Ostfalia
Hochschule für angewandte Wissenschaften

Fakultät Informatik

Vergesslichkeit als Feature

Kann die Imitation menschlicher Schwächen helfen Privacy Anforderungen besser umzusetzen?

Julia Justinger, Tanja Heuer, Ina Schiering, Reinhard Gerndt

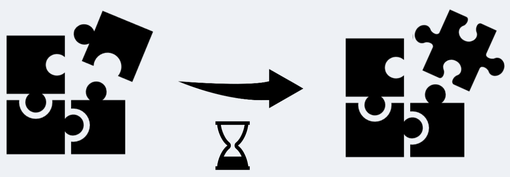
Einführung

- Menschen geben mehr private Informationen über sich preis, wenn sie mit einer Maschine reden als mit einem Menschen
- Private Informationen schützen
- Vertraulichkeit, Transparenz, Datensparsamkeit und Löschen von Daten sind von besonderer Bedeutung für die Interaktion mit sozialen Robotern
- **„Mängel“ des menschlichen Gedächtnis als Realisierungskonzepte für den Datenschutz**

Abbildung: Das Modell Pepper als Beispiel für einen sozialen Roboter. Foto: Natasza Szczypien, Ostfalia

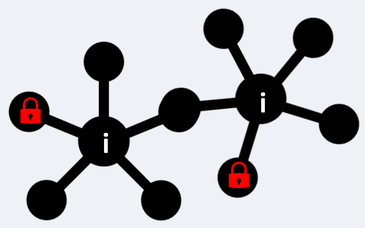
False Memory Effekt

- Privacy Pattern **Use of Dummies** [1]
- Erinnerungen dürfen lückenhaft oder auch **fehlerhaft** sein
- Bedeutung exakter Daten schwindet, je weiter ein Ereignis in der Vergangenheit liegt
- Informationen nach einer bestimmten Zeit durch Dummies ersetzen



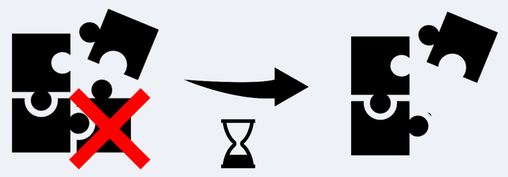
Detail Trigger

- Security Pattern **Authentication Enforcer** [2]
- Erinnerungen über spezifische **Schlüsselwörter** hervorrufen wie Ort, Anlass oder andere Personen
- Alternative zur bekannten Authentisierung
- Abfrage aus einem Pool von Informationen



Vergessen

- Privacy Pattern **Limited Data Retention** [3]
- Je länger eine Erinnerung zurückliegt, desto weniger Details sind vorhanden
- Nach bestimmtem Zeitraum werden alte Daten mit neuen **überschrieben** und somit gelöscht



Diskussion

- Schutz verschiedener Bereiche durch unterschiedliche Passwörtern bzw. Wächterattribute
- Nicht als Ersatz für bewährte Maßnahmen zu IT Sicherheit und Datenschutz, sondern als Ergänzung
- Je nach Anwendungen und Anforderungen muss die Realisierung von Lebenszeit und Verarbeitung für entsprechenede Informationen festgelegt werden
- Mehrzahl der NutzerInnen eher nachlässig mit ihren Daten, vor allem aus Bequemlichkeit oder weil sie davon einen gewissen Komfort haben
- Hoffnung, dass sich die Maßnahmen durch die Tarnung als Schwäche, für die Anwender natürlicher anfühlen und so weniger lästig erscheinen

[1] UC Berkeley School of Information. [n. d.]. Use of Dummies. Retrieved June 3, 2019 from https://privacypatterns.org/patterns/ Use-of-dummies
[2] Munawar Hafiz, Paul Adamczyk, and Ralph E. Johnson. 2012. Growing a Pattern Language (for Security). In Proceedings of the ACM International Symposium on New Ideas, New Paradigms, and Reflections on Programming and Software (Onward! 2012). ACM, 139–158.
[3] Christoph Bier and Erik Krempel. 2012. Common privacy patterns in video surveillance and smart energy. In 2012 7th International Conference

Julia Justinger (B.Sc.)
Wissenschaftliche Mitarbeiterin
Ostfalia Hochschule für angewandte Wissenschaften
Fakultät Informatik
Salzdahlumer Str. 46/48, 38302 Wolfenbüttel
E-Mail: j.justinger@ostfalia.de