
Bitte hier unbedingt Matrikelnummer und Adresse eintragen, sonst keine Bearbeitung möglich.

Postanschrift: FernUniversität, D-58084 Hagen

Name, Vorname

Straße, Nr.

PLZ, Wohnort

FERNUNIVERSITÄT
in Hagen
EINGANG

MI

FERNUNIVERSITÄT
in Hagen
58084 Hagen

Fakultät für Mathematik und Informatik

Kurs: 01867 „Sicherheit im Internet II“

Klausur am 23.09.2006

Hörerstatus:

- ☐ Vollzeitstudent
- ☐ Teilzeitstudent
- ☐ Zweithörer
- ☐ Gasthörer
- ☐ Bachelor
- ☐ Lehramt
- ☐ . . . . . .

Klausurort:

- ☐ Berlin
- ☐ Bochum
- ☐ Frankfurt
- ☐ Hamburg
- ☐ Karlsruhe
- ☐ Köln
- ☐ München
- ☐ Bregenz
- ☐ Wien
- ☐ . . . . . .

Zutreffendes unbedingt ankreuzen !

Aufgabe	1	2	3	4	Summe
erreichbare Punktzahl	12	18	20	26	76
bearbeitet					
erreichte Punktzahl					

Note: _____

Hagen, _____ Betreuer: _____

FernUniversität in Hagen

Fakultät für
Mathematik und Informatik
Lehrgebiet Parallelität & VLSI
Prof. Dr. J. Keller
58084 Hagen, 23.09.2006

Bescheinigung zur Vorlage beim Finanzamt

Herr/Frau _____

geb. am _____ , Matr.-Nr.: _____ ,

hat am 23.09.2006 von 10:00 - 13:00 Uhr an der Klausur zum Kurs

01867 „Sicherheit im Internet II“

in _____ teilgenommen.

(Stempel) (Prof. Dr. J. Keller)

FernUniversität in Hagen

Fakultät für
Mathematik und Informatik
Lehrgebiet Parallelität & VLSI
Prof. Dr. J. Keller
58084 Hagen, 23.09.2006

Leistungsnachweis / Zertifikat

Herr/Frau _____

geb. am _____ , Matr.-Nr.: _____ ,

hat im SS 2006 m i t E r f o l g an der Klausur zum Kurs

01867 „Sicherheit im Internet II“

teilgenommen.

Note: (Siegel) (Prof. Dr. J. Keller)

Hinweise zur Klausur des Kurses 01867 am 23.09.2006

- Die Klausurdauer beträgt: drei Stunden (10:00 bis 13:00 Uhr)
- **Es sind keine Hilfsmittel erlaubt.**
- Legen Sie Ihren Studenten- und Personalausweis zur Überprüfung durch die Aufsicht bereit.
- Füllen Sie vor Beginn der Klausur unbedingt das Deckblatt aus - und zwar in leserlicher Druckschrift.
- Füllen Sie bitte vor Inangriffnahme der Klausuraufgaben den/das Leistungsnachweis/Zertifikat leserlich aus (natürlich bis auf die Note und Unterschrift). **Andernfalls wird kein Leistungsnachweis erstellt.**
- Die Bescheinigung für das Finanzamt ist nur mit Unterschrift und Stempel gültig. Nur vollständig ausgefüllte Bescheinigungen werden von uns abgestempelt, unterschrieben und Ihnen zugestellt.
- Überprüfen Sie die Vollständigkeit der Aufgabenstellungen! Die Klausur umfasst insgesamt 11 Seiten mit 4 Aufgaben.
- Schreiben Sie auf alle Lösungsbögen Ihren Namen und Ihre Matrikelnummer !
- Tragen Sie Ihre Lösungen in die dafür vorgegebenen Felder ein. Falls Sie damit nicht auskommen, benutzen Sie bitte die Rückseite der vorhergehenden Aufgabe. Verweisen Sie in diesem Fall darauf, dass diese Rückseite beschrieben ist.
- Bei Abgabe Ihrer Arbeit heften Sie bitte die ersten Seiten des übergebenen Klausur-exemplares (Deckblatt, Bescheinigungen und Hinweise zur Klausur) vor Ihre Lösungsblätter. Kontrollieren Sie zum Schluss, dass Sie Ihre gesamte Arbeit geheftet abgeben. Nachträglich eingereichte Lösungen werden von uns nicht akzeptiert.
- Die zum Bestehen der Klausur erforderliche Punktzahl liegt noch nicht fest. Sie wird erst aus der tatsächlich erreichten Punkteverteilung ermittelt, liegt aber sicher nicht über 50% bzw. unter 30% der erreichbaren Punkte.
- Die Korrektur der Klausur wird voraussichtlich bis Anfang November 2006 erfolgt sein. Wir bitten, von vorzeitigen Nachfragen abzusehen.

Bei der Bearbeitung der Klausur wünschen wir Ihnen viel Erfolg!

Ihre Kursbetreuer

Name, Vorname: _____ Matrikelnr.: _____

Aufgabe 1 (12P)

Welche zwei Datenbanken/ Tabellen verwaltet ein DNS-Server?

Welche Funktion erfüllen diese Datenbanken?

Was versteht man unter Spoofing und was ist DNS-Spoofing?

Was passiert bei einem IP—spoofing, wenn IP-Adressen mit DHCP vergeben werden?

Beschreiben Sie kurz die lineare Kryptoanalyse!

Name, Vorname: _____ Matrikelnr.: _____

Lineare Kryptoanalyse ist ein known-plaintext-Angriff, um welche Art des Angriffs handelt es sich bei differenzieller Kryptoanalyse?

Welche Zustände kann das Q-Bit bei Quantencomputern annehmen?

Name, Vorname: _____ Matrikelnr.: _____

Aufgabe 2 (18P)

Welche Güterarten werden bei e-commerce unterschieden? Nennen Sie Beispiele!

Bei Bezahlung mit Kreditkarte durch einen Angreifer entsteht bei Widerspruch des rechtmäßigen Inhabers der Kreditkarte ein Schaden. Wie versuchen Kreditkartenfirmen diesen Schaden zu minimieren?

Was ist double spending?

Name, Matrikelnr.:
Vorname: _____ _____

Um eine digitale Münze zu verändern, so dass man nach einer digitalen Signatur die Veränderung wieder rückgängig machen kann, ohne die Signatur zu zerstören, wählt der Kunde eine Zufallszahl z und sendet der Bank die unsignierte Münze UM (M Datensatz der Münze, K_p public key, K_g private key, n der zu den Schlüsseln gehörende Modulus).

$UM = M \cdot z^{K_p} \bmod n$.

Die Bank erstellt die digitale Signatur $SM = UM^{K_g} \bmod n$.
Wie kann der Kunde nun die Münze M der Bank signieren?

Was macht ein Rewebber/ wie arbeitet dieser?

Wie ist es möglich, die vom Client angewählten Webseiten trotz eingesetztem Rewebber ohne direkten Zugriff auf den Anonymisierungs-Host und den Client nachzuvollziehen?

Worauf muss beim Aufsetzen eines Rewebber-Host geachtet werden?

Name, Vorname: _____ Matrikelnr.: _____

Aufgabe 3 (20P)

Was macht ein VPN?

Wie funktioniert CHAP?

Was stellt CHAP sicher?

Ordnen Sie die folgenden Protokolle Layer 2/ Layer 3 zu!

Protokoll	Layer
PPP	
CHAP	
IPSec	
PAP	
PPTP	
L2TP	

Welche Übertragungsmodi bei IPSec gibt es?

Name, Matrikelnr.:
Vorname: _____ _____

Wie funktioniert die Verschlüsselung bei IPSec, wenn Authentification Header und anschließend Encapsulation Security Payload (ESP) eingesetzt werden? Schildern Sie die Veränderungen im IP-Header und in der IP-Nutzlast und ob symmetisch oder asymmetrisch verschlüsselt wird.

Was leistet ein Intrusion Detection System (IDS)?

Ein findiger Hacker hat sich Administrationsrechte auf einem Rechner innerhalb eines Subnetzes verschafft und hört z.B. mit Etherreal den Netzwerkverkehr ab. Leider sieht er nur den Datenverkehr den gehackten Rechner betreffend und Broadcasts. In welcher Art von Netzwerk befindet sich der Rechner?

Warum würde man ein IDS vor der Firewall eines Netzwerkes platzieren wollen?

Name, Vorname: _____ MatrikelNr.: _____

Aufgabe 4 (26P)

Nennen Sie die für Internet Service Provider gültigen Vorschriften aus dem Kurstext.

Was trägt man in die probability impact Matrix ein, welche Funktionen erfüllt sie?

Was ist beim Entwurf sicherer Systeme mit Interposition gemeint?

Handelt es sich bei der Java-Sandbox um einen Wrapper, Interposition, Compartmentalization oder Identifikation und Authentisierung?

Wozu benötigt man das Lightweight Directory Access Protocol?

Name, Matrikelnr.:
Vorname: _____ _____

Wie kann es sein, dass ein IDS auf einem Rechner vor der Firewall einen Angriff um 17:38 Uhr feststellt und ein andres IDS hinter der Firewall denselben Angriff um 17:20 protokolliert, was ist zu tun, damit der Fehler beseitigt wird?

Nennen Sie die ersten zwei erforderlichen Schritte zur Konstruktion eines sicheren Systems. Untergliedern und diskutieren Sie dabei die typischen ersten zwei Teilphasen eines Projekts im Hinblick auf das Thema Sicherheit.