Sichere IT-Systeme

Günter Müller, Sven Wohlgemuth

Institut für Informatik und Gesellschaft,
Abteilung Telematik, Friedrichstraße 50
Albert-Ludwigs-Universität Freiburg, D-79098 Freiburg i. Br.
{mueller, wohlgemuth}@iig.uni-freiburg.de

Abstract: Die Entwicklung und Prüfung von sicheren Komponenten und einem sicheren Gesamtsystem ist das Ziel des Schwerpunktprogramm 1079 „Sicherheit in der Informations- und Kommunikationstechnik“ der Deutschen Forschungsgemeinschaft. Dieser Artikel skizziert dieses Schwerpunktprogramm und stellt mit dem Projekt ATUS dessen Beitrag zur Nutzerforschung vor.

1 DFG-Schwerpunktprogramm „Sicherheit in der Informations- und Kommunikationstechnik“

Aufgrund der Vielzahl an persönlichen, mobilen Endgeräten und einer globalen technischen Infrastruktur ist es nicht ausreichend, einzelne Sicherheitsmechanismen vorzugeben. Vielmehr ist IT-Sicherheit nur durch individuell bestimm- und verfügbare Funktionalität, durch deren methodische und evaluierbare Implementierung und durch vertrauenswürdige Sicherheitsinfrastrukturen erreichbar. Daraus ergibt sich die wesentliche Anforderung an die IT-Systeme, dass alle Beteiligten nach dem Konzept der mehrseitigen Sicherheit [RPM97] die aus ihrer Sicht wünschenswerte Sicherheit selbst festlegen können und diese von einem sicheren Gesamtsystem gewährleistet wird.

Ziel des Schwerpunktprogramms „Sicherheit in der Informations- und Kommunikationstechnik“ (SPP Sicherheit), das von der Deutschen Forschungsgemeinschaft (DFG) seit Ende 1999 für die Dauer von sechs Jahren gefördert wird, ist die theoretische Entwicklung sowie die Prüfung von sicheren Komponenten, Systemen und Anwendungen, die zu einem sicheren Gesamtsystem integriert werden [Wo03]. Gemeinsam forschen dreizehn Universitäten und Forschungseinrichtungen an der Konzeption und dem Entwurf dieses sicheren Gesamtsystems anhand eines beispielhaften Kaufs und der Kontrolle einer digitalen Bahnfahrkarte über einen standortbasierten, virtuellen Fahrkartenautomaten [GMW03]. Jedoch entsteht aus sicheren Komponenten nicht notwendigerweise ein sicheres Gesamtsystem. Zur Analyse dieser Hypothese wurde ein Demonstrator aus den sicheren Komponenten der SPP-Projekte implementiert. Im Folgenden und in den nachfolgenden drei Artikeln werden insgesamt vier Projekte stellvertretend für das SPP Sicherheit vorgestellt.

Damit Sicherheitswerkzeuge auch für den Sicherheitslaien einsetzbar werden, ist die Benutzbarkeit eine unbedingte Anforderung an ein sicheres Gesamtsystem. Im SPP Sicherheit untersucht das Projekt ATUS (A Toolkit for Usable Security) der Albert-

Ludwigs-Universität Freiburg den Zusammenhang zwischen Sicherheit *und* Benutzbarkeit.

2 Benutzbare IT-Sicherheit

Die Sicherheit heutiger Systeme wird zu einem erheblichen Umfang von der Bereitschaft der Anwender bestimmt, die verfügbaren Sicherheitsmechanismen zu verwenden. Untersuchungen [Wa98, WhTy99, Ge03] zeigen, dass heutige Benutzungsschnittstellen zu technisch orientiert sind. Anwender unterschätzen die Folgen von ungenügender Sicherheit und sind somit nicht bereit, den derzeit erheblichen Aufwand zur Nutzung von Sicherheitsmechanismen zu erbringen [MuSt98]. Das Projekt ATUS untersucht den Zusammenhang von Sicherheit *und* Benutzbarkeit in zwei Aspekten: Einerseits wird das Verhalten der Anwender bezüglich der Nutzung von Sicherheitsfunktionen in Tests erforscht, andererseits werden bei verallgemeinerbaren Fehlhandlungsursachen Gestaltungsrichtlinien für die Benutzungsschnittstellen von Sicherheitswerkzeugen abgeleitet sowie geeignete Sicherheitswerkzeuge entwickelt und erprobt.

2.1 Systemtest von Sicherheitswerkzeugen

Die Sichtung des Standes der Wissenschaft in der Software-Ergonomie [Ni93, De96] und der Human Computer Interaction (HCI) [HLP97, Di98] zeigt, dass Sicherheit und Benutzbarkeit bisher unabhängig voneinander betrachtet worden sind. Eine gewisse Ausnahme bildet die Nutzerforschung des Daimler-Benz-Kollegs [MuRa99]. Die dortigen Untersuchungen ergaben, dass eine messbare Abhängigkeit zwischen den Faktoren Sicherheit und Benutzbarkeit besteht. Dabei konnte gezeigt und in ATUS auch bestätigt werden, dass weniger die ergonomische Aufbereitung der Oberflächen die Benutzbarkeit bestimmt, sondern dass primär die dem Anwender oft unverständliche Präsentation der vorhandenen Sicherheitsmechanismen für die Nichtnutzung verantwortlich ist [MuSt98, GeKa00, Ge03].

Für die Evaluation bestehender Sicherheitswerkzeuge (Netscape-Browser, Internet-Explorer und die Signiersoftware „SignTrust Mail“ der Deutschen Post AG) erwiesen sich die heuristische Evaluation [NiMa94] und der Cognitive Walkthrough [Wh94] als nur bedingt geeignet [Ge03], da sie u.a. nicht auf das Erkennen von Sicherheitslücken ausgerichtet sind und potentielle Fehlhandlungen des Nutzers nur schwer erkennen können. In Kombination mit einer erweiterten Sicherheitsevaluation und einer zugehörigen Vergleichsheuristik wurden diese beiden Inspektionsmethoden modifiziert und zu einem Systemtestverfahren namens USE (Usability Security Evaluation) zusammengefasst [Ge03]. Als Vergleichsheuristik haben sich die ISO-Kriterien für Benutzbarkeit [De96] bereits im Vorfeld als zu konzeptionell und ergonomisch orientiert erwiesen, so dass sie speziell auf die Anforderungen der IT-Sicherheit angepasst wurden [GeKa00].

Bei der Evaluation der Signiersoftware „SignTrust Mail“ konnten 120 Benutzbarkeitsprobleme identifiziert werden [Ge03]. Davon sind 25% schwerwiegend, d.h. der Proband konnte nicht ohne fremde Hilfe die notwendigen Schritte zur Erfüllung einer gestellten

Aufgabe durchführen. Als sicherheitskritisch wurden 89% der Benutzbarkeitsprobleme eingestuft, d.h. sie gefährden das Sicherheitsniveau des Systems. Beispielsweise wird die asymmetrische Kryptographie von mehr als dreiviertel der Testpersonen nicht korrekt gehandhabt.

2.2 Identitätsmanagement als benutzbares Sicherheitswerkzeug

Mit dem Identitätsmanagement [GJM01] wurde ein verständliches Sicherheitswerkzeug für den Sicherheitslaien entwickelt, das es ihm ermöglicht, seine personenbezogenen Daten zu schützen. Der Anwender kann sein Auftreten gegenüber seinen Kommunikationspartnern selber bestimmen und aushandeln. Gleichzeitig bleibt er dabei gegenüber unbeteiligten Dritten vollständig anonym. Die Komplexität der Sicherheitskonfiguration konnte durch Implikationen und der daraus folgenden Einteilung in nutzer- und systemkontrollierte Schutzziele stark reduziert werden, so dass ausschließlich die Bestimmung des Grades der Anonymität und der Art der Zurechenbarkeit an der Benutzungsschnittstelle verbleiben müssen [JeGe00]. Durch die Abstraktion der nutzerkontrollierten Schutzziele zum Objekt der Teilidentität muss der Nutzer keine für ihn komplizierten Sicherheitskonzepte kennen und kann durch die Auswahl von Teilidentitäten sein System konfigurieren.

Zur Validierung des Identitätsmanagements wurde ein Prototyp für mobile Endgeräte entwickelt und in den Demonstrator des SPP Sicherheit integriert [GMW03]. Systemtests ergaben deutlich weniger Fehlhandlungen bei verbesserter Sicherheit verglichen mit Tests derselben Anwendung ohne den Identitätsmanager [Ge03].

3 Ausblick

Es wurde gezeigt, dass Benutzungsschnittstellen bestehender Sicherheitswerkzeuge für den Sicherheitslaien schwer bzw. kaum verständlich und nicht fehlerfrei zu bedienen sind. Mit dem Identitätsmanagement wurde ein Sicherheitswerkzeug für den Sicherheitslaien entwickelt, das jedoch die individuellen Erwartungen und Fähigkeiten seiner Anwender nicht berücksichtigt. Für die adaptive Gestaltung von Benutzungsschnittstellen erweist sich die bisherige undifferenzierte Einteilung in Experten, Normalnutzer und Laien in der HCI [KoWa99, HLP97] als unzureichend. Seit Januar 2003 wird diesbezüglich eine Befragung durchgeführt [Ka03]. Die zu prüfenden Hypothesen beziehen sich auf Eigenschaften wie „Bereitschaft zur Nutzung von Sicherheitsmechanismen“, „Sicherheitsbewusstsein“ und „Sicherheitskompetenz“. Die Daten sowohl dieser Befragung als auch die Ergebnisse der Systemtests dienen als Input zu einer differenzierten Nutzermodellierung und damit als Voraussetzung für eine adaptive Benutzungsschnittstelle von Sicherheitswerkzeugen.

Literatur

[De96] Deutsches Institut für Normung. DIN EN ISO 9241 Teil 10: Grundsätze der Dialoggestaltung, 1996.

[Di98] Dix, A., Finlay, J., Abowd, G., Beale, R.: Human-Computer Interaction, Volume 2, Prentice Hall, 1998.

[Ge03] Gerd tom Markotten, D.,: Benutzbare Sicherheit für informationstechnische Systeme, Dissertation an der Albert-Ludwigs-Universität Freiburg, 2003.

[GeKa00] Gerd tom Markotten, D., Kaiser, J.: Benutzbare Sicherheit – Herausforderungen und Modell für E-Commerce-Systeme, in: Wirtschaftsinformatik, Heft 6, S. 531-538, Dezember 2000.

[GJM01] Gerd tom Markotten, D., Jendricke, U., Müller, G.: Benutzbare Sicherheit – der Identitätsmanager als universelles Sicherheitswerkzeug, in: Müller, G., Reichenbach, M., (Hrsg.), Sicherheitskonzepte für das Internet, Kapitel 7, S. 135-146, Springer-Verlag Berlin, Mai 2001.

[GMW03] Gerd tom Markotten, D., Wohlgemuth, S., Müller, G.: Mit Sicherheit zukunftsfähig. PIK Sonderheft Sicherheit 2003, 26(1):5-14, 2003.

[HLP97] Helander, M., Landauer, T.K., Prabhu, P.V. (Hrsg.): Handbook of Human-Computer Interaction, 1997.

[JeGe00] Jendricke, U., Gerd tom Markotten, D.: Usability meets Security – The Identity-Manager as your Personal Security Assistant for the Internet, in: Proceedings of the 16th Annual Computer Security Applications Conference, Dezember 2000.

[Ka03] Kaiser, J.: Besteht eine Beziehung zwischen Nutzbarkeit und Sicherheit? - Entwurf einer Empirie zur Nutzung heutiger Sicherheitsmechanismen in IT-Anwendungen, in: PIK Sonderheft „Sicherheit 2003“, 2003.

[KoWa99] Kobsa, A., Wahlster, W. (Eds.): User Models in Dialog Systems, Springer Verlag, Berlin, 1989.

[MuRa99] Müller, G., Ranneberg, K. (Hrsg.): Multilateral Security in Communications – Technology, Infrastructure, Economy, Addison-Wesley, 1999.

[MuSt98] Müller, G., Stapf, K.-H. (Hrsg.): Erwartung, Akzeptanz, Nutzung, Band 2 der Mehrseitige Sicherheit in der Kommunikationstechnik. Addison Wesley Longman Verlag GmbH; 1998.

[Ni93] Nielsen, J.: Usability Engineering. Academic Press. 1993.

[NiMa94] Nielsen, J., Mack, R.L. (Hrsg.) Usability Inspection Methods, New York, John Wiley & Sons, 1994.

[RPM97] Rannenberg, K., Pfitzmann, A., Müller, G.: Sicherheit, insbesondere mehrseitige IT-Sicherheit. In Günter Müller und Andreas Pfitzmann (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik, S. 21-29. Addison-Wesley Longman Verlag GmbH, 1997.

[Wa98] Waidner, M.: Open Issues in Secure Electronic Commerce. Technical Report, IBM Research Division, Zürich, Oktober 1998.

[Wh94] Wharton, C., Rieman, J., Lewis, C., Polson, P.: The Cognitive Walkthrough Method: A Practitioner's Guide, in: Nielsen, J., Mack, R., (Hrsg.): Usability Inspection Methods, S. 105-140, John Wiley & Sons, 1994.

[WhTy99] Whitten, A., Tygar, J.D.: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In Proceedings of the 8th USENIX Security Symposium, August 1999.

[Wo03] Wohlgemuth, S., Gerd tom Markotten, D., Jendricke, U., Müller, G.: DFG-Schwerpunktprogramm „Sicherheit in der Informations- und Kommunikationstechnik“. It-Information Technology, Methoden und innovative Anwendungen der Informatik und Informationstechnik, 45(1), 2003.