

Usability im digitalen Selbstschutz

Zwiebel zum Heulen und Schlüssel zum Glück?

Helga Huppertz

SIGINT 2010 – 23. Mai 2010

Befund

Eine Erfolgsgeschichte:

Aufklärung über die Erosion von Grundrechten, Überwachung,
Datensammelwut ...

Befund

Eine Erfolgsgeschichte:

Aufklärung über die Erosion von Grundrechten, Überwachung, Datensammelwut ...

Keine Erfolgsgeschichte:

Kein sprunghafter Anstieg der Nutzung von Techniken zum digitalen Selbstschutz

- ▶ Anonym surfen
- ▶ Emails / Datenträger verschlüsseln
- ▶ etc.

Befund

Viele haben etwas zu verbergen und wollen sich schützen.

Viele benutzen keine Payback-Karten mehr.

Wenige benutzen Tools wie TOR, GPG/PGP...

Thesen

Was unterscheidet Benutzer und Nicht-Benutzer von Tools wie TOR, GPG/PGP?

Thesen

Was unterscheidet Benutzer und Nicht-Benutzer von Tools wie TOR, GPG/PGP?

Gelegentlich: Aufklärung, Problembewusstsein

Thesen

Was unterscheidet Benutzer und Nicht-Benutzer von Tools wie TOR, GPG/PGP?

Gelegentlich: Aufklärung, Problembewusstsein

Mit Sicherheit: Technikkompetenz und technisches Selbstvertrauen

Thesen

Für technisch unbedarfte, gleichwohl problembewusste Anwender ist der Einstieg in den digitalen Selbstschutz sehr dornig.

Für breite Bevölkerungskreise fehlt es an geeigneten (zielgruppengerechten) Tools / Benutzungsschnittstellen.

Einwände

„Da müssen die eben durch...“

Kann man mit Schulung kompensieren...

Einwände

„Da müssen die eben durch...“

Kann man mit Schulung kompensieren...

Passiert aber nicht. Siehe Befund.

Noch etwas

Wer digitalen Selbstschutz betreibt, wird sich eher für die Verteidigung digitaler Bürgerrechte einsetzen.

Wer sich ohnmächtig fühlt, lässt sich eher für verordnete „Sicherheit“ mit eingebauter Überwachung, Backdoor und Zensur begeistern.

Usability-Potenziale ausloten!

Was ist Usability?

- ▶ Eine Produkt-Eigenschaft
- ▶ Ein mögliches Entwurfsziel
- ▶ Deutsch: Gebrauchstauglichkeit (~~Benutzerfreundlichkeit~~)
- ▶ Usability spielt sich an der Benutzungsschnittstelle ab

Was ist Usability?

EN ISO 9241-11:

„Das Ausmaß, in dem ein Produkt durch bestimmte Benutzer in einem bestimmten Nutzungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen“

Was ist Usability?

EN ISO 9241-11:

„Das **Ausmaß**, in dem ein Produkt durch bestimmte Benutzer in einem bestimmten Nutzungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen“

Was ist Usability?

EN ISO 9241-11:

„Das **Ausmaß**, in dem ein Produkt durch **bestimmte Benutzer** in einem bestimmten Nutzungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen“

Was ist Usability?

EN ISO 9241-11:

„Das **Ausmaß**, in dem ein Produkt durch **bestimmte Benutzer** in einem **bestimmten Nutzungskontext** genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen“

Was ist Usability?

EN ISO 9241-11:

„Das **Ausmaß**, in dem ein Produkt durch **bestimmte Benutzer** in einem **bestimmten Nutzungskontext** genutzt werden kann, um **bestimmte Ziele** effektiv, effizient und zufriedenstellend zu erreichen“

Ein Beispiel



(Größe 42)

Hohe Usability für:

Ein Beispiel



(Größe 42)

Hohe Usability für:

- ▶ Personen mit Schuhgröße 42, die

Ein Beispiel



(Größe 42)

Hohe Usability für:

- ▶ Personen mit Schuhgröße 42, die
- ▶ durch den Matsch

Ein Beispiel



(Größe 42)

Hohe Usability für:

- ▶ Personen mit Schuhgröße 42, die
- ▶ durch den Matsch
- ▶ trockenen Fußes von A nach B kommen wollen.

Ein Beispiel



(Größe 42)

Wenig oder null Usability falls:

- ▶ Schuhgröße < 40 / Schuhgröße > 42
- ▶ kein Matsch
- ▶ Ballett, Klettern, Fußball...

Andere Richtung...

Gesucht: gebrauchstaugliches Schuhwerk für diese Benutzergruppe,
Kontext, Ziel...



Wie entsteht Usability?

- ▶ niemals am Ende des Entwicklungsprozesses
- ▶ ideal: Benutzerzentrierter Entwicklungsprozess
- ▶ besser als nichts: Heuristiken und Guidelines beherzigen

Benutzerzentrierter Entwicklungsprozess

- ▶ definierte Usability-Ziele
- ▶ interdisziplinär
- ▶ iterativ (Iterationen durch Usability-Ziele gesteuert)
- ▶ Benutzerbeteiligung in allen Phasen
- ▶ parteilich

→ Guerrilla HCI / Discount Usability

Investitionen in Usability

Als Entwurfsziel etabliert:

- ▶ Online-Shopping (generiert Umsatz)
- ▶ Sicherheitskritische Anwendungen (Bedienfehler sind fatal)

Wettbewerbsvorteil erkannt:

- ▶ Produktdesign bei Handys, Navis usw.

Versprechen und Erwartungen

- ▶ Werbung: fast jedes Produkt will „benutzerfreundlich“ sein.
- ▶ Scheinbare Usability hält oft nur bis zur Kaufentscheidung.
- ▶ Getäuschte Anwender oft sehr nachsichtig: 'technisches Stockholm-Syndrom'.

Wirkung mangelnder Usability

- ▶ hohe kognitive Belastung
- ▶ Fehler
- ▶ Frustration
- ▶ verzögerte Zielerreichung
- ▶ Scheitern
- ▶ ... (erweiterbar)

HCI

- ▶ HCI = Human-Computer Interaction.
- ▶ Interdisziplinäres Forschungsgebiet: Informatik, Psychologie, Soziologie, Linguistik, Mediendesign ...
- ▶ Vielfach Übertragung „altbekannten Wissens“ auf neuen Kontext.
- ▶ Viele Forschungsgegenstände, Usability-Konzepte sind ein Bereich

Mentales Modell

- ▶ Repräsentation eines Sachverhalts im menschlichen Bewusstsein.
- ▶ Benutzer haben bzw. produzieren **immer** mentale Modelle.
- ▶ Wir produzieren unweigerlich „Erklärungen“ für Wahrgenommenes.
- ▶ Gedächtnis: Analogien, Andocken an Bekanntes.

Mentales Modell

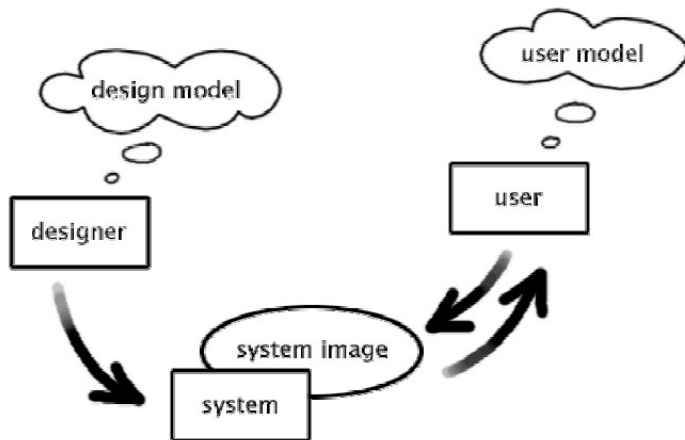
Grundregeln:

- ▶ Benutzer bei der Entwicklung eines geeigneten mentalen Modells unterstützen
- ▶ Bei Benutzern existierende mentale Modelle geeignet adressieren
- ▶ Nur selten ist das mentale Modell des Entwicklers ein geeignetes Modell für den Benutzer
- ▶ Konsistenz!

Wie gut ein Benutzer mit einer Software (oder anderen Produkten) zurechtkommt, ist sehr stark von mentalen Modellen abhängig.

Mentales Modell

Verschiedene mentale Modelle:



Metaphern

- ▶ Werden durch Symbole, Bezeichnungen, Verhalten ausgedrückt
- ▶ Einzel und als „Gesamteindruck“
- ▶ Unterstützen mentale Modelle
- ▶ Analogien (realweltliche Metaphern) müssen konsistent sein

Konventionen

- ▶ Nutzungskontext umfasst auch Denkweise und Erfahrungshintergrund der Zielgruppe
- ▶ Oft bestehen (informelle) Regeln zur Bedeutung bestimmter Symbole, Formen, Farben, Bezeichnungen
- ▶ Diesen Interpretationsrahmen berücksichtigen und unterstützen
- ▶ Kreativität ist meistens ganz falsch

Grundsätze der Dialoggestaltung

- ▶ Aufgabenangemessenheit
- ▶ Selbstbeschreibungsfähigkeit
- ▶ Steuerbarkeit
- ▶ Erwartungskonformität
- ▶ Fehlertoleranz
- ▶ Individualisierbarkeit
- ▶ Lernförderlichkeit

Beispiele für Heuristiken

- ▶ Speak the User's Language
- ▶ Minimize User's Memory Load
- ▶ Consistency
- ▶ Feedback

Usability

Nette Lektüre:

Donald A. Norman: The Design of Everyday Things
MIT Press, London, 1988

Probleme im digitalen Selbstschutz

Unterschiedlich hohe Hürden:

- ▶ Keine Payback-Karte mehr benutzen
- ▶ Andere als die voreingestellte Suchmaschine benutzen
- ▶ Verschiedene und gute Passwörter verwenden und verwalten
- ▶ Anonym surfen
- ▶ Privacy-Settings, Pseudonyme, Pseudoidentitäten verwenden und verwalten
- ▶ Daten, Emails, Datenträger verschlüsseln

Probleme im digitalen Selbstschutz

Schulungsaufwand



Nutzungshäufigkeit

Schulung vs. Usability

Beispiel: Email-Verschlüsselung mit GPG/PGP

Metaphern mit verschiedener Bedeutungen in GPG/PGP und in der Umwelt des Benutzer (RL)

- ▶ Schlüssel
- ▶ Signatur
- ▶ symmetrisch, asymmetrisch
- ▶ privat, öffentlich

Entwickler-Metaphern machen Entwicklern kein Kopfzerbrechen.

Beispiel: Email-Verschlüsselung mit GPG/PGP

Eine Schulung zu GPG/PGP **muss** den Benutzer mit den system-internen Bedeutungen dieser Metaphern vertraut machen.

Sonst nicht korrekt benutzbar.

Hohe kognitive Belastung.

Unnötig hohe Belastung?

Beispiel: Email-Verschlüsselung mit GPG/PGP

Alternativen?

Beispiel: Email-Verschlüsselung mit GPG/PGP

Alternativen?

- ▶ Briefumschlag/Versandbox?
 - ▶ Denkbar für öffentliche Schlüssel
 - ▶ Briefumschlag/Versandbox wäre dann voradressiert
 - ▶ Passende Metapher für private Schlüssel?

Beispiel: Email-Verschlüsselung mit GPG/PGP

Alternativen?

- ▶ Briefumschlag/Versandbox?
 - ▶ Denkbar für öffentliche Schlüssel
 - ▶ Briefumschlag/Versandbox wäre dann voradressiert
 - ▶ Passende Metapher für private Schlüssel?
- ▶ Vorhängeschloss?
 - ▶ Denkbar für öffentliche Schlüssel
 - ▶ Passende Metapher für private Schlüssel: tatsächlich Schlüssel

Beispiel: Email-Verschlüsselung mit GPG/PGP

Es wurde noch keine überzeugende alternative Metapher gefunden, die den Funktionsumfang abdeckt.

Alternative Metaphern müssten konsistent gelten:

- ▶ Über alle Funktionen
- ▶ Bis in alle Rückfragen und Fehlermeldungen hinein

Beispiel: Email-Verschlüsselung mit GPG/PGP

Funktionsumfang?

Muss das sein?

Man denke an

- ▶ Tool-Vielfalt für Audio-/Video-Konvertierung (im Hintergrund: ffmpeg)
- ▶ Tool-Vielfalt für Grafik-Bearbeitung

Johnny Can't Encrypt

1999 - 2006 in Fortsetzungen (Auswahl):

- ▶ „Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0“
- ▶ „Has Johnny learnt to encrypt by now?“
- ▶ „Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software“

Fazit: leichte Verbesserungen dank Automatisierung. Mehr nicht.

Forschungsmotiv: Unternehmenssicherheit

Anne Adams, Martina Angela Sasse in „Users are not the Enemy“ (1999):

- ▶ Insecure work practices and low security motivation among users can be caused by security mechanisms and policies that take no account of **users' work practices, organizational strategies, and usability**.
- ▶ Designers of security mechanisms must realize that [these factors] are the **key to successful security system**.

Forschungsmotiv: Unternehmenssicherheit

Ka-Ping Yee in „User Interaction Design for Secure Systems“
(2002):

- ▶ 10 „key principles for user interaction design in secure systems“
- ▶ Absicht: „to provide a reasonable starting point for talking about user interaction in secure systems“

(Keines dieser Principles ist neu.)

Beispiel VPN

- ▶ Positives Beispiel einer einfachen, funktionierenden Metapher.
- ▶ Mehr brauchen viele Benutzer nicht zu wissen: Ein sicherer Tunnel.



Beispiel: TOR

- ▶ Die Zwiebel-Metapher leitet sich aus dem mentalen Modell des Entwicklers ab.
- ▶ Wieviel **muss** ein Benutzer über die Kaskade wirklich wissen? Vielleicht gar nichts?
- ▶ Wäre statt Zwiebel eine Tunnel-Analogie denkbar?



Beispiel: TOR

Sportliche Übung:

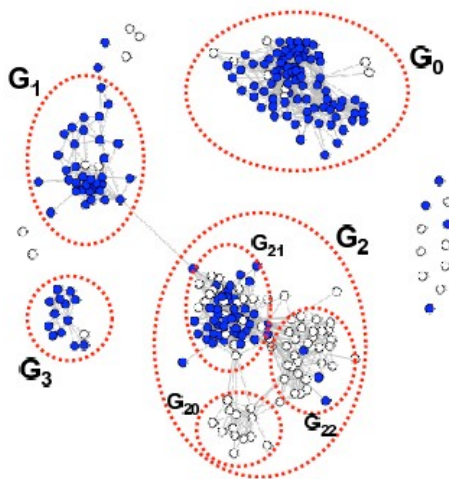
- ▶ Erkläre einer Person mit wenig technischem Selbstvertrauen die Verwendung von TOR.
- ▶ Verwende dabei folgende Begriffe **nicht**:
 - ▶ Zwiebel/Onion
 - ▶ (Exit) Node
 - ▶ Client, Server
- ▶ Geht das?

Beispiel: Privacy-Settings

Kleine Auswahl an Publikationen (2010):

- ▶ Lujun Fang, Kristen LeFevre: „Privacy wizards for social networking sites“
- ▶ Patrick Gage Kelley et al.: „Standardizing privacy notices: an online study of the nutrition label approach“
- ▶ Heather Richter Lipford et al.: „Visual vs. compact: a comparison of privacy policy interfaces“
- ▶ ...

Beispiel: Privacy-Settings



Beispiel: Privacy-Settings

Acme

information we collect

ways we use your information

information sharing

	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out			
cookies						
demographic information		opt out	opt out			
financial information						
health information						
preferences		opt out	opt out			
purchasing information		opt out	opt out			
social security number & govt ID						
your activity on this site		opt out	opt out			
your location						

Access to your information

The site gives you access to your contact data and some of its other data identified with you.

How to resolve privacy-related disputes with this site
Please see our customer service department.

acme.com

5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 405-320-3333
help@acme.com

Beispiel: Privacy-Settings

The screenshot shows a window titled 'Legend' with a menu bar (File, Edit, Sort). Below the menu bar is a legend with three colored squares: green for 'Allow', yellow for 'Some allow, some deny; expand trees for details', and red for 'Deny'. The main area is a grid with categories on the left and user groups on top. The 'College' row and 'Best Friends' column are highlighted with a thick black border.

	Users and Groups	All My Friends	Best Friends	Family	Shady Friends	All My Networks	Friends of Friends
Basic Information	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Contact Information	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Education Information	Yellow	Yellow	Green	Green	Yellow	Yellow	Red
College	Yellow	Green	Green	Green	Green	Yellow	Red
Grad School	Yellow	Green	Green	Green	Green	Green	Red
High School	Yellow	Yellow	Green	Green	Red	Yellow	Red
Personal Information	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow

Beispiel: Privacy Settings in Facebook

The image shows a screenshot of a Facebook profile page for Jason Watson. At the top, there are four tabs: "Main View", "Search View", "Network View", and "Friends View". A yellow box highlights these tabs and a yellow callout box points to them with the text: "HTML Tabs Allow Users to View Profile From Different Audiences". The profile information includes: Name: Jason Watson, Networks: UNC Charlotte Grad Student, Sex: Male, Relationship Status: Married, Birthday: January 1, 1971, and Hometown: Concord, NC. Below the profile picture, there are sections for "Mini-Feed" (showing no recent activity) and "Information".

Beispiel: Privacy Settings in Facebook


The screenshot shows the Facebook search interface. At the top, navigation tabs include 'Main View', 'Search View' (highlighted in yellow), 'Network View', and 'Friends View'. Below these are links for 'Profile', 'Friends', 'Networks', and 'Inbox'. The search bar contains 'Jason Watson' and the scope is set to 'All Networks'. The results are divided into two sections: 'Search view from outside network' and 'Search view from inside network'. Both sections show a profile card for Jason Watson, a UINC Charlotte Grad Student '10. The 'outside network' view shows a 'Poke item!' link, while the 'inside network' view shows 'Send Message', 'Poke item!', 'View Friends', and 'Add to Friends' links.

Main View | **Search View** | Network View | Friends View


Profile edit Friends Networks Inbox Home Account Privacy Logout

Searching for Jason Watson within All Networks Advanced | Filter Results

Search view from outside network

	Name: Jason Watson Networks: UINC Charlotte Grad Student '10 Matches: Name	Poke item!
---	---	----------------------------

Search view from inside network

	Name: Jason Watson Networks: UINC Charlotte Grad Student '10 Field: Software & Information Systems Matches: Name	Send Message Poke item! View Friends Add to Friends
---	---	--

Beispiel: Privacy Settings in Facebook

Task Analysis				
	Facebook		Prototype	
	Accuracy %	Avg. Comfort	Accuracy %	Avg. Comfort
T1	45.3	5.4	98.4	6.3
T2	37.5	4.7	100	6.7
T3	89.6	5.8	100	6.7
T4	72.9	6.1	81.3	6.4
T5	85.4	4.8	89.6	6.2
Avg	66.14	5.4	93.86	6.4

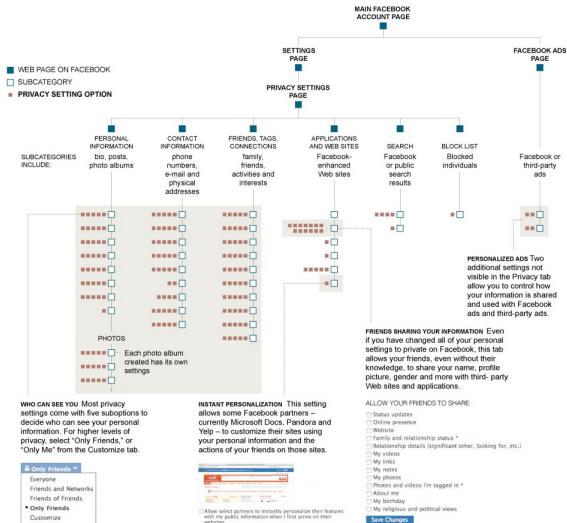
Heather Richter Lipford et al: „Understanding Privacy Settings in Facebook with an Audience View“ (2008)

Beispiel: Privacy-Settings

<sarcasm>

Über diese vielen guten Anregungen werden sich die Verantwortlichen bei Facebook & Co. sicher freuen.

</sarcasm>



Beispiel: Privacy-Settings

„Anti-Usability“

Beispiel: Adventures

Benutzerwünsche

Ein Hauptproblem: (Un-)Übersichtlichkeit

- ▶ Unterscheidung von Schutzziele
- ▶ Welche Sorte Tools für welche Schutzziele?
- ▶ Welche konkreten Tools?

Benutzerwünsche

Oft genannter Wunsch: „gute“ Browser-Konfiguration

- ▶ One-Click-Lösung
- ▶ mit „allem“: Cookies, Anonymisierung, Werbung(!), ...

Benutzerwünsche

Ein anderer Vorschlag: Eine Art Gütesiegel.

- ▶ Wie Bio oder FairTrade oder die Lebensmittel-Ampel.
- ▶ Etwas, das bestimmt, was vertrauenswürdig ist.

Benutzerwünsche

Ein anderer Vorschlag: Eine Art Gütesiegel.

- ▶ Wie Bio oder FairTrade oder die Lebensmittel-Ampel.
- ▶ Etwas, das bestimmt, was vertrauenswürdig ist.

Ist so etwas auch nur im Ansatz denkbar?

- ▶ Wer würde das ausstellen?
- ▶ Nach welchen Kriterien?

Benutzerwünsche

Ein anderer Vorschlag: Eine Art Gütesiegel.

- ▶ Wie Bio oder FairTrade oder die Lebensmittel-Ampel.
- ▶ Etwas, das bestimmt, was vertrauenswürdig ist.

Ist so etwas auch nur im Ansatz denkbar?

- ▶ Wer würde das ausstellen?
- ▶ Nach welchen Kriterien?

Oder läuft es vielleicht auf die Frage hinaus, wer schneller ist?

Probleme im digitalen Selbstschutz

Usability-Potenziale im Bereich des digitalen Selbstschutzes sind erkennbar.

Usability-Potenziale im Bereich des digitalen Selbstschutzes sind noch nicht annähernd ausgelotet.

Und erst recht nicht umgesetzt.

Mit Sicherheit hat Usability im digitalen Selbstschutz emanzipatorisches Potenzial.

Emanzipatorisches Potenzial

1. Nutzung digitaler Bürgerrechte
2. Verteidigung digitaler Bürgerrechte
3. Vervielfältigung von Aufklärung

Danke für eure Aufmerksamkeit!



<helga@testschmie.de>