JOHANN WOLFGANG GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

Fachbereich Wirtschaftswissenschaften
Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security

Fachbereich
Wirtschaftswissenschaften

Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security
www.m-chair.net

Prof. Dr. Kai Rannenberg

Telefon +49 (0)69-798 34701
kai.rannenberg@m-chair.net

Abschlussklausur Vorlesung „Informations- und Kommunikationssicherheit: Infrastrukturen, Technologien und Geschäftsmodelle“, WS 2008/2009

Punktezahl: 90
Mindestpunktezahl zum Bestehen: 45
Veranstalter:. Dr. Martin Reichenbach, 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:	8	12	14	7	15

Aufgabe:	**6**	**7**	**8**	**9**	**Gesamt**
Punkte:	16	6	6	6	90

Punkte insgesamt:	**Note:**

1. Authentifizierung (8 Punkte)

1.1 Sie greifen ein System mit fünfstelligen PINs, die nur aus Ziffern bestehen, an. Wie groß ist die Wahrscheinlichkeit, bei einem Versuch die (eine) korrekte PIN zu raten, wenn alle PINs gleich wahrscheinlich sind? **(2 Punkte)**

1/10^5 = 1/100.000

1.2 Nennen Sie 3 Maßnahmen, mit denen Sie persönlich für eine höhere Sicherheit Ihrer Passwörter sorgen können. **(3 Punkte)**

-unterschiedliche PWs wählen; -lange PWs wählen; -keine Wörterbuchwörter

1.3 Warum werden bestimmte Authentifizierungsfaktoren meistens im Rahmen von Multi-Faktor-Authentifizierung verwendet? Erklären Sie anhand eines Beispiel-Faktors. **(3 Punkte)**

z. B. Tokens sind alleine unsicher, weil sie verloren gehen können. Daher findet oftmals eine ergänzende Kontrolle statt (PIN). Das „Etwas Wissen" ergänzt etwa um den „Etwas Haben"-Ansatz.

2. Identitätsmanagement (12 Punkte)

2.1 Der Klassifizierung von Identitätsmanagementsystemen liegen die verschiedenen Schichten der Identität nach Durand zugrunde („Tier 1-3 Identities"). Nennen und beschreiben Sie diese kurz. **(6 Punkte)**

Pro Nennung und pro Beschreibung jeweils 1 Punkt.

- Tier 1: True („My") Identity
  - Meine tatsächliche und persönliche digitale Identität
  - Wird ausschließlich von mir kontrolliert
  - (Bspl. Selbsterstelltes Profil in einer Social Community)
- Tier 2: Assigned („Our") Identity
  - Digitale Identität, die uns zugeordnet wird.
  - Zuordnung erfolgt durch 3. Parteien (implizit klar)
  - (Bspl. Sozialversicherungsnummer)
- Tier3: Abstracted („Their") Identity
  - Aus Identitätsattributen Abgeleitet
  - Zuordnung zu einer Gruppe / Zuordnung einer Gruppenidentität

2.2 In Bezug auf welchen Faktor unterscheiden sich die verschiedenen Schichten der Identität voneinander? Erläuter Sie anhand dieses Faktors, wie sich die Schichten voneinander abgrenzen. **(4 Punkte)**

- Kontrolle (1 Punkt)
- Tier 1 Identity wird komplett vom Individuum kontrolliert. Die Tier 2 Identität kann nur zum Teil vom Individuum kontrolliert werden (die Attribute der Tier 2 Identität sind dem Individuum allerdings bekannt). Die Tier 3 Identität kann nicht vom Individuum kontrolliert werden (das Vorhandensein einer Tier 3 Identität kann, muss aber nicht zwingend, dem Individuum bekannt sein). (3 Punkte)

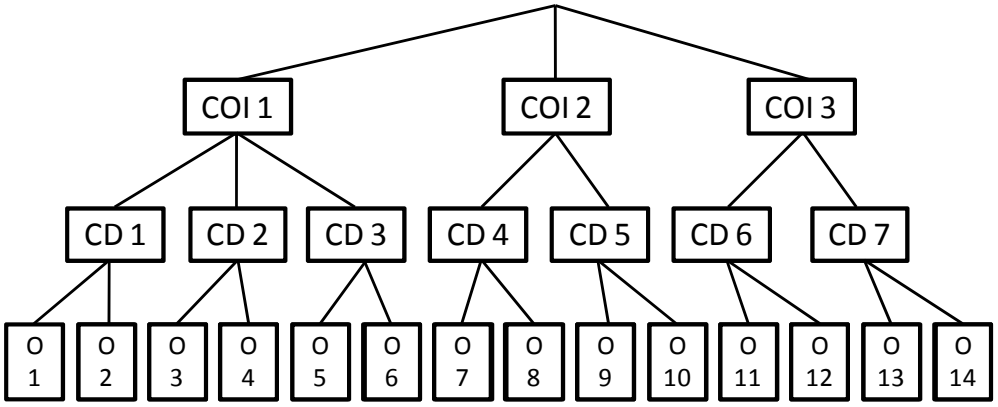
2.3 Sie haben ein Semester lang regelmäßig die Vorlesung Informations- und Kommunikationssicherheit besucht. Jetzt beschließen Sie, Ihre eigene Identität und Privatsphäre im Internet besser zu schützen. Nennen Sie zwei der in der Vorlesung vorgestellten Privacy Enhancing Technologies. **(2 Punkte)**

- The Anonymizer
- Mixmaster – Anonymous Remailer
- Onion Routing
- Java Anonymous Proxy
- Tor Network
- Cookie Cooker
- P3P – Platform for Privacy Preferences
- Reachability Management

- Idemix
- Beschreibung IdM II, Folien 23

3. Zugangskontrolle (14 Punkte)

Nach erfolgreich absolviertem BWL-Studium schaffen Sie den Direkteinstieg in eine Investmenbank. Dort erkennen Sie auf Anhieb, dass die Security Policy der Bank auf dem Chinese Wall Modell basiert, das sie bereits während ihres Studiums kennen gelernt haben.



Sie erkennen sofort, dass es insgesamt 3 Konfliktklassen (COI) „IPO-Beratung“, „Outsourcing-Beratung“, „Hedging-Beratung“ und 7 Firmen-Datensätze (CD) gibt. Insgesamt sind diesen 14 Objekte (O) zugeordnet.

3.1 Nennen Sie zunächst drei Voraussetzungen, von denen mindestens eine erfüllt sein muss, damit Sie auf ein Objekt zugreifen dürfen. **(6 Punkte)**

Access Control Vorlesung, Folie 37

3.2 Sie stehen kurz vor ihrem ersten Arbeitsauftrag und Systemzugriff. Gibt es zum jetzigen Zeitpunkt bereits Objekte, auf die Sie grundsätzlich wegen der Chinese Wall Policy nicht zugreifen dürfen? **(2 Punkte)**

Nein

3.3 Nach einem halben Jahr ist ihre Probezeit vorbei und sie hatten bereits Zugriff auf die Objekte 1,7, und 8. Welche weiteren Objekte können zukünftig für Sie noch relevant werden? **(6 Punkte)**

2, 11, 12, 13, 14 (6 Punkte wenn alle richtig sind)

4. Biometrie & Social Engineering (7 Punkte)

4.1 Im Rahmen der öffentlichen Diskussion um die Erhebung, die Speicherung und die Verwendung biometrischer Identifikationsmerkmale wurde vom Chaos Computer Club der Fingerabdruck des amtierenden Bundesinnenminister, Wolfgang Schäuble, veröffentlicht.
Welche Funktion müsste ein Zugangsberechtigungssystem, das auf Fingerabdruckdaten basiert, bieten, um den Missbrauch von Wolfgang Schäubles Fingerabdruck zu erschweren? Erläutern Sie diese Funktion anhand eines Beispiels. **(7 Punkte)**

(3,5 Punkte für Funktion, 3,5 Punkte für Beispiel)

Berücksichtigung weiterer Identifizierungsmerkmale

- Z.B. zusätzlicher Einsatz einer PIN

Lebenderkennung:

- Puls
- Elektrische Eigenschaften der Haut (spezifischer Widerstand)
- Farbe der Haut
- Absorptionseigenschaften im Infrarotbereich
- Reflexionseigenschaften im Ultraschallbereich
- Schweißaustritt

5. Netzsicherheit (15 Punkte)

5.1 Sie haben im Laufe der Vorlesung Authentifizierungsmechanismen für das GSM-Netz kennen gelernt. Sichert deren Sicherheitsmodell Sie als Nutzer in einer ähnlichen Art und Weise ab, wie auch der Netzbetreiber abgesichert wird, oder bestehen Unterschiede hinsichtlich der umgesetzten Schutzmaßnahmen? Wenn Sie Unterschiede sehen, beschreiben Sie diese kurz, wenn für beide Seiten derselbe Mechanismus eingesetzt wird, nennen Sie diesen. **(3 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.

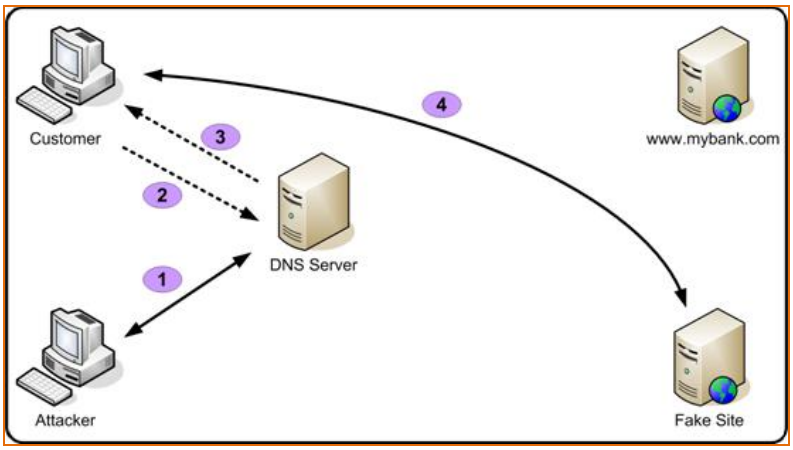
5.2 Wie schätzen Sie in Anbetracht der im GSM-Netz verwendeten Sicherheitsmechanismen die Abhörsicherheit der Kommunikation ein? Angenommen, Sie wollten über den GSM-Kanal vertraulich Daten austauschen: welche zusätzlichen Möglichkeiten zur Erreichung dieses Ziels sähen Sie? **(2 Punkte für die Einschätzung, 2 Punkte für den Vorschlag zur Absicherung)**.

Antwort: Keine end-to-end-Vertraulichkeit, da nur die Funkstrecke mit fragwürdigem Protokoll verschlüsselt.

Antwort: Zusätzliches Sicherheitsprotokoll VPN zwischen den Endpunkten einsetzen, um vertraulichen Kanal zu schaffen.

5.3 Stellen Sie den Kommunikationsablauf während einer DNS-Spoofing-Attacke dar. **(8 Punkte)**

Antwort:



(1)Angriff gegen DNS-Server, Austausch IP-Adresse von „www.mybank.com“ gegen IP von „Fake Site“

(2)Anfrage nach IP-Adresse von „www.mybank.com“.

(3)Antwort: IP von „Fake Site“ (da ausgetauscht)

(4)Benutzer wird auf „Fake Site“ umgelenkt, potenziell ohne es zu bemerken.

6. Kryptographie (16 Punkte)

Während Sie potenzielle Namen für Ihre neue Katze diskutieren, fällt einem Ihrer Bekannten auf, dass 2 der vorgeschlagenen Namen, n1 und n2, unter einer ihm bekannten kryptographischen Hashfunktion h dieselben Werte liefern.

6.1 Ist dies theoretisch möglich, obwohl Hashfunktionen Sicherheitseigenschaften haben, die diesen Fall verhindern sollten? **(2 Punkte)**

Ja. Die Kollisionsresistenz macht sie zwar schwer zu finden, aber aufgrund der Kompression muss es solche Paare geben. Der geschilderte Fall ist zwar unwahrscheinlich, aber kann vorkommen.

6.2 Welcher Angriff, der mittels öffentlicher Schlüssel durchgeführt werden kann, macht Zertifizierung notwendig? **(2 Punkte)**

Antwort: Um MitM-Angriffe zu verhindern, wird eine Zertifizierung nötig.

6.3 Welchen pragmatischen Ansatz wählen Designer von Sicherheitslösungen, um die logistischen Probleme der Verwendung symmetrischer und asymmetrischer Kryptografie zu umgehen? Nennen Sie den Ansatz und beschreiben Sie die Vorgehensweise anhand eines allgemein verwendbaren, sicheren Protokolls für Client-Server-Kommunikation anhand je eines gängigen Verschlüsselungs- und Signaturalgorithmusses **(1 Punkte fürs Nennen, 2 Punkte fürs Beispiel)**.

Antwort: Hybridverfahren, die jeweiligen Nachteile ausschließen (Nachteile sichere Schlüsselverteilung bei Symm., Performance bei asymm. Kryptosystemen).
Symmetrisch: AES, Triple DES; Asymmetrisch: RSA, Elliptic Curve
Antwort: 1) Schlüsselerzeugung symm. 2) Verschlüsselung der Nachrichten mit symm Schlüssel 3) Anforderung Public Key des Empfängers 4) Schlüsselverteilung des symm. Keys per asymm. Krypto, d.h. Versenden des mit dem Symm. Schlüssel verschlüsselten Nachricht PLUS des mit dem Public Keys des Empfänger verschlüsselten Symm.Keys an Empfänger 5) Der Empfänger entschlüsselt das Paket mit seinem Privaten Schlüsselteil, erhält so den Symmetrischen Schlüssel zur Entschlüsselung der ursprünglichen Nachricht.

6.4 Sie sind vom deutschen Geheimdienst engagiert worden, für die Bundesregierungdas Codewort für den Zugang zur Büchse der Pandora zu verschlüsseln. Sie wählen den Kryptoalgorithmus RSA mit den Primzahlen p=3, q=11 und dem öffentlichen Exponenten e=3.

a) Berechnen Sie dazu n **(1 Punkt)**

b) Berechnen Sie aus den Parametern den geheimzuhaltenden Exponenten d und erklären Sie, warum man üblicherweise zur Verschlüsselung einen kleineren „öffentlichen“ Exponenten wählt als zur Entschlüsselung **(2 Punkte fürs Berechnen, 2 für die Erklärung)**

c) Verschlüsseln Sie ein beliebiges Zeichen des Klartextes bzw. Codeworts „ANGIE“ mit A(00), B(01) … Z(25), Blank (26) **(2 Punkte)**

d) Zeigen Sie, dass das Entschlüsseln dieses einen Cipher-Textes wieder den Ursprungs-Klartext ergibt.

(2 Punkte).

Antwort:

a) n = p*q = 3*11 = 33

b) e*d mod (p-1)*(q-1) =
3 * d mod (3-1) * (11-1) =
3*d mod 20 =
21 mod 20 = 1
=> d = 7
Aus Performance gründen ist e oft der kleinere der beiden, da die rechenintensiveVerschlüsselung damit auf leistungsschwächeren Geräten (z.B. PDAs, Mobiltelefone) performanter wird.

c) Example M = “E” = “04”
Verschlüsselung des Message-Blockes “04”
(4**3) mod 33 = 64 mod 33 = 31

d) Entschlüsselung des Cipher-Blockes “31”
(31**7) mod 33 = 27 512 614 111 mod 33 = 4

7 Computer System Security (6 Punkte)

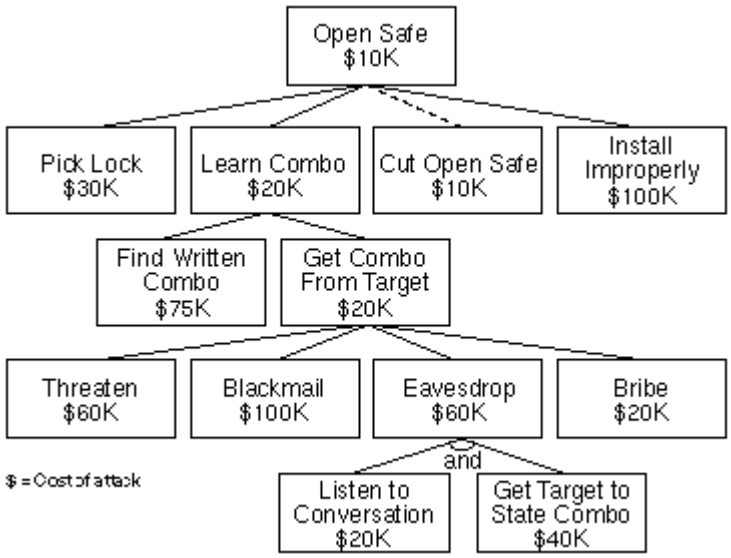
Nennen Sie 6 gängige Kategorien (Typen) von Viren, und beschreiben Sie kurz.deren Angriffspunkt bzw. Wirkung **(6 Punkte)**.

Antwort: s. Folien Computersicherheit

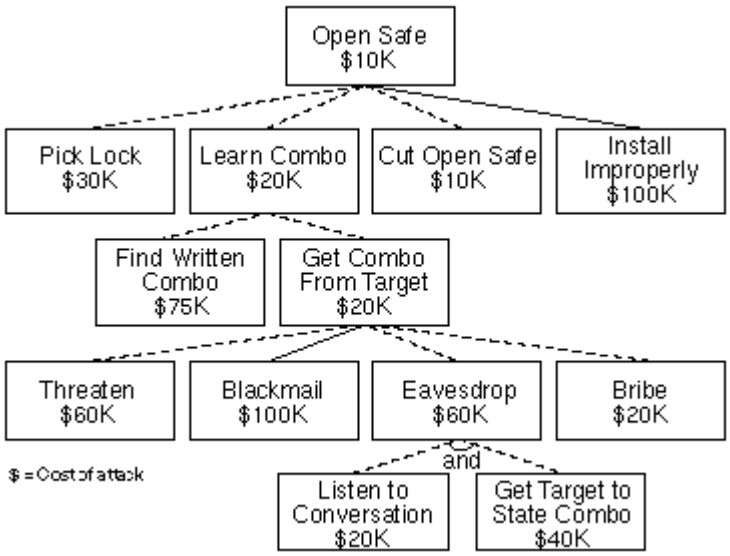
8 Security Engineering (6 Punkte)

Der nachfolgend gezeigte Angriffsbaum beschreibt die Kosten für die zur Öffnung eines Tresors notwendigen Schritte und zeigt durch die gestrichelte Linie den Schritt, mit dem der

Safe am günstigsten geöffnet werden kann. Markieren Sie durch gestrichelte Linien die möglichen Schritte, die es mit **weniger als $100K** ermöglichen, den Safe zu öffnen. **(4 Punkte).**



Antwort:



9 Evaluation Criteria (6 Punkte)

Nennen Sie die vier wichtigsten Motivationsfaktoren für die Zertifizierung und Evaluierung von IT-Prozessen, -Systemen und –Produkten?. **(4 Punkte).**

Skizzieren Sie den typischen Ablauf einer Produktevaluierung (2 Punkte).

Antwort: s. Folien Evaluation Criteria