

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

Fachbereich
 Wirtschaftswissenschaften

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

Prof. Dr. Kai Rannenberg

Telefon +49 (0)69-798 34701
 Telefax +49 (0)69-798 35004
 E-Mail: kai.rannenberg@m-chair.net

Dipl.-Wirt.-Inf. Markus Tschersich

E-Mail: markus.tschersich@m-chair.net

Dipl.-Kfm. Marvin Hegen

E-Mail: marvin.hegen@m-chair.net

Abschlussklausur der Vorlesung „Mobile Business II“, SS 2010

Punkteanzahl: 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 <i>(Bitte eintragen)</i>	
---	--

Studiengang	<i>Diplom (MBU2_SWI6)</i> <i>Master (MOB2)</i>
--------------------	---

Aufgabe:	1	2	3	4	5	6	7	Gesamt
Punkte:								

Note:	
--------------	--

Aufgabe 1: LBS-Ortung, Navigation und Kartografie (9 Punkte)

Letztens haben Sie sich mit einem Freund über Ihre Lehrveranstaltung Mobile Business II unterhalten. Ihr Freund, der ein begnadeter Wanderer ist, fand die Möglichkeiten mobiler Endgeräte sehr interessant. Auf diese Weise kann man Wanderrouten untereinander austauschen und hat mit dem mobilen Endgerät auch immer eine aktuelle Karte dabei. Er selbst hat eine Online Community namens „WalkyTalky“ für Wanderer gegründet, aber seiner Meinung nach fehlen dort die Möglichkeiten dieser mobilen Endgeräte. Wanderer sind schließlich beim Laufen draußen und nicht zuhause vor dem Computer. Sie sind begeistert von seiner Idee und wollen ihn darin unterstützen, die Community um mobile Dienste zu erweitern. Dazu müssen aber noch einige Fragen geklärt werden.

- a) Welche verschiedenen ortsbezogenen Informationen sollte das gewählte Kartenmaterial den Wanderern zur Verfügung stellen? (4 Punkte)

(pro Information 1 Punkt)

Wege, Wassertiefe, Vegetation, Wasservorkommen, Name des Gewässers, Fischvorkommen, ...

- b) Nennen Sie drei verschiedene Ortungsverfahren und wählen Sie ein Ortungsverfahren aus, welches am besten für den Anwendungsfall der Wanderer geeignet ist. Begründen Sie Ihre Wahl. (5 Punkte)

(1 Punkt pro genanntes Ortungsverfahren, 1 Punkt für die Auswahl des geeigneten Verfahrens, 1 Punkt für die richtige Begründung.)

GPS, Galileo, Position Sender, Funkzellenortung, WLAN Empfang von Satelliten-Signalen zur Ortsbestimmung

Auf Satelliten basierende Ortung ist am besten, da in ländlichen Regionen nicht immer eine Funkabdeckung gewährleistet ist.

Aufgabe 2: Die Google Economy (12 Punkte)

Google hat mit seiner Mitgliedschaft in der Open Handset Alliance einen bedeutenden Einfluss auf das mobile Betriebssystem Android. Zusätzlich hat Google mit dem Nexus One Anfang 2010 auch eigene Smartphones auf den Markt gebracht. Nennen Sie vier begründete Beispiele dafür, welche strategische Bedeutung Android, die Mitgliedschaft in der Open Handset Alliance und die eigene Hardware für die Firma Google haben. (12 Punkte)

- Kontrolle über das mobile Betriebssystem auf mobile devices erlangen (Differenzierungsstrategie)
- Einflussnahme im Rahmen der Zusammenarbeit mit Mobile Device Equipment Herstellern in der Mobile Handset Alliance (Wettbewerbsvorteil)
- Integration der Produktwelt von Google (Seamless) zur Festigung der Kundenbindung
- Steigerung der Umsätze mit kontextorientierter Werbung im mobilen Internet (Übertragung des Geschäftsmodells vom Internet ins mobile Internet)
- Besetzen eines Teils der Wertschöpfungskette der Telekommunikationsindustrie (Content & Innovation bzw. Service Bereich) – z.B. Location Based Services oder Herstellung eigener Endgeräte
- Integration mit dem Google Marketplace und dadurch einfacherer Zugang zu den Entwicklerkompetenzen (long tail effect) – Nachahmungseffekt von Apple

4 Antworten: Je Antwort 3 Punkte = 12 Punkte insgesamt

Aufgabe 3: Kryptographie (18 Punkte)

Mit einem Freund/einer Freundin haben Sie kürzlich diskutiert, dass die Nutzung Ihres Instant Messaging Programmes nicht die höchste Stufe an Vertraulichkeit bietet, da sämtliche Kommunikation unverschlüsselt übertragen wird. Als Besucher der Veranstaltung „Mobile Business II“ machen Sie sich Gedanken darüber, wie man Verschlüsselung für diesen Messenger umsetzen könnte.

- a) Geben Sie in wenigen Schritten wieder, wie eine Verschlüsselung/Entschlüsselung bei symmetrischen und asymmetrischen Kryptosystemen abläuft. (8 Punkte)

(0,8 Punkte pro korrekten Schritt)

Symmetrische Verschlüsselung:

1. Sender S erzeugt geheimen Schlüssel k
2. S sendet k an Empfänger E (über sicheren Kanal)
3. S verschlüsselt Nachricht M mit k und erhält Chiffretext C
4. S sendet C an Empfänger E
5. Empfänger E entschlüsselt C mit Schlüssel k und erhält Nachricht M

Asymmetrische Verschlüsselung:

1. Empfänger E erzeugt asymmetrisches Schlüsselpaar (pub / priv)
2. E sendet öffentlichen Schlüssel pub an Sender S
3. Sender S verschlüsselt Nachricht M mit pub und erhält Chiffretext C
4. S sendet C an Empfänger E
5. E entschlüsselt C mit privatem Schlüssel priv und erhält Nachricht M

- b) Machen Sie sich Gedanken über die jeweiligen Vor- und Nachteile der in a) vorgestellten Kryptosysteme. Nennen Sie bis zu drei Punkte pro Verschlüsselungssystem. (6 Punkte)

(1 Punkt pro korrekte Nennung)

Symmetrische Kryptosysteme:

Vorteile:

- Algorithmen sind schnell

Nachteile:

- Komplexe Schlüsselverwaltung
- Schlüsselaustausch erfordert existierenden sicheren Kanal

Asymmetrische Kryptosysteme:

Vorteile:

- Keine geheime Information muss über unsicheren Kanal ausgetauscht werden
- Nur ein Schlüssel pro Endpunkt

Nachteile:

- Algorithmen sind langsam
- Anfällig für Man-in-the-middle Attacken

(Weitere Nennungen möglich, sofern plausibel)

- c) Welche der in b) genannten Vor- und Nachteile sind besonders für Instant Messaging einschlägig? Wählen Sie zwei Punkte aus und begründen Sie kurz Ihre Wahl. (4 Punkte)

(0,5 Punkte pro Nennung; je 1,5 Punkte für Beschreibung)

- Algorithmen sind schnell: Besonders relevant für IM, da Daten in Echtzeit übertragen werden müssen. Sticht besonders beim Versand von großen Datenmengen hervor (Multimedia).
- Komplexe Schlüsselverwaltung: Bei Peer-to-Peer-Systemen, wie IM muss ein Nutzer je einen geheimen Schlüssel pro Kommunikationspartner verwalten.

- Schlüsselaustausch erfordert existierenden sicheren Kanal: Ist in den meisten Fällen nicht gegeben, da Kommunikationspartnerschaft den Austausch eines geheimen Schlüssels erfordert. Dies ist ohne zusätzlichen sicheren Kanal über das Web nicht möglich.
- Keine geheime Information muss über unsicheren Kanal ausgetauscht werden: Behebt obiges Problem.
- Algorithmen sind langsam: Kritisch bei Echtzeitanwendungen wie IM, da u.U. große Datenmengen (Multimedia) versandt werden müssen.

Aufgabe 4: Evaluierung des Designs von mobilen Anwendungen und Diensten (8 Punkte)

Nennen Sie vier Design-Evaluierungsmethoden, ordnen diese einer der fünf Kategorien (Observational, Analytical, Experimental, Testing, Descriptive) zu und beschreiben die Methode kurz. (8 Punkte)

(1 Punkt je Nennung und 1 Punkt für die jeweilige richtige Beschreibung)

mobile business		Design Evaluation Methods
Observational	Case study	Studies artifact in depth in business environment
	Field study	Monitors use of artifact in multiple projects
Analytical	Static analysis	Examines structure of artifact for static qualities (e.g. complexity)
	Architecture analysis	Studies how artifact fits into technical IS architecture
	Optimization	Demonstrates inherent optimal properties of artifact or provides optimality bounds on artifact behavior
	Dynamic analysis	Studies artifact in use for dynamic qualities (e.g. performance)
Experimental	Controlled experiment	Studies artifact in controlled environment for properties (e.g. usability)
	Simulation	Executes artifact with artificial or historical data
Testing	Functional (black box) testing	Executes artifact interfaces to discover failures and identify defects
	Structural (white box) testing	Performs coverage testing of some metric (e.g. execution paths) in the artifact implementation
Descriptive	Informed argument	Uses information from the knowledge base (e.g. relevant research) to build a convincing argument for the artifact's utility
	Scenarios	Scenarios: Construct detailed scenarios around the artifact to demonstrate its utility

[based on Hevner et al. 2004] 5

Aufgabe 5: Mobile Brokerage und Mobile Payment (18 Punkte)

a) Erklären Sie den Unterschied zwischen Push und Pull Services anhand von Mobile Brokerage. Beschreiben Sie dazu, welche Parteien beteiligt sind und wie die Kommunikation zwischen diesen jeweils abläuft. (5 Punkte)

(0,5 Punkte pro Nennung der Partei, Max 1 Punkt; 2 Punkte pro Beschreibung)

- Partei: Client und Server
- Push
 - User konfiguriert Settings
 - Server sendet Informationen (z. B. über Aktienkurse) an Mobilgerät des Clients (Users)

- Pull
 - User (Client) fordert Informationen (Website) an
 - Server sendet entsprechende Informationen (Website)

b) Nennen Sie die Ihnen aus der Vorlesung bekannten vier Schutzziele (Protection Goals) für IT-Sicherheit und erklären Sie diese Ziele anhand eines Szenarios aus dem Bereich des Mobile Payment. (8 Punkte)

(0,5 Punkte pro Nennung, Max. 2; 1 Punkt Szenarien; 1,5 Punkte wenn anhand eines Szenarios beschrieben, Max 6)

- Confidentiality (Vertraulichkeit)
 - Beschreibt den Schutz vor unautorisiertem Informationserwerb, d.h. Information wird falscher Person bekannt.
 - Beispiel: Andere Person kann die PIN oder andere Kontodaten auslesen.
- Integrity (Integrität)
 - Verlust der Integrität resultiert aus unautorisierter Informationsveränderung, d.h., Information wurde beabsichtigt oder unbeabsichtigt verändert.
 - Beispiel: verfälschte Überweisungen
- Accountability (Zurechenbarkeit)
 - Verlust der Zurechenbarkeit bedeutet, dass die für eine Transaktion verantwortliche Person (oder das System) nicht eindeutig identifiziert werden konnte
 - Beispiel: Verantwortlicher für eine Zahlung/Transaktion/Abbuchung kann nicht ermittelt werden.
- Availability (Verfügbarkeit)
 - Ein Verlust der Verfügbarkeit kann durch unautorisierten aber bemerkten Eingriff in die Systemfunktionalität verursacht werden. Als Konsequenz kann auf benötigte Daten/Informationen nicht zugegriffen werden bzw. der Zugriff auf diese wird verzögert.
 - Beispiel: Bei Verlust der Verfügbarkeit kann auf benötigte Daten/Informationen nicht zugegriffen werden bzw. der Zugriff auf diese wird verzögert.

c) Nennen Sie die unterschiedlichen Parteien, die in Mobile Payment-Szenarien beteiligt sein können und beschreiben Sie kurz deren individuelle Interessen. (5 Punkte)

(0,5 Punkte pro Nennung, Max 2,5 und 0,5 Punkte pro Beschreibung, Max 2,5)

1. Customers: Only a small number of (trustworthy) parties should have access to personal financial data.
2. Merchants: Accepted payments should be enforceable.
3. Network operators: Offering of new (security-relevant) services (e.g. billing services)
4. Banks: Controlling the payment-process
5. Central Banks: No direct C2C payments to avoid a shadow currency

Aufgabe 6: Datenschutz & Identitätsmanagement (16 Punkte)

a) Nennen und beschreiben Sie die Data Protection Principles im Kontext von Kommunikationsdiensten. (3 Punkte)

(0,5 für Nennung, 0,5 für richtige Beschreibung)

- **Data minimisation:**
The service should be offered with a minimum of needed data.
- **Information of data subject:**
The person, whose data is being stored, should know what has been stored.
- **Acceptance not without consent:**
The data subject is to be asked in advance.

b) Grenzen Sie die Begriffe *Data Protection* und *Privacy* voneinander ab. (4 Punkte)
(2 Punkte je Begriff)

- **Data protection** is the protection against adverse or unasked usage of data from the personal sphere of a person.
- **Privacy**, on the other side, is the right “to be left alone”, e.g. to be unobserved or to be anonymous.

[WaBr1890]

- **Why ensuring the rights of freedom?**
 - Right of informational self-determination as a fundamental human right, derived from the Constitution (Grundgesetz) - “Volkszählungsurteil” (BVG83)
 - Protection against too extensive governmental control

c) Nennen Sie die drei Ebenen (Tiers) von Identitäten, beschreiben diese und grenzen sie voneinander ab. (9 Punkte)

(1 Punkt je Nennung + 2 Punkte je richtiger Beschreibung und Abgrenzung)

mobile business Identity Concepts: View of Identity (Control)

- **Tier 1 (T1):** True ('My') identity
- **Tier 2 (T2):** Assigned ('Our') identity
- **Tier 3 (T3):** Abstracted ('Their') identity
- The different tiers can be distinguished by the factor 'control': **Who controls the identity?**

[Durao3]

mobile business Identity Concepts Tier 1: True Identity

- A Tier 1 (true - 'My') identity is my true and personal digital identity and is owned and controlled entirely by me, for my sole benefit.
- T1 identities are both timeless & unconditional.

mobile business Identity Concepts Tier 3: Abstracted Identity

- A Tier 3 (abstracted - 'Their') identity is an abstracted identity in that it identifies us through our demographics and other reputation like attributes, but does not need to do so in a 1:1 manner.
 - T3 identities speak to the way in which companies aggregate us into different marketing buckets for the purposes of advertising or communicating with us.
 - E.g., we're either a 'frequent buyer' or a 'one time customer' etc.
 - T3's are typically based upon our behaviour in our interactions with business.
 - The entire CRM market caters to T3 identities.

[Durao3]

mobile business Identity Concepts Tier 2: Assigned Identity

- A Tier 2 (assigned - 'Our') identity refers to our digital identities that are assigned to us by corporations (e.g. our 'customer accounts').
 - Our job title (assigned to us by our employer)
 - Our cell phone number (assigned to us by our mobile phone operator)
 - Our United Mileage Plus number (assigned to us by United Airlines)
 - Our social security number (assigned to us by the Government)
 - Our credit card number (assigned to us by our credit card companies)

[Durao3]

Aufgabe 7: Regulierung mobiler Telekommunikation (9 Punkte)

a) Nennen und beschreiben Sie drei Formen von Marktversagen, die eine Notwendigkeit zur Regulierung im Mobilfunkmarkt verursachen können. (3 Punkte)

- Externe Effekte
- Natürliche Monopole
- Dominierende Lieferanten/Anbieter
- Politische Fehler

Je Antwort 0,5 Punkte, je Beschreibung 0,5 Punkte

b) Beschreiben Sie die Gründe und Ziele von Regulierung am Beispiel von Roaming-Gebühren in der EU sowie die Konsequenzen für Endkunden und Mobilfunkanbieter. (6 Punkte)

Gründe:

- Marktversagen (Telcos mit zu viel Marktmacht → Dominierende Anbieter)
- Fehlende Preistransparenz
- Zu hohe Preise

Ziele:

- Schutz der Konsumenten (Aufklärung)
- Anregen von Wettbewerb (Preiswettbewerb)
- [allgemein] Wohlfahrtsmaximierende Verteilung von Ressourcen

Konsequenzen:

- Preisobergrenze für Anbieter
- Niedrigere Preise für Sprach-, Text- und Datendienste
- Höhere Transparenz durch Preisobergrenze
- (SMS im Ausland teilweise günstiger als im Inland)

Je Grund/Ziel/Konsequenz 1 Punkt