



## Prüfungsthemen und Regeln für die Klausur

### „GSS – Grundlagen der Systemsoftware“

Für die Klausur über die GSS-Vorlesung werden die im folgende aufgeführten Themen festgelegt. Aus diesen Themen werden zu gleichen Teilen Fragen gestellt, die a) konkretes Wissen abfragen und b) angemessenes Verständnis von Zusammenhängen und Grundsätzen erfordern.

Zugelassene Hilfsmittel:

- Keine!

Weitere Regeln:

- **Die Nutzung von IT und mobilen Geräten einschließlich Handys ist nicht gestattet.** Auf das Einsammeln von derartigen Geräten wird zunächst verzichtet. Kommt es zu Situationen, wo z.B. das Handy klingelt oder z.B. der Eindruck entsteht, dass SMS geschrieben/gelesen oder Nachrichten abgerufen werden, wird derjenige gebeten werden, das entsprechende Gerät bis zum Ende der Prüfung abzugeben.
- **Davon unabhängig führt jeder Täuschungsversuch – ob mit IT oder ohne – zum Einzug der Klausur und die Bewertung als „nicht bestanden“!**

Nach der Klausur wird die Korrektur mindestens eine Woche in Anspruch nehmen. Die entsprechenden Noten und Scheine werden dann über die Prüfungssekretariate zur Kenntnis gegeben.

Rechtschreibfehler und Grammatik gehen selbstverständlich nicht in die Notengebung ein, wenn allerdings die Antwort unleserlich ist, kann dies sehr wohl das Ergebnis negativ beeinflussen. Es wird keine Minuspunkte geben, d.h. entweder die Antwort ist korrekt, dann gibt es Punkte, oder sie ist falsch, dann entsprechend keine Punkte. Bei den Fragen wird die zu erzielende Punktezahl jeweils angegeben.

Eine Einsicht in die bewerteten Klausuren in Gegenwart einer Aufsichtsperson ist am FB Informatik der Universität Hamburg nach einer Terminabsprache bis ca. Mitte September 2009 möglich. Hierbei können auch Fragen gestellt und beantwortet werden, die die Klausur, Bewertung, etc. betreffen. Danach werden die Klausuren an die Prüfungssekretariate gegeben. Ggf. muss von dieser Regel abgewichen werden, wenn ein Prüfungssekretariat andere Anforderungen stellt.

## **Themen**

Die folgenden Themen werden in den Folien behandelt und sind damit Gegenstand der Klausur. Wenn die Darstellung der Folien nicht ausreicht, ist geeignete Literatur für die Vorbereitung hinzuziehen.

### **– Einführung**

- Begriffe der IT-Sicherheit rund um „Risiko“ und deren Zusammenhänge

### **– Datenschutz**

- Grundrecht auf informationelle Selbstbestimmung
- Dt. Definition von „Processing“
- Transfer von Daten in andere Länder
- Bedeutung des Kontexts für die Interpretation von Daten im Sinne des Datenschutzes
- Auswahl der geltenden Datenschutzregeln
- Erlaubnis zur Verarbeitung
- Privacy Engineering
- Technische und organisatorische Maßnahmen (zum Datenschutz)
- Datenschutzbeauftragter und Verhältnis zum IT-Sicherheitsbeauftragten

### **– Kryptographie**

- Symmetrische Verfahren mit gemeinsamen Geheimnis
- Unterschied zwischen ECB und CBC
- Unterschied zwischen UNCONDITIONAL und CONDITIONAL Security
- Public-Key Verfahren mit Schlüsselpaar

- Unterschiedlicher Einsatz für Private bzw. Public Key, z.B. am Beispiel einer Email
- Vergleich zwischen Public-Key und symmetrischen Verfahren
- Eigenschaft von Hash-Funktionen
- Hash-Funktion mit geheimen Schlüssel
- Kerckhoff's Prinzip

### **– Software und Sicherheit**

- Bedeutung und Beispiele für „Keep it Simple“
- Funktionsweise von Buffer Overflows
- Beispiele für unsichere C-Funktionen
- Funktionsweise von „Canaries“

### **– Authentisierung**

- Bedeutung von Identifizierung
- Unterschied zur Authentisierung, Kategorien von Faktoren zur Authentisierung, starke (vs. schwacher) Authentisierung
- Übertragung von Hashes anstelle von Passwörtern

### **– Biometrie**

- Verschiedene biometrische Verfahren aufzählen und Fehlerraten bzw. Stärken/Schwächen kennen
- generelle Bedrohungen für biometrische Systeme

### **– Access Control**

- Aufgabe des Reference Monitors (Guards)
- Discretionary vs. Mandatory Access Control
- Vorteile von Role-Based Access Control
- Was sind ACLs und Capabilities? An was (Principal = Subject vs. Object) werden diese festgemacht? Wann gebunden?

## **– TCP/IP Protocol Basics**

- TCP Three Way Handshake
- Unterschied zwischen (default) FTP vs passivem FTP

## **– Firewalls**

- Prinzip der geringsten Berechtigung auf Netzwerkebene
- Filterung = Network Segregation zwischen Netzen unterschiedlicher Sicherheit
- Definitionen von Firewall, Network Monitoring, IDS, Honeypots und Log Server
- Unterschied zwischen statischem und dynamischen (statefull inspection) Packet Filtering
- Rolle und Aufgabe eines Proxies, Beispiele für übliche Proxies.
- Rolle und Aufgabe von Demilitarisierten Zonen (DMZ) und Beispiele