JOHANN WOLFGANG GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

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

Abschlussklausur der Vorlesung: „Informations- und Kommunikationssicherheit“ Sommersemester 2005

Fachbereich
Wirtschaftswissenschaften

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

Prof. Dr. Kai Rannenberg
Dipl. Inf. Heiko Rossnagel

Telefon +49 (0)69-798 25301
Telefax +49 (0)69-798 25306
E-Mail kai.rannenberg@m-lehrstuhl.de

21. Juli 2005

Punktezahl: 90
Veranstalter: Prof. Dr. Kai Rannenberg
Zugelassene Hilfsmittel: Keine

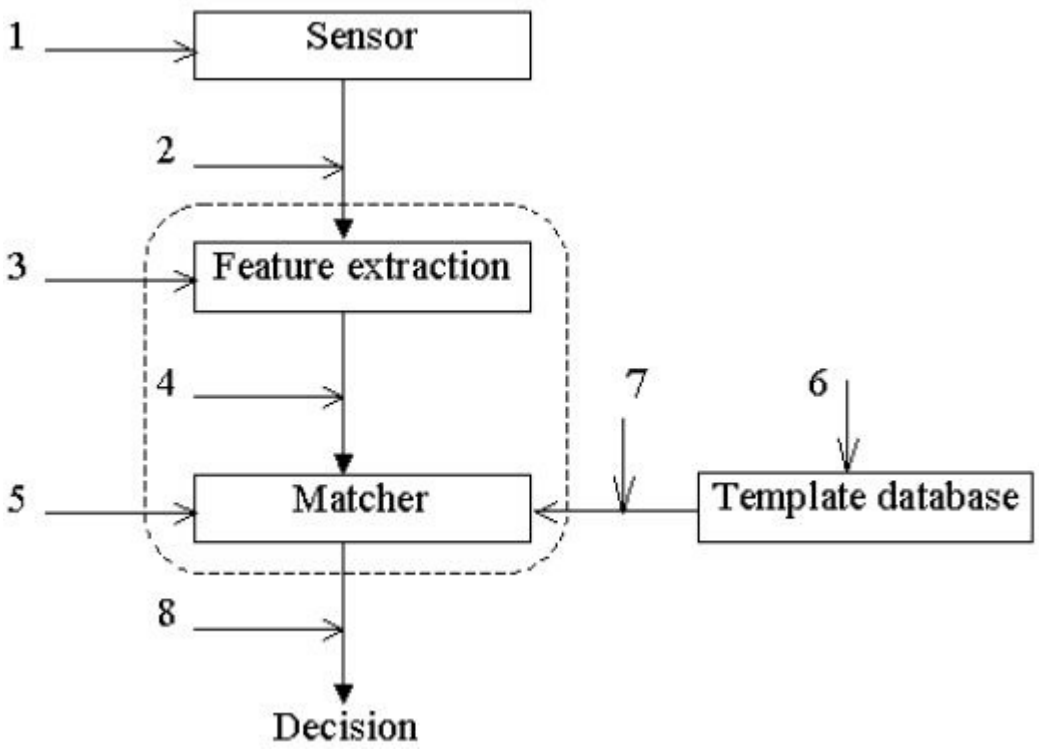
Die Klausur gilt ab 45 Punkten als bestanden.

Wir wünschen viel Erfolg!

Aufgabe 1: (IT-Sicherheit – 8 Punkte)
Nennen und erklären Sie kurz die vier primären Schutzziele der IT-Sicherheit.

Lösung:
Vertraulichkeit (2 Punkte)
Vertraulichkeit bezeichnet den Schutz vor der unbefugten Preisgabe von Informationen an Dritte.
Verfügbarkeit (2 Punkte)
Verfügbarkeit ist der Schutz vor unbefugter Vorenthaltung von Informationen oder Diensten, etwa Informationsdiensten.
Integrität (2 Punkte)
Integrität schützt vor unbefugter Manipulation von Daten und Systemen. Integre Daten sind weder während der Übermittlung noch auf dem Endgerät durch Unbefugte verfälscht oder verändert worden.
Zurechenbarkeit (2 Punkte)
Zurechenbarkeit bezeichnet die Tatsache, dass Aktionen oder Dokumente den urhebenden Personen oder Institutionen zugeordnet werden können, so dass diese, z.B. im Nachhinein nicht in der Lage sind, die Durchführung dieser Transaktion zu bestreiten.

Aufgabe 2: (Authentication – 16 Punkte)
In der folgenden Abbildung ist ein Biometrisches System schematisch dargestellt. Weiterhin sind 8 mögliche Angriffspunkte eingezeichnet. Wählen Sie 4 dieser möglichen Angriffspunkte aus und beschreiben Sie, wie der entsprechende Angriff erfolgen kann (je 4 Punkte).



Lösung:

1. *Utilising an imitation biometric (e.g. a prosthetic finger). Many methods have been developed to easily produce such devices and, in the case of commercially available fingerprint systems, have shown a success rate of between 67 – 100%, mostly dependent on the quality of the original source print (a willing volunteer's print works better than one lifted from a glass, for example). Methods to counteract these issues, such as identifying if it is real, living tissue are showing some promise.*

2. *Although more complex, it is possible to replay previously submitted biometric data to cause a false positive identification. A potential solution to this is for the system to challenge the sensor device with a secure request for additional information. For example, if the system requests the sensor to repeat certain randomly selected parts of the captured data, then the system can establish if the data has really come from the sensor.*
3. *By attacking the system at the feature module point, it is possible, albeit unlikely, for an attacker to force the system to produce values unrelated to the sensor input that subsequently generates a false positive result.*
4. *By replacing the system generated feature values with known valid ones will result in unauthorised access.*
5. *If the matcher can be forced into generating an incorrectly high matching score, then a false positive will result.*
6. *The template matching component is particularly vulnerable since incorrect data stored here (through error, collusion or attack) is open to abuse at any time. A template may be added, edited, removed or replaced in order that an invalid user is authenticated. Database security is the key here to reducing vulnerability since unsecured templates can be reverse-engineered and synthetic data added.*
7. *By intercepting the transmission of the template data, and replacing the original templates with false data, a false positive can be generated.*
8. *By attacking at the decision end of the system, the binary result 'Yes / No' can be modified to falsify the result.*

Attack (1) is perhaps the most intuitive, whilst the remaining attack techniques require a more intimate understanding of the specific authentication system and typically some degree of access to its inner workings. However, all component parts of the authentication system represent a potentially exploitable issue.

Aufgabe 3: (Access Control – 12 Punkte)
Alice kann die Datei *x* lesen, die Datei *y* lesen und schreiben und die Datei *z* ausführen. Bob kann die Datei *x* lesen und schreiben, die Datei *y* schreiben aber nicht lesen und hat keinerlei Zugriff auf die Datei *z*.
a) Schreiben sie eine Menge von Access Control Listen für diese Situation. Welche Liste bezieht sich auf welche Datei? (6 Punkte)
b) Schreiben sie eine Menge von Capability Listen für diese Situation. Auf wen bezieht sich welche Liste? (6 Punkte)

Lösung:
a) Datei x: Alice: read; Bob: read, write (je =1 Punkt pro Person)
Datei y: Alice: read, write; Bob: write (je =1 Punkt pro Person)
Datei z: Alice: execute; Bob: - (je =1 Punkt pro Person)
b) Alice: x: read; y: read, write; z: execute (je =1 Punkt pro Datei)
Bob: x: read, write; y: write; z:- (je =1 Punkt pro Datei)

Aufgabe 4: (Cryptography – 22 Punkte)
a) Verschlüsseln Sie die Nachricht "KLAUSURAUFSICHT" mit Hilfe der Vigenere Chiffre. Verwenden Sie dazu den Schlüssel „KEY". Verwenden Sie die im Folgenden dargestellte Vigenere-Tabelle. (8 Punkte)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

b) Beschreiben Sie die Schwachstelle der Vigenere Chiffre und skizzieren Sie eine Möglichkeit, diese zu beseitigen. (Hinweis: One Time Pad) (6 Punkte)
c) Nennen Sie die Vor- und Nachteile von symmetrischen Verfahren gegenüber asymmetrischen. (4 Punkte)
d) Nennen und beschreiben Sie eine Methode, die Vorteile von symmetrischer und asymmetrischer Kryptographie zu verbinden. (4 Punkte)

Lösung:

a) UPYEWSBESPWGMLR (0,5 Punkte pro Buchstabe + 0,5 falls alles korrekt ist)

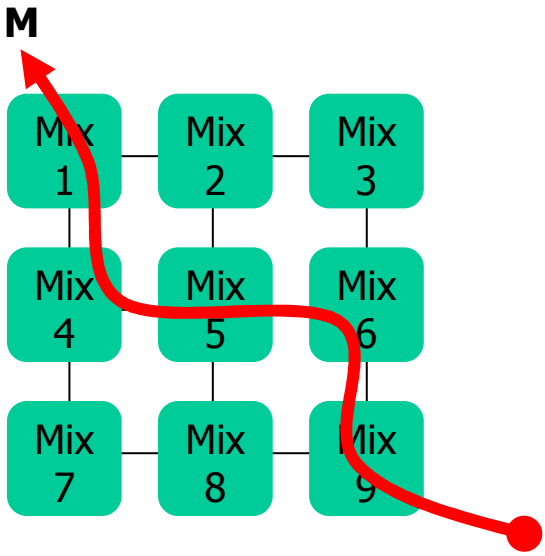
b) Schwachstelle: Schlüssellänge. Es treten Wiederholungen auf, wenn der gleiche Buchstabe des Schlüssels über dem gleichen Buchstaben des zu verschlüsselnden Textes auftritt. Der Abstand dieser Wiederholungen ist ein Vielfaches der Schlüssellänge. Mit diesen Informationen und bei einer kurzen Schlüssellänge lässt sich dann die Chiffre recht einfach brechen.
Lösung: Verwenden einer großen Schlüssellänge (idealerweise gleichlang wie der zu verschlüsselnde Text)

c) Vorteil: Effizienter. Symmetrische Verfahren lassen sich viel schneller berechnen als asymmetrische.
Nachteil: Schlüsselverteilungsproblem. Bei n Benutzern müssen n(n-1)/2 Schlüsselaustausche stattfinden.*

d) Hybride Verfahren: Mit Hilfe asymmetrischer Verfahren wird ein symmetrischer Schlüssel übertragen, mit dem dann die eigentliche Kommunikation verschlüsselt wird. Das Schlüsselverteilungsproblem wird dank des asymetrischen Verfahrens sehr viel einfacher lösbar, und durch die Verschlüsselung der eigentlichen Kommunikation mittels symmetrischer Verfahren bleibt die Performance erhalten.

Aufgabe 5: (Identity Management – 10 Punkte)

Im Folgenden ist ein Mix-Netzwerk abgebildet, in dem die Route einer Nachricht vom Sender frei gewählt werden kann. Wie muss eine Nachricht aufgebaut sein, um die folgende Route zu nutzen: Mix 9, Mix 6, Mix5, Mix 4, Mix 1 ?



Lösung:
{Am9, c9(Am6, c6(Am5, c5(Am4, C4 (Am1, c1(r,M), r2) ,r3) ,r4) ,r5)}

Aufgabe 6: (Computer System Security – 8 Punkte)

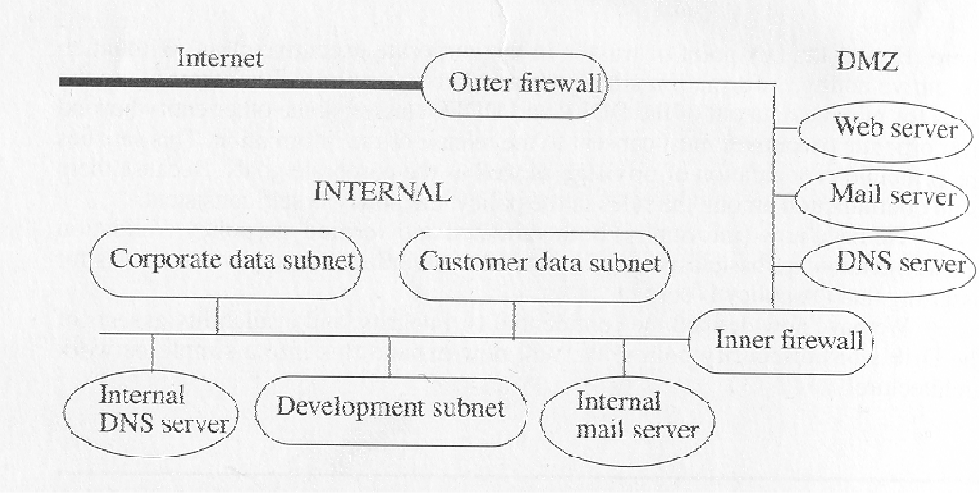
a) Was ist ein Virus? (2 Punkte)
b) Nennen und beschreiben Sie kurz die zwei Phasen der Aktivität eines Viruses. (4 Punkte)
c) Nennen Sie zwei Security Enhancing Techniques. (2 Punkte)

Lösung:

a) Ein Virus ist ein Programm, das sich selbst replizieren kann, indem es sich beispielsweise in andere Dateien hineinkopiert, und das eventuell noch andere (schädliche) Aktionen durchführen kann.
b) Insertion Phase: Virus kopiert sich selbst in eine Datei
Execution Phase: Virus führt eine (schädliche) Aktion aus.
c) Virus scanners, Code Signing, Trusted Operating Base, Checksums and/or Encryption, Intrusion Detection Systems (IDS), Heuristic virus scanners

Aufgabe 7: (Network Security – 10 Punkte)

a) Bob möchte Alice einen elektronischen Liebesbrief schicken. Sein Nebenbuhler Charlie ist am gleichen Subnetz angeschlossen. Beschreiben sie kurz Sie zwei mögliche Angriffe, die Charlie durchführen könnte. (4 Punkte)
b) Was können Alice und Bob machen, um eine vertrauliche Kommunikation zu ermöglichen? (2 Punkte)
c) Gegeben sei die im Folgenden abgebildete Netzwerktopologie. Sie möchten nun ein ungesichertes WLAN aufstellen, um Gästen einen Internetzugang zu bieten. In welchem Netzsegment würden Sie das WLAN ansiedeln, um die Sicherheit des Firmenintranets nicht zu gefährden? (2 Punkte)



d) Was ist ein IMSI-Catcher? (2 Punkte)

Lösung:

a) Angriff auf Vertraulichkeit: Charlie könnte den Liebesbrief abhören.
Angriff auf die Integrität: Charlie könnte den Inhalt des Briefes verändern
Angriff auf die Verfügbarkeit: Charlie könnte die Übertragung des Briefes durch einen DOS-Angriff verhindern.
Angriff auf die Zurechenbarkeit: Charlie könnte sich selbst als Absender des Briefes eintragen.

b) Indem sie ihre Kommunikation auf einer höheren Netzwerkschicht verschlüsseln. Beispielsweise mit IPSEC oder SSL.

c) Außerhalb des äußeren Firewalls oder in der DMZ

d) Ein Gerät, das sich gegenüber einem Handy als Base Station ausgibt und somit die Kommunikation des Benutzers abhören kann.

Aufgabe 8: (Evaluation Criteria – 4 Punkte)
Nennen Sie zwei der Gruppen, die Interesse an Evaluationen von IT-Systemen und Produkten haben und jeweils eines der Ziele, die diese Gruppen an einer Evaluation haben. (4 Punkte)

Lösung:

1. Endnutzer	*Kompatibilität von Systemen und Software mit Sicherheitsanforderungen*
2. Hersteller	*Werbung, Image, Anforderungen von Kunden, etwa öffentlichen (militärischen) Auftraggebern*
3. Evaluierer	*Einnahmequelle*
4. Zertifizierer	*Einnahmequelle, Hoheitliche Aufgabe der Überwachung der Evaluierer.*