Prüfungsprotokoll Vertiefung - Freiling geb. Gärtner
Verlässliche verteilte Systeme I+II (je V4), Information Warfare (V2), Datenkommunikation (V2)

Matthias Hensler

14. Juli 2005

Beisitzer war Martin Mink.

Professor Freiling ließ die Wahl der Reihenfolge. Wir einigten uns auf die Theorie (VVS II) und dann ein Konglomerat aus VVS I, InfoWar und Datkomm. Insgesamt wurden die Fächer tatsächlich so geprüft, daß man eigentlich keine Grenze zwischen den Fächern ziehen kann und eher ein Überblick über das gesamte Vertiefungsgebiet gefragt wurde.

Die Prüfung dauerte etwa 45 Minuten, wobei ich die Zeit für Theorie auf etwa 20 Minuten schätzen würde. Grundlagen waren für VVS I+II die Vorlesungsfolien aus dem WS 2004/05, bzw. SS 2004, für Information Warfare das Buch von Denning, und DatKomm hab ich anhand der Folien aus dem WS 2004/05 gelernt (gehört habe ich DatKomm jedoch als V4 im WS 2001/02 mit doch recht unterschiedlichen Stoff, weshalb wir uns mehr oder weniger auf Protokolle und TCP/IP beschränkt haben und die Vorlesung nur als V2 geprüft wurde).

Für die Vorbereitung haben wir 2,5 Monate zur dritt gelernt, wobei die meiste Zeit in VVS II investiert wurde.

- Womit sollen wir am liebsten anfangen? *(auf CHT geeinigt)*
- Mit CHT haben wir ja gezeigt das Ω der schwächste Fehlerdetektor für Consensus ist, wie geht man generell vor um eine solche Aussage zu treffen? *(zeigen das der Fehlerdektor ausreichend ist um Algorithmus zu implementieren und mit beliebigen Algorithmus den Fehlerdektor emulieren)*
- Wie läuft das bei CHT? *(durch FLP gezeigt das Fehlerdektor notwendig ist für Consensus. Algorithmus für $\diamond S$ gehabt (was ja äquivalent zu Ω), jetzt für Statemachine A und Fehlerdetektor D versuchen Ω zu emulieren. Dafür CHT grob umrissen (Exchange, Simulation, Tagging, sowie ansatzweise Korrektheit durch Stabilization und Extraction erläutert). Problem*

des bivalenten Zustands beim kritischen Index vom Tagging erwähnt, und das der vollständige Beweis in der Vorlesung nicht dran war)

- Der kritische Index wird ja zwangsläufig immer kleiner (u.a. auch Argument des Beweises, das der Index ja kleiner wird wenn er abstürzt), erreicht er nicht immer 1? *(Frage und Antwort hier sicher unvollständig und ungenau wieder gegeben, auch nicht ganz verstanden. Lief darauf hinaus, daß (mit dem vom Professor vorgeschlagenem Argument) dann auch die Konfiguration* c_0 *bivalent sein müsste, was die Eigenschaft von Consensus verletzt)*

- Wo fließen die Eigenschaften von Consensus im Beweis ein? *(dieser ganze Abschnitt war ein wenig schwammig und unpräzise und mehr durch Ideen geprägt, wie z.B. die Integrity dadurch gewährleistet ist, daß wenn sich in einem Pfad im DAG einmal entschieden wurde auf diesem Pfad nichts anderes mehr rauskommen kann. Termination aufgrund des Taggings und dem Aufbau des DAGs. Agreement schließlich durch die gesamte Beweiskonstruktion)*

- Wir hatten noch ein Problem für das Ω ausreichend war? *(erst TRB gesagt, aber durch Erläuterung des Algorithmus direkt klar das noch viel stärker als Consensus)*

- Wir hatten verschiedene Broadcast-Algorithmen... *(klar: Reliable Broadcast mit Total Order Eigenschaft. Kurz Idee mit Best-Effort Broadcast und anschließendem Consensus umrissen)*

- Es könnte sein, daß die Source abstürzt nachdem einige Prozesse die Nachricht bekommen haben, aber diese kommt nicht aus dem Consensus raus, weil der sich zufällig immer für eine der anderen Nachrichten entscheidet. Ist das ein Problem? *(die Eigenschaften setzen eventual delivery nur für korrekte Prozesse voraus, der Algorithmus klappt also)*

- In VVS I haben wir von Safety gesprochen, gibt es sowas auch bei VVS II? *(Byzantine angesprochen und was damit modelliert werden kann)*

- Helfen Protokolle die byzantinische Eigenschaften erfüllen auch in der Praxis für Sicherheit? *(zunächste argumentiert, daß in der Praxis die byzantine Prozesse sich „verschwören“ können, trotzdem geht ja Byzantine vom worst-case aus, also nicht wirklich das Argument. Tatsächlich liegt in der Praxis keine stochastisch unabhängige Verteilung vor, so daß bei identischen Systemen alle gleich verwundbar sind und man schwierig die Voraussetzung mit* $n > 3t$ *erfüllen kann)*

- Klassifizierung und Maße für die Verfügbarkeit von Systemen? *(Zuverlässigkeitsfunktion, MTTF,* $v(t)$*, Erwartungswert, bei konstanter Ausfallrate* $e^{-\lambda t}$*, Badewannenkurve, etc.)*

- Einsatz in der Praxis, falls Systeme im 10 jährigen Tests beispielsweise immer nach 10 Minuten gehackt waren, wäre die MTTF nur 10 Minuten, ist das sinnvoll? *(solche Metriken am besten nur auf Hardware einsetzen, im Sicherheitsbereich problematisch und wenig aussagefähig)*

- Wenn man die eMails auf meinem Laptop lesen wollte, wie würde man vorgehen? *(generell erstmal IP rausfinden, Portscan um offene Ports zu finden, für diese versuchen Exploits einzusetzen, etc.)*

- Weitere Szenarien denkbar? *(im lokalen Netzwerk mitsniffen, z.B. bei Hubs mit Netzwerkkarte in Promiscuous Mode, oder durch ARP-Spoofing)*

- TCP Connection Hijacking für Telnet? *(Client mit RST abhängen, richtige Sequenznummern erraten und mit Server kommunizieren)*

- Datkomm: wie funktioniert das mit den Sequenznummern? *(zwei Stück, eine je Seite. Pakete enthalten eigene Sequenznummer die hochgezählt wird, sowie Sequenznummer des nächsten Pakets welches man von der Gegenseite erwartet)*

- Wie geht Denning grundsätzlich in ihrem Buch vor? *(zwei Parteien: Offensive und Defensive, arbeiten auf Informationsressourcen, eingeteilt in Container, Transporter, Sensoren, Rekorder und Prozessoren)*

- Parallelen zu Sicherheit in VVS I? *(beispielsweise Noninterference, Informationstransport über Covert Channels wie CRT-Monitore über Van-Eck Sensoren mitlesen)*

- Schutz davor? *(abgeschirmte Räume, spezielle Zugangskontrollen, etc. viel aufgezählt...)*

- Wenn der Verdacht besteht das in meinen Rechner eingebrochen wurde, wie vorgehen? *(Logfiles auf Anomalien prüfen, z.B. auch auf extra Logsserver vorhalten. Festplatte ins sichere System und untersuchen, ...)*

- Kann ich davon ausgehen das mein andere System tatsächlich sicher ist? *(nein, immer Vertrauen in entsprechende Komponenten notwendig. Je nach Einsatzgebiete so viel wie möglich selber konstruieren/überprüfen, etc.)*

- Passwort bei SSH erraten? *(wenn gutes Passwort gewählt nicht praxistauglich, da Wartezeit zwischen jedem Fehlversuch, ggf. aber Brute-Force mit Standard User-/Passwortkombinationen gegen viele Systeme um Erfolg zu steigern)*

- Was für Ähnlichkeiten der offensiven und defensiven Methoden die Denning beschreibt hatten wir in VVS I? *(einige aufgezählt: für Defensive z.B. Signaturen, Zugangskontrollen, Verschlüsselung, für Offensive beispielsweise Schwachstellen, Spoofing, ...)*

Fazit

Schwierigkeiten hatte ich hauptsächlich mit MTTF bei der ich mal wieder einige Sachen durcheinander geworfen habe. Ansonsten wurde sehr breit gefragt, aber auch so, daß ich immer sehr gut Dinge erläutern und aufzählen konnte.

Die Prüfung war insgesamt sehr locker und angenehm. Meistens reichte es Beispiele zu bringen und näher drauf einzugehen, ohne alles bis ins letzte Detail erklären zu müssen. Der Prüfungsstoff war gut abgedeckt und stark übergreifend abgefragt. Eine Grenze, wie schon eingangs erwähnt, läßt sich höchstens zwischen VVS II und dem Rest der Fächer ziehen.

Kleinere Schwächen fielen nicht ins Gewicht. Es wurde mehr Wert auf breite Abdeckung gelegt und das zu jedem Gebiet überzeugend was erzählt werden konnte. Die Prüfung wurde mit 1.0 bewertet.