JOHANN WOLFGANG GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

Fachbereich Wirtschaftswissenschaften
Institut für Wirtschaftsinformatik
Lehrstuhl für M-Commerce & Mehrseitige Sicherheit

Fachbereich
Wirtschaftswissenschaften

Institut für Wirtschaftsinformatik
Lehrstuhl für M-Commerce & Mehrseitige Sicherheit
www.m-lehrstuhl.de

Prof. Dr. Kai Rannenberg

Telefon +49 (0)69-798 25301
Telefax +49 (0)69-798 25306

Abschlussklausur Vorlesung „Informations- und Kommunikationssicherheit: Infrastrukturen, Technologien und Geschäftsmodelle“, SS 2006

Punktezahl: 90
Mindestpunktezahl zum Bestehen: 45
Veranstalter: Prof. Dr. Kai Rannenberg
Zugelassene Hilfsmittel: Keine

Achtung – geben Sie das Aufgabenblatt zusammen mit der Klausur ab!

Wir wünschen viel Erfolg!

Matrikelnummer *(Bitte eintragen!)*	

Aufgabe:	**1**	**2**	**3**	**4**	**5**
Punkte:					

Aufgabe:	**6**	**7**	**8**	**9**	**Gesamt**
Punkte:					

Punkte aus den Übungsaufgaben	**Punkte insgesamt:**	**Note:**

1 Schutzziele (10 Punkte)

1.1 Nennen Sie die klassischen technischen Schutzziele der IT-Sicherheit (2 Punkte)
Antwort: Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit

1.2 Erläutern Sie diese kurz anhand von Ihnen frei gewählter Beispiele (8 Punkte)

2. Authentifizierung (12 Punkte)

Neben Ihrer Tätigkeit als Student arbeiten Sie als Hilfskraft in einer europäischen Bank mit Zutrittsbeschränkungen und sollen Ihrem Vorgesetzten ein auf Smartcards basiertes Authentifizierungssystem erarbeiten. Die dabei verwendeten Smartcards schreiben ein Passwort mit 4 Zeichen, das nur aus Ziffern besteht (PIN), vor.

2.1 Wie viele verschiedene Passworte sind unter diesen Bedingungen möglich? (4 Punkte)
Antwort: 10 hoch 4 Möglichkeiten = 10000 Möglichkeiten

2.2 Wie viele Passworte sind möglich, wenn der Benutzer neben Zahlen auch Groß- und Kleinbuchstaben wählen kann, dabei aber darauf achten muss, dass das Passwort mindestens eine Zahl enthält? Gehen sie davon aus, dass das Passwort nach wie vor eine Länge von 4 hat. (6 Punkte)
Antwort: (62 hoch 4) – (52 hoch 4) Möglichkeiten = 153104 Möglichkeiten

2.3 Erläutern sie kurz eine Möglichkeit, wie ein Serviceanbieter das Erraten von Passwörtern durch Angreifer erschweren kann. (2 Punkte)
Antwort: Passwortrichtlinien erzwingen stärkere Passwörter und machen so das Erraten schwerer. Darüber hinaus kann der Account nach n Fehlversuchen gesperrt werden usw.

3. Zugangskontrolle (10 Punkte)

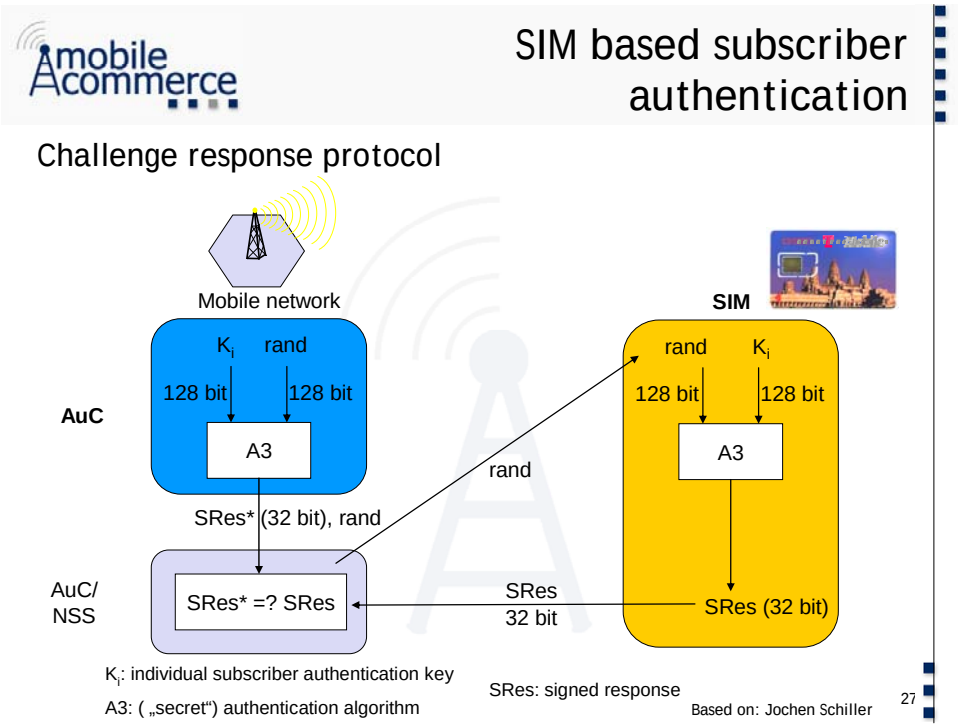
In dieser Vorlesung haben Sie das Chinese Wall-Sicherheitsmodell kennen gelernt.

3.1 Was sind die Schutzziele dieses Modells, und was sind die charakteristischen Merkmale des Modells? Erläutern Sie diese unter zu Hilfenahme der in der Vorlesung verwendeten Definitionen und Formeln. (10 Punkte)
Antwort: Vertraulichkeit und Integrität
Definitionen und Formeln finden sich auf den Folie 36 – 37 des Access Control Foliensatzes.

4. Netzsicherheit (22 Punkte)

Sie haben im Laufe der Vorlesung Authentifizierungsmechanismen für das GSM-Netz kennen gelernt. Stellen Sie sich nun vor, dass Sie sich nach der Klausur im sonnigen Spanien mit Ihrem mobilen Endgerät in ein dortiges Netz einbuchen wollen.

4.1 Welche Annahmen werden dabei über die Verteilung von Schlüsseln und die Geheimhaltung von Algorithmen getroffen, um den heimatlichen Mobilfunkanbieter zu schützen? Erläutern Sie unter Verwendung einer Skizze, wie dabei das Challenge-Response Verfahren involviert ist. Hinweis: Verwenden Sie die Begriffe „Authentication Centre“ und „„A3“. Die Länge von Zeichenketten kann vernachlässigt werden. (12 Punkte)
Antwort: Die Authentifizierungsschlüssel sind im Bereich des heimatlichen Mobilfunkanbieters und auf der SIM-Karte des Kunden gespeichert und nur diesen Parteien zugänglich. Der heimatliche Mobilfunkanbieter des Kunden bekommt eine Anfrage des spanischen Anbieters, den Kunden zu identifizieren. Mit Hilfe des kundenspezifischen Schlüssels und einer Zusatzzahl wird durch den Algorithmus „A3“, „SRes“ gebildet. Die Zufallszahl wird an die SIM des Mobilfunkkunden übermittelt, welche mit Hilfe desselben Schlüssels und Algorithmus ebenso „SRes“erzeugt und dies als Authentifizierungscredential an den heimatlichen Anbieter zur Prüfung übersendet.



4.2 Sichert diese Sicherheitsmodell Sie als Nutzer in einer ähnlichen Art und Weise ab oder bestehen Unterschiede hinsichtlich der umgesetzten Schutzmaßnahmen und warum? (5 Punkte)

Nein! Es findet ausschließliche eine Authentifizierung des Nutzers gegenüber dem Netz statt. Dadurch werden verschiedene Attacken, unter anderem Man-in-the-Middle-Angriffe, ermöglicht.

4.3 Innerhalb einer Demilitarisierten Zone (im Sinne der IT-Sicherheit) ist die Bedrohung:

a. Genauso groß wie im Internet
b. Geringer als Internet, aber höher als im internen Firmennetzwerk
c. Zu vernachlässigen, da demilitarisiert.

Begründen Sie Ihre Antwort (5 Punkte).

Antwort: Da die DMZ durch eine zusätzliche Firewall vom Internet abgeschottet ist, ist a) nicht plausibel. c) ist nicht plausibel, da es der Zweck einer DMZ ist, nach außen offene Services zu beheimaten, das Risiko ist also höher einzuschätzen als in einem privaten Netzwerk.

b) ist korrekt.

5. Identitätsmanagement (11 Punkte)

5.1 Ordnen Sie die folgenden Eigenschaften einer der durch die Profiling Challenge untersuchten Personen zu (je 1 Punkt) und vermerken Sie die Lösung im Lösungsheft. Falsche Antworten führen zu Abzügen in Höhe von jeweils 0,5 Punkten. Insgesamt werden jedoch keine negative Punkte für diese Aufgabe vergeben. (5 Punkte)

	Stefano Crosta	Santiago de Compostella	Giles Hogben	Paolo Alto	Henry Krasemann
Betreibt >100 Domains					
Actor / Model					
Wahlheimat Italien					
Nachwuchs steht bevor					
Joint Research Center (JRC)					

5.2 Aus der Vorlage der Profiling Challenge kennen Sie verschiedene Verfahren, Daten über andere Personen über das Internet zu sammeln. Nennen sie drei verschiedene Dienste, mit denen solche Informationen erlangt werden können. (6 Punkte)

Antwort:

- Web-Archive (Internet Archive, Google Cache…)
- Suchmaschinen (Google, Yahoo…)
- Communities (OpenBC, MySpace…)

Nennung von 3 konkreten Beispielen ist ausreichend.

6 Verschlüsselung (17 Punkte)

6.1 Welches Problem der symmetrischen Verschlüsselung löst asymmetrische Kryptographie? Schildern sie die gelösten und weiterhin bestehenden Probleme. (6 Punkte)

Antwort:

Die Schlüsselverteilung, da öffentliche Schlüssel nicht geheim gehalten werden müssen. So können sie ohne bedenken auf einem Server abgelegt werden, darüber hinaus ist nur noch ein Schlüssel pro Benutzer nötig, und nicht mehr ein Schlüssel pro kommunizierendem Nutzerpaar. Um MitM-Angriffe zu verhindern, wird zusätzlich eine PKI/Zertifizierung nötig.

6.2 Welcher der folgenden RSA-Schlüssel ist gültig? (Hinweis: p=5, q=3)

a. d=3, e=3, n=15
b. d=4, e=2, n=15
c. d=3, e=4, n=15

Begründen Sie kurz Ihre Antwort (8 Punkte)

Antwort: (p-1)(q-1)=8

b) ungültig, da 4 nicht teilerfremd zu 8.
c) ungültig, da 3 * 4 = 4 (!= 1) mod 8, also 4 nicht multiplikatives Inverses von 3.
a) ist korrekt

6.3 Nennen Sie die zwei wichtigen Eigenschaften, die eine Hashfunktion erfüllen sollte. (2 Punkte)

Antwort:

Kollisionsresistenz: Es ist sehr schwer, zwei Werte zu finden, die von der Hashfunktion auf dieselbe Ausgabe abgebildet werden.
Einwegeigenschaft: h(x) leicht zu berechnen, h^-1(x) nicht.

(Kompression: Hashfkt. bilden Eingaben beliebiger Länge auf Ausgaben fester Länge ab).

6.4 Nennen sie eine symmetrische Verschlüsselungsfunktion (0,5).
Antwort: AES, DES, Triple DES,…

6.5 Nennen sie einen asymmetrischen Signaturalgorithmus (0,5).
Antwort: RSA, DSA

7. Evaluation (8 Punkte)

Nach der Eröffnung ihres kleinen Startup-Unternehmes im Bereich des Gartenbaus nehmen Sie die Dienste dreier Berater in Anspruch, um ihre IT-Sicherheitsinfrastruktur auf Schwachstellen untersuchen zu lassen und Lösungsvorschläge aufzuzeigen. Dabei schlagen die Berater ihnen folgende drei Varianten vor:

a. Berater A: Zur Absicherung der Infrastruktur sollte der komplette Maßnahmenkatalog des Grundschutzhandbuchs umgesetzt werden. Bei kleinen Unternehmen wie dem Ihren sei dies auch preislich durchaus zur Aufrechterhaltung der ordnungsgemäßen Geschäftstätigkeiten vertretbar, da das Grundschutzhandbuch ja kostenlos beim BSI erhältlich sei.
b. Berater B: Infrastrukturen sollte man aufgrund der internationalen Vergleichbarkeit auf jeden Fall nach ISO/IEC 17799:2000 untersuchen.
c. Berater C: Eine individuelle Umsetzung von Bausteinen des Maßnahmenkataloges des Grundschutzhandbuches sollte nach Prüfung der Gesamtlage des Unternehmens anvisiert werden.

7.1 Welchem dieser Vorschläge sind sie eher geneigt zuzustimmen und warum. (8 Punkte)
Antwort: Variante c ist richtig. Eine vollständige Umsetzung des Maßnahmenkataloges des Grundschutzhandbuches ist nicht sinnvoll, da viele diese Maßnahmen im Einzelfall nicht zutreffen oder stark überzogene Aufwendungen erfordern würden, die der Situation nicht angepasst sind. ISO/IEC 17799:2000 hat nicht mit Infrastrukturen zu tun und ist daher von vorneherein auszuschließen.