Usability und/oder Security?

Markus Dahm
Software-Ergonomie
Fachbereich Medien
FH Düsseldorf
40474 Düsseldorf
markus.dahm@fh-duesseldorf.de
www.medien.fh-duesseldorf.de/dahm

Christoph Thiel
IT-Sicherheit
Fachbereich Medien
FH Düsseldorf
40474 Düsseldorf
christoph.thiel@fh-duesseldorf.de
www.medien.fh-duesseldorf.de/thiel

Abstract

In der Usability-Community liegt der Focus (natürlich) vor allem darauf, dem Benutzer die Arbeit mit der Software oder dem elektronischen Gerät so einfach wie möglich zu machen. Eine Randbedingung, die dabei nicht sehr häufig behandelt wird, ist die Sicherheit der Anwendung. Mit „Sicherheit“ ist hier im Wesentlichen der Schutz vor Missbrauch bzw. Manipulation von Daten oder Ressourcen gemeint.

Es scheint so zu sein, dass sich die beiden Ziele Gebrauchstauglichkeit und Sicherheit sehr häufig in der Umsetzung gegenseitig ausschließen: Eine sehr sichere Anwendung ist meistens eher aufwändiger zu benutzen und zu warten, eine einfach zu benutzende Anwendung vernachlässigt häufig die Sicherheit. Können diese Ziele miteinander in Einklang gebracht werden?

Keywords

Usability, Security, Widersprüchliche Anforderungen, Gesundheitskarte, HBCI, RFID, Software-Engineering

1.0 Überblick

1.1 Usability und Security

Die Informatik-Disziplinen „Security“ und „Usability“ haben beide das gleiche Ziel: Das Beste für den Benutzer. Security schützt den Benutzer vor Nachteilen bei der Verwendung von Software, Usability möchte die Verwendung so einfach wie möglich machen.

Leider stehen beide Zielrichtungen häufig im Widerspruch zueinander:

- Alleine das Einrichten einer möglichst sicheren Infrastruktur stellt bereits ein Hindernis für das einfache Benutzen von Software dar, wie die meisten bestätigen können, die selbst ein WLAN-Netzwerk in einer homogenen Umgebung eingerichtet haben.
- Aber auch Techniken wie die Sicherung von E-Mails durch Zertifikate sind sowohl in der Einrichtung als auch der Verwendung meistens sehr aufwändig und damit nicht aufgabenangemessen.
- Beim online-Banking ist der Widerspruch ebenfalls eklatant: Jeder möchte natürlich maximale Sicherheit seiner Kontodaten, die wenigsten Kunden gönnen sich aber die Sicherheit des HBCI-Verfahrens durch Anschaffung, Einrichtung und Benutzung eines zusätzlichen Kartenlesers.
- Die ständigen Nachfragen der User Account Control (UAC) von Windows Vista bei der Installation oder Modifikation von Software erhöhen zweifelsfrei die Sicherheit, gehen dem Benutzer aber sehr schnell auf die Nerven.

1.2 Sicheres oder Benutzbares Internet ?

Aufgrund der weiten Verbreitung und Wichtigkeit auch im beruflichen Einsatz sind sowohl Sicherheit als auch Usability ein wesentlicher Bestandteil der Anforderungen und natürlich auch jeder ernsthaft eingesetzten Software.

Die werbewirksam eingesetzten Techniken von „Web 2.0“ stellen durch ihre direkten Interaktionsmöglichkeiten des Benutzers erhöhte Anforderungen an die Gestalter der Software, wiederum sowohl in Hinsicht auf ihre Usability als auch ihre Security.

1.3 Wie beide Aspekte verbinden?

Mit diesem Beitrag soll vor allem darauf aufmerksam gemacht werden, dass sich Anforderungen bezüglich der Sicherheit und der Usability häufig zunächst wiedersprechen. Lösungen können daher prinzipiell nicht in einer bloßen Kosmetik der Oberfläche oder in nachträglich eingefügten Prozessen bestehen. Vielmehr muss nicht nur das Interaktionskonzept explizit beide Ziele (Sicherheit und Ergonomie) ansprechen –beide Anforderungsbereiche müssen fast immer auch im Design und der Architektur der Software berücksichtigt werden.

1.4 Beispiele

In den folgenden Kapiteln werden wir die Probleme der Widersprüchlichkeit der Anforderungen im Detail einiger Beispiele erörtern.

2.0 Vertraulichkeit

Ein wichtiger Grundwert der IT-Sicherheit ist die Vertraulichkeit der ausgetauschten Informationen: Niemand außer Sender und Empfänger sollte die Informationen entziffern können. Ein Lauscher mag die Sendung vielleicht lesen, soll sie aber nicht verwenden können.

2.1 WLAN

Wer heute einen DSL-Anschluss bestellt, bekommt meistens einen WLAN-Router für kleines Geld oder gar gratis dazu. WLAN ist ja auch sehr bequem: das lästige Verkabeln entfällt, trotzdem ist in der ganzen Wohnung der Internetzugang verfügbar.

Abb 1: WLAN-Router (Bild: AVM)

Wer allerdings sein WLAN offen und ungeschützt betreibt, muss mit verheerenden Folgen rechnen: Wenn sich z.B. Unbekannte über dieses WLAN an einer illegalen Tauschbörse beteiligen, haftet der WLAN-Betreiber, bis zu einigen Tausend Euro. Aus einer Urteilsbegründung des LG Hamburg[1]: „Gemäß § 1004 BGB habe die Anschlussinhaberin als Störer für Schutzrechtsverletzungen zu haften". „Weiter ist allgemein bekannt, dass ungeschützte WLAN-Verbindungen von Dritten missbraucht werden können, um über einen fremden Internetanschluss ins Internet zu gelangen". „Die Verwendung der WLAN-Verbindung zu solchen Zwecken löse Prüf- und Handlungspflichten aus. Zumutbar sei es auch, fachliche Hilfe in Anspruch zu nehmen" (heise.de WLAN).

Das bedeutet, dass der typische Heim-Anwender sich einige bis viele Stunden mit der sicherheitstechnisch korrekten Einrichtung seines Heim-WLANs befassen muss.

Dabei sind häufig sowohl die Anleitung als auch die sind Durchführung kompliziert, um sowohl den Router als auch jedes Gerät im Netzwerk korrekt zu konfigurieren.

Einige Hersteller bieten zwar technische Unterstützung mittels USB-Sticks, aber auch dafür wird einiges an Erfahrung benötigt.

➔ Mit den entsprechenden Konfigurationen können WLAN-Netze ausreichend sicher betrieben werden. Leider ist die Konfiguration sehr häufig aufwändig.

2.2 Verschlüsselung

Nur mit Hilfe von Verschlüsselungslösungen kann die Vertraulichkeit von Informationen allgemein sichergestellt werden. Für die Sicherung interner Datenbestände eines Unternehmens können dazu File/ Folder-Encryption (FFE), Festplattenverschlüsselung oder Containerverschlüsselung eingesetzt werden.

Grundsätzlich muss man zwischen rein clientbasierten Lösungen und Client-Server-Anwendungen unterscheiden. Erstere benötigen für die Verwaltung der kryptografischen Schlüssel meist zusätzliche Datenbanken, welche hohe Zusatzanforderungen an Installation und Betrieb stellen. Zudem sind rein clientbasierte Systeme in der Regel nicht in der Lage, zeitnah auf Änderungen der Verschlüsselungspolicy, z. B. den Entzug von Entschlüsselungsrechten für Benutzer, zu reagieren. Hingegen haben Client-Server-Systeme den Vorteil, dass Konfigurations- und Schlüsselmanagement durch eine Serverkomponente automatisch erledigt werden und keine zusätzlichen Datenbanken benötigen.

Schlüsselverwaltung und Authentifizierung basieren überwiegend auf Public Key Mechanismen und benötigen für den sicheren Betrieb eine Public-Key Infrastruktur (PKI). Eine gebrauchstaugliche Verschlüsselungslösung sollte sowohl benötigte PKI-Komponenten selbst beinhalten, als auch mit bereits bestehenden PKIs zusammenarbeiten können. Hierbei ist auch darauf zu achten, dass eine Standardschnittstelle für Sicherheitstoken unterstützt wird, damit man nicht eine unangenehme und teure Überraschung erlebt, wenn die Verschlüsselungssoftware nicht mit der verwendeten Chipkarte zusammenarbeitet. Zur Reduktion des Aufwandes bei der Benutzerverwaltung ist es ein Muss, dass die Lösung sich an externe Verzeichnisdienste wie z. B. Microsoft Active Directory oder Novell eDirectory andocken kann.

Sehr nützlich ist es, wenn aus verschlüsselten Dateien automatisch verschlüsselte E-Mail-Anhänge erzeugt werden können, welche beim E-Mail-Empfänger über ein mitgeteiltes Passwort und evtl. mithilfe einer kostenlos zur Verfügung gestellten Software entschlüsselt werden können.

Der GAU der Verschlüsselung sind verschlüsselte Daten, an die auch der rechtmäßige Besitzer nicht mehr herankommt, z. B. aufgrund von Schlüsselverlust o.ä. Selbst im Fall eines Totalausfalls des Security-Servers oder einer anderen schlüsselverwaltenden Instanz, z. B. nach einem Brandschaden, müssen verschlüsselte Dateien noch entschlüsselt werden können.

Eine im größeren Stil einsatzfähige Lösung muss hier eine schnelle und un-

1 LG HH, Aktenzeichen 308 O 407 / 06

Brau, H., Diefenbach, S., Hassenzahl, M., Koller, F., Peissner, M. & Röse, K., (Hrsg.): Usability Professionals 2008

komplizierte Lösung bieten. Im Sinne der schnellen Datenverfügbarkeit und der Business Continuity ist eine solche Option unverzichtbar.

Neben der in der Natur der Sache liegenden Forderung nach Sicherheit, muss eine solche Verschlüsselungslösung weitere Anforderungen erfüllen, um praxistauglich zu sein: Es sollte eine transparente Verschlüsselung eingesetzt werden, so dass der Benutzer keinerlei Auswirkungen spürt, die Verschlüsselung weder manuell anstoßen, noch sich darüber Gedanken machen muss, ob überhaupt verschlüsselt werden soll. Schließlich sollte eine Rollentrennung zwischen IT und Sicherheitsverwaltung möglich sein.

➔ Dazu muss eine Lösung über eine zentrale „einfache“ Administration und über sinnvolle Identifizierungs- und Authentisierungsmechanismen verfügen. Auch Nicht-Techniker ohne Experten-Know-how über Kryptografie sollten die Rolle des Sicherheitsadministrators übernehmen können. Sie sollen jederzeit in der Lage sein, die Verschlüsselungsregeln festzulegen und der „Policy“ (den Richtlinien) gemäß anzupassen.

3.0 Identifikation und Authentifizierung

3.1 RFID-Tags auf einzelnen Artikeln

Um die Verkaufskette (supply chain) möglichst durchgängig zu automatisieren, gehen Bestrebungen dahin, die Barcodes auf allen Produkten durch RFID-Tags zu ergänzen oder zu ersetzen. Das ermöglicht sowohl zeitnahes Materialmanagement als auch ein berührungsfreies Kassieren (Metro).

Für den Verbraucher bedeutet das einerseits Vorteile, da Schlangen an der Kasse so vermieden werden könnten. Für die Filial-Mitarbeiter bedeutet das eine Entlastung, sowohl an der Kasse als auch bei der Warendisposition.

Abb 2: RFID-Tag an der Ware (Bild: Metro)

Nachteile bezüglich der Sicherheit ergeben sich für den Verbraucher durch die Möglichkeit, die RFID-Tags nicht nur an der Kasse sondern auch durch beliebige andere RFID-Leser auszulesen. Dadurch lassen sich Käufer fast beliebig nach ihren Gewohnheiten ausspähen.

Als fast unwirkliche Kulmination erscheint in diesem Zusammenhang das Tagging von Menschen. Ende 2005 hat die Food and Drug Administration (FDA) der USA grünes Licht für implantierbare Tags gegeben: "Die FDA hat den Weg für den so genannten "VeriChip" der US-Firma Applied Digital Solutions [ADS] frei gegeben. Dieser etwa reiskorngroße Chip wird unter der Haut eingepflanzt und kann diverse Informationen speichern, die über einen speziellen Scanner ausgelesen werden können. (hae) Als Anwendung wird dabei die schnelle Identifikation von Kindern und Häftlingen aber auch von Patienten in großen Krankenhäusern genannt.

➔ RFID-Tags sind eine hervorragende technische Unterstützung für berührungslose Informationsübermittlung auch sehr vieler kleiner Objekte (Waren). Die damit verbundenen Annehmlichkeiten und Vorteile für viele Beteiligte sind andererseits mit erheblichen Sicherheitsbedenken verbunden.

3.2 Biometrie

Wäre es nicht sehr einfach, wenn man sich nicht beliebig viele Benutzernamen und nicht zu erratende Passworte merken müsste? Wenn statt dessen „man selbst“ immer alle Daten zur Authentifizierung bei sich, sogar in sich tragen würde? Genau das ist die Idee bei der Identifizierung und gleichzeitiger Authentifizierung durch körperliche Eigenschaften.

Die Gebrauchstauglichkeit ist dadurch sehr hoch, da der Prozess der Erkennung, je nach Verfahren und Merkmal, sehr einfach und schnell gemacht werden kann.

Verfahren wie Iris-Erkennung sind mit erhöhtem technischem Aufwand verbunden und haben auch eine hohe Akzeptanzhürde. Nicht selten sind dagegen Scanner für Fingerabdrücke in Laptops oder auch auf USB-Speichersticks.

Abb 3: Fingersensoren (Bild: Visortech, Acer)

Damit kann im Prinzip sehr einfach und ohne mentale Belastung des Benutzers eine Zugriffskontrolle und Authentifizierung durchgeführt werden. Allerdings sind die einfachen Ausführungen, wie sie in Consumer-Geräten eingesetzt werden, auch relativ einfach zu überlisten - teilweise durch Anhauchen oder mit Tesafilm oder Gummibärchen übertragene Fingerabdrücke (Uni B) oder, etwas aufwändiger: „Um einen Fingerabdruck nachzumachen braucht man nur einen Deckel einer Plastikflasche, etwas Sekundenkleber, eine Digitalka-

mera, sowie Holzleim und einen speziellen, hautfreundlichen Kleber.“ (CCC).

➔ Biometrische Sensoren könnten Authentifizierungen sehr einfach in der Benutzung machen. Sie sind aber auch eher einfach bei einem ernsthaften Angriff zu überlisten.

4.0 Kombination von Geheimhaltung, Identifikation und Authentifizierung

4.1 HBCI-Kartenleser

Sehr viele Bankkunden verwalten Ihre Konten online: Überweisungen, Kontostand oder Daueraufträge sind schnell und bequem von zu Hause zu bearbeiten. Dass dabei privateste Daten wie Kontonummern und Geheimzahlen über öffentliche Netze, oder gar über ein ungeschütztes WLAN, gesendet werden, ist den meisten nicht mehr täglich bewusst. Bei der Sicherheit verlässt man sich dabei gerne auf die Verschlüsselung der Daten. Dabei ist auch die für Angriffe anfällig, da die gleiche Hardware sowohl die Banking-Applikation als auch ggf. die Schadsoftware betreibt.

Abb 4: Kartenleser der Klasse 3 (Bild: SCM)

Dabei würden sich viele mehr Sicherheit wünschen, wenn sie nicht selber damit befasst wären, wie eine Studie der IT-Sicherheits-Firma RSA.com in 2006 ergeben hat:

„70% der Kunden sind stark an Sicherheitsmaßnahmen interessiert, die hinter den Kulissen angewendet werden (z.B. risikobasierte Authentifizierung); 81% der Kunden würden sich wohler fühlen, wenn ihre Bank eine derartige Technologie implementiert hätte

87% sind an Site-to-User-Authentifizierung interessiert; mehr als 50% wünschen dies sogar zusätzlich zu oben genannter Technologie“ (hbi.de 2006).

Immerhin hat auch der Urheber der Studie, RSA.com, bereits erkannt, dass Sicherheit nicht nur mit technisch orientierten Mitteln, wie Verschlüsselung, erreicht wird; zusätzlich muss der Benutzer als ein Glied in der Sicherheitskette mit einbezogen werden:

„Consumers value better security, but financial institutions need to provide it with a minimum level of perceived distraction.

Consistency of process increases *the perception of ease-of-use* and reduces the perceived distraction in performing security measures online.

It is important to consistently reassure users as to the security of their online information without needlessly alarming them“[2]

➔ Der Sicherheitsgewinn gegenüber Attacken wäre beträchtlich, die Anschaffung, Installation und Integration von HBCI-Kartenlesern scheint jedoch zu aufwändig zu sein.

4.2 Die Gesundheitskarte

Die elektronische Gesundheitskarte kommt - und mit ihr der Heilberufsausweis (HBA). Mit diesem können

2 Interessant ist hier auch die Unterscheidung zwischen „echter Ablenkung“ und „wahrgenommener Einfachheit“.

und müssen Ärzte und Zahnärzte in Zukunft die von ihnen in Form „elektronischer Rezepte“ ausgestellter Verordnungen mit qualifizierten elektronischen Signaturen versehen. Apotheker müssen dann als Gegenstelle die dispensierten Verordnungen mit ihrem HBA ebenfalls elektronisch signieren.

Abb 5: Die Gesundheitskarte (Bild: BMG)

Der HBA dient also insbesondere als Signaturkarte für die Erstellung qualifizierter elektronischer Signaturen. Dabei werden dem Benutzer (Arzt, Zahnarzt, Apotheker) gemäß Signaturgesetzgebung zunächst die zu signierenden Daten angezeigt, bevor er nach erfolgreicher Eingabe einer PIN (Signatur-PIN) die Erzeugung genau einer Signatur auslösen kann. Die PIN-Eingabe muss dabei lokal erfolgen, d.h. direkt an einem HBA-Kartenterminal.

So sinnvoll dieses Vorgehen aus Sicherheitssicht für qualifizierte elektronische Signaturen sein mag, so stellt die Vorstellung, dass Ärzte und Apotheker gezwungen sein könnten, täglich unzählige Male ihre PIN an einem festen Kartenterminal einzugeben, um pro PIN-Eingabe jeweils ein einziges elektronisches Rezept gegenzuzeichnen, die Gebrauchstauglichkeit des HBA und damit der elektronischen Gesundheitskarte akut in Frage.

Um den täglichen Umgang mit der elektronischen Signatur in Praxen, Kliniken und Apotheken zu erleichtern, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) technische Richtlinien

für Stapel- und Komfortsignaturen herausgegeben. Diese sollen „Vielsignierern“ nach Eingabe der Signatur-PIN mehrere Signaturen ermöglichen, ohne dass dadurch die Sicherheit und rechtliche Bedeutung der Signatur gefährdet wird.

Die Stapelsignatur erlaubt die Erzeugung mehrerer Signaturen unmittelbar hintereinander - nach dem Anzeigen der zu signierenden Dokumente (Stapel) und der daran anschließenden einmaligen Eingabe der PIN.

Die Komfortsignatur erfordert noch weniger Aufwand des Benutzers als die Stapelsignatur: Zunächst erfolgt die PIN-Eingabe, anschließend kann über einen längeren Zeitraum (z. B. Öffnungsdauer der Praxis) signiert werden. Dabei muss sich der Benutzer jedoch vor Signieren eines Dokuments oder Dokumentenstapels mittels eines RFID-Tokens oder eines Biometriemoduls authentisieren. Um sicherzustellen, dass der Token nur vom rechtmäßigen Besitzer verwendet werden kann, sind folgende Möglichkeiten vorgesehen:

- Die Aktivierung des Tokens durch eine 4stellige PIN
- Die Aktivierung des Tokens durch ein biometrisches Merkmal des Besitzers
- Andere geeignete Sicherheitsmaßnahmen, die einen Verlust oder die unkontrollierte Nutzung verhindern.

Die Verwendung einer Token-PIN wäre aus Sicherheitssicht wünschenswert, widerspricht aber wiederum dem Komfortgedanken. Es wird daher dem Benutzer auch erlaubt, seine Token-PIN zu deaktivieren, d.h. den RFID-Token ohne Authentisierung zu nutzen. Dabei bleibt aus Usability-Sicht offen, ob und ggf. wie der Nutzer in die Lage versetzt werden kann, die Tragweite dieser Entscheidung zu verstehen und die entsprechende Verantwortung zu übernehmen.

Die Nutzung eines Biometriemoduls stößt auf rechtliche und sicherheitstechnische Probleme. Biometrische Verfahren, die zusätzlich zur wissensbasierten Benutzerauthentisierung angewendet werden, müssen gemäß Signaturgesetzgebung einer Bewertung gemäß Sicherheitsmechanismenstärke "mittel" genügen. Bisher sind Biometriekomponenten nicht entsprechend zertifizierbar. Dazu müsste zunächst eine Methodik zur Bewertung des Angriffspotentials biometrischer Verfahren entwickelt werden.

➔ Auch bei der Anwendung der Gesundheitskarte ist es nicht einfach, einen Kompromiss zwischen Usability und Sicherheit zu finden. Beide Anforderungen sind jedoch entscheidend für den Erfolg dieses Konzepts in der Praxis.

5.0 Fazit

Als Fazit kann (wieder einmal) darauf hingewiesen werden, dass „gute“ Software mehr ist als lediglich funktionierende Software. Im gesamten Entwicklungsprozess müssen vielfältige funktionale und nicht-funktionale Anforderungen, wie die der Sicherheit und Gebrauchstauglichkeit, berücksichtigt werden, um allen, auch sich zunächst widersprechenden, Anforderungen gerecht zu werden.

Wird aber eine Anwendung primär als möglichst einfach zu benutzen gestaltet, werden dabei gegebenenfalls Sicherheitsaspekte übersehen.

Im Nachhinein eingebrachte Sicherheitsanforderungen führen wiederum typischerweise zu zusätzlichen Prozessschritten, die die normale Abfolge unterbrechen. Beispiele dafür sind Programme zur Ver- und Entschlüsselung, die nachträglich auf Dateien angewandt werden oder mehrfache Eingaben von verschiedenen Passworten. Dieses führt mit Sicherheit zu einer schlechteren Usability der Anwendungen.

Für beide Anforderungsgebiete, Usability und Security gilt sicher, dass die jeweiligen Anforderungen so früh wie möglich im Software-Entwicklungsprozess ermittelt werden sollten, um in der Umsetzung angemessen berücksichtigt zu werden.

6.0 Literaturverzeichnis

6.1 Bücher

Cranor, F.; Garfinkel, S. (2005): Security and Usability, Sebastopol: O‘ Reilly

6.2 Weblinks – Stand 26.5.2008

BSI: http://www.bsi.bund.de/literat/studien/-BioFinger/BioFinger_I_I.pdf - BSI-Studie zur Fingerabdrucksensoren

CCC: http://chaosradio.ccc.de/ctv001.html - Anleitung zum Nachmachen von Fingerabdrücken

DGK: http://www.die-gesundheitskarte.de

hae: http://www.haefely.info – Implantierbarer RFID-Chip

hbi.de: http://www.hbi.de/clients/ RSA/info/07-17-06_Usability_Concept_Testing_Release-.doc (Bereich Infomaterial: „RSA Security-Studie über Sicherheit von online-Banking“)

Metro: http://www.metrogroup.de/servlet/-PB/menu/1155070_l1/index.html RFID-Tags

RFID: http://www.heise.de/tp/r4/artikel-/18/18845/1.html Gefahren von RFID

Uni B: http://www.informatik.uni-bremen.de/~lechner/SoftwareTrends-Web/index.htm - Fingerabdrucksensoren

WLAN: http://www.heise.de/newsticker-/meldung/77921 - Urteil gegen Betreiber von ungesichertem WLAN