

Anwendungssysteme – Übung 08

T. Bullmann, N. Lehmann, S. Rolfs, S. Reim, M. Höhne, J. Cwojdzinski

1. Aufgabe: Konzept „Privatsphäre“

a) 1) **Surfen im Internet**

- Daten werden bis zu 6 Monate gespeichert
- Social Networks („What happens in the facebook, stays in the facebook.“)

2) **Behandlung im Krankenhaus**

- Betreiber erheben und speichern Daten zur Optimierung von unternehmensinternen Prozessen
- Schweigepflicht der Ärzte

3) **Unverletzlichkeit der Privatsphäre in der Wohnung**

- Telemarketing (outbound)
- Zeugen Jehovas

b) **Surfen im Internet, dann Behandlung im Krankenhaus, dann Unverletzlichkeit der Privatsphäre in der Wohnung**

Surfen im Internet (Social Networks) ermöglicht Interessengemeinschaften durch kollaborative Filter gesamtgesellschaftliche Aussagen zu treffen.

Wenn Daten über den Gesundheitszustand einer Person bei oder nach der **Behandlung im Krankenhaus** in falsche Hände gerät kann das kritische Auswirkungen auf das sozioökonomische Leben haben.

Sollte die **Unverletzlichkeit der Privatsphäre in der Wohnung** dennoch verletzt werden ist das subjektiv störend/nervend und kann sogar objektiv bedrohliche Ausmaße annehmen.

c) **Wie kann jemand herausfinden welche Webseiten sie besucht haben?**

- Es wird ein Programm installiert, das den zukünftigen Browserverlauf aufzeichnet und dem Angreifer übermittelt. Das aktuelle Surfverhalten lässt Rückschlüsse auf das vergangene Surfverhalten zu.

Wie kann ein Angreifer herausfinden welche Webdienste sie benutzen (welche Bank)?

- Per man-in-the-middle Taktik die versendeten Pakete auslesen nach Ziel-IPs, somit ließe sich eine gewünschte Seite ermitteln, z.B. Bankenseiten oder Onlinezahldienste

2. Aufgabe: Privatsphäre und RFID-Chips

- a) RFID steht für Radiofrequenz-Identifikation. Mit dieser Technik werden Daten berührungslos und ohne Sichtkontakt von einem Datenträger, dem sog. Transponder oder Tag zu einem RFID-Lesegerät und umgekehrt übertragen.

RFID-Technologie wird zur Identifizierung von Objekten oder Subjekten mittels elektromagnetischer Wellen verwendet. Dabei werden vom Sender Bitfolgen übertragen und vom Empfänger bestätigt oder verworfen.

Aktiv:

- Funktionsweise: Stromquelle ist eine Batterie oder ein Akku.
- Einsatzgebiete: Schlüssel mit oder ohne Zugangsberechtigung

Passiv:

- Funktionsweise: Stromquelle wird bei Nutzung aktiv zugeführt, d.h. per Induktion erzeugt.
- Einsatzgebiete: Tieridentifikationschips

Die zusätzlichen Tags bieten Möglichkeiten zusätzliche Informationen zu speichern, wie z. B. ob es sich bei dem Objekt um ein Objekt oder Subjekt handelt, oder welcher Regionalität es angehört usw.

- b) Szenario 1:

Das „Unternehmen meines Vertrauens“ verwendet seit Neuem nicht mehr Barcodes, sondern RFID. „Payback-Karten“ werden damit überflüssig, da automatisiert personalbezogene Käuferprofile erstellt werden können.

Dieses ist bedenklich im Sinne von Wettbewerbsverzerrung (UWG, GWB) die aufgrund der vorliegenden Informationen entstehen könnten und dem Datenschutz, da ich nun stillschweigend der Speicherung und Verwendung meiner Daten mit dem Kauf vertraglich zustimme.

Quellen:

- <http://www.hannover.ihk.de/ihk-themen/standort-branchen/handel/betrieb1/techno/rfid3.html?type=123>
- http://dSPACE.icsy.de:12000/dSPACE/bitstream/123456789/244/1/2009-05-Henrici-Fleuren-RFID_Sicherheit_Privatsph%3a4re.pdf

Szenario 2:

Am Flughafen (oder anderen sicherheitskritischen Bereichen) ermöglichen RFID-Chips Behörden die Verfolgung (Tracking) aller Personen.

Dieses ist bedenklich im Sinne des Datenschutzes.

Quelle: <http://www.zdnetasia.com/techguide/wireless/0,39044905,61963458,00.htm>