mobile business

Exercise 5

Trust and technology acceptance

Picture source: http://engagerx.org/whats-trust-got-to-do-with-it-for-pharma/#prettyPhoto[gallery12049]/0/

Mobile Business I (WS 2016/17)

Fatbardh Veseli, M.Sc.

Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt a. M.

Overview
Practical Exercise No. 5

- **Exercise 1 (Mobile Trusted Devices)**
- **Exercise 2 (Technology Acceptance)**
- **Exercise 3 (Customer Trust in Mobile Business)**

Exercise 1 (Mobile Trusted Devices)

a) What is a TPM?

Trusted Platform Module (TPM)

- The TPM is a chip to make computers more secure as a part of the TCG specification.
- It is like a hard coded smartcard with the big difference that it is not bound to a concrete user, but to a system (e.g. a PC).
- ***Other usages:*** PDAs, mobile devices, and consumer electronics.
- Passive chip, can neither influence the booting process nor the operation directly
- Has a unique identifier and so serves for the identification of the system.

Exercise 2: Mobile Market Players

b) Recall from the lecture the main players (parties) in a mobile market and their interests.

Mobile Market Players

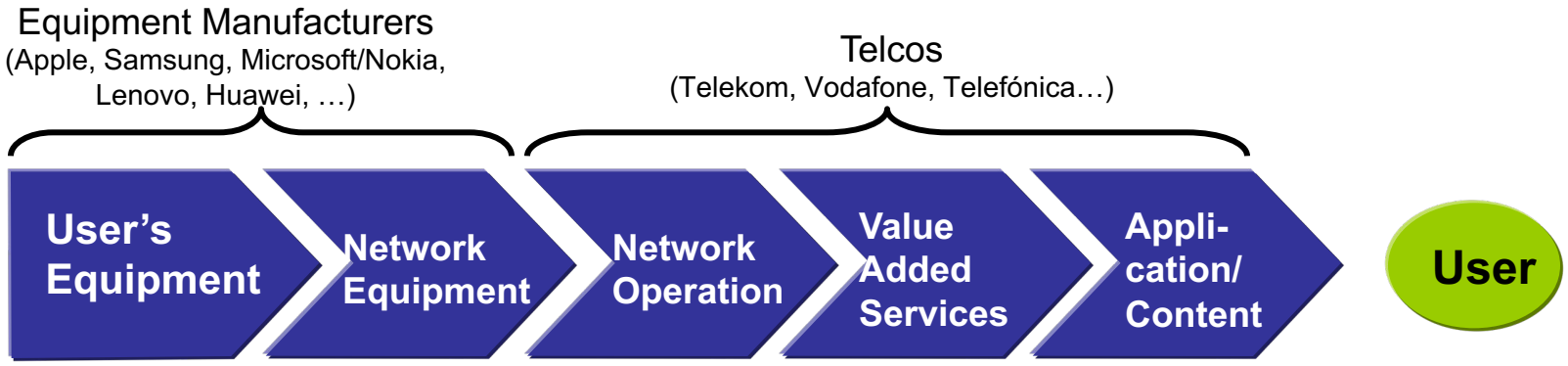
- Mobile equipment manufacturers
- (Mobile) Telecom Operators
- MVNOs
- Content providers
- Application service providers
- Private customers
- Corporate buyers
- Corporate users
- Intelligence agencies

Mobile Equipment Manufacturers

- In the past, main manufacturers of mobile devices were mobile phone manufacturers (e.g. Nokia, Motorola), producing both hardware and the software.
- Meanwhile the value chain for mobile devices has become more complex: Significant parts may come from third parties, e.g.
  - hardware from ARM, Infineon, Texas Instruments,
  - software from Google, Microsoft.
- The more a manufacturer is perceived as the provider of the respective platform, the more risks of the mobile platform are affecting them.
- Today, mobile devices are sold particularly as part of a powerful ecosystem (Google, Apple, Microsoft).

Mobile equipment & IT value chain

GSM World



IBM, Infineon, ...
MS, ...
Dell, …
Cisco,...
Telekom Vodafone ...
MS, IBM, ...
MS, SAP, Telekom, Google ...

IT World (based on [SAP])

(Mobile) Telecom Operators

- Functions of mobile operators that relate to trusted computing:
  - operate networks,
  - provide communication services,
  - maintain direct customer relationships,
  - provide mobile devices to customers (often by subsidising their costs).
- Powerful players in the mobile market:

Mobile Virtual Network Operators

Definition:

A **mobile virtual network operator** (MVNO) is a company that does not own a licensed frequency spectrum and wireless infrastructure, but resells wireless services under their own brand name, using the network of another mobile network operator.

Explanation:

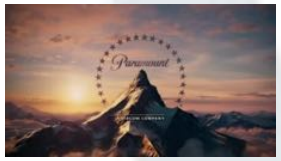
- An MVNO's roles and relationship to the mobile phone operator vary by market.
- In general, an MVNO is an entity or company that works independently of the operator and can set its own tariff structures.

congstar, blau MOBILFUNK, TURKCELL EUROPE, ortel MOBILE, ALDI TALK MEDION mobile, mobilcom debitel, simyo, FONIC Das ist die Wahrheit., 1&1

Content Providers

- Are producing and/or distributing digital content (e.g. music, movies, games, ring tones, TV)
- Interest in:
  Securing their property rights on the provided content
  ➲ Digital Rights Management (DRM)

BMG BERTELSMANN
JESTA digital
SONY PICTURES

warner | music | group
EMI
VIACOM
NBCUniversal
Walt Disney PICTURES
THE WALL STREET JOURNAL.
Spotify

Application Service Providers

- Providing mobile application services (e.g. LBS, mobile banking, mobile payment services)
- Interest in:
  Ensuring that the devices used by customers for authenticating transactions are not compromised.

Private Customers

- Usually not concerned about security of their mobile device.
- Interest in:
  Functionality, usability and design properties of their mobile device

➲ Security failures are perceived as a mistake made by the device manufacturer/mobile OS provider/ mobile network operator.

Corporate Buyers

- IT managers, technical staff and system administrators
- Concerned about mobile devices and mobile access causing security holes in their enterprise system.

➲ Most security-conscious customers

➲ Benefit from Mobile Device Management solutions (cf. Section “Usage Scenarios for Trusted Mobile Platforms”)


ZEIT ONLINE | DATENSCHUTZ

START POLITIK WIRTSCHAFT MEINUNG GESELLSCHAFT KULTUR WISSEN DIGITAL STUDIUM

Start › Digital › Datenschutz › Trusted Computing: Bundesbehörden sehen Risiken beim Einsatz von Windows 8

TRUSTED COMPUTING

Bundesbehörden sehen Risiken beim Einsatz von Windows 8

Microsoft will bei Windows 8 den neuen Trusted-Computing-Standard nutzen. Experten der Bundesregierung haben darin ein Sicherheitsproblem für Behörden gesehen.

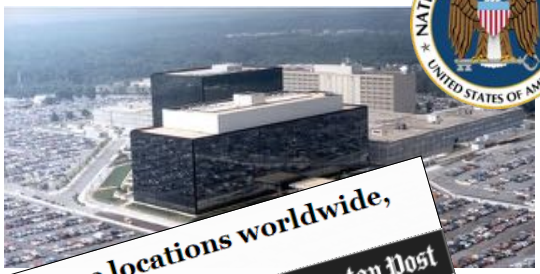
[Zeit2013]

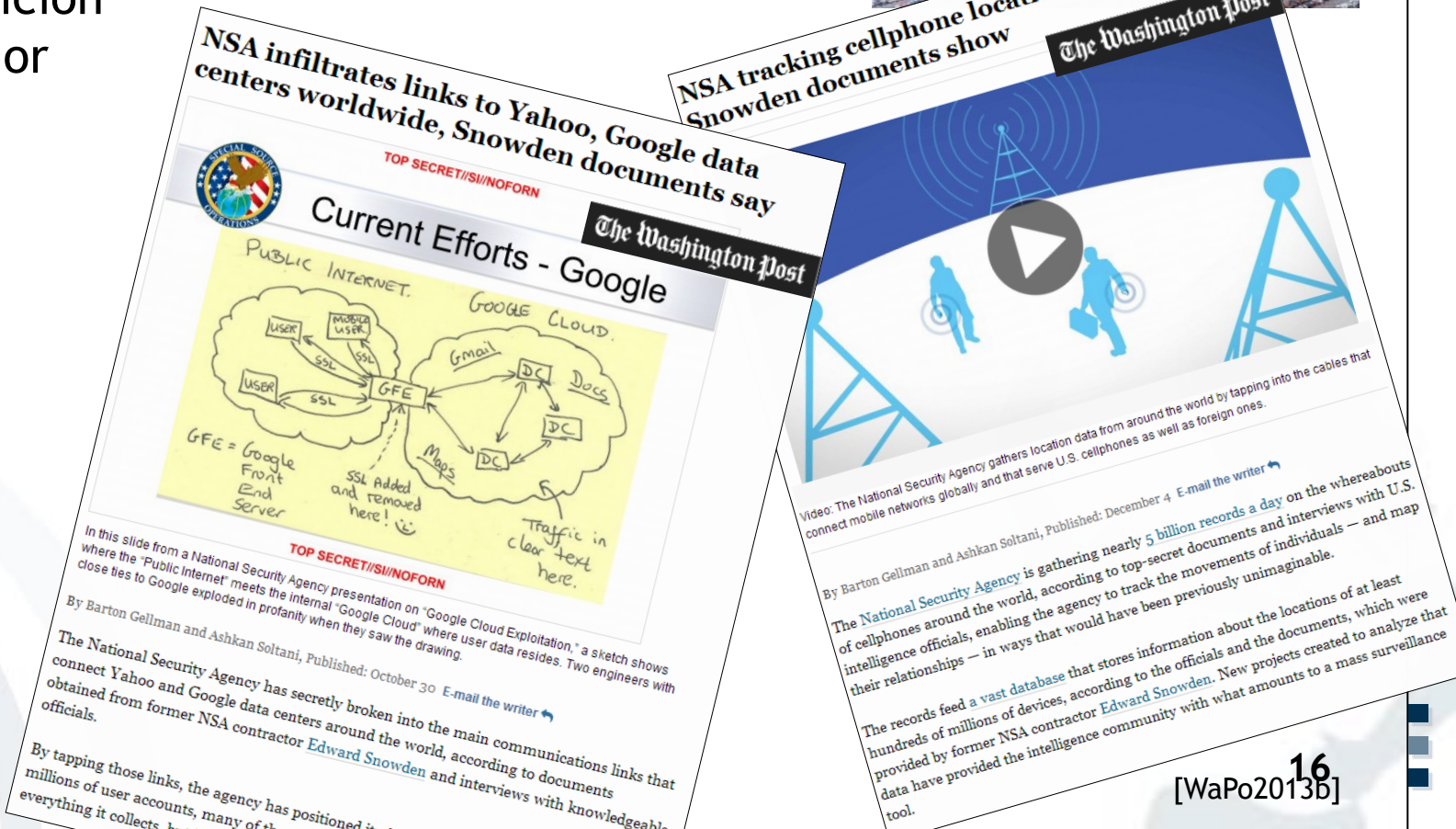
Corporate Users

- Are using mobile infrastructures predominantly for business needs.
- Like private users, but with usage restrictions imposed by employers or (Mobile)OS for security purposes
  - This includes corporate users who are allowed to bring and use personally owned mobile devices (*Bring your own device - BYOD*)

Intelligence Agencies

- Eavesdrop (and manipulate?) globally exchanged information to gather intelligence, regardless of whether a suspicion exists or not.





NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say

The Washington Post

TOP SECRET//SI//NOFORN

Current Efforts - Google

TOP SECRET//SI//NOFORN

In this slide from a National Security Agency presentation on "Google Cloud Exploitation," a sketch shows where the "Public Internet" meets the internal "Google Cloud" where user data resides. Two engineers with close ties to Google exploded in profanity when they saw the drawing.

By Barton Gellman and Ashkan Soltani, Published: October 30 E-mail the writer

The National Security Agency has secretly broken into the main communications links that connect Yahoo and Google data centers around the world, according to documents obtained from former NSA contractor Edward Snowden and interviews with knowledgeable officials.

By tapping those links, the agency has positioned

millions of user accounts, many of

everything it collects,

NSA tracking cellphone locations worldwide, Snowden documents show

The Washington Post

Video: The National Security Agency gathers location data from around the world by tapping into the cables that connect mobile networks globally and that serve U.S. cellphones as well as foreign ones.

By Barton Gellman and Ashkan Soltani, Published: December 4 E-mail the writer

The National Security Agency is gathering nearly 5 billion records a day on the whereabouts of cellphones around the world, according to top-secret documents and interviews with U.S. intelligence officials, enabling the agency to track the movements of individuals — and map their relationships — in ways that would have been previously unimaginable.

The records feed a vast database that stores information about the locations of at least hundreds of millions of devices, according to the officials and the documents, which were provided by former NSA contractor Edward Snowden. New projects created to analyze that data have provided the intelligence community with what amounts to a mass surveillance tool.

[WaPo2013a]

[WaPo2013b]

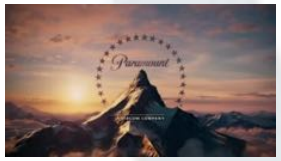
Exercise 1: Mobile Market Players

c) Imagine a scenario where content providers would decide to enforce their own interests in the market. What would the impact for the other parties be and how do you foresee the other market players would react?

Recalling the interests of Content Providers

- Are producing and/or distributing digital content (e.g. music, movies, games, ring tones, TV)
- Interest in:
  Securing their property rights on the provided content
  ➲ Digital Rights Management (DRM)

BMG BERTELSMANN
JESTA digital
SONY PICTURES

warner | music | group
EMI
VIACOM
NBCUniversal
WALT DISNEY PICTURES
THE WALL STREET JOURNAL.
Spotify

Digital Rights Management (DRM)

- Mobile device could provide a facility that can be integrated within a DRM infrastructure, e.g.
  - device authentication,
  - cryptographic functions,
  - certificate management support.

Usage Scenarios and Players

Players and security features they are especially interested in

Usage Scenarios/ Players	Mobile Equipment manufacturers	Mobile operators	MVNOs	Content providers	Appl. Service providers	Private customers	Corp. buyers	Corp. users	Intelligence Agencies
Secure OS	++	++	++		+	+	++	+	
Digital Rights Management	+	+	+	++					
Device misuse prevention						+	++	+	
Storage of additional credentials	+				+	+	+		
Secure corporate network interaction		+			+		++	+	
Mobile Wallet	++	++				+			

Based on [PiskRannRoss2005]

Discussion

- How do you foresee the other entities would react?
- Who would be the main entities that could be impacted and how?
- Are there any other entities that you would consider important in the modern mobile market ecosystems?

Exercise 1 (Mobile Trusted Devices)

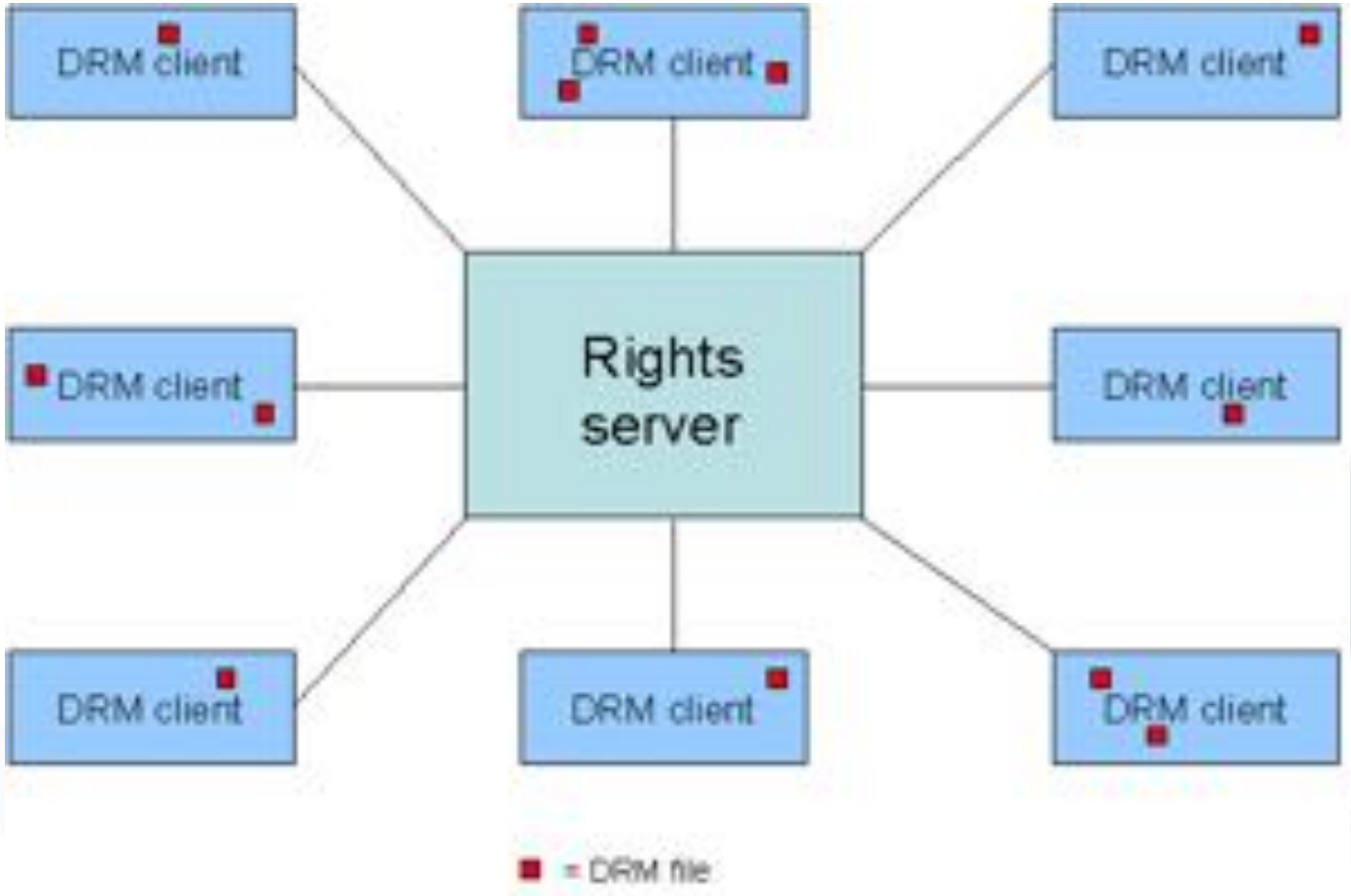
d) How can a TPM be used to implement digital rights management (DRM)?

TPM and DRM

- TC enables DRM (Digital Rights Management) to run in a secure way. DRM specifies rights for digital content that is enforced by an underlying PKI (Public Key Infrastructure).
  - For instance, rights that a file cannot be printed or copied can be specified for a word document.
  - Rights can also be connected to digital content so it for instance will “self-destruct”after a certain amount of time and/or only be used a certain number of times.
  - DRM documents and software can be tied to a specific computer/user.
- However, it could disable legitimate uses of digital content
  - Backup copies of legitimate CD/DVDs
  - Lending materials through a library
  - Using copyrighted materials for research or education

[CBC09]

A view on the architecture for a DRM using TPM



[GuSt04]

Exercise 1 (Mobile Trusted Devices)

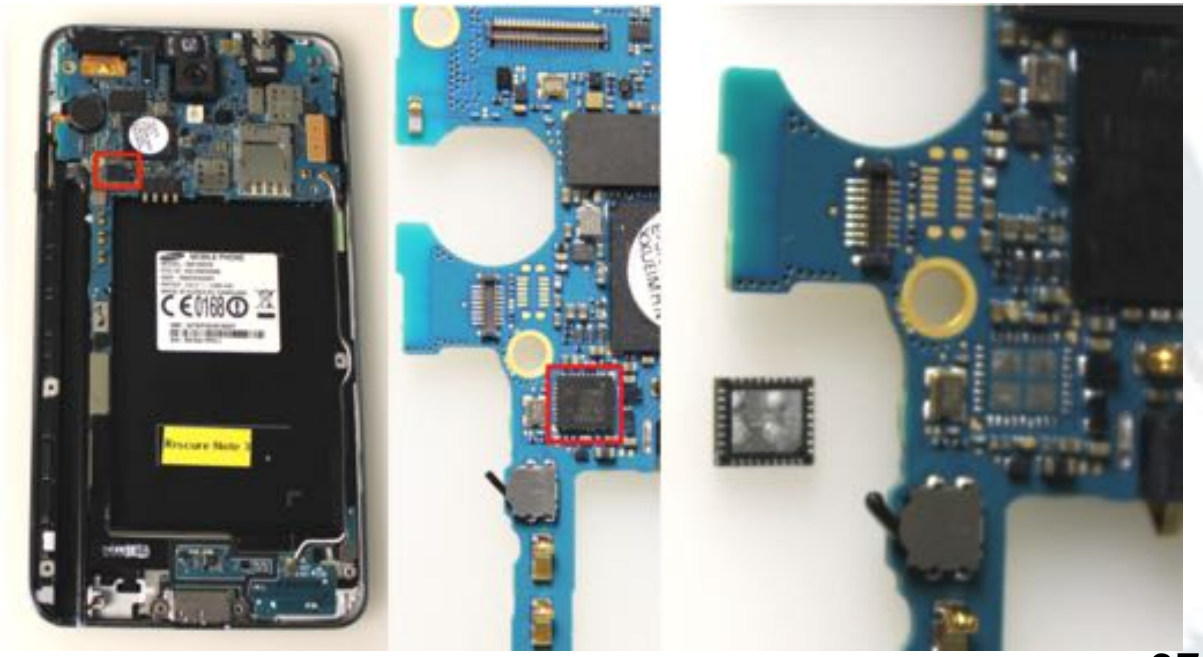
e) What is a Secure Element?

Secure Element (SE)

- Secure Elements (SE) are hardware tokens that offer secure services, e.g. tamper-proof storage and cryptographic operations.
  - Smart card (contact or contactless)
  - SIM/UICC cards
  - Smart/Secure microSD cards
  - Embedded Secure Elements (eSE)

Embedded Secure Element (eSE)

- Secure microcontroller
- Unremovable part of the mainboard of the device (usually a smartphone)
- Interchanging or extraction of the secure element is not possible (unlike other SE form factors).
- eSE use various types of inter-faces (SWP, DWP, I2C, USB, proprietary interface).



[Riscure 2014]

Overview
Practical Exercise No. 5

- **Exercise 1 (Mobile Trusted Devices)**
- **Exercise 2 (Technology Acceptance)**
- **Exercise 3 (Customer Trust in Mobile Business)**

Exercise 2 (Technology Acceptance)

a) Distinguish between the terms “innovation”, “acceptance”, and adoption”.

Terminology

- **Innovation (process)** is the adoption of an idea or behaviour (whether a system, policy, program, device, process, product, or service), that is new to the adopting organisation.
- The **adoption (process)** is a sequence of stages a potential adopter goes through before accepting a new product or service.
- **Adoption** is interpreted as the decision to purchase while **acceptance** refers to the decision to use the product.

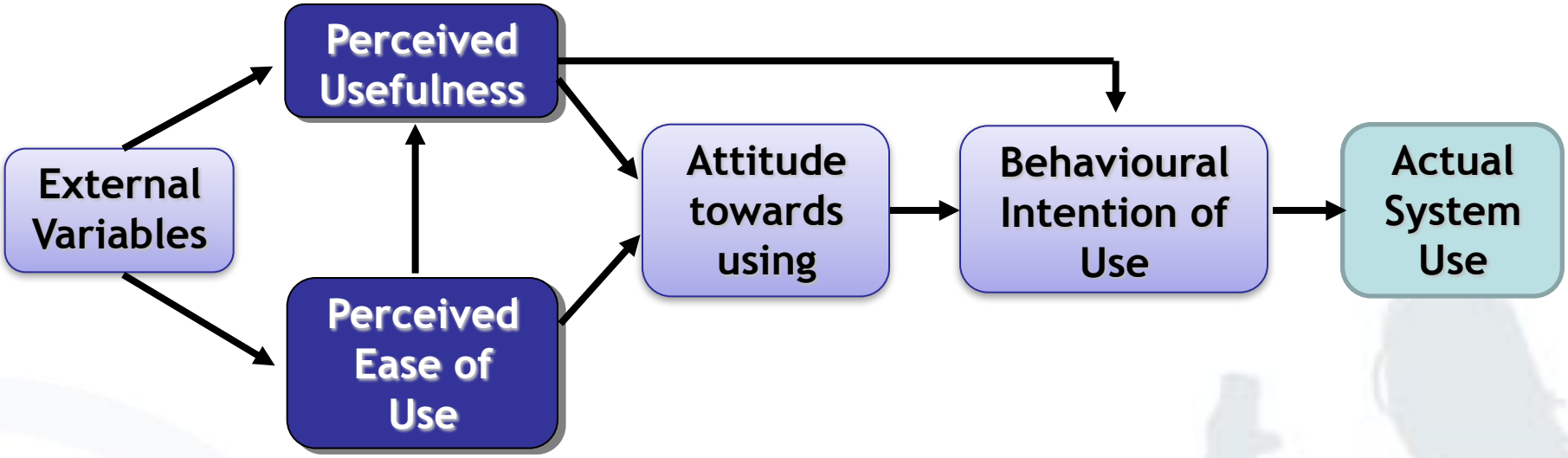
Exercise 2
Background

- Mobile applications and services in M-Business can increase the connectedness of their users.
- However, there are several issues related to consumers' acceptance for mobile services and applications, which need to be considered:
  - Willingness to pay for services
  - Network effects
  - Ease of Use
  - Quality of service
  - Product limitations
  - Trust in service provider
  - …

Exercise 2 (Technology Acceptance)

a) Explain the fundamentals of the Technology Acceptance Model (TAM).

Technology Acceptance Model



[Davis1989]

TAM
Background info

(Recker, 2015)

Overview
Practical Exercise No. 5

- **Exercise 1 (Mobile Trusted Devices)**
- **Exercise 2 (Technology Acceptance)**
- **Exercise 3 (Customer Trust in Mobile Business)**

Exercise 3 (Customer Trust in Mobile Business)

a) Define the term “trust”. Discuss the main characteristics and parties in a trust relationship.

Definition: Trust

- "*A state involving confident positive expectations about another's motives with respect to oneself in situations entailing risk*" [BoHo91].
- The definition highlights the main characteristics of trust:
  1. Trust relationships involves two parties: *trustor* & *trustee*.
  2. The trustor has faith in the trustee's honesty and believes the trustee will not betray him.

Trust
Open discussion

- How do you assess the trustworthiness of a product in electronic / mobile business?
- How do you assess the trustworthiness of a company you engage in mobile business with?
- How do you assess the trustworthiness a web-page you visit to buy something?
- Which factors from the past influence the perception of trustworthiness of a company?

mobile business

Trust: personal thoughts of chosen company executives

(Edelman, 2014)

Exercise 3 (Customer Trust in Mobile Business)
Open discussion

b) What is the general assumption about the risk and time in a trust relationship?

- Trust involves uncertainty and risk.
- Trust involves the future.
- It is continuous.

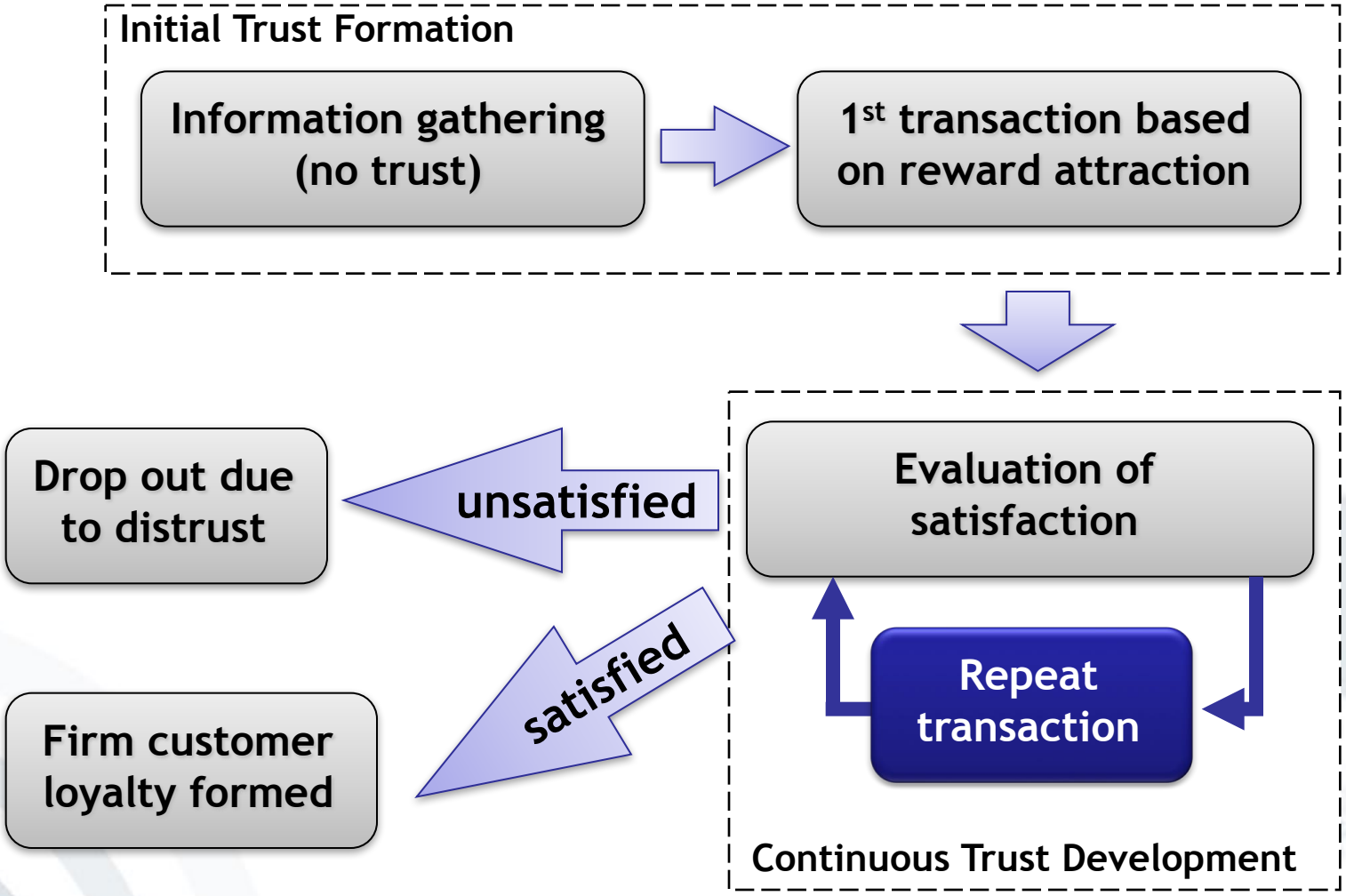
Exercise 3 (Customer Trust in Mobile Business)

c) Explain the concept of trust development lifecycle.

Initial Trust Formation

- In order to build an initial trust formation, service providers *must* disseminate information, cultivate interest, etc.
  - ***Enhance customer familiarity***, as people tend to trust the familiar, e.g. by general publicity or advertisements.
  - ***Build vendor reputation***, as a good reputation suggests certainty and less risk in conducting business.
  - ***Deliver high-quality information***, as the information posted on a company has a high impact on the customers' perception.
  - ***Elicit third-party recognition and certification***, as the independent nature of third-party certification helps customers to feel more secure in doing business with the M-Business provider.
  - ***Provide attractive rewards***, such as free trials or gift cards helping to attract new customers.

Trust Development Life Cycle



[SiauShen2003]

Components of Customer Trust in M-Business

- Reliability and security of mobile technology are equally important, since failures in the early stages of the usage of M-Business reduce the customers' trust significantly.
- As mobile technology evolves, the trust focus shifts from technology to the mobile service provider.

Continuous Trust Building Overview

- It is important to maintain a trust relationship, as creating trust is time-consuming and trust can easily be destroyed.
- There are several successful methods derived from E-Business that can be adopted by M-Business companies to overcome trust barriers.

Continuous Trust Building Details 1

- ***Improve site quality:***
  - User-friendly design of web-sites accessed by mobile devices (e.g. giving customers sufficient information for purchases) helps to convey the vendor's competence.
- ***Sharpen business competence:***
  - Refers to the skills, technical knowledge, and expertise in operating M-Business applications.
- ***Maintain company integrity:***
  - Providers need to be congruent with regard to the actions and the promises given to their customers.
- ***Post privacy policy:***
  - Similar to E-Business providers, M-Business providers should post their privacy policy online, so customers are informed about the information being processed
  - ➲ Helps to build transparency.

Continuous Trust Building Details 2

- ***Strengthen security controls:***
  - In order to have secure M-Business transactions, technologies need to be in place that help to allow Multilateral Security for all involved parties.
- ***Foster a Virtual Community:***
  - By building virtual communities, mobile service providers can replicate the success of web-based online communities and create positive evaluations by their users.
- ***Encourage communication and increase accessibility:***
  - In order to build synergies, the users should be brought into close communication with the M-Business provider, reducing information asymmetries and fostering the provider's credibility and trustworthiness.
- ***Use external auditing to monitor operations:***
  - External auditing helps to maintain the customers' trust by keeping the provider to behave fair and legally.

mobile business

Example: A survey on consumer trust

(Centrify, 2016)

Exercise 2
Customer Trust in Mobile Business

- Summarize the framework for building trust in M-Business

A Framework for Building Trust in M-Business

Mobile Service Providers	Familiarity Reputation Information Quality 3rd-Party Recognition Attractive Rewards	Site Quality Competence Integrity Privacy Policy Security Controls Open Communication Community Building External Auditing
Mobile Technology	Feasibility	Reliability Consistency
	Initial Trust Formation	*Continuous Trust Development*

[SiauShen2003]

Processed lectures in this exercise

- ***Lecture 12:*** Mobile Trust Devices
- ***Lecture 13:*** Acceptance and Success Factors in Mobile Business

Preparation for the coming week (Q&A session)

- Please send your questions via mail (mb1@m-chair.de) no later than Thursday, 2.2.2017 at 14:00.
- The Q&A sesion will follow next week, Tuesday, 7.2.2017 at 10:00.

Literature

- [Ajze1980] Ajzen, I.: *Understanding Attitudes and Predicting Social Behavior*, Prentice-Hall, Englewood Cliffs, NJ, 1980.
- [BarnesHuff2003] Barnes, S.J., Huff, S.L.: *Rising Sun: iMode and the Wireless Internet*, Communications of the ACM, Vol. 46, No. 11, pp. 79-84, 2003.
- [BoonHolmes1991] Boon, S., Holmes, J.: *The dynamics of interpersonal trust: Resolving uncertainty in the face of risk*, in Hinde, R., Groebel, J. (Eds.): *Cooperation and Prosocial Behaviour*, Cambridge University Press, Cambridge, pp. 190–211, 1991.
- [BüllingStamm2004] Büllingen,F., Stamm, P.: *Mobile Multimedia-Dienste: Deutschlands Chance im globalen Wettbewerb*, Bundesministerium für Wirtschaft und Arbeit, 2004.
- [Davis1989] Davis, F. D.: *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*, MIS Quarterly Vol. 13, No. 3, pp. 319-339, 1989.
- [HungKuChang2003] Hung, S.-Y., Ku, C.-Y., Chang, C.-M.: *Critical factors of WAP services adoption: An empirical Study*, Electronic Commerce Research and Applications, No. 2, pp. 42-60, 2003.
- [Istheory2013] *Theories used in IS Research*, http://istheory.byu.edu/wiki/Theory_of_reasoned_action, accessed 2013-10-15.

Literature

- [JarLanTakTuu2003] Jarvenpaa, S.L., Lang, K.R., Takeda, Y., Tuunainen, V.K.: *Mobile Commerce at Crossroads*, Communications of the ACM, Vol. 46, No. 12, pp. 41-44, 2003.
- [Marcussen2002] Marcussen, C.: *Comparing SMS and WAP in Europe with i-mode in Japan*, www.crt.dk/uk/staff/chm/wap/smsimode.pdf, accessed 2007-01-12, 2002.
- [NohriaLeestm2001] Nohria, N., Leestma, M.: *A moving Target: The Mobile-Commerce Customer*, MIT Sloan Management Reviews, Spring 2001.
- [Nttdocomo2007] NTT DoCoMo, www.nttdocomo.com, accessed 2007-12-18.
- [RistKoivuKest2005] Ristola, A., Koivumaki, T., Kesti, M.: *The Effect on Familiar Mobile Device and Usage Time on Creating Perceptions Towards Mobile Services*, International Conference on Mobile Business (ICMB'05) , pp. 384-391, 2005.
- [Rogers2003] Rogers, E. M.: *The Diffusion of Innovations*, 5th Edition, Free Press, New York, London, Toronto, Sidney, 2003.
- [SiauShen2003] Siau, K., Shen, Z.: *Building Customer Trust in Mobile Commerce*, Communications of the ACM, Vol. 46, No. 4, pp. 91-94, 2003.
- [VenMorDavDav2003] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D.: *User acceptance of information technology: Toward a unified view*, MIS Quarterly, vol. 27, no. 3, pp. 425-478, 2003.

Literature

- [CBC09] CBC News, Aug 2004. The pros, cons, and future of DRM. http://www.cbc.ca/news/technology/the-pros-cons-and-future-of-drm-1.785237 (last accessed 27 Jan 2017)
- Centrify, “Centrify Consumer Trust Survey” (Jun 2016) https://www.youtube.com/watch?v=FZcInZ6N3Lc (last accessed 27 Jan 2017)
- Edelman, “What is trust” (Jan 2014), https://www.youtube.com/watch?v=90u3b5WahEk (last accessed 27 Jan 2017)
- Donahue, Jill (EngageRx), “What’s trust got to do with it? – for pharma” (Nov 1025) http://engagerx.org/whats-trust-got-to-do-with-it-for-pharma/#prettyPhoto (last accessed 27 Jan 2017)
- Recker, Jan (QUT, Feb 2015): Technology Acceptance Model (https://www.youtube.com/watch?v=ydlFH1q2NHw) (last accessed (last accessed 27 Jan 2017)
- [GuSt04] Gustafsson, D. & Stewén, T (Sep 2004). Trusted Computing & Digital Rights Management – Theory & Effects, Växjö University, ISSN 1650-2647.