# Prüfungsprotokoll
## Diplomprüfung Vertiefungsgebiet „Verlässliche Verteilte Systeme“

**Prüfer:** Prof. Freiling geb. Gärtner (FF)

**Beisitzer:** Martin Mink (MM)

**Prüfling:** Matthias Majuntke (P)

**Prüfungsstoff:** Verlässliche Verteilte Systeme 1 (V4)
Verlässliche Verteilte Systeme 2 (V4)
Datenkommunikation (Spaniol/Thissen) (V3)
Teil V aus dem Buch *Practical Unix & Internet Security* von Simson, Garfinkel

**Prüfungsdatum:** 21. April 2005

**Note:** 1.0

**Allgemeines:** Die Prüfungsatmosphäre war sehr angenehm. Mir kam die Prüfung ziemlich lang vor (ca. 50 min.) – es wurden also noch viele kleine Fragen zwischendurch gestellt, die ich aber nicht alle aufgeschrieben habe. Ich habe das Protokoll nach bestem Wissen und Gewissen erstellt, bin mir aber nicht sicher, ob es wirklich vollständig ist. Ich wünsche allen, die sich von Prof. Freiling prüfen lassen, ebensoguten Erfolg.

## Protokoll

**FF:** Womit sollen wir denn anfangen? Haben Sie sich schon eine Reihenfolge ausgesucht?

**P:** Ich würde am liebsten mit VVS2 anfangen.

**FF:** Dann fangen wir mit der Theorie an und werden dann immer praktischer. Haben Sie einen Vorschlag für den Einstieg? Was hat Sie denn in der VVS2 besonders interessiert?

**P:** Ich fand die Byzantine-Sache ganz interessant.

**FF:** Warum nennt man die byzantine Prozesse denn byzantine? Da gibt es so eine Geschichte. Erzählen Sie diese doch mal.

**P:** Es waren einmal mehrere Generäle, die mit ihren Divisonen... (Geschichte erzählt)

**FF:** Wie ist das BGP denn formell definiert?

**P:** Persistency, Consistency, Termination erklärt

**FF:** Da gibt es so eine grundlegende Annahme bezüglich der Anzahl der fehlerhaften Prozesse. Wie beweist man die denn?

**P:** Die Annahme ist $n > 3t$. Dann Gegenbeispiel für drei Prozesse erklärt, von denen einer fehlerhaft ist.

**FF:** Wie beweist man das für $n$ Prozesse?

**P:** Reduktion erklärt, $\frac{n}{3}$ Prozesse simulieren einen Prozesse der unterliegenden Schicht.

**FF:** Wir hatten in der Vorlesung zwei Prozesse, die BGP lösen. Erläutern Sie doch mal einen.

**P:** Consensus in fünf Stufen erläutert - zwischendurch einige Zwischenfragen welche Eigenschaften warum und wie erfüllt werden.

**FF:** Sie haben jetzt erklärt wie man Consensus löst, aber das ist doch nicht das BGP?

**P:** BGP, BA, IC sind äquivalent.

**FF:** Wie zeigt man das?

**P:** BGP→BA und umgekehrt erklärt.

**FF:** Das mit den fünf Stufen ist ja ziemlich kompliziert. Der andere Consensus-Algorithmus ist doch viel einfacher. Warum nimmt man den denn nicht einfach.

**P:** Wegen der exponentiellen Komplexität.

**FF:** Warum ist die Komplexität exponentiell?

**P:** In Grundzügen den Algorithmus erläutert. Der Algorithmus wird $n \cdot (n-1) \cdot (n-2) \cdots$ mal rekursiv aufgerufen.

**FF:** Wie ist denn ein synchrones System definiert?

**P:** Schranken auf Nachrichtenlaufzeit und Taktgeschwindigkeit der Prozessoren (hier stand ich zuerst ein wenig auf dem Schlauch)

**FF:** Da gibt es die Idee mit den Synchronizern...

**P:** Synchronizer erklärt

**FF:** Wie sieht denn für einen Prozess so ein synchrones System aus?

**P:** ? Prozess läuft in Schleife: Führt seine Anweisungen aus, dann `tick()`.

**FF:** Übergang zur Praxis. Es wird ja oft von Zuverlässigkeit und Verfügbarkeit gesprochen. Was ist denn da der Unterschied?

**P:** Zuverlässigkeit: Wahrscheinlichkeit, dass das System bis Zeitpunkt $t$ noch nicht ausgefallen ist. Verfügbarkeit: Wahrscheinlichkeit, dass das System zum Zeitpunkt $t$ nicht ausgefallen ist.

**FF:** Geben Sie doch mal ein Beispiel für ein System, das zuverlässig, aber nicht verfügbar ist und umgekehrt.

**P:** Beispiele aus der Vorlesung ...

**FF:** Ein Händler, der im Internet einen Online-Shop betreibt, was ist für den wichtiger?

**P:** Verfügbarkeit

**FF:** Wenn man die Zuverlässigkeit mit wenig Aufwand erhöhen möchte, kann man ja z.B. IP-Failover machen. Malen Sie doch mal auf.

**P:** Hingemalt und erklärt. Auch wie die Übernahme der IP-Adressen funktioniert. Zwischendurch einige Zwischenfragen, z.B. warum extra LAN oder serielles Kabel zur Fehlererkennenung.

**FF:** Wie ist denn die Zuverlässigkeit von zusammengesetzen Systemen, insbesondere von IP-Failover?

**P:** Doppelt so lange MTTF

**FF:** Bei IP-Failover haben Sie ARP-Reply erwähnt. Das kann man ja auch für Spoofing einsetzen. Was ist denn das?

**P:** Spoofing: Austausch der Absenderadresse. Beispiel für ARP-Spoofing (Man-in-the-Middle) und IP-Spoofing (DNS) gegeben.

**FF:** Malt zwei Prozesse, die mittels Telnet kommunizieren hin. Mit IP-Spoofing kann man ja auch eine bestehende Verbindung übernehmen. Wie und warum geht das denn?

**P:** Richtige Sequenznummer raten und losschicken.

**FF:** Was für eine Sequenznummer? Erläutern Sie doch mal TCP und IP

**P:** Hier habe ich dann TCP/IP erklärt. Es wurden noch mehrere Fragen gestellt, den Verbindungsauf- und abbau sollte ich hinmalen...

**FF:** Wie kann man denn eine Verbindung abhängen?

**P:** Gesetztes RST-Flag an den einen.

**FF:** Kann man das alles auch bei SSH machen?

**P:** SSH erklärt. Nachrichten Einschleusen: nein; Man-in-the-Middle bei schlechtem Schlüsselmanagement schon.

**FF:** Im IP-Header gibt es ja noch das Identification-Feld. Wofür ist das denn gut?

**P:** Fragmentierung

**FF:** Ja da gibt es noch so ein Port-Scanning wo man das Feld benutzt...(ihm fällt der Name nicht ein)

**P:** Idle-Scanning

**FF:** Das scheinen Sie ja zu wissen, da brauch ich also nicht weiterfragen. Was gibt es denn im Netz für Möglichkeiten von DoS?

**P:** Man kapert z.B. andere Rechner und macht verteiltes DoS.

**FF:** Was kann ich mit nur einem Rechner machen

**P:** Prinzipiell den anderen mit Anfragen überlasten, hängende TCP-Verbindungen,... Hinweis, das sowas aber von einem guten IDS verhindert wird.

**FF:** Wenn man in einer Firma den Verdacht hat, das ein Mitarbeiter geheime Daten an die Konkurrenz weitergibt, was kann man denn da machen?

**P:** Falls er die Daten elektronisch weitergibt, dann kann man seine Aktivitäten am Rechner aufzeichnen.

**FF:** Ist das denn erlaubt?

**P:** Wenn es im Arbeitsvertrag so vereinbart wurde, dann schon.

**FF:** Wie kann man denn feststellen, ob jemand auf mein System eingebrochen ist?

**P:** Logdateien analysieren, auf untypisches Verhalten achten, Integritätschecks gegen Backups oder mit z.B. Tripwire...

**FF:** Soll ich dann immer die Polizei verständigen?

**P:** Wenn der Schaden ein gewisses Maß übersteigt, eigentlich schon.

**FF:** Wenn ich eine Firma bin, die selbst Security-Produkte vertreibt, würde ich dann auch jeden Einbruch melden?

**P:** Dann vielleicht nicht. Das würde dann öffentlich werden und somit peinlich für mich.

**FF:** Hat noch jemand eine Frage?

**MM:** Wie kann man denn IP-Spoofing auf Protokollebene verhindern?

**P:** ??? – Er wollte darauf hinaus, dass IPv6 mit Krypto Authentifizierung ermöglicht und wie das funktioniert. Das wusste ich zwar nicht, aber habe erwähnt, dass IPsec und IPv6 diese Möglichkeit bieten.

**FF:** Dann gehen Sie doch bitte mal nach draußen...