedächtnisprotokoll zur mündlichen Diplomprüfung
17. März 2010 (WS 2009/10, RWTH Aachen)

Florian Weingarten

Inhalt:

- Peer-to-Peer Systeme (aka. Massively Distributed Systems) (V3, nach Vorlesung im WS 2009/10)
- Sichere verteilte Systeme (aka. Communication Systems Engineering I) (V3, nach Vorlesung im SS 2009)
- IT Security I+II (V3+V3, nach Folienskript von SS 2009 und WS 2009/10)

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: ca. 50 Minuten

Prüfungsnote: 1.3

Achtung: Hierbei handelt es sich *nicht* um ein offizielles Prüfungsprotokoll der RWTH sondern um ein privates Gedächtnisprotokoll, das ca. eine Stunde nach der Prüfung angefertigt wurde. Ich habe mit Sicherheit einige Sachen vergessen und gebe natürlich keine Garantie auf Korrektheit.

Prof. Wehrle fragt mich ob ich eine bestimmte Reihenfolge haben möchte. Ich wähle SVS, P2P und zuletzt IT Security.

Sichere verteilte Systeme

- Wozu will man ein Schichtenmodell? (Abstraktion, Kapselung, Austauschbarkeit unterer Layer, etc.)
- Welche Schichten gibt es im OSI Modell? Beispiel für ein Protokoll des Presentation Layer? (ASN1)
- Allgemein: Was sind Dienste, Dienstprimitive, etc.
- Mal das Beispiel „Ich werfe einen Brief in einen Briefkasten“ ins Schichtenmodell einordnen und alles durchkauen (für welche Schicht sind Adresse und Briefmarke relevant, was ist die ICU, ICI, PCI, etc.)
- Schicht 1 genauer erklären (Welche Aufgaben? Wozu braucht man Leitungscodes?)
- 4B5B Leitungscode genau erklären
- Character Stuffing und Bit Stuffing
- Unterschied Layer 2a und Layer 2b
- Flusskontrolle auf Layer 2 (Stop-and-Wait, XON/XOFF, ...)

Peer-to-Peer Systeme

- Unterschied: unstrukturiertes vs. strukturiertes P2P System
- TTL bei Gnutella erklären (Was ist, wenn das Netz sagt, dass die Daten nicht da sind?)
- Pastry erklären (Geometrie, Flexibilität in Routen- und Nachbarschaftswahl, Join erklären (Routing Table Zeilenweise von anderen Knoten kopieren und anpassen), Proximity, ...)

IT Security 1

- Diffie-Hellman erklären (was ist das, welche Parameter gibt es, auf welcher Annahme basiert die Sicherheit, wie geht Man-in-the-Middle, ...)
- Wie kann man Diffie-Hellman gegen Replay Attacken schützen?
- Wie kann man Authenticated Diffie-Hellman machen?
- Wie wirds bei IKEv1 und bei TLS gemacht?
- Was sind digitale Signaturen? Was steht in einem Zertifikat drin? (Public Key, Ablaufdatum, für wen wird es ausgestellt, etc.)
- Wie kommen die Zertifikate in die Browser? Wer entscheidet, welche darein kommen? (Frau Meyer wollte darauf hinaus, dass viele Zeritifkatsaussteller sich in die Browser „einkaufen“ und das nicht so toll ist)

IT Security 2

- Bisschen was zu Phishing
- Biometrie (Unterschied zu Passwortauthentifizierung, Inter- und Intraclass, False Reject Rate, False Accept Rate, ...)
- Unterschied zwischen Smartcards und Magnetstreifenkarten
- Wenn man am Terminal seine PIN eingibt, authentifiziert man sich dann gegenüber der Karte, der Bank oder dem Terminal?
- SET erklären (Dual Signatures, ...)
- Was glauben Sie warum sich SET nicht durchgesetzt hat?
- Phishing in Bezug auf Kreditkarten (wer leidet darunter am meisten, Banken, Kunden oder Verkäufer?)

Fazit

Die Prüfungsatmosphäre war sehr angenehm. Beide Prüfer waren sehr locker drauf. Herr Wehrle hatte eine Schüssel mit Süßigkeiten und Getränke auf dem Tisch stehen, die er einem anbietet. Die ganze Prüfung wirkte wie eine „Plauderstunde“. Ich habe nur sehr wenig Sachen aufgeschrieben, fast alles mündlich gemacht. Prof. Wehrle ist leider ewig lange auf seinem Post-Beispiel rumgeritten, wobei ich mich etwas verhaspelt habe.

Prof. Wehrle fragt alles aus dem Stehgreif und meiner Einschätzung nach nicht sehr ins Detail, Prof. Meyer dagegen hat sich mehrere Zettel vorbereitet und fast alle Fragen von Ihren Zetteln abgelesen. Was mich sehr irritiert hat ist, dass Frau Meyer einem keinerlei Gestik als Feedback gibt. Sie stellt eine Frage und hört danach einfach zu was man zu erzählen hat ohne eine Miene zu verziehen, was dazu führt, dass man sich nicht sicher ist, ob man völligen Mist oder genau das richtige erzählt.

Ich würde eigentlich beide als Prüfer weiterempfehlen. Die Vorlesungen aber nur bedingt. Jemand der Wert auf exakte Definitionen legt ist hier leider oft (bei allen vier Vorlesungen) nicht ganz richtig aufgehoben. Beim Lernen muss man sich ungewöhnlich viele Dinge selber zusammenreimen, weil viele Sachen zu oberflächlich und für meinen Geschmack zu „unmathematisch“ behandelt werden, was auf die Dauer leider etwas nervt.

Lernzeit waren für alle vier Vorlesungen insgesamt etwa 4 Wochen, das ist (in einer Gruppe) aufjedenfall nicht zu wenig (auch wenn Prof. Wehrle auf seiner Webseite eine Lernzeit von 3 Monaten für seine Prüfungen empfiehlt ;-)).