USecureD

Guideline-Template

Deliverable E2.1c

Projekt	USecureD – Usable Security by Design
Förderinitiative	Einfach intuitiv – Usability für den Mittelstand
Förderkennzeichen	01MU14002
Arbeitspaket	AP 2.1
Fälligkeit	–
Autor	Hartmut Schmitt (HK Business Solutions)
Status	final
Klassifikation	öffentlich

HKBS

HK Business Solutions GmbH
Hartmut Schmitt
Mellinweg 20
66280 Sulzbach
schmitt@hk-bs.de

KMU
(Konsortialführer)

Technology
Arts Sciences
TH Köln

Technische Hochschule Köln
Prof. Dr.-Ing. Luigi Lo Iacono
Betzdorfer Straße 2
50679 Köln
luigi.lo_iacono@th-koeln.de

Hochschule
(Konsortialpartner)

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Abstract

Im Projekt USecureD werden Musterlösungen und praxistaugliche Werkzeuge entwickelt, die kleine und mittlere Unternehmen (KMU) bei der Entwicklung bzw. bei der Auswahl betrieblicher Anwendungssoftware mit dem Qualitätsmerkmal „Usable Security“ unterstützen.

Ziel von Teilarbeitspaket AP 2.1 war es, Entwurfswerkzeuge wie Patterns und Entwicklungsrichtlinien zu entwickeln, die Softwarearchitekten und Entwickler bei der Auswahl und Umsetzung benutzerfreundlicher Sicherheitsfunktionen und -mechanismen im Kontext betrieblicher Anwendungssoftware unterstützen. Im Rahmen dieser Arbeiten wurde ein Beschreibungstemplate für Entwicklungsrichtlinien (Guidelines) entwickelt, die eine systematische Herstellung von Gestaltungslösungen mit dem Qualitätsmerkmal Usable Security unterstützen.

Schlagworte

Template, Beschreibungsvorlage, Guideline, Entwicklungsrichtlinie, Richtlinie, Usable Security, IT-Security

Inhaltsverzeichnis

1 Aufgabenstellung

Entwicklungsrichtlinien (Design Guidelines) sind wichtig, um bereits bei der Entwicklung von Systemen möglichst viele Ursachen für spätere Schwachstellen zu eliminieren [vgl. Birolini 1997]. Werden Richtlinien im Rahmen der Softwareentwicklung eingesetzt, tragen sie zur Gewährleistung einer besseren Softwarequalität bei und verringern gleichzeitig die Komplexität von Entwicklungsprojekten.

Zielstellung innerhalb des USecureD-Projekts war es, praxisgerechte Entwicklungsrichtlinien zu definieren, die Softwarehersteller in die Lage versetzen, strukturiert betriebliche Anwendungssysteme mit dem Qualitätsmerkmal gebrauchstauglicher Informationssicherheit zu entwickeln. Diese USecureD- Richtlinien sollten so konzipiert sein, dass sie als Arbeitsgrundlage für Softwareingenieure bzw. Systementwickler und zugleich als Kommunikationsbasis im Entwicklungsteam dienen können. Sie sollten mit besonderem Augenmerk auf betriebliche Anwendungssysteme entwickelt und ausgestaltet werden, jedoch auch auf andere Anwendungsdomänen übertragbar sein.

Ein weiteres Ziel dieses USecureD-Teilarbeitspakets war es, die entwickelten Richtlinien mit zusätzlichen Ressourcen und weiterführenden Informationen anzureichern (z.B. mit Umsetzungsbeispielen, Hinweisen zur Wirkungsweise und zu vertiefender Literatur). Hierdurch werden dem Softwareingenieur bzw. -entwickler nachvollziehbare Entscheidungshilfen zur Verwendung einzelner bzw. zur sinnvollen Kombination mehrerer Guidelines bei der Dialog- und Interaktionsgestaltung gegeben. Ferner sollten sämtliche USecureD-Richtlinien in Form einer konsolidierten, frei zugänglichen Sammlung zur Verfügung zu gestellt werden, die es je nach Qualitätszielen, technischen Aspekten o. ä. erlaubt, eine Auswahl aus den universalen Entwicklungsrichtlinien zu treffen und diese bei Bedarf individuell anzupassen.

Diese Zielsetzung machte es erforderlich, eine Beschreibungsvorlage zu erstellen, mit der alle erstellten Richtlinien einheitlich und in einem gut leserlichen Format dokumentiert werden können. Die Vorgehensweise zur Entwicklung dieses Guideline-Templates wird im folgenden Abschnitt beschrieben.

2 Vorgehensweise

Um eine geeignete Beschreibungsvorlage zu entwickeln, wurden zunächst allgemeine Informationen zu Richtlinien recherchiert, insbesondere zu Usability Guidelines ([Beschnitt 2009a-c], [Lynch & Horton 2009], [Nielsen 2005]).

Im nächsten Schritt wurden diverse Veröffentlichungen zu Guidelines bzw. frei zugängliche Guideline-Sammlungen untersucht, insbesondere hinsichtlich Aufbau und Strukturierung der Guidelines. Die Autoren bzw. Herausgeber dieser Guidelines waren Wissenschaftler, (Berufs-)Verbände, Organisationen (Regierungsbehörden, NGOs) und Software- bzw. Systemhersteller.

Thematisch können die untersuchten Guidelines unterschieden werden in

- **Usable Security** Guidelines
  - Usable Security Guideline Sets: [Chiasson et al. 2007], [Herzog & Shahmehri 2007], [Hof 2012], [Nurse et al. 2011], [Yee 2002], [Yee 2005])
  - Arbeiten, die einzelne Guidelines vorstellen bzw. Hinweise zu Guidelines enthalten: [Bravo-Lillo 2011], [Furnell et al. 2007], [Hardee et al. 2006], [Johnston et al. 2003], [Sasse et al. 2001], [Whitten 2004], [Whitten & Tygar 1999]
- allgemeine Richtlinien für die **Gestaltung von Benutzeroberflächen**: [Mayhew 1992], [Smith & Mosier 1986]
- **Usability** Guidelines
  - Usability-Guideline-Sammlungen: [gUPA 2012], [Shneiderman & Plaisant 2004]
  - Usability-Heuristiken: [Nielsen 1994], [Nielsen 1995]
  - Guidelines für Texte in Masken [Microsoft 2010b] bzw. Meldungen [Microsoft 2010a]
  - Arbeiten zur Fehlersicherheit [Laubheimer 2015] bzw. Fehlertoleranz [Nielsen 2001]
- **Accessibility** Guidelines: [AARP 2004], [Pernice & Nielsen 2015]
- **User Experience** Guidelines: [Pandhi 2006]
- **Trust** Design Guidelines: [Patrick et al. 2005]
- **Privacy** Guidelines: [Microsoft 2008]
- Guidelines für die Erstellung von (Business) **Websites** bzw. **Onlineshops**: [Bevan 2005], [HHS 2006], [Lynch & Horton 2009], [Nielsen & Tahir 2001], [Travis 2015], [WSA 2008]
- Guidelines für die Herstellung von **Apps**: [Boswell 2012]
- **Security** Guidelines
  - Security-Guideline-Sammlungen: [BSI 2012], [Checkmarx 2015], [Levin et al. 2007], [OWASP 2010], [Ross et al. 2014], [SAFECode 2011]
  - Guidelines zum Umgang mit Passwörtern [GCHQ & CPNI 2015]

Im Rahmen der Sammlung und Konsolidierung dieser Guidelines – Strukturierung, Bilden von Clustern, Verschlagwortung – bildete sich die im Folgenden vorgestellte Beschreibungsvorlage heraus. Diese wurde von den Projektpartnern unter Forschungs- und Praxisgesichtspunkten abgestimmt und anschließend für die Erstellung bzw. Dokumentation der USecureD-Richtlinien genutzt.

Durch die Dokumentation der USecureD-Richtlinien wurde sichergestellt, dass das entwickelte Guideline-Template für die Zwecke im USecureD-Projekt geeignet ist. Bei der Erstellung der USecureD-Richtlinien wurden in vielen Fällen Guidelines verschiedener Autoren zusammengeführt, damit eine möglichst gut handhabbare Sammlung von Richtlinien entsteht, über die sich Softwareingenieur bzw. -entwickler, die die primäre Zielgruppe dieser Ergebnisse sind, schnell einen Überblick verschaffen können.

3 Guideline-Template

Name	*eindeutiger Name der Richtlinie*
Quellen	*Quellenangaben und Literaturhinweise zu der beschriebenen Richtlinie*
Synonyme	*bekannte Synonyme bzw. anderssprachige Namen für die beschriebene Richtlinie*
Richtlinie	*Formulierung der Richtlinie (in Aufforderungsform und aktiver Sprache)*
Kontext	*Beschreibung der Situation bzw. Ausgangslage, in der eine bestimmte Richtlinie anwendbar ist / angewendet werden sollte*
Beispiele	*bekannte Verwendungen und Illustrationen der beschriebenen Richtlinie*
Verwandte Richtlinien	*Richtlinien, die ein ähnliches Problem adressieren wie die beschriebene Richtlinie oder die in Kombination mit der beschriebenen Richtlinie verwendet werden können*
Kategorie	*Kategorie der Richtlinie (z. B. Usable Security, Usability oder Security)*
Tags	*zur Richtlinie passende Schlagworte, um die Durchsuchbarkeit des Katalogs auf der USecureD-Plattform zu verbessern*
Log history	*Feld zur Protokollierung von Ereignissen, wie zum Beispiel das aktuelle Änderungsdatum der Richtlinie*

4 Beispiel-Richtlinie

Name	Sichtbarer Sicherheitszustand
Quellen	(Nurse u. a. 2011)
Synonyme	Allow for visibility of system state
Richtlinie	Mache den aktuellen Sicherheitszustand des Systems für den Nutzer sichtbar.
Kontext	Ein System sollte den Nutzer jederzeit angemessen darüber informieren, was gerade passiert (Nielsen 1995). Die Anzeige des aktuellen Sicherheitszustands kann in vielen Fällen genutzt werden, um dem Nutzer ein passives Feedback über die Informationssicherheit zu geben. Die Anzeige des aktuellen Sicherheitszustands trägt zum Aufbau von Vertrauen bei und gilt daher als Kriterium für erfolgreiche Mensch-Maschine-Interaktion in Sicherheitsanwendungen ((Johnston, Eloff, und Labuschagne 2003), (Nielsen 1994), (Yee 2002)). Die Anzeige des aktuellen Zustands darf allerdings nicht aufdringlich sein (Herzog 2007), z. B. darf der Nutzer nicht die gesamte Zeit mit Sicherheitswarnungen konfrontiert werden (Sasse, Brostoff, und Weirich 2001).
Beispiele	Beispiele für die Anzeige des aktuellen Sicherheitszustands sind Begriffe wie “Passwort-Schutz” oder “verschlüsselt” bei passwortgeschützten bzw. verschlüsselten Dokumenten, aktive Symbole, wenn in einem System momentan Sicherheitsfunktionen ausgeführt werden, oder Vorhängeschlösser, um in Browsern die Verwendung von Secure Sockets Layer (SSL) bzw. Transport Layer Security (TLS) anzuzeigen (Nurse u. a. 2011).
Verwandte Richtlinien	[Sichtbare Sicherheitsfunktionen]
Kategorie	Usable Security
Tags	Sichtbarer Sicherheitszustand, Sichtbare Sicherheitsfunktionen, Selbstbeschreibungsfähigkeit, Vertrauen
Log history	[04/26/2016]: Added to repository

5 Quellen

[AARP 2004] American Association of Retired Persons (2004): AARP Audience-Centered Heuristics. Verfügbar unter: http://redish.net/images/stories/PDF/AARP%20Audience-Centered%20Heuristics.pdf [11.07.2016]

[BESCHNITT 2009a] Martin Beschnitt (2009): Usability-Guidelines: Teil 1 – Definition & Abgrenzung. Verfügbar unter: http://www.usabilityblog.de/2009/08/usability-guidelines-teil-1-definition-abgrenzung/ [11.07.2016]

[BESCHNITT 2009b] Martin Beschnitt (2009): Usability-Guidelines: Teil 2 – Vor- & Nachteile. Verfügbar unter: http://www.usabilityblog.de/2009/08/usability-guidelines-teil-2-vor-nachteile/ [11.07.2016]

[BESCHNITT 2009c] Martin Beschnitt (2009): Usability-Guidelines: Teil 3 – Bestehende Guideline-Sets. Verfügbar unter: http://www.usabilityblog.de/2009/09/usability-guidelines-teil-3-bestehende-guideline-sets/ [11.07.2016]

[BEVAN 2005] Nigel Bevan (2005): Guidelines and Standards for Web Usability. In: Proceedings of HCI International 2005, Lawrence Erlbaum, Hillsdale, NJ

[BIROLINI 1997] Alessandro Birolini (1997): Zuverlässigkeit von Geräten und Systemen. Springer, Berlin

[BOSWELL 2012] Wendy Boswell (2012): App Usability Guidelines from a User Perspective. Verfügbar unter: https://software.intel.com/en-us/blogs/2012/11/13/app-usability-guidelines-from-a-user-perspective [11.07.2016]

[BRAVO-LILLO 2011] Cristian Antonio Bravo-Lillo (2011): Improving Computer Security Dialogs: An Exploration of Attention and Habituation. Dissertation, Carnegie Mellon University, Pittsburgh, PA

[BSI 2012] Bundesamt für Sicherheit in der Informationstechnik BSI (2012): Leitfaden Informationssicherheit: IT-Grundschutz kompakt. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf [11.07.2016]

[CHECKMARX 2015] Checkmarx Inc. (2015): Secure Development Kit. Verfügbar unter: https://www.checkmarx.com/wp-content/uploads/2015/10/Poster.pdf [11.07.2016]

[CHIASSON ET AL. 2007] Sonia Chiasson, Robert Biddle, Anil Somayaji (2007): Even Experts Deserve Usable Security: Design guidelines for security management systems. In: Symposium on Usable Security and Privacy (SOUPS) Workshop at Usable IT Security Management (USM), S. 1-4

[FURNELL ET AL. 2007] Steven Furnell, Dimitris Katsabas, Paul Dowland, Fraser Reid (2007): A Practical Usability Evaluation of Security Features in End-User Applications. In: Hein Venter, Mariki Eloff, Les Labuschagne, Jan Eloff, Rossouw Solms (Hrsg): New Approaches for Security, Privacy and Trust in Complex Environments: Proceedings of the IFIP TC-11 22nd International Information Security Conference (SEC 2007), S. 205–216. Springer US

[GCHQ & CPNI 2015] Government Communications Headquarters & Centre for the Protection of National Infrastructure (2015): Password Guidance: Simplifying Your Approach. Verfügbar unter: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf [11.07.2016]

[GUPA 2012] German UPA e.V., Arbeitskreis Qualitätsstandards (2012): German UPA Qualitätsstandard für Usability Engineering. Verfügbar unter: http://germanupa.de/data/mediapool/n070_qualitaetsstandard_der_german_upa.pdf [11.07.2016]

[HARDEE ET AL. 2006] Jefferson B. Hardee, Ryan West, Christopher B. Mayhorn (2006): To Download or Not to Download: An Examination of Computer Security Decision Making. interactions - A contradiction in terms? 13(3), S. 32–37. ACM, New York, NY

[HERZOG & SHAHMEHRI 2007] Almut Herzog, Nahid Shahmehri (2007): Usable Set-up of Runtime Security Policies. Information Management & Computer Security 15(5), S. 394-407. Emerald Group

[HHS 2006] Health and Human Services (2006): Research-Based Web Design & Usability Guidelines. Verfügbar unter: http://www.usability.gov/sites/default/files/documents/guidelines_book.pdf [11.07.2016]

[HOF 2012] Hans-Joachim Hof (2012): User-Centric IT Security: How to Design Usable Security Mechanisms. In: Lasse Berntzen, Stephan Böhm, Guadalupe Ortiz (Hrsg.): CENTRIC 2012 - The Fifth International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, S. 7-12. IARIA

[JOHNSTON ET AL. 2003] J. Johnston, Jan Eloff, Les Labuschagne (2003). Features: Security and Human Computer Interfaces. In: Computers and Security 22 (8), S. 675–684. Elsevier Advanced Technology Publications, Oxford

[LAUBHEIMER 2015] Page Laubheimer (2015): Preventing User Errors: Avoiding Unconscious Slips. Verfügbar unter: https://www.nngroup.com/articles/slips/ [11.07.2016]

[LEVIN ET AL. 2007] Timothy E. Levin, Cynthia E. Irvine, Terry V. Benzel, Ganesha Bhaskara, Paul C. Clark, Thuy D. Nguyen (2007): Design Principles and Guidelines for Security. SecureCore Technical Report. Verfügbar unter: ftp://ftp.isi.edu/isi-pubs/tr-648.pdf [11.07.2016]

[LYNCH & HORTON 2009] Patrick J. Lynch, Sarah Horton (2009): Contents Web Style Guide 3. Verfügbar unter: http://webstyleguide.com/wsg3/ [11.07.2016]

[MAYHEW 1992] Deborah J. Mayhew (1992): Principles and Guidelines in Software User Interface Design. Prentice Hall, Englewood Cliffs, NJ

[MICROSOFT 2008] Microsoft Corporation (2008). Privacy Guidelines for Developing Software Products and Services, Version 3.1. Verfügbar unter: http://download.microsoft.com/download/3/8/5/385BEAE9-72E9-4F7F-A798-9D54F896351A/privacy_guidelines_for_developers.pdf [11.07.2016]

[MICROSOFT 2010a] Microsoft Corporation (2010): Error and Informational Message Guidelines. Verfügbar unter: https://msdn.microsoft.com/en-us/library/bb158646.aspx [11.07.2016]

[MICROSOFT 2010b] Microsoft Corporation (2010): User Interface Text Guidelines. Verfügbar unter: https://msdn.microsoft.com/en-us/library/bb158574.aspx [11.07.2016]

[NIELSEN 1994] Jakob Nielsen (1994): Usability Inspection Methods. John Wiley & Sons, New York, NY

[NIELSEN 1995] Jakob Nielsen (1995): 10 Usability Heuristics for User Interface Design. Verfügbar unter: https://www.nngroup.com/articles/ten-usability-heuristics/ [11.07.2016]

[NIELSEN 2001] Jakob Nielsen (2001): Error Message Guidelines. Verfügbar unter: https://www.nngroup.com/articles/error-message-guidelines/ [11.07.2016]

[NIELSEN 2005] Jakob Nielsen (2005): Sixty Guidelines From 1986 Revisited. Verfügbar unter: https://www.nngroup.com/articles/sixty-guidelines-from-1986-revisited/ [11.07.2016]

[NIELSEN & TAHIR 2001] Jakob Nielsen, Marie Tahir (2001): Homepage Usability: 50 Websites Deconstructed. New Riders Publishing, Thousand Oaks, CA

[NURSE ET AL. 2011] Jason R. C. Nurse, Sadie Creese, Michael Goldsmith, Koen Lamberts (2011): Guidelines for Usable Cybersecurity: Past and Present. In: 2011 Third International Workshop on Cyberspace Safety and Security (CSS), S. 21-26. IEEE

[OWASP 2010] OWASP Foundation (2010): OWASP Secure Coding Practices: Quick Reference Guide. Verfügbar unter: https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf [11.07.2016]

[PANDHI 2006] Dax Pandhi (2006). How to Create the Best User Experience for Your Application. Verfügbar unter: https://msdn.microsoft.com/en-us/library/aa468595.aspx [11.07.2016]

[PATRICK ET AL. 2005] Andrew S. Patrick, Pamela Briggs, Stephen Marsh (2005): Designing systems that people will trust. In: Lorrie Faith Cranor & Simson Garfinkel (Hrsg.): Security and Usability: Designing Secure Systems That People Can Use, S. 75-99, O'Reilly, Sebastopol, CA

[PERNICE & NIELSEN 2015] Kara Pernice, Jakob Nielsen (2015): Usability Guidelines for Accessible Web Design. Verfügbar unter: https://www.nngroup.com/reports/usability-guidelines-accessible-web-design/ [11.07.2016]

[ROSS ET AL. 2014] Ron Ross, Janet Carrier Oren, Michael McEvilley (2014): Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems (NIST Special Publication 800-160 - Initial Public Draft). Verfügbar unter: http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf [11.07.2016]

[SAFECODE 2011] SAFECode - Software Assurance Forum for Excellence in Code (2011): Fundamental Practices for Secure Software Development. 2. Auflage. Verfügbar unter: http://www.safecode.org/publication/SAFECode_Dev_Practices0211.pdf [11.07.2016]

[SASSE ET AL. 2001] Martina Angela Sasse, Sacha Brostoff, Dirk Weirich (2001): Transforming the “Weakest Link”: A Human-Computer Interaction Approach for Usable and Effective Security. In: BT Technology Journal 19(3), S. 122–131. Kluwer Academic Publishers, Hingham, MA

[SHNEIDERMAN & PLAISANT 2004] Ben Shneiderman, Catherine Plaisant (2004): Designing the User Interface: Strategies for Effective Human-Computer Interaction, 4. Auflage, Addison-Wesley, Boston, MA

[SMITH & MOSIER 1986] Sidney L. Smith, Jane N. Mosier (1986): Guidelines for designing user interface software. Verfügbar unter: http://hcibib.org/sam/ [11.07.2016]

[TRAVIS 2015] David Travis (2015): 247 web usability guidelines. Verfügbar unter: http://www.userfocus.co.uk/resources/guidelines.html [11.07.2016]

[WHITTEN 2004] Alma Whitten (2004): Making Security Usable. Dissertation, Carnegie Mellon University, Pittsburgh, PA

[WHITTEN & TYGAR 1999] Alma Whitten, J. D. Tygar (1999): Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: Proceedings of the 8th Conference on USENIX Security Symposium, Washington, D.C.

[WSA 2008] Website Standards Association (2008): Business Website Usability Guidelines. Verfügbar unter: http://websitestandards.org/images/WSAUsabilityDraft.pdf [11.07.2016]

[YEE 2002] Ka-Ping Yee (2002): User Interaction Design for Secure Systems. In: ICICS '02 Proceedings of the 4th International Conference on Information and Communications Security, S. 278–290, Springer, London

[YEE 2005] Ka-Ping Yee (2005): Guidelines and strategies for secure interaction design. In: Lorrie Faith Cranor & Simson Garfinkel (Hrsg.): Security and Usability: Designing Secure Systems That People Can Use, S. 247-273, O'Reilly, Sebastopol, CA