Deutsche Telekom Laboratories
An-Institut der Technischen Universität Berlin

Nutzerzentriertes Security & Privacy Engineering mittels Verhaltenssimulationen

Sebastian Möller
Tobias Hirsch
Niklas Kirschnick
Hanul Sieger
Joachim Meyer

Table of contents

1 Motivation

Anforderungen an die Sicherheit von Computersystemen und den Schutz der Privatsphäre ihrer Nutzer haben in den letzten Jahren aufgrund der Entwicklung vor allem im Bereich mobiler Geräte, internetbasierter Dienste und sozialer Netzwerke zugenommen. Neben den rein technischen Aspekten möglicher Sicherheitslücken in informationstechnischen (IT) Systemen – beispielsweise bei der Nutzung von Passwörtern beim Login zu PCs, Computernetzen oder webbasierten Diensten – ist ein wichtiger Aspekt der durch den Benutzer selbst „verursachte" Sicherheitsmangel. Das Wort „Verursachung" soll hierbei keine Schuldzuweisung suggerieren: Angenommene Gründe für die Sicherheit reduzierendes Nutzerverhalten liegen vielmehr in Diskrepanzen zwischen dem Verhalten von Experten und Laien (letzterer von Systementwicklern häufig als „unsachgemäßer" Gebrauch angesehen, vgl. Adams & Sasse, 1999), der geringen Gebrauchstauglichkeit der Systeme (Tognazini, 2005), und in der ungünstigen Kosten-Nutzen-Relation der zu erwartenden Gefährdung (Herley, 2009).

In der Tat ist die Sicherheit bei IT-Systemen mit wenigen Ausnahmen (bspw. Firewalls) nur ein sekundäres Kriterium. Das Ziel des Nutzers einer IT-Anwendung ist normalerweise die Erfüllung einer anderen Primäraufgabe, bspw. das Versenden einer E-Mail oder die Durchführung einer Buchung. Diese Aufgabe soll mit größtmöglicher Effektivität, Effizienz und zur größten Zufriedenheit des Nutzers erfüllt werden können – dann erfüllt das System die Hauptkriterien der Gebrauchstauglichkeit (Usability). Sicherheitsmechanismen bringen den Nutzer meist von der Primäraufgabe ab, bspw. durch Abfrage eines Passwortes oder einer PIN, Aufforderung zur Überprüfung eines Zertifikates, oder Warnung vor Sicherheitsrisiken. Angesichts seines Primärzieles wägt ein Nutzer intuitiv ab zwischen dem Aufwand, den er in die Sekundäraufgabe „Sicherheit" steckt, und dem erwarteten Nutzen. Letzterer ist fast immer nur indirekt und mit erheblicher zeitlicher Verzögerung spürbar – Sicherheitsrisiken machen sich erst deutlich nach der Interaktion bemerkbar, und lassen sich für den Nutzer meist nicht auf konkretes Fehlverhalten zurückführen.

Zur gezielten Adressierung der Sicherheit und der Sicherung der Privatsphäre bei IT-Systemen ist es deshalb unerlässlich, das Verhalten des Nutzers im Umgang mit sicherheitsrelevanten IT-Systemen zu analysieren und zu formalisieren, sowie relevante Einflussfaktoren zu identifizieren. Diese Einflussfaktoren müssen schon früh im Entwicklungsstadium der Systeme berücksichtigt werden, um Designentscheidungen auf ihre Konsequenzen zu analysieren und kostenintensives Re-Design zu vermeiden. Im Bereich der Gebrauchstauglichkeit von IT-Systemen hat sich hierfür das sog. Usability Engineering bewährt, welches bei allen Schritten der Systementwicklung Methoden aufzeigt, die bei konsequenter Anwendung zu optimaler Usability bei minimalen eingesetzten Ressourcen führen können. Ein äquivalentes Vorgehen ist auch zur Durchsetzung von Sicherheit und Privatsphäre wünschenswert; leider hat sich das Security & Privacy Engineering jedoch bislang noch nicht durchgesetzt. Stattdessen werden zur Erreichung des Zieles Sicherheit fast ausschließlich technische Lösungen entworfen . Dabei sind viele bekannte Angriffspunkte nicht durch technische Maßnahmen zu schließen, bspw. Attacken durch sog. Social Engineering, die nicht die technische Überwindung von Sicherheitsmaßnahmen suchen, sondern den Benutzer z.B. zur Preisgabe seiner Passwörter bringen (Herley, 2009).

Die Haupthindernisse bei der nutzerzentrierten Entwicklung von Security- und Privacy-Mechanismen sind

Mangelndes Grundlagenwissen über die relevanten Einflussfaktoren auf das Nutzerverhalten und die Nutzerbewertung bei sicherheitskritischen IT-Systemen

Fehlendes Wissen über Nutzer und ihr Verhalten bei den Systementwicklern

Mangelnde Ressourcenzuteilung im Entwicklungsprozess

Das erste Hindernis kann nur durch eine fokussierte Erforschung der psychophysikalischen Grundlagen überwunden werden. Hierzu hat sich in den vergangenen Jahren das Forschungsfeld Usable Security entwickelt, welches eine Reihe von regelmäßigen Konferenzen und Sitzungen organisiert und ganz erheblich zum Wissenszuwachs beigetragen hat (vgl. Fischer-Hübner et al., 2011). Zur Überwindung des zweiten und dritten Hindernisses ist es notwendig, dem Entwickler als dem Architekten des IT-Systems effiziente Werkzeuge an die Hand zu geben, welche es ihm ermöglichen, Nutzerverhalten zu antizipieren und daraus resultierende Sicherheitsmängel mit geringem Aufwand zu beseitigen oder wenigstens zu minimieren. Hierdurch kann ein Optimum zwischen den sich teilweise widersprechenden Zielgrößen Usability einerseits und Security bzw. Privacy anderseits gezielt eingestellt werden.

Im Folgenden werden erste Schritte zu einem nutzerzentrierten Security & Privacy Engineering vorgestellt. Hierzu werden zunächst bekannte Einflussfaktoren auf das Nutzerverhalten analysiert und klassifiziert (Kapitel 2). Anschließend wird Nutzerverhalten formal beschrieben, um daraus ein Verhaltensmodell und eine Simulationsumgebung zu entwickeln (Kapitel 3). Die Evaluierung der Simulationsumgebung in einer Mikrowelt zeigt, dass das Verfahren prinzipiell geeignet ist, Sicherheit, Privatsphäre und Gebrauchstauglichkeit automatisiert und damit sehr effizient im Produktentwicklungszyklus zu berücksichtigen.

2 Einflussfaktoren auf das Nutzerverhalten

Im Rahmen dieses Beitrages beschäftigen wir uns mit Systemen, die eine Interaktion des Benutzers zur Beeinflussung der Sicherheitsfunktionen zulassen, bspw. über grafische Nutzerschnittstellen, biometrische Sensoren oder ähnliches. Abb. 1 zeigt eine Taxonomie von Einflussfaktoren auf das Nutzerverhalten bei der Interaktion mit solchen Systemen.

Zu den allgemeinen psychologischen Faktoren zählen das persönliche Risikoverhalten und das Vertrauen in Institutionen und Personen sowie die Sorge um die Privatsphäre (Zimbardo & Gerrig, 2008). Dieses Verhalten kann zur Charakterisierung einer Person genutzt werden, dennoch sind die Verhaltensweisen in einzelnen Bereichen im Einzelfall nicht immer konsistent und direkt übertragbar. Einzelne Personen können in einem Bereich ein eher laxes Risikoverhalten an den Tag legen, in einem anderen Bereich hingegen sehr sorgfältig auf Sicherungsvorkehrung achten. Dennoch lässt sich aus dem persönlichen Risikoverhalten zumindest eine statistische Wahrscheinlichkeit hinsichtlich des Verhaltens im Bereich IT-Sicherheit ableiten, wie das auch in anderen Bereichen möglich ist (Zuckerman & Kuhlman, 2000). Analog gilt dies für die Sorge um Privatsphäre und um das Vertrauen in einbezogene Institutionen, Firmen, und Personen (RISEPTIS Group, 2009).

Das persönliche Erleben und die (tagesaktuelle) Berichterstattung spielen ebenfalls eine Rolle. Aktuelle Medienberichte zu Virenattacken in der Presse können zu einer momentan erhöhten Wachsamkeit – also einer zumindest kurzfristigen Verhaltensänderung – führen (Coleman 1993). Das gleiche gilt für Erfahrungsberichte aus dem persönlichen Umfeld, wenn z.B. Arbeitskollegen, Freunde oder Verwandte von erlebten IT-Angriffen erzählen (Wash, 2010).

Des Weiteren gibt es noch eine Reihe IT-spezifischer Einflussfaktoren. Zu den untersuchten Faktoren, die das menschliche Verhalten bei der Benutzung von IT-Sicherheitssystemen beeinflussen, gehören die Selbsteinschätzung des IT-Wissens und die Erfahrungen mit Angriffen auf die IT-Sicherheit. Einhergehend mit der Selbsteinschätzung ist auch die Einsicht in die Wirksamkeit des IT-Sicherheitssystems seitens des Nutzers von Bedeutung für sein Verhalten. Fallen z.B. fehlende Kenntnis der Wirksamkeit oder Nützlichkeit zusammen mit einer gewissen Unbequemlichkeit in der Handhabung der Maßnahmen, so neigen Nutzer dazu, Sicherheitsregeln zu umgehen oder unwirksam zu machen (Adams & Sasse, 1999).

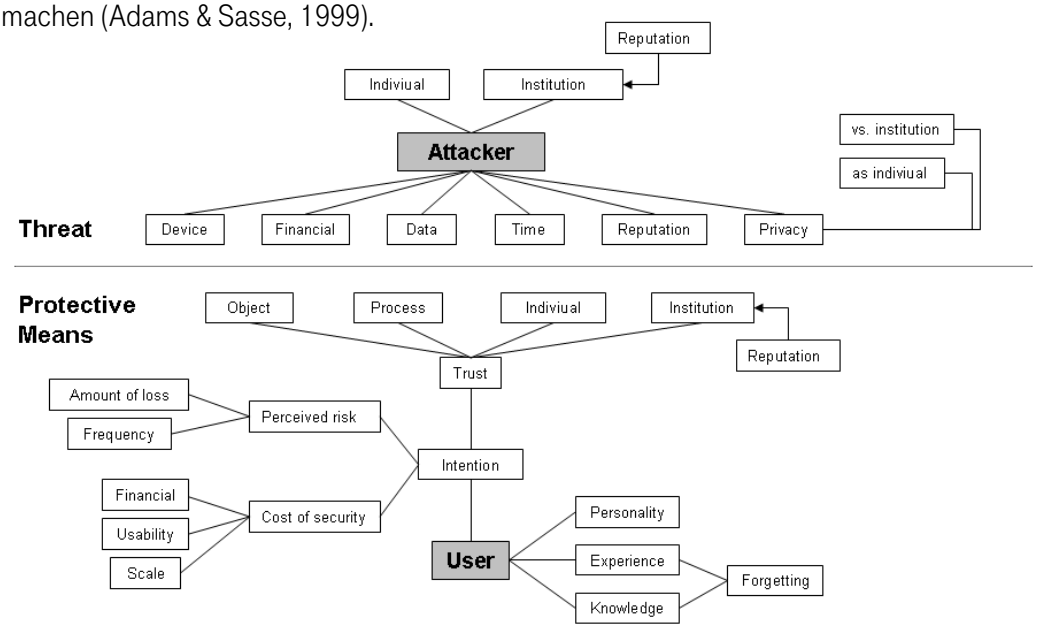

Abb. 1: Taxonomie von Einflussfaktoren auf das Nutzerverhalten (Sieger et al., 2011).

Neben den Sicherheitsaspekten hat natürlich auch die Gebrauchstauglichkeit des Systems einen großen Einfluss auf das Nutzerverhalten. Dies bezieht sich auf die Anordnung der Elemente einer Nutzerschnittstelle, ihre Beschriftung, sowie die Reihenfolge der Interaktionsschritte. Hierbei sollten die kognitiven Mehrbelastungen durch die Sicherheitsmethoden minimiert werden, um diese gegenüber den eigentlichen Handlungszielen nicht ungünstig in der Kosten-Nutzen-Abwägung erscheinen zu lassen; ansonsten kann es zu einer Unterminierung des Sicherheitsziels kommen (Adams & Sasse, 1999). Die kognitiven Kosten für die Einhaltung von Sicherheitsrichtlinien addieren sich in den meisten Fällen zu denjenigen des eigentlichen Handlungsziels, wie sich aus Untersuchungen zur kognitiven Belastung von Authentifizierungsmethoden entnehmen lässt (Renaud, 2005; Uzoka et al., 2009; Weir et al., 2009). In einer konkreten Nutzungssituation gibt es seitens des Nutzers implizit Abschätzungen bezüglich der persönlichen Kosten-Nutzen-Relation zwischen dem gewünschten Ziel und dem dazu aus Nutzersicht – d.h. anhand seines vorhandenen IT-Wissens – nötigen Aufwand. Hierbei neigen viele Nutzer dazu, den zur Bereitstellung von Sicherheit und Privatsphäre erforderlichen Aufwand als zu hoch anzusehen. Die mögliche Höhe des Verlusts muss in einem sinnvollen Verhältnis zu dem zu betreibenden Sicherheitsaufwand stehen: Erscheint dem Laien die Möglichkeit eines erfolgreichen Angriffs zu gering, so werden Sicherheitssysteme ignoriert, abgeschaltet oder unterwandert (Herley 2009).

3 Vorhersage von Nutzerverhalten

Modelle des Nutzerverhaltens wurden und werden mit unterschiedlichen Zielsetzungen erstellt, auf unterschiedlichen Abstraktionsniveaus und mit unterschiedlichen Ergebnissen. Zu den bekanntesten Modellansätzen zählen kognitive Modelle, welche die Interaktion von Komponenten menschlicher Wahrnehmung, Erkennung und Aktion beschreiben (bspw. EPIC, Meyer & Kieras, 1997; ACT-R, Anderson & Lebiere, 1998; oder SOAR, Newell, 1990), GOMS-Modelle, welche die menschlichen Fähigkeit zur Problemlösung formalisiert (Goals, Operators, Methods, and Selection Rules; vgl. Card et al., 1983), statistische Modelle, welche auf Basis empirischer Daten und maschinellem Lernens Wahrscheinlichkeiten von Nutzeraktionen antizipieren (bspw. Araki & Doshita, 1997), sowie regelbasierte Modelle (bspw. López-Cózar et al., 2003), welche prototypisches Nutzerverhalten anhand von Regeln aus den Eigenschaften der Systems und des Nutzers ableiten.

Generell nimmt man an, dass das Nutzerverhalten durch das sog. mentale Modell, welches sich ein Nutzer vom System macht, beeinflusst wird (vgl. Raja 2009). Die Untersuchung dieses mentalen Modells kann Aufschluss über eine geeignete Modellierung im Sinne der o.a. Modelltypen geben. So zeigten bspw. Asgharpour et al. (2007), dass sich die mentalen Modelle von erfahrenen und unerfahrenen Computernutzern deutlich bezüglich der wahrgenommenen Risiken unterscheiden. Ein Verhaltensmodell für den hier vorliegenden Fall sollte daher neben Systemeigenschaften auch die o.a. Einflussfaktoren auf das Nutzerverhalten berücksichtigen. Wir schlagen vor, dies mit Hilfe von Regeln zu tun, welche vorgegebene Wahrscheinlichkeiten für bestimmte Nutzeraktionen verändern.

Ausgehend von diesen Überlegungen wurde an der TU Berlin die sog. MeMo-Werkbank entwickelt (Möller et al., 2006). Diese formalisiert Mensch-Computer-Interaktionen durch 4 ausführbare Modelle: Ein Aufgabenmodell des Systems (beschreibt, welche Aufgaben mit Hilfe des Systems erledigt werden können), ein Interaktionsmodell des Systems (beschreibt anhand eines Zustandsgraphen, wie eine Aufgabe mit Hilfe des Systems gelöst werden kann), ein Aufgabenmodell des Nutzers (welches vom System-Aufgabenmodell abweichen kann, wenn divergierende Ziele verfolgt werden), und ein Interaktionsmodell des Nutzers (beschreibt, welche Schritte vom Nutzer voraussichtlich während der Interaktion durchlaufen werden). Die Systemmodelle lassen sich sehr einfach vom Entwickler spezifizieren. Das Nutzer-Aufgabenmodell kann durch gezielte Abweichungen vom System-Aufgabenmodell abgeleitet werden.

Interessant ist hier vor allem das Nutzer-Interaktionsmodell. Dieses belegt zunächst mögliche Pfade durch die Systemzustände mit Wahrscheinlichkeiten. Dabei wird dem direkten (zielführenden) Pfad normalerweise die größte Wahrscheinlichkeit zugewiesen, auf Basis von zunächst empirisch ermittelten Daten. Von diesem direkten Pfad werden nun mittels Wenn-Dann-Regeln gezielt Abweichungen generiert. Diese können als Bedingung Eigenschaften des Systems (bspw. ein Bedienfeld befindet sich an der falschen Stelle oder ein Link ist nicht durch Unterstrich kodiert und wird deshalb voraussichtlich nicht gefunden) oder Eigenschaften des Nutzers (bspw. der Nutzer ist der englischen Sprache nicht mächtig und kann deshalb eine englische Beschriftung nicht interpretieren) enthalten, und Erhöhen dann die Wahrscheinlichkeit für Abweichungen vom zielführenden Pfad.

Bei sicherheitsrelevanten Funktionen kann man wegen der eingangs angesprochenen Primär- und Sekundäraufgabenproblematik nicht von zielführenden Pfaden sprechen, aber dies ist auch nicht notwendig, denn alle Pfade (die der Primäraufgabe und die der sekundären Sicherheitsaufgabe) können mit Wahrscheinlichkeiten belegt werden, welche dann durch entsprechende Regeln verändert werden. Entsprechend den Wahrscheinlichkeiten kann dann auf Knopfdruck eine Vielzahl von möglichen Nutzerinteraktionen mit dem System (bzw. seinem Systemmodell) simuliert werden. Diese Simulationen werden aufgezeichnet und die Log-Daten nach verschiedenen Kriterien ausgewertet. Bspw. kann der Entwickler die Ursachen von nicht sicherheitskonformem Verhalten in Form der es verur-

sachenden Wahrscheinlichkeiten und Regeln bestimmen. Die Regeln spiegeln das beobachtete Verhalten von Nutzern wider und sollten von Experten auf Basis empirischer Tests definiert werden. Bislang zeigte sich, dass eine geringe Anzahl (20-30) von Regeln bereits zu recht guten relativen Vorhersagen beim Vergleich verschiedener Systemvarianten ausreichen.

Die modifizierte Tetris-Applikation wurde mit der MeMo-Werkbank modelliert, und die simulierten Interaktionen wurden mit experimentell beobachtetem Nutzerverhalten verglichen. Dabei konnten zwei wichtige empirisch beobachtete Effekte auch in der Simulation adäquat nachgestellt werden: Nutzer, die häufiger Sicherheitsangriffen ausgesetzt wurden, legten ein risikobewussteres Spielverhalten an den Tag; Nutzer mit einem zuverlässigen Alarmsystem halten sich häufiger an die Warnungen als Nutzer eines unzuverlässigen Alarmsystems. Die Modellierung solcher Effekte zeigt, dass durch eine adäquate Simulation Nutzerverhalten in kritischen Kompromiss-Situationen (hier Spielen vs. Aufwände für Sicherheitsmechanismen und damit Zeit- und Punktverlust) zumindest bezüglich der relativen Ausprägung im Vergleich verschiedener Systemvarianten richtig beschrieben werden kann. Mit der einmal trainierten MeMo-Werkbank kann diese Simulation automatisch und auch vergleichend mit unterschiedlichen Systemvarianten erfolgen, ohne Zuhilfenahme von Probanden.

4 Ausblick

In diesem Beitrag wurde eine nutzerzentrierte Sicht auf die Gestaltung sicherheitskritischer und die Privatsphäre berührender IT-Systeme nahegelegt. Dazu wurden zunächst Einflussfaktoren auf das Nutzerverhalten identifiziert, und es wurde ein neues Verfahren zur automatischen Simulation von Nutzerverhalten beschrieben. Dieses Verfahren kann den Entwicklungsprozess auf effiziente Weise dahingehend unterstützen, dass optimale Kompromisse zwischen einer hohen Gebrauchstauglichkeit einerseits und hohen Sicherheitsanforderungen andererseits gefunden werden; es legt damit einen Grundstein für ein Security & Privacy Engineering, welches Sicherheitsziele im Entwicklungsprozess verankert und dabei die Interessen der Nutzer wahrt.

Das Verfahren wurde bislang nur in einer künstlichen Mikrowelt gestestet. Aktuell überprüfen wir, ob es auch mit einem realen Bezahlsystem in realistischen Versuchsumgebungen korrekte Ergebnisse liefert. Hierbei soll neben dem Sicherheitsaspekt auch die Privatsphäre der Nutzer sowie das dafür relevante Nutzerverhalten analysiert werden. Daneben möchten wir weitere nutzerzentrierte Methoden in einen Security & Privacy Engineering Lifecycle integrieren. Wir sind überzeugt, dass sich damit auf effiziente Weise Widersprüche zwischen gegenläufigen Nutzeranforderungen auflösen lassen und somit insgesamt sicherere, die Privatsphäre respektierende IT-Systeme gestalten lassen. Letztendlich werden sich Sicherheitsanforderungen nur dann realistisch erfüllen lassen, wenn neben der technischen Sicherheit auch das Nutzerverhalten quantitativ erfasst und in Anforderungsprofilen berücksichtigt werden kann.

5 Danksagung

Die beschriebene Nutzersimulation wurde im Rahmen des durch die Deutsche Telekom AG geförderten Projektes „Usability & Security“ an der TU Berlin und der Ben-Gurion University of the Negev implementiert. Die Autoren danken Klaus-Peter Engelbrecht und Noam Ben-Asher für ihre Arbeiten im Rahmen dieses Projektes.

6 Literatur

Adams, A., Sasse, M.A. (1999). “*Users Are Not the Enemy*”, Communications of the ACM, 42(12), 40-46.

Anderson, J.R., Lebiere, C. (1998). “*The Atomic Components of Thought*”, Lawrence Erlbaum Associates, Mahwah NJ.

Araki, M., Doshita, S. (1997). “*Automatic Evaluation Environment for Spoken Dialogue Systems*”, Proc. ECAI’96: Workshop on Dialogue Processing in Spoken Language Systems, Springer, London, 183–194.

Asgharpour, F., Liu, D., Camp, J.L. (2007). “*Mental Models of Computer Security Risks*”, Proc. Workshop on the Economics of Information Security.

Ben-Asher, N., Meyer, J., Parmet, Y., Möller, S., Englert, R. (2010). ”*An Experimental Microworld for Evaluating the Tradeoffs Between Usability and Security*”, in: Symposium On Usable Privacy and Security (SOUPS) 2010, Usable Security Experiment Reports (USER) Workshop, July 14-16, Redmond WA.

Card, S.K., Moran, T.P., Newell, A. (1983). “*The Psychology of Human-Computer Interaction*”, Lawrence Erlbaum, Hillsdale NJ.

Coleman, C.-L. (1993), “*The Influence of Mass Media and Interpersonal Communication on Societal and Personal Risk Judgments*”, Communication Research, 20:611-628.

Engelbrecht, K.-P., Quade, M., Möller, S. (2009). “*Analysis of a New Simulation Approach to Dialogue System Evaluation*”, Speech Communication 51, 1234-1252.

Fischer-Hübner, S., Grimm, R., Lo Iacono, L., Möller, S., Müller, G., Volkamer, M., (2011). „*Gebrauchstaugliche Informationssicherheit. ‚Usable Security and Privacy‘*“, in: <kes> – Die Zeitschrift für Informations-Sicherheit 4/2011, SecuMedia Verlags-GmbH, Ingelheim, 6-10.

Herley, C. (2009). “*So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users*”, NSPW09, Oxford.

López-Cózar, R., de la Torre, A., Segura, J.C., Rubio, A.J. (2003). “*Assessment of Dialogue Systems by Means of a New Simulation Technique*”, Speech Communication 40(3), 387–407.

Meyer, D.E., Kieras, D.E. (1997). ”*A Computational Theory of Executive Cognitive Processes and Multiple-task Performance: Part 2. Accounts of Psychological Refractoryperiod Phenomena*”, Psychological Review 104, 749-791.

Möller, S., Ben-Asher, N., Engelbrecht, K.-P., Englert, R., Meyer, J. (2011). "*Modeling the Behavior of Users Who are Confronted with Security Mechanisms*", Computers & Security 30, 242-256.

Möller, S., Englert, R., Engelbrecht, K., Hafner, V., Jameson, A., Oulasvirta, A., Raake, A., Reithinger, N. (2006). "*MeMo: Towards Automatic Usability Evaluation of Spoken Dialogue Services by User Error Simulations*", in: Proc. 9th Int. Conf. on Spoken Language Processing (Interspeech 2006 – ICSLP), Pittsburgh PA, 1786-1789.

Newell, A. (1990). "*Unified Theories of Cognition",* Harvard University Press, Cambridge MA.

Raja, F.; Hawkey, K. & Beznosov, K. (2009). "*Revealing Hidden Context: Improving Mental Models of Personal Firewall Users*", Proc. of the 5th Symposium on Usable Privacy and Security, 1-12.

Renaud, K. (2005). "*Evaluating Authentication Mechanisms*", Cranor, L.F., Garfinkel, S. (Eds.), Security and Usability. O'Reilly, pp. 103–128.

RISEPTIS Group (2009). "*Trust in the Information Society*", European Commission and Think-Trust, Brussels.

Sieger, H., Kirschnick, N., Möller, S. (2011). "*Poster: Towards a User Behavior Model in Computer Security*", in: Proc. 2011 Symposium On Usable Privacy and Security (SOUPS 2011), July 20-11, Pittsburgh PA.

Tognazzini, B. (2005). "*Design for Usability*", Security and Usability: Designing Secure Systems that People Can Use, Lorrie Faith Cranor and Simson Garfinkle, ed., O'Reilly, August, 1, 31 – 46.

Uzoka F.M.E and Nzinge T. (2009). "*Empirical Analysis of Biometric Technology Adoption in Botswana*", Journal of Software and Systems, 82: 1550-1564, Elsevier.

Wash, R. (2010). "*Folk Models of Home Computer Security*", Symposium on Usable Privacy and Security.

Weir, C. S., Douglas, G., Carruthers, M., Jack, M. A. (2009). "*User Perceptions of Security, Convenience and Usability for eBanking Authentication Tokens*", Computers and Security, 28, 47–62.

Zimbardo, P., Gerrig, R. (2008). „Psychologie", 18. Auflage. Pearson Studium, München.

Zuckerman, M., Kuhlman, D.M. (2000). „*Personality and Risk-Taking: Common Bisocial Factors*", Journal of Personality, Volume 68, Issue 6, pages 999–1029.