

## Prüfungsprotokoll

Kurs: 1678 Verteilte Systeme  
Prüfling: Guenther Rasch  
Prüfer: Prof. Dr. Icking  
Datum: 26.11.2010 / 10:40 Uhr

### Verteilte Systeme

- Definition der vert. Systeme, deren Eigenschaften, Vor- und Nachteile erläutert
- Transparenz detaillierter erklärt, verschiedenen Arten aufgezählt und Fehler- und Nebenläufigkeitstransparenz erklärt

### Kommunikation

- Internet-Schichten-Modell aufgezählt und mit OSI-Modell verglichen, den Kommunikationsfluss zwischen den Schichten erklärt (z.B. Vermittlungsschicht = logische Host-zu-Host-Verbindung...)
- Vermittlungsschicht genauer erklärt (Aufgaben, Dienste, Bestandteile)
- Transportschicht mit UDP/TCP erklärt: Unterschiede zwischen den Protokollen, Anwendungen aufgezählt

### Zeitsynchronisation

- Varianten aufgezählt und warum Zeitsynchronisation wichtig ist
- als Verfahren NTP erklärt

### Kryptographie

- warum Kryptographie? → Ziele
- welche Verfahren gibt es grundsätzlich (symmetrisch / asymmetrisch) und wo liegen die Stärken und Schwächen
- unterschiedliche Verfahren für symmetrische und asymmetrische Verfahren aufgezählt (Verschiebechiffre, Substitutions-Chiffre, Vigenere-Chiffre usw.)
- Angriffsmöglichkeiten bei Verschiebe- und Substitutions-Chiffre und warum → Häufigkeitsanalyse der Sprache, Buchstaben-Verteilung
- Vigenere-Chiffre erklärt, Angriffsmöglichkeit mittels Koinzidenz-Index erklärt
- RSA: wie funktioniert es? → grundlegendes mathem. Problem, Schlüsselaustausch
- Signatur, wie funktioniert diese

### Verteilte Dateisysteme

- NFS: welche Transparenz, wie funktioniert NFS, der Vorgang des Mountens
- CVS: Funktionsweise, welche Erfordernisse aus der Gruppenarbeit werden erfüllt, wie funktioniert das Arbeiten mit CVS mit Versionen (Merge! erklärt) und ist es auch für Einzelpersonen nützlich und warum?

## **Fazit:**

Hr. Prof. Dr. Icking ist absolut als Prüfer zu empfehlen. Nachdem die Prüfung aufgrund technischer Schwierigkeiten (Videoprüfung) einen „schweren Start“ hatte, war der Prüfungsverlauf mit einer lockeren Einleitung wieder auf Kurs. Hr. Prof. Dr. Icking versteht es einfach, nicht das Gefühl einer klassischen Prüfungssituation aufkommen zu lassen. Ich wurde von ihm bereits mit 1802 geprüft und hatte wieder das Gefühl, ein Fachgespräch zu führen; absolut angenehme Situation!

Ich kann jedem Prüfling nur empfehlen, sich wie auf einen Vortrag vorzubereiten. Fragen kamen eigentlich nur zur Einleitung eines Themenbereichs; ich habe versucht, möglichst frei die Schwerpunkte darzustellen. Es kamen dann vereinzelt Zwischenfragen, aber insgesamt lief die Prüfung sehr flüssig ab und Prof. Dr. Icking ergänzte manches noch mit Kommentaren / Ausführungen.

# Prüfungsprotokoll

*Kurs:* 01678 – Verteilte Systeme

Datum: 29.03.2010

Prüfer: Dr. Christian Icking

Beisitzer: Dr. Lihong Ma

Dauer: 30 Minuten

Note: 1,0

---

## Fragen:

- Was ist ein verteiltes System?
- **Transparenz**
  - Was ist Transparenz?
  - Welche Arten von Transparenz gibt es?
- **Replizierte Systeme**
  - Welche Besonderheiten gibt es hier (Konsistenz + Aktualität müssen sicher gestellt werden)
  - Welche Mechanismen gibt es dazu?
- **Verschlüsselung**
  - Warum verwendet man Verschlüsselung? (Integrität, Authentifizierung, ...)
  - Welche Arten gibt es? (symmetrisch / asymmetrisch)
  - Wie sieht es mit der Leistungsanforderung bei beiden Verfahren aus? (asymmetrisch benötigt mehr Rechenzeit)
  - Was ist das Problem bei der symmetrischen Verschlüsselung? (Schlüssel muss übertragen werden)
  - Gibt es da eine Lösung? (Ja: Diffie-Hellman)
  - Wie funktioniert das?
  - Wie funktioniert RSA?
- **Versionsverwaltung**
  - Wer braucht so was?
  - Wozu wird das verwendet? (Aktualität, Isolation, ...)
  - Welche Befehle kennen Sie?
  - Was bedeutet Awareness?
  - Wie kann man das bei CVS realisieren? (Anzeige bzw. versenden von Emails)
- **Uhrzeitsynchronisation**
  - Wozu benötigt man das?
  - Wie funktioniert NTP?

## Fazit:

Dr. Icking ist unbedingt als Prüfer weiterzuempfehlen. Am Anfang der Prüfung fragt er, was man beruflich macht und ob man da auch etwas mit verteilten Systemen zu tun hätte. Er versucht allgemein die Atmosphäre zu lockern, was auch sehr gut klappt. Gegebenenfalls wird noch einmal nachgehakt, wenn man etwas nicht genau erklärt hat oder er weist einen in die richtige Richtung.

Die Prüfung wurde von Herrn Dr. Icking durchgeführt. Beisitzerin war Frau Dr. Lihong Ma. Herr Icking hat es verstanden durch ein kurzes Vorgespräch meine Nervosität verfliegen zu lassen. Die Atmosphäre war während der gesamten Prüfung sehr freundlich und hatte eher den Charakter eines netten Fachgesprächs. Die Prüfung wurde mit 1,3 benotet. Von Herrn Icking wurden folgende Themen angesprochen:

- Was ist ein verteiltes System?
  - Was ist Transparenz allgemein und einige Transparenzarten im Detail?
  - Was ist Migration?
  - Protokoll-Schichtenmodell:
    - Wofür gibt es die Transportschicht?
    - Was macht die Transportschicht?
    - Was ist TCP?
    - Was ist UDP?
    - Was ist der Unterschied zwischen TCP und UDP?
    - Beispiele für Anwendungen von TCP und UDP mit Begründung.
    - Wofür gibt es die Vermittlungsschicht?
    - Was ist IP?
    - Wie funktioniert Vermittlung?
  - Was sind die Ziele der Kryptographie?
  - Welche kryptographischen Verfahren kennen Sie?
  - Welche Angriffsmöglichkeiten gibt es allgemein?
  - Welche Angriffsmöglichkeiten gibt es beim Vigenere-Verfahren? (Koinzidenzindex wichtig!)
  - Welche asynchronen Verfahren kennen Sie?
  - Wie ist der Ablauf von RSA?
    - Wie wird ein Schlüsselpaar erstellt?
    - Was wird mit dem öffentlichen Schlüssel gemacht? (Veröffentlicht, direkt oder über ein TrustCenter)
    - Wie wird eine Nachricht verschlüsselt?
    - Wie wird eine Nachricht signiert?
  - Was ist eine Versionsverwaltung?
  - Wofür braucht man eine Versionsverwaltung? Was sind die Vorteile?
  - Warum sollte man CVS auch nutzen, wenn man alleine an einem Projekt arbeitet? (Backup, Log)
-

Gedächtnisprotokoll Mündliche Prüfung 1678 – Verteilte Systeme  
Bachelor-Studiengang  
Datum: 31.03.2008  
Prüfer: Herr. Dr. Icking  
Beisitzer: Frau Dr. Lihong Ma  
Dauer: ca. 30 Min  
Note: 1,0

**Was ist ein verteiltes System? Was ist der Sinn und Zweck von verteilten Systemen?**

**Transparenz, was ist das und was versteht man unter den jeweiligen Unterkategorien?**

**Was macht TCP? Unterschiede zu UDP? Nennen Sie Beispiele für die jeweiligen Protokolle. Warum verwendet man UDP für DNS und nicht TCP? Wie ist das Schichtenmodell aufgebaut?**

**Welche Protokolle gibt es denn auf der Anwendungsschicht?**

**Was macht http genau? Wie funktioniert das mit den URLs, wie sind Sie aufgebaut?**

**Was macht ftp genau? Welche Befehle für ftp kennen Sie? Wie ist es mit der Sicherheit bei ftp? Warum hat man dennoch ftp eingesetzt und warum setzt man es heute immer noch ein, wenn es doch unsicher ist?**

**Warum verschlüsselt man die Kommunikation?**

**Welche Verschlüsselungsverfahren kennen Sie? Wie funktioniert DES? Wie funktioniert das mit dem privaten Schlüssel und wie funktioniert das mit dem öffentlichen Schlüssel?**

**Was sind denn die Vorteile bei der Verwendung von Public-Key-Verfahren? Wie kann man denn die Vorteile von beiden Verfahren nutzen und wie macht man das? (Stichwort: Austausch des symmetrischen Schlüsselwortes über asymmetrisches Verschlüsselungsverfahren)**

**Welche Möglichkeiten zur Verbesserung von Gruppenarbeit kennen Sie?**

**Was ist CVS und wie funktioniert es genau? Was sind die Anforderungen an ein CVS? Was ist ein Merge und wie funktioniert das?**

**Unterstützt BSCW auch zwei gleiche Versionen wie es in CVS gehandhabt wird?**

Hr. Dr. Icking schafft eine angenehme Prüfungsatmosphäre in der die Nervosität schnell verfliegt. Bei den Fragen kommt es stark auf das Verständnis des Zusammenhangs an, aber auch Detailwissen. Die Fragestellungen sind entgegen dem obigen Eindruck relativ „offen“ gestellt. Man sollte also vermeiden nur irgendwelche Stichpunkte hinzuklatschen und sich vom Prüfer alles aus der Nase ziehen zu lassen, sondern versuchen in seinen Antworten auch stets die Zusammenhänge zu erläutern und darzustellen. Als Prüfer kann ich Dr. Icking uneingeschränkt empfehlen.

**Gedächtnisprotokoll - Fachprüfung Kurs 1678 „Verteilte Systeme“ - Bachelor Informatik**  
**Prüfer: Dr. Icking**  
**Beisitzerin: Dr. Ma**  
**Datum: 07.04.08**  
**Note: 1,0**

Dr. Icking begrüßte mich in seiner bekannt lockeren Art und wir haben uns dann kurz über den Verlauf meines Studiums und über den Kurs unterhalten. Ich konnte es mir nicht verkneifen, über die fürchterliche deutsche Übersetzung des Basistextes zu lästern ;-). Danach ging es sofort mit der Prüfung los.

**Was überhaupt sind verteilte Systeme?**

**Wie unterscheiden Sie sich von Großrechnern? (Vorteile / Nachteile)**

**Was ist mit Transparenz gemeint?**

**Was ist mit Fehlertransparenz gemeint?**

**Wie funktioniert das Client-Server Modell?**

**Welche Alternativen zum Client-Server -Modell gibt es?**

**Welche Arten von P2P Netzwerken gibt es? Wie funktioniert die Suche nach Diensten?**

**Die andere Alternative zum Client-Server-Modell?**

**Welchen Problemen begegnet man bei den replizierenden Systemen?**

**Was ist das ISO/OSI-Referenzmodell?**

**Was sind Protokolle / Dienste?**

**Was sind Firewalls?**

**Was ist SSL?**

**Was ist SSH?**

**Wieso wird Verschlüsselung angewendet?**

**Wo kann man das einsetzen?**

**Prinzipielle Arbeitsweise der asymmetrischen Kryptosysteme?**

**Wie ist der Ablauf beim Versenden einer verschlüsselten E-Mail?**

**Wie ist der Ablauf beim Versenden einer signierten E-Mail?**

**Mathematische Grundlagen von RSA?**

**Wieso werden asymmetrische Verfahren nicht zur Verschlüsselung großer Datenmengen verwendet?**

**Wie kann verteilte Kooperation an einem Softwareprojekt aussehen?**

**Wie funktioniert CVS?**

**Welche sind die meistbenutzten Befehle von CVS?**

**Wie läuft der Merge ab?**

**Wann findet der Merge statt?**

**Was passiert, wenn ein automatischer Merge nicht stattfinden kann?**

Dann war der offizielle Teil der Prüfung zu Ende, ich habe noch einiges über meine praktische Erfahrungen mit verteilten Systemen erzählt, dabei sind wir speziell auf Versionskontrollsysteme eingegangen. Auch während der Prüfung habe ich sehr viele Fragen im Kontext meiner beruflichen Praxis beantwortet. Alles in allem, eine recht entspannte Prüfungsatmosphäre, bezüglich der Fragen gab es keine Überraschungen. Ich kann Dr. Icking als Prüfer uneingeschränkt empfehlen.

Gedächtnisprotokoll Mündliche Prüfung 1678-Verteilte Systeme  
Bachelor-Studiengang  
Harry Hübner  
Datum: 15.02.2008  
Prüfer: Dr. Icking  
Dauer: ca. 30min

Was ist ein verteiltes System?

Ziele eines verteilten Systems?

Vorteile eines verteilten Systems gegenüber einem zentralen System?

- Wirtschaftlichkeit
- Verteiltheit bietet in manchen Fällen natürlichere Lösungen
- Geschwindigkeit
- Skalierbarkeit

Transparenz. Welche Arten von Transparenz gibt es?

Was ist NFS?

Wie funktioniert NFS?

Was muss man auf dem Server und auf dem Client tun, damit NFS funktioniert?

Mounten und Automounter näher erläutern

Bietet NFS Unterstützung um gemeinsam an einer Datei zu arbeiten?

Von diesem Thema aus sind wir übergeleitet auf CVS.

Was benötigt man, wenn man gemeinsam an Dateien arbeiten will?

Anforderungen an ein CVS?

- Aktualität
- Isoliertheit
- Integration
- ...

Einige Befehle von CVS erläutern?

Wenn ein Merge notwendig ist, wo wird dieser ausgeführt?

- Hier ist wichtig, dass der Merge nicht auf dem Server ausgeführt wird, sondern die Änderungen lokal mittels Update übernommen werden. Der Benutzer committed die gesamte Datei samt seinen Änderungen.

Warum ist Verschlüsselung notwendig?

Eigenschaften eines sicheren Systems aufzeigen

- Vertraulichkeit
- Integrität
- ...

Welche Angriffe gegen einen verschlüsselten Text gibt es?

Wie kann man Vigenere brechen?

Warum gibt es Verfahren mit öffentlichem und geheimen Schlüssel?

Funktionsweise RSA?

Grobe Funktionsweise der Mathematik hinter RSA?

Funktionsweise Digitale Signatur?

Kann man einen Text signieren und verschlüsseln?

Welche verbindungslosen und verbindungsorientierten Übertragungsverfahren gibt es?

Herr Dr. Icking ist als Prüfer uneingeschränkt zu empfehlen. Er schafft eine angenehme Atmosphäre, in der die Aufregung schnell verfliegt.

Kurzprotokoll der Prüfung zum Kurs „Verteilte Systeme“ (1678) im Bachelor-Studiengang Informatik bei Herrn Dr. Icking am 09.03.2007

Was ist ein verteiltes System?

(vernetzte autarke Rechner, Zweck: gemeinsame Nutzung von Ressourcen, Skalierbarkeit, Transparenz, Verfügbarkeit, Openness etc.)

Was genau ist mit Transparenz gemeint?

(inkl. Beispiele)

Wie wird Transparenz bei NFS erreicht? Wie genau funktioniert NFS? Wie kommt der Client an die Dateien? -> Automounting etc.

Wie kann man sinnvoll gemeinsam an den gleichen Dateien arbeiten?

CVS erläutern: Repository, wichtige Befehle, Merging etc.

Sicherheit: Was muss geschützt werden? Womit kann dies erreicht werden?

Verschlüsselung mit privaten Schlüsseln und Angriffsmöglichkeiten, auch Vigenere-Chiffre/Koinzidenzindex (wie genau kommt man darüber an die Schlüssellänge)

Wie können Vertraulichkeit, Integrität und Authentifizierung mit öffentlichen Schlüsseln erreicht werden? RSA, digitale Signatur, Schlüsselaustausch

Worauf basiert RSA? Schwierigkeit der Faktorisierung großer Zahlen / Einwegfunktion (Habe hier auch noch erklärt, wer welchen Schlüssel hat, wie die Schlüssel überhaupt erzeugt werden, Eulersche Funktion, Euklidischer Algorithmus, multiplikatives Inverses etc.)

Kommunikation: ISO-OSI-Schichtenmodell; allgemeines Prinzip bzw. Zweck und alle einzelnen Schichten erläutert

Dies sind die Fragen, an die ich mich noch erinnern kann. Da ich zu jedem Thema ziemlich ausgeholt habe, weiß ich nicht ganz genau, welche Details Herrn Dr. Icking besonders wichtig waren. Ich vermute aber, es kommt auf das Verstehen der Zusammenhänge und das Erläutern der wichtigen Schlagwörter an. Er hakt auch nach, wenn man eine Frage nicht detailliert genug beantwortet. Wenn man mal nicht genau weiß, worauf er mit einer Frage hinaus will, sollte man dies durch Nachfragen gleich klären, dann gibt es sicher keine Verständnisprobleme.

Herr Dr. Icking ist sehr sympathisch, und die Benotung ist fair.

Ich wünsche Euch allen viel Glück!!

Verteilte Systeme Gedächtnisprotokoll  
Kurs: Verteilte Systeme 10/05  
Prüfer: Dr. Icking  
Datum: 20.05.06  
Note: 1,0

## Fragen

- Netzwerkschichten
  - OSI Protokoll aufzählen
  - Vermittlungsschicht und Transportschicht ausführen
- Verschlüsselung
  - Warum wird verschlüsselt
  - Public Key Verfahren (RSA)
  - Wie erreicht man Vertraulichkeit, Integrität und digitale Signaturen mit Public Key Verfahren
- NFS
  - Wie funktioniert es
- CVS
  - Warum braucht es Versionskontrolle
  - Eigenschaften
  - Ablauf
  - Merging

# Gedächtnisprotokoll

**Prüfung:** Bachelor Fachprüfung „Verteilte Systeme – 1678“

**Prüfer:** Prof. Icking

**Datum:** 20.05.06

**Dauer:** ca. 25min.

1. Was ist ein verteiltes System?
2. Was versteht man unter Transparenz?
3. Verteiltes Dateisystem NFS. Welche Transparenz gibt es da?
4. Wie funktioniert NFS?
5. Was muss der Administrator am NFS-Server/Client vorbereiten, damit NFS läuft?
6. Wie funktioniert der Automount-Mechanismus?
7. Welche Vorteile bringt Automount für NFS-Server/Client?
8. Thema Sicherheit. Was muss geschützt werden?
9. Wie bzw. warum können klassische Verschlüsselungsverfahren relativ leicht gebrochen werden?
10. Wie kann man die Vigenère-Verschlüsselung brechen?
11. Wie funktioniert ein modernes Verschlüsselungsverfahren, wie z.B. RSA?
12. Wie funktioniert das Public-Key Verfahren bei digitaler Signatur?
13. Thema Zeit. Warum benötigt man in verteilten Systemen überhaupt möglichst synchrone Uhren?
14. Welche Möglichkeiten der Zeitsynchronisierung gibt es da?
15. Synchronisierung physischer Uhren. wie läuft das prinzipiell ab? (hier ging es um die Einbeziehung der RoundTripZeit)
16. Was macht man, wenn man die Uhr eigentlich zurückstellen müsste? Geht das?
17. Thema verteiltes Arbeiten. Was können sie empfehlen, wenn eine verteilte Gruppe z.B. an einem SW-Projekt zusammen arbeiten soll? (-> CVS)
18. Was ist CVS? Wie funktioniert es? (hier auch die allg. Anforderungen an die verteilte Gruppenarbeit erklärt)

19. Wann können da Probleme auftreten? (-> Thema Merge, wann funktioniert der autom. Merge nicht mehr, was kann man dagegen tun, wo wird der Merge durchgeführt -> lokal!)

20. Nach welchem Verfahren funktioniert der autom. Merge bei CVS?

21. Welche Befehle stehen am CVS-Client zur Verfügung? (-> hier waren die fürs Arbeiten am wichtigsten CVS-Kommandos gefragt, habe auch noch das Tagging erklärt)

Prof. Icking ist, wie auch Prof. Keller, mittlerweile schon weithin bekannt als sehr ruhiger Prüfer, der schnell eine entspannte Prüfungsatmosphäre schafft. Wichtig ist ihm offensichtlich das Grundverständnis und die Zusammenhänge. Wenn er merkt das man zu einem Thema fit ist, geht er gleich weiter zur nächsten Frage. Ich kann Prof. Icking also nur empfehlen.

Die hier aufgeführte Fragenliste ist nicht unbedingt vollständig sondern repräsentiert einfach jene Fragen, die mir in Erinnerung geblieben sind.

## **Protokoll zur Prüfung Verteilte Systeme, 1678**

Datum : 12.5.2005  
Dauer : ca. 30 Min  
Prüfer : Dr. Icking  
Beisitzer: Dr. Ma  
Note: 1,0

### **Fragengebiete**

Definition verteiltes System

Austausch und Koordination bei verteilten Systemen durch Kommunikation :  
wie erfolgt die Kommunikation in verteilten Systemen?  
was wurde dazu definiert?

OSI Schichten Modell im einzelnen vorstellen :  
wie heißen die Schichten ?  
was tun sie / wofür sind sie definiert / was ist ihnen zugeordnet (Bsp TCP = Transport Layer etc) ?  
wie erscheint die Kommunikation von außen , wie findet sie tatsächlich statt ? ( Übertragung durch den ganzen Stack, die ganze Protokollfolge)

Netzwerkschicht und Transportschicht: welche verbindungslose und verbindungsorientierte Protokolle gibt es ?

TCP / UDP im Detail : wie funktioniert das Fehlermodell bei TCP ?  
(Erläuterungen zu Segmentierung, Sequenzierung, Pufferung, Retransmit etc.)  
Können Pakete in unterschiedlicher Reihenfolge ankommen; wie sieht falsche Paketierung für die oberen Schichten aus? (ab Schicht 4 aufwärts darf die Reihenfolge nicht mehr falsch sein, TCP sorgt dafür, daß nach oben die Pakete ausschließlich in der richtigen Reihenfolge weitergegeben werden)

UDP : wozu UDP? für welche Art von Anwendungen ?  
Konkret : DNS Client stellt Anfrage erneut wenn ein Paket nicht ausgeliefert wurde,  
Video/Soundübertragung über Internet

FTP als Protokoll :  
wie funktioniert es, welche(r) Verbindungsaufbau(ten) findet/n statt, welche Authentifizierung,  
warum ist es unsicher, welche Gründe sprechen dafür, es trotzdem zu benutzen ?  
Wie funktioniert anonymous ftp?

HTTP als Protokoll :  
welche Möglichkeiten hat man mit HTTP (put-get.. aber hauptsächlich als Browser) ?  
welche Daten kann man sich damit anschauen (Typ von Daten/Dateien) ?

SOAP : was ist das ?  
SOAP über HTTP über Firewalls : wie funktioniert das ?

Firewalls allgemein: welche Architekturen gibt es ?

Sicherheit: warum Verschlüsselung ?  
(Authentifizierung Absender, Integrität der Daten, ...)

Welche Methoden existieren zur Verschlüsselung ?

Öffentliche/geheime Schlüssel: RSA Verfahren (kurzer Anriß der Methode zur Erzeugung des öffentlich/geheimen Schlüsselpaares)

Wer hat welchen Typ von Schlüssel bei Ver/Entschlüsselung mit public/private Key und nutzt ihn wofür ? (sowohl bei Verschlüsselung als auch digitaler Signatur) -- ganz genau!!

Uhrzeitsynchronisation: warum benötigt man sie, wie kann sie durchgeführt werden ? verschiedene Algorithmen angerissen.

CVS:

was ist CVS , wozu wird es benutzt, wie sieht es bei Änderungen aus (viele Benutzer ändern, was passiert beim Commit ) ?

wozu lokaler update, wie können merge Konflikte gelöst werden ?

2-Wegeverfahren : was ist durch das 2-Wegeverfahren nicht abgedeckt ?

In welchem Fall führen parallele Änderungen nicht zu Problemen ?

Dr. Icking ist ein sehr guter Prüfer; die Prüfungsatmosphäre empfand ich als recht locker. Die Fragen waren sehr konkret und es wurde auch entsprechend nachgefragt, wenn die Antworten nicht gleich detailliert genug waren (vor allem beim Thema Verschlüsselungsverfahren).

**Fragmente eines Prüfungsprotokolls**  
**Kurs 1678 (Verteilte Systeme), Version WS 2003/04**  
**Prüfer: Dr. Icking**  
**Beisitzerin: Dr. Ma**

**Datum: 15. 02. 2005, 12<sup>30</sup> Uhr**

Ich habe mir leider nicht alle Fakten des Prüfungsgesprächs merken können. Die Prüfung begann zu meiner großen Freude nicht mit der nahegelegenen Frage:

**Was ist ein verteiltes System?**

Dr. Icking stieg gleich in KE5 bzw. KE7 ein, indem er erst einmal allgemein fragte, **wie eine in der Welt verteilte Gruppe ihre Arbeit koordinieren könne**. Nachdem ich die Anforderungen und Beispiele simplen verteilten Arbeitens erläutert habe, sollte ich **die Arbeitsweise von CVS** mit dem Konfliktverhalten bei mehrfachem Einchecken (Baumbildung, Merge) erläutern. Beim Merge hat er ganz schön nachgehakt. Nächste Fragen: **Wie sieht es mit dem BSCW aus, kann man dort eine ähnliche Versionenverwaltung durchführen? Was macht BSCW bei differierenden Versionen?** Ich gab zu, daß ich zwar CURE, aber nicht BSCW aus der praktischen Arbeit kenne, und erläuterte die Zusammenarbeit über CURE, die zum Glück ähnlich zu der im BSCW abläuft (verschiedene Versionen ja, Merge aber nicht).

Nun ein Sprung zu NFS: **Wie funktioniert NFS?**

**Was macht der Client genau, um an die Dateien zu kommen?**

**Was macht der NFS-Server zum Bereitstellen der Dateien?**

Bei diesem Thema habe ich RPC angesprochen und den Portmapper recht ausführlich abgehandelt.

Nächster Sprung: **Ist es wichtig, daß alle Rechner die gleiche Zeit haben, wenn ja: warum?**

(Standardantworten make und Prozeßsynchronisation). Nun sollte ich **Verfahren zur Uhrensynchronisation erläutern**. Ich habe kurz erwähnt, daß ich die alle ausführlich kann ;-)) und dann Cristians Algorithmus erläutert, Nachfragen gab es zu **Schwachstellen in Cristians Algorithmus** und zur **maximalen Abweichung bei Cristians Algorithmus**.

Erneuter Sprung, diesmal zu Verschlüsselung mit der leichten Einstiegsfrage, **warum ein Verschiebechiffre nicht sicher ist**, weiter dazu, **wie sicher das Verfahren von Vigenère ist** und **Wie kann die Vigenère-Verschlüsselung geknackt werden** und **wie kann man die Vigenère-Verschlüsselung sicherer machen**. Das habe ich auch recht ausführlich erläutert. Nun sollte ich erläutern, **wie die Arbeit mit Public-Key-Systemen abläuft**. Dabei stellte Dr. Icking Szenarien vor, und ich erzählte, wer nun mit welchem Schlüssel was macht und woher die Schlüssel kommen und wohin sie gehen. Nach der Funktionsweise von RSA wurde nicht gefragt, schade. Weiterhin sollte ich **die Gründe für Verschlüsselungsverfahren aufzählen** und kurz gängige **Brute-Force-Angriffe ansprechen** (Klartext-, Chiffretextangriff).

Weitere Sprünge: **Was sind Peer-to-peer-Systeme, wie funktionieren sie? Was sind Prozesse und Threads, was gehört alles dazu?**

**Wie kommunizieren Threads miteinander?**

**Wie meldet man sich in einem P2P-Netzwerk an?**

**Wie kann man in einem P2P-Netzwerk suchen?**

Das sollte ich noch **FTP erläutern**, begründen, **warum FTP trotz aller Schwachstellen noch heute eingesetzt wird** (keine Klartextpaßwörter bei anonymem FTP) und **HTTP kurz erläutern**.

Nicht erwähnt wurden die Kapitel Nebenläufigkeit, Transaktionen und das OSI-Modell samt den Protokollen der unteren Schichten.

Dr. Icking stellte vor allem Zwischenfragen, wenn ich ein Thema nicht von selbst ausführlicher erläuterte. Die Atmosphäre war ruhig und unaufgeregt, was sicher auch daran lag, daß ich mich mit dem Thema recht gut auskenne. Normalerweise bin ich bei Prüfungen viel nervöser. Die Benotung war angesichts meiner Unkenntnis von BSCW wohlwollend, auch daß ich mich beim NFS-Client verhaspelte, wurde mir nicht angekreidet.

Wer Prüfungen vorzieht, in denen weniger die Zusammenhänge, sondern mehr konkrete, kurz beantwortbare Probleme nachgefragt werden, wird sich eher für Prof. Haake entscheiden wollen. Beide Prüfer, Dr. Icking und Prof. Haake, können m. E. aber bedenkenlos empfohlen werden.



Fach: 1678 Verteilte Systeme (WS 03/04) basierend auf Coulouris & Co.  
Prüfung: Bachelor Fachprüfung Wahlfach  
Prüfer: Dr. Icking  
Beisitzer: Dr. Lihong Ma  
Datum: 4. Okt. 2004  
Note: 1.0

Was ist ein Verteiltes System?

Komponenten auf vernetzten Computern, die mithilfe von Nachrichten kommunizieren. Ziel ist die gemeinsame Nutzung von Ressourcen. Sei es Hard- oder Software.

Welche Alternative gibt es?

Der zentrale Großrechner, der beispielsweise Terminals bedient.

Welche Vor- und Nachteile hat ein Verteiltes System gegenüber einem Großrechner?

Wirtschaftlichkeit und Skalierbarkeit. Vorteil eines Großrechners ist die zentrale Administration.

Wie sieht es mit der Sicherheit aus?

Ein Verteiltes System bietet natürlich mehr Angriffspunkte, da es Schnittstellen nach außen für die Kommunikation bereitstellen muss.

Wie sieht das ISO-OSI-Kommunikationsmodell aus?

Die Schichten aufgezählt und zu jeder ihre Funktion genannt und ein Pendant aus dem Internet-Verkehr, soweit vorhanden, aufgezeigt.

Wie kommunizieren die Schichten miteinander?

Im Prinzip kommunizieren sie direkt mit ihrem Pendant auf einem anderen Knoten, nutzen dafür aber die Dienste der unter ihr liegenden Schicht und bieten Dienste nach oben hin an.

Was macht TCP?

Auf der Vermittlungsschicht, verbindungsorientiert. Teilt den Datenstrom in Pakete und bietet zusätzliche Dienste wie Sessioning, Flusskontrolle, Prüfsummen in Header/Daten.

Warum braucht man dann überhaupt noch UDP?

Kleiner, schneller, weniger Overhead, verbindungslos. Beispiel DNS, wenn nur eine Nachricht/Anfrage abgesetzt werden soll.

Was passiert bei UDP, wenn das Paket nicht ankommt?

Das Programm muss sich selbst darum kümmern, auf Fehler zu reagieren. Keine Auslieferungsgarantie.

Können Pakete auch unterschiedliche Wege nehmen? Kommen sie dann korrekt an?

IP-Protokoll nummeriert die Pakete durch. Durch adaptives Routing können die Pakete durchaus andere Wege nehmen. Der Empfänger setzt sie dann wieder zusammen.

Was ist SOAP?

Simple Object Access Protocol. Ein Austauschformat, das auf XML-Basis basiert und mit http übertragen wird.

Wie sieht es möglicherweise mit einer Firewall aus?

Das Microsoft Online Update als Beispiel genannt, das auf SOAP basiert. SOAP nutzt den Port 80, der eigentlich für reines http gedacht ist, und kann somit die Firewall passieren, da der Port 80 für Webanfragen oft offen ist.

Im konkreten Fall: Nutzt ein Benutzer die Webseite von Microsoft für das Windows Update, so ist zu diesem Zeitpunkt der Port 80 auf Empfängerseite auf jeden Fall geöffnet und Microsoft kann diesen Kanal somit mit SOAP nutzen, um Informationen über den zu updatenden Rechner zu übertragen.

Was ist ein Prozess?

Abstraktion eines auszuführenden Programms, das von der CPU bearbeitet werden kann.

Was ist ein Thread?

LWP. Gemeinsamer Adressraum unterschiedlicher Stack. Vorteil: schnelles Erzeugen, Verwalten, Wechseln.

Haben Threads denn auch einen eigenen Bereich für Daten im Speicher?

Ja.

Wie können die Threads einen Adressraum miteinander kommunizieren?

Sie können in den gemeinsamen Adressraum schreiben und ein anderer kann dort auslesen.

Wer weist Prozesse zu?

Scheduler. Prozesse die ausgeführt werden möchten reihen sich in eine Queue ein. Je nach Strategie werden sie dann ausgeführt: Round Robin, First Come first served.

Wie sieht es mit der Migration aus?

Preemptiv und non-preemptiv. Preemptiv: Zeitpunkt des Einfrierens relevant, Erzeugung auf anderem Knoten, Übertragung der Daten vor oder nach dem Einfrieren.

Was wird alles übertragen?

Prozessorzustand, Datenspeicher und ggf. geöffnete Dateien.

Wie kann ich die Kommunikation sichern?

Kryptographie.

Warum macht man das?

Vertraulichkeit, Integrität, Verbindlichkeit, Verfügbarkeit, Authentizität

Welche klassischen Verfahren kennen Sie?

Verschiebchiffre, Cäsar und Rot13, unsicher da alle Variationen/Schlüssel schnell durchprobiert  
Permutationschiffre, Zeichen untereinander vertauschen, auch als Matrix möglich oder als besondere Form in der Hillman-Chiffre Substitutionschiffre, jedem Zeichen ein festes Zeichen zugeordnet, unsicher da statistische Methoden

Wie kann man beim Vigenere-Chiffre den Ciper-Text brechen?

Über den Koinzidenzindex eine mögliche Schlüssellänge ermitteln und dann statistische Verfahren auf den Schlüssel anwenden.

Nun ist Vigenere schon ziemlich sicher, wie kann man ihn noch sicherer machen?

Langer Text, langer Schlüssel. Je länger der Schlüssel gegen den Gesamttext wird, desto sicherer.

Welche modernen Verfahren kennen Sie?

Symmetrische bzw. Secret Key und Asymmetrische bzw. Public Key.

Nennen Sie ein Verfahren für die symmetrische Verschlüsselung.

DES.

Welche Verfahren werden mit Public-Key eingesetzt?

RSA und ElGamal/Diffie Hellman

Auf welchem mathematischen Problem beruht RSA?

Faktorisierung der Produkte von großen Primzahlen. Anschließend ausführlich das Verfahren und die Ermittlung der Schlüssel erklärt. Gaußsche Funktion, ermitteln von  $e$ , diophantische Gleichung zum Ermitteln von  $g$ ...

Wie funktioniert das Public-Key-Verfahren im Mailaustausch?

Versenden des öffentl. Schlüssels. Verschlüsselung einer Mail mit dem öffentl. Schl. und anschl. entschlüsseln auf dem eigenen Rechner mit dem eigenen privaten Schl.

Wie signiere ich eine Mail digital?

Hash der Nachricht mit dem priv. Schl. verschlüsseln. Die Empfänger können mithilfe des öffentlichen Schlüssels den codierten Hash entschlüsseln, den Hash der Nachricht bilden und beide vergleichen.

Kann man eine Mail signieren und gleichzeitig verschlüsseln?

Ja, ....

Warum kann der Faktor Zeit in Verteilten Systemen eine Rolle spielen?

Elektronische Transaktionen. Beispiele Banken, Ebay,.... Außerdem Zeitstempel.

Welche Möglichkeiten gibt es für die Synchronisation?

Logische Uhren: Geschehen-Vor-Relation, mit PID, Vektoruhren Physikalische Uhren: Christians Algorithmus, Berkley Algo., NTP. NTP genauer erklärt. Genauigkeit 10 ms übers Internet.

Wenn man festgestellt hat, dass ein Rechner nicht synchron läuft, was macht man dann, da man bei einem negativen Ergebnis die Zeit ja nicht zurückstellen darf?

Zeit anhalten oder um strenge Monotonie zu gewährleisten, die Zeit per Software langsamer laufen lassen.

Wenn wir Entwickler wären, welche Möglichkeiten kennen Sie, mit Hilfe eines Verteilten Systems an einem gemeinsamen Projekt zu arbeiten?

Hier habe ich rückgefragt, ob wir bei Versionskontrolle sind, da ich mir die Frage auch im Bereich CSCW & Co. hätte vorstellen können. Ja.

Versionkontrollsysteme: RCS, CVS, Subversion. Ein Zentrales Repository, das die Daten, Versionen und History auf einem zentralen Server bereithält.

Wie ist die Arbeitsweise von CVS?

Auschecken, arbeiten, einchecken.

Was passiert wenn wir die gleiche Datei bearbeiten, kann es zu Problemen kommen?

Ja, Versionsgraph kann entstehen. Beim Einchecken kann es zu Problemen kommen, wenn eingefügt wird bei semantischer Abhängigkeit oder ganz allgemein, wenn in der gleichen Zeile gelöscht und eingefügt wird.

Und was passiert dann?

Der erste der Eincheckt gewinnt. Seine Version steht im CVS-Server. Der andere muss zuerst ein Update seiner Daten ausführen, mögliche Konflikte lokal lösen und kann dann anschließend einchecken.

Es war eine sehr angenehme Prüfung und ich kann Herrn Dr. Icking als Prüfer nur empfehlen. Ich hatte den Eindruck, dass es auf ein allgemeines Grundverständnis der Thematik ankommt. Beispielsweise musste ich nicht erklären, was der Koinzidenzindex nun genau ist, obwohl der Begleittext ausführlich auf die mathematischen Grundlagen zum Verfahren eingeht. Nur beim RSA habe ich ein wenig ausgeholt. Wobei ich aber auch hier nicht auf die diophantische Gleichung, außer vom Nennen, eingegangen bin. Ob es überhaupt nötig war, die Schlüsselerzeugung und das Verfahren so darzustellen, weiß ich nicht. Ich habe den Eindruck, dass es auch ohne gegangen wäre.

## Verteilte Systeme

Datum: 16.03.2004

Prüfer: Dr. Icking

Prüfung: Diplom I

Note: 1,3

- Was ist ein verteiltes System?
- Welche Alternativen gibt es zu einem verteilten System?
- Vorteile/Nachteile eines verteilten Systems gegenüber einem Großrechner?
- OSI-Referenzmodell erläutern – hab den Ablauf im Protokollstapel mit erklärt.
- Unterschied zwischen TCP und UDP erläutern.
- Wie kann man Kommunikation schützen?
- Verfahren mit geheimem Schlüssel erklären.
- Verschiedene einfache Verschlüsselungsverfahren mit Angriffsmöglichkeiten nennen.
- Verfahren mit öffentlichem Schlüssel erklären.
- Digitale Signatur erläutern.
- Hab den Unterschied zwischen Verschlüsselung und Signatur bei der Erzeugung des Schlüsselpaares angesprochen.
- Was ist NFS?
- Was hat der Administrator vor dem Einsatz von NFS zu tun?
- Wie findet die Authentifizierung bei NFS statt?
- CVS erklären mit Benachrichtigung und Merge.
- Wann wird es beim Merge-Schritt zu einem Konflikt kommen?

Und dann war die Zeit um. Dr. Icking lässt einen ausführlich erklären und greift nur lenkend ein. Insgesamt waren die Fragestellungen darauf ausgerichtet zu erfahren, ob der Prüfling den Gesamtüberblick über das Thema hat. Weniger ging es um Detailfragen. Herr Icking ist ein sympathischer Prüfer und unbedingt zu empfehlen.

**Allen Viel Erfolg !!!**