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-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 2008

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 insgesamt:	**Note:**

1. Authentifizierung (8 Punkte)

1.1 Sie greifen ein System mit vierstelligen 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)**

1/10^4 = 1/10.000

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).

2. Identitätsmanagement (16 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 Im Rahmen der Profiling Challenge wurden verschiedene Informationen über 3 Zielpersonen erhoben. Ordnen Sie die unten dargestellten Ergebnisausschnitte der entsprechenden Identitätsschicht den dazugehörigen Zielpersonen zu. Geben Sie hierzu an welcher Ausschnitt welchem Tabellenfeld zugeordnet werden muss. **(4,5 Punkte)**

	Bernd Ueberschär	Jan Camenisch	Thierry Nabeth
Tier 1 Identity	A1	B1	C1
Tier 2 Identity	A2	B2	C2
Tier 3 Identity	A3	B3	C3

Ausschnitt 1: Persönliche Profilangabe

- Name der Zielperson
- Alter: 45
- Sternzeichen: Krebs
- Chinesisches Sternzeichen: Tiger
- Wohnort: Fontainebleau
- Lieblingsfilme: Bladerunner, The Game…

Ausschnitt 2: Persönlichkeitstyp

- Wikipediaeinträge werden nur selten früh morgens und des Öfteren später abends editiert.
- Ergo: Zielperson vermutlich der Gruppe der Nachtmenschen als der Frühaufsteher zurechenbar.

Ausschnitt 3: Berufliche Kontaktdaten

- Department of Fishery Biology
- Düsternbrooker Weg 20
- D-24105 Kiel, Germany
- Tel: ++49 431 600 45 72

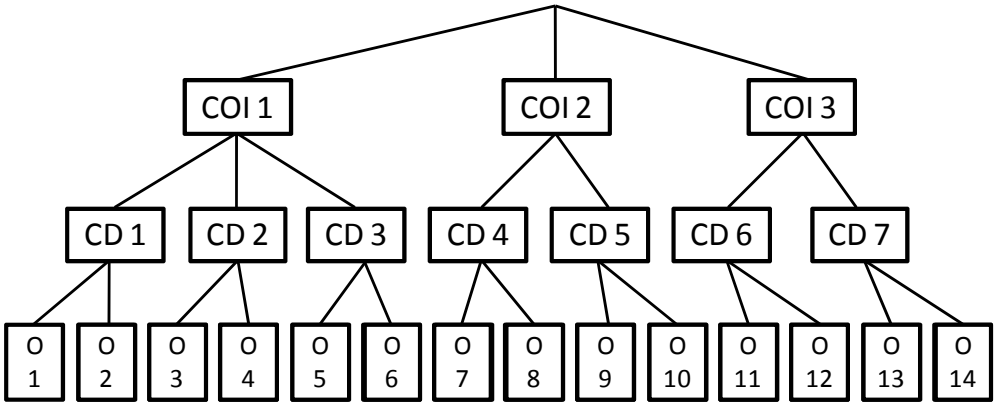
Pro richtiger Zuordnung der Ebene 1 Punkt, pro richtiger Zuordnung des Namens 0,5 Punkte.
Ausschnitt 1 → C1
Ausschnitt 2 → C3
Ausschnitt 3 → A2

2.4 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 eine der in der Vorlesung vorgestellten Privacy Enhancing Technologies. **(1,5 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) 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 Auftrag 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 (14 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

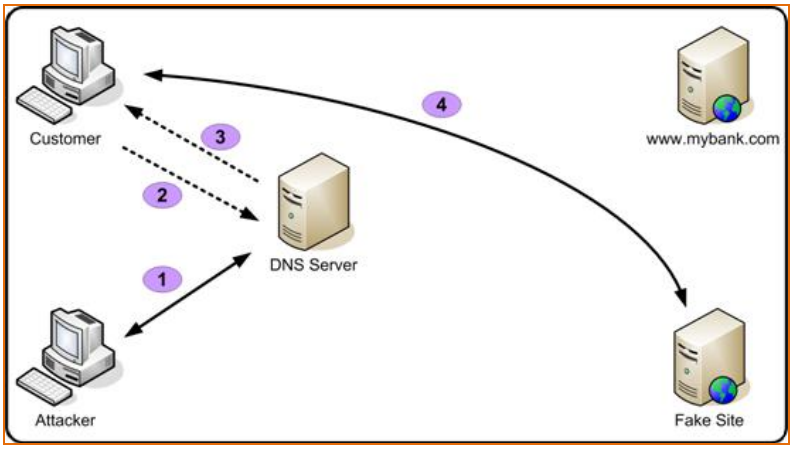
4.2 Neben dem Computer-Based und dem Human-Based Social Engineering ist das „Reverse Social Engineering“ eine weitere typische Ausprägung des Social Engineerings. Beschreiben Sie kurz, was unter Reverse Social Engineering zu verstehen ist und geben Sie hierzu ein Beispiel. **(7 Punkte)**
RSE: Angreifer versucht, dass Opfer ihm die gewünschten Informationen selbstständig, freiwillig und aktiv gibt. (3 Punkte)

Beispiel aus dem Gastvortrag: Angreifer stellt sich telefonisch als neuer Supportmitarbeiter beim Opfer vor und überredet dieses zur Preisgabe von Username, Login-Domäne und Passwort. (4 Punkte)

5. Netzsicherheit (13 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 Operator 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 Stellen Sie den Kommunikationsablauf während einer DNS-Spoofing-Attacke dar. **(10 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.

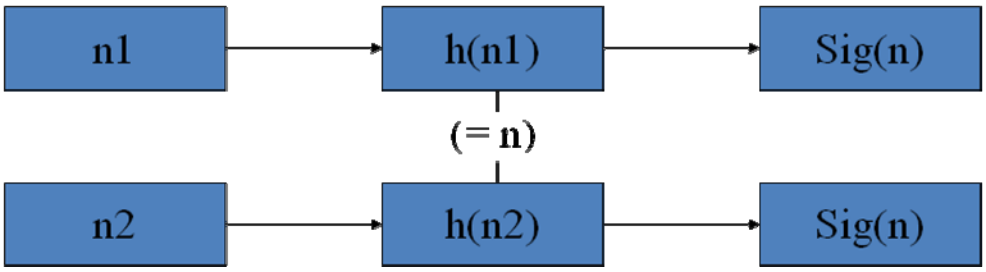
6. Kryptographie (10 Punkte)

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 Beschreiben Sie einen möglichen Angriff, bei dem Ihr Bekannter unter Anwendung solcher Werte n1 und n2 signierte Dokumente gegeneinander austauschen kann, wenn h im Rahmen der Signaturerstellung als Hashfunktion verwendet wurde. **(8 Punkte)**

Antwort:



7 Verschlüsselung (5 Punkte)

7.1 Welches logistische Problem der symmetrischen Verschlüsselung löst asymmetrische Kryptographie? **(1 Punkt)**
Antwort: Schlüsselverteilung.

7.2 Welcher Angriff, der mittels öffentlicher Schlüssel durchgeführt werden kann, macht Zertifizierung notwendig? **(2 Punkte)**
Antwort: Um MitM-Angriffe zu verhindern, wird eine Zertifizierung nötig.

7.3 Nennen Sie eine symmetrische Verschlüsselungsfunktion **(1 Punkt)**.
Antwort: AES, DES, Triple DES…

7.4 Nennen Sie einen asymmetrischen Signaturalgorithmus **(1 Punkt)**.
Antwort: RSA, DSA…

8 Computer System Security (10 Punkte)

Nennen Sie 5 gängige Kategorien (Typen) von Viren, und beschreiben Sie diese kurz. **(10 Punkte)**.
Antwort: s. Folien Computersicherheit