Designansatz und Evaluation von Kindgerechten Securitywarnungen für Smartphones

Wiebke Menzel, Sven Tuchscheerer, Jana Fruth, Christian Krätzer, Jana Dittmann

Arbeitsgruppe Multimedia and Security, Institut ITI
Fakultät für Informatik
Otto-von-Guericke Universität Magdeburg Universitätsplatz 2
39106 Magdeburg
jana.fruth, kraetzer, sven.tuchscheerer, jana.dittmann@iti.cs.uni-magdeburg.de
wmenzel@mail.cs.uni-magdeburg.de

Abstract: Dieser Konferenzbeitrag beschreibt die Entwicklung und empirische Validierung eines Designs von Securitywarnungen für Smartphones für Kinder im Grundschulalter (7-10 Jahre). Das Design der Warnmeldungen soll an die Fähig- und Fertigkeiten, zum Beispiel visuelle, akustische, taktile Wahrnehmung und Leseleistung, von Kindern im Grundschulalter angepasst sein. Dafür wurden etablierte Designkriterien speziell für Kinder ausgewählt und darauf aufbauend ein Designansatz entwickelt. Anschließend wurde das entwickelte Design für Securitywarnungen in einen Prototyp überführt, der eine simulierte Schutzsoftware für die entwickelten Securitywarnungen präsentierte. Zur empirischen Validierung des Designs wurde eine geeignete Evaluationsmethodik gewählt. Dabei diente als Zielstellung eine „How good? “ Evaluation, die überprüft, ob gewünschte Eigenschaften eines Systems bzw. Designs eingehalten werden. Für die Validierung wurden darüber hinaus ein schriftliches Protokoll und ein Fragebogen erstellt. Schließlich wurde mit dem entwickelten Designansatz auf Grundlage der gewählten Evaluationsmethodik mit 13 Grundschulkindern eine Nutzerstudie durchgeführt. Die Auswertung der daraus resultierenden Daten ergab, dass die meisten Grundschulkinder wenig sensibilisiert sind im Bezug auf Sicherheit von Smartphones. Am Ende dieses Beitrages werden Empfehlungen für die Gestaltung von Securitywarnungen auf Smartphones für Kinder und weitere Forschungsvorhaben gegeben.

1 Einleitung

Bisher ist die Nutzung von Virenscannern für Smartphones - im Unterschied zum Desktop-IT Bereich - wenig verbreitet, obwohl diese aufgrund zunehmender Bedrohungslage wichtig wären. Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) wird es zukünftig in größerem Umfang Angriffe auf mobile Endgeräte, wie Smartphones, geben [BSI10]. Beim Smartphone existieren viele Schnittstellen, wie zum Beispiel Bluetooth, SMS, WLAN, UMTS und somit auch verschiedenste Angriffsmöglichkeiten. Speziell beim Smartphone geht es unter anderem um die Gefahr des Verlustes bzw. Ausspionierens von personenbezogenen Daten, wie Adressbücher und Standortdaten und eines finanziellen Schadens, also um den Security-Bereich. Bisherige Securitywarnungen sind vorrangig (teils ausschließ-

lich) für Standardnutzer gestaltet, wohingegen die Entwicklung nutzerspezifischer Warnmeldungen bisher ein Novum ist. Im Rahmen einer Untersuchung zu SSL-Security Warnungen bei Webbrowsern wurde festgestellt, dass Warnungen, welche den spezielle Kontext und den Anwender berücksichtigen zu signifikant angemesseneren Reaktionen der User führen [SEA+09]. Dieser Umstand wird dadurch intensiviert, dass jedes zweite Kind im Alter von 6 bis 13 bereits ein eigenes Mobiltelefon besitzt [KIM11]. Die Sättigungsrate steigt mit dem Alter an und darüber hinaus besitzen Kinder bereits Mobiltelefone mit zahlreichen Funktionen und Schnittstellen, wie z.B. Bluetooth. Aus diesen Gründen soll in diesem Beitrag ein speziell auf Smartphones abgestimmter nutzerspezifischer Designansatz für eine Schutzsoftware für Kinder entwickelt werden.

2 Designansatz von Securitywarnungen zur Darstellung auf Smartphones für Kinder

Im Folgenden werden Designkriterien für Ereignis basierte Securitywarnungen für Smartphones für die Nutzergruppe „Grundschulkinder“ entwickelt. Zur Auswahl der Designkriterien wird zwischen optischen, akustischen und haptischen Design unterschieden. Das akustische und haptische Design soll in Kombination mit dem optischen Design die Lenkung der Aufmerksamkeit auf die Securitywarnung unterstützen bzw. verstärken. Die Kombination der drei Designs wird logisches Design genannt [Bol98].

2.1 Auswahl der Designkriterien

Bei der Gestaltung des visuellen Designs sollen z.B. Denkweisen und Fähigkeiten von Grundschulkindern mit einbezogen werden. Hierbei ist insbesondere das „magische und animistische Denken “ von Kindern interessant [WL02]. Dieses besagt, dass Kinder dazu tendieren Gegenständen und Dingen eine „Seele “ zuzuordnen. So könnte z.B. ein sprechendes Smartphone als Charakter bzw. Figur einer Warnung verwendet werden. Auf Grundlage einer breiten Recherche zu aktuellen Computerspielen und Kindersendungen ab 6 Jahren [kik] im April 2011 konnten weitere Designkriterien erschlossen werden. Im Ergebnis dieser Recherche wurden Darstellungen realer Gegenstände, Personen und Sachverhalte zumeist verfremdet bzw. reduziert, sehr fantasievoll und in 2D oder 2,5D abgebildet. Seitens der AG Multimedia and Security wurde ein Interview mit dem Experten Prof. Dr. med. Gerhard Jorch, Direktor der Universitätskinderklinik des Universitätsklinikum Magdeburg, durchgeführt. Ein Ergebnis des Interviews ist, dass Kinder schlecht zwischen Realität und Fiktion unterscheiden können. Um Kindern den Unterschied zwischen Realität und digitaler Welt zu verdeutlichen, wird meist eine verfremdete Darstellung auf digitalen Medien gewählt. Für das Design von Securitywarnungen von Smartphones könnten ebenfalls Analogien - im Sinne von fiktiven Darstellungen -, wie z.B. die Erschaffung von Fantasiewesen für die Securitywarnungen, gewählt werden. Dieses Designprinzip ist Kindern aus Computerspielen und Trickfilmen bekannt und es ist an die Erfahrungs- und

Phantasiewelt der Kinder angelehnt. Bei der Typographie, d.h. der Art und Weise, wie Text in das Design eingebaut ist, sollten dem Nutzer wichtige Informationen konkret und direkt mitgeteilt werden [Bol98]. Zu beachten ist die Verwendung von Begriffen, die für Kinder verständlich sind. Außerdem fällt manchen Grundschulkindern das Lesen schwer, so dass der Text kurz, kindgerecht und in angemessener Schriftgröße und auf einheitlichem Hintergrund zur Erhöhung des Kontrastes sein sollte. Darüber hinaus könnte im akustischen Design zusätzlich eine Sprachausgabe zur Unterstützung integriert werden. Es sollte eine serifenlose Schriftart gewählt werden, da sich diese besser zum Lesen auf einem digitalen Display eignet [Jür03]. Zur Darstellung verschiedener Kritikalitätsstufen (siehe Kapitel 2.2) kann, wie bei aktueller Schutzsoftware im Desktop-IT Bereich und Smartphones, eine Farbkodierung genutzt werden. Jedoch sollte ein für Kinder bekannter Zusammenhang, wie z.B. Ampelfarben und nicht z.B. Ein Tacho, genutzt werden. Bei der Gestaltung des akustischen Designs könnte wie bereits erwähnt eine Sprachausgabe zum Text erfolgen. Des Weiteren kann durch die Wahl eines entsprechenden Warntons, also Tonhöhe, -länge, -wiederholungen, die Securitywarnung unterstützt bzw. verstärkt werden. Eventuell könnte auch ein den Kindern bereits bekannter Ton genutzt werden, wie z.B. der Ton einer Tuba, der u.a. Gefahr signalisiert - wie in der Vertonung von „Peter und der Wolf “. Jedoch sollte vermieden werden, dass die Securitywarnung von den Kindern nicht ernst genommen bzw. als konsequenzloses Spiel angesehen wird. Beim haptischen Design spielen insbesondere die Möglichkeiten eines Smartphones eine Rolle. So kann bei der Gestaltung das Touchscreendisplay genutzt werden. Dieses ermöglicht eine intuitive Bedienung. Eventuell können außerdem weitere Sensoren zur Unterstützung der Bedienung, wie z.B. Lagesensor, genutzt werden [iPhb]. Des Weiteren kann durch Vibration ebenfalls die Aufmerksamkeit auf die Securitywarnung unterstützt bzw. verstärkt werden. Bei der Wahl der Vibration, also Vibrationsstärke, - Dauer, -wiederholungen, sollte eine mögliche Überforderung des Nutzers beachtet werden. Insgesamt kann beim logischen Design durch eine geeignete Kombination des optischen, akustischen, haptischen Designs die Aufmerksamkeit von Grundschulkindern auf die Securitywarnungen gelenkt werden. Dabei kann die Nutzung von multimedialen Signalen den Umgang des Kindes mit der Securitywarnung erleichtern. Hierbei ist jedoch eine mögliche Überforderung durch zu viele Signale zu vermeiden.

2.2 Bedrohungsskala

Für das Design der Securitywarnungen ist es sinnvoll eine Bedrohungsskala zu entwerfen, um zwischen unterschiedlichen Bedrohungslagen differenzieren zu können. Es wird zwischen drei Kritikalitätsstufen unterschieden: Bei Kritikalitätsstufe 0 ist ein gefahrloses Nutzen des Smartphones möglich. Diese Stufe sollte die Standardstufe des Smartphones sein. Die Stufe tritt ein, wenn eine Überprüfung des - als ideal funktionierend angenommenen - Schutzprogramms ergibt, dass kein Sicherheitsrisiko besteht bzw. Virus vorhanden ist. Bei der Kritikalitätsstufe 1 kann das Smartphone weiter benutzt werden, ist jedoch gefährdet. Dieses tritt dann zu, wenn eine Aktion, die ausgeführt werden soll, ein Sicherheitsrisiko darstellt. Bei Kritikalitätsstufe 1 steht folglich die Handlungsanweisung,

die z.B. eine Infizierung des Smartphones mit einer Schadsoftware verhindert, im Vordergrund. Bei der höchsten Kritikalitätsstufe 2 besteht ein Sicherheitsrisiko für Smartphone und Besitzer. Das Smartphone ist hier zum Beispiel mit einem Virus infiziert, der Daten ausspionieren oder das Gerät beschädigen kann. Bei Kritikalitätsstufe 2 sollte das Smartphone vom Kind ausgeschaltet und den Eltern bzw. einem kompetenten Erwachsenen gegeben werden.

2.3 Designentwurf

Auf Grundlage der ausgearbeiteten Designkriterien soll nun ein Design für eventbasierte Securitywarnungen für Smartphones für die Nutzergruppe Grundschulkinder entwickelt werden. Hierbei wird das visuelle Design in mehrere Komponenten aufgeteilt. Zum einen wurde eine fantasievolle Figur im Zeichentrickstil entwickelt, die sich je nach Kritikalitätsstufe in Farbe und Mimik unterscheidet. Diese Figur warnt und gibt Handlungsanweisungen über eine Sprechblase mit einheitlich weißen Hintergrund zur Erhöhung des Kontrastes. Des Weiteren wird eine serifenlose Schriftart genutzt, um dem Nutzer das Lesen auf dem digitalen Display zu erleichtern. Je nach Bedrohungsskala ist die Figur Grün (Kritikalitätsstufe 0), Gelb (Kritikalitätsstufe 1) oder Rot (Kritikalitätsstufe 2) gefärbt. Die Wahl dieser drei Farben lässt sich auf eine Ampel, die Grundschulkindern bekannt sein sollte, beziehen. Um die Gefahr mit einem - dem Kind - bekannten Symbol zu verdeutlichen, wird das visuelle Design durch weitere Komponenten erweitert. So wird ein grünes Häkchen (Kritikalitätsstufe 0) oder Blaulicht (Kritikalitätsstufe 1 und 2) im Zeichentrick- bzw. Comic-Stil verwendet. Dieses befindet sich in einer Sprechblase, die über der Figur abgebildet ist. Um das optische Design der Securitywarnung zu vervollständigen, wird die Figur mit Textblase und Symbolen in eine Warnmeldungsbox, die dem gängigen iPhone-Oberflächen-Design entspricht, eingefügt. Innerhalb der Warnmeldungen gibt es mehrere Interaktionsmöglichkeiten mit dem Button „Warum? “ zum Anzeigen einer genaueren Erläuterung zur Warnmeldung, dem Button „Weiter“ zum Anzeigen der nächsten Ansicht einer Warnmeldung und dem Button „OK“ zur Kenntnisnahme und zum Schließen der Warnmeldung. Die Securitywarnung ist in zwei Ansichten unterteilt (siehe Abb. 1). Bei der ersten Ansicht erscheint die Figur, die „Achtung! “ sagt. Beim Klicken auf den Button „Weiter“ erscheint die zweite Ansicht der Warnmeldung, in der die Figur mögliche Handlungsweisen näher erläutert. Mit Klick auf den „OK“-Button schließt sich die Warnmeldung. Mit Klick auf den „Warum? “-Button erscheint eine genaue Erläuterung der Gefahr und warum dem Nutzer die entsprechende Handlungsanweisung gegeben wurde. Durch die zwei Ansichten lässt sich die Konzentration der Kinder besser auf die Warnmeldung lenken. Die Aufmerksamkeit wird so vom aktuellen Benutzungsszenario auf die Securitywarnung gelenkt und die Securitywarnung lässt sich nicht beim ersten Klick schließen. Stattdessen wird das Kind durch die erste Securitywarnung aus dem Geschehen geführt und erhält nach dem Klicken auf „Weiter“ nähere Informationen. So ist es auch möglich bei der zweiten Ansicht der Securitywarnung mehr Textinformationen einzubauen.

Die „Warum? “-Ansicht der Securitywarnung soll ähnlich wie die anderen Securitywarnungen aufgebaut sein. Hier ist die Figur eine neutrale Informationsauskunft. Als neutrale

Abbildung 1: Aufbau der Securitywarnung: Kritikalitätsstufe 2

Färbung wurde weiß gewählt. Das Weiß soll darstellen, dass die Figur nicht weiß, ob Gefahr droht oder nicht bzw. nur informiert. Das akustische Design besteht aus einem kurzen Standard-Warnton [Sad]. Dieser soll betonen, dass es sich bei der Securitywarnung z.B. nicht um ein Spiel handelt. Ein Ton aus einer Comicserie könnte zu einem zu sehr spielerischen Umgang führen. Der Ton wird je nach Kritikalitätsstufe einmalig oder zweimalig beim Erscheinen der Securitywarnung abgespielt werden. Das akustische Design kommt nicht zum Einsatz, wenn beim Smartphone der Ton deaktiviert ist. Das haptische Design besteht aus dem Bedienen des Touchscreendisplays und je nach Kritikalitätsstufe aus einer kurzen und zum Teil wiederholten Vibration des Smartphones beim Erscheinen der Securitywarnung. Die Vibration wird nicht verwendet, wenn beim Smartphone diese Funktionalität deaktiviert ist. Das logische Design, also die Kombination aus optischen, akustischen und haptischen Design, ist je nach Kritikalitätsstufe verschieden. Die möglichen Kombinationen können so anhand der Kritikalitätsstufe ausgewählt werden und so die einzelnen Kritikalitätsstufen unterstützen. Die einzelnen Kritikalitätsstufen sind im logischen Design voneinander abgegrenzt und zeigen den Kindern die Prägnanz der Securitywarnung. Dabei wird aber eine mögliche Überforderung durch zu viele Signale vermieden und der Einsatz von Ton in Kombination mit Vibration lediglich bei der höchsten Kritikalitätsstufe angewandt.

Wenn der Ton deaktiviert ist, soll das fehlende akustische Design durch ein zusätzliches Vibrationssignal ausgeglichen werden. So gibt es in diesem Fall bei Kritikalitätsstufe 1 zusätzlich eine kurze einmalige Vibration. Bei Kritikalitätsstufe 2 gibt es, wenn der Ton deaktiviert ist eine zweimalige Vibration. Bei Deaktivierung der Vibration des Smartphones bleibt das zweimalige Abspielen des Warntons bei Kritikalitätsstufe 2. Sollten sowohl

Kritikalität	optisches Design	akustisches Design	haptisches Design	
0	Figur & entsprechende Textnachricht & Farbkodierung grün & Häckchen	kein Warnton	Bedienung mittels Touchscreen	keine Vibration
1	Figur & entsprechende Textnachricht & Farbkodierung gelb & Blaulicht	Warnton kurz & einmalig		keine Vibration
2	Figur & entsprechende Textnachricht & Farbkodierung rot & Blaulicht	Warnton kurz & zweimalig		Vibration kurz & einmalig

Abbildung 2: Logisches Design der Securitywarnungen nach Kritikalitätsstufen, Ton und Vibration aktiviert

Ton als auch Vibration deaktiviert sein, besteht die Warnmeldung ausschließlich aus dem optischen Design. Im Folgenden wird bei der prototypischen Implementierung (siehe Kapitel 3.1) und der damit verbunden Nutzerstudie (siehe Kapitel 3.2) die Aktivierung von Ton und Vibration als Voraussetzung angesehen.

3 Evaluation des Designansatzes

Evaluationsziel ist die ist die Entwicklung nutzerspezifischer Smartphone- Securitywarnungen für Grundschulkinder. Die Evaluation soll also überprüfen, ob das - in Kapitel 2 - entwickelte Design zu den Bedürfnissen und Voraussetzungen der Zielgruppe passt. Dabei dient als Zielstellung eine „How good? “ Evaluation, die überprüft, ob gewünschte Eigenschaften eines Systems bzw. Designs eingehalten werden. Die „How good? “ Evaluation wird der summativen Evaluation zugeordnet, die auf die globale Bewertung der Software abzielt und den gewünschten mit dem erreichten Zustand vergleicht. Um die Zielstellung später durch eine Evaluation überprüfen zu können, wurden Forschungsfragen, die in der Auswertung (siehe Kapitel 3.3) beantwortet werden, aufgestellt. Darüber hinaus werden Evaluationswerkzeuge (siehe Kapitel 3.1) benötigt, um bei einer selbst durchgeführten Nutzerstudie (siehe Kapitel 3.2) die Zielstellung, also die aufgestellten Forschungsfragen, zu überprüfen.

3.1 Evaluationswerkzeuge

Bei den Evaluationswerkzeugen wird im Folgenden zwischen technischen und nichttechnischen Werkzeugen unterschieden. Als technisches Werkzeug wird ein Prototyp angesehen, der die Möglichkeit bietet, während einer Nutzerstudie die entwickelten Security-

warnungen anzuzeigen. Der Prototyp besteht aus zwei Programmen. Zum einen aus dem Hauptprogramm zur Anzeige der entwickelten Securitywarnungen, das die Probanden bedienen. Zum anderen aus einem Kontrollprogramm, mit dem Warnmeldungen über Bluetooth im Hauptprogramm angezeigt werden können. Während der Nutzerstudie bedient der Proband das Testgerät, ein iPhone 3G [iPha], mit dem Hauptprogramm, während ein Helfer, für den Probanden nicht sichtbar, ein zweites iPhone mit dem Kontrollprogramm bedient. So ist es möglich ein Schutzprogramm, das den Nutzer mittels Securitywarnungen warnt, zu simulieren. Das Hauptprogramm besteht aus einem implementierten Mal-Spiel. Dieses soll den Probanden eine Aufgabe während der Versuchsdurchführung geben und dient somit als Anwendungskontext zur Anzeige der Securitywarnungen. Im Kontrollprogramm, das über Bluetooth im Hauptprogramm Securitywarnungen anzeigen lassen kann, gibt es je Securitywarnung einen Button. Um zu verhindern, dass das Spiel unbeabsichtigt vom Probanden beendet wird, ist beim entsprechenden Testgerät die Menütaste mit einem Stück Pappe verdeckt, sowie mit einem schwarzen Klebeband überklebt. Die Ausschalttaste ist ebenfalls unauffällig mit schwarzem Klebeband verdeckt. Die Verhinderung eines unbeabsichtigten Beenden des Programms ist nötig, da sonst die Verbindung zwischen Hauptprogramm und Kontrollprogramm unterbrochen werden würde. Das würde den Versuch ungewollt vorzeitig beenden. Des Weiteren werden mit dem Prototypen Messdaten, die Rückschlüsse auf die Handhabung der Probanden mit den entwickelten Securitywarnungen zulassen, erfasst und in ein Logfile gespeichert. Das nicht-technische Werkzeug besteht aus mehreren Komponenten. Zum einen werden während der Nutzerstudie die Probanden bei der Ausführung der Aufgabe und Interaktion mit dem Prototyp beobachtet. Diese Beobachtungen werden in einem schriftlichen Protokoll, das der Versuchsleiter der Nutzerstudie anfertigt, festgehalten. Des Weiteren wird die Methode des lauten Denkens eingesetzt, um die Gedanken und Gefühle des Probanden während des Versuchs zu erfahren und ebenfalls schriftlich protokolliert. Eine Überforderung des Protokollanten wird vermeiden, in dem ein vorgefertigtes, strukturiertes Protokoll verwendet wird. Schließlich wird als weiteres nicht-technisches Werkzeug im Anschluss an jeden Versuch mit dem Prototypen ein - speziell für Kinder entwickelter - Fragebogen, der die Beurteilung durch die Probanden aufzeigt, verwendet. Der Fragebogen soll speziell auf die Bedürfnisse von Grundschulkindern abgestimmt sein, also nicht zu lang und in einer geeigneten Schrittgröße, um die Konzentration aufrecht zu erhalten. Verwendet werden sollten ebenfalls viele Bilder und Symbolik, wie z.B. Smileys, um zu motivieren und Text zu vermeiden. Fragearten des Fragebogens sind z.B. Bewertungsfragen, offene Fragen und Kontrollfragen. Die Kinder werden beim Ausfüllen des Fragebogens durch einen Helfer unterstützt. Der Helfer liest die Fragen vor und setzt die Antwortkreuze bzw. schreibt bei offenen Fragen die Antwort des Probanden auf. So wird das Lesen und Ausfüllen des Fragebogens zusätzlich erleichtert, da dieses v.a. Grundschulkindern teilweise noch schwer fällt.

3.2 Durchführung der Nutzerstudie

Die Evaluation wurde im Rahmen einer Nutzerstudie an einer Grundschule in Magdeburg durchgeführt. Es gab die Möglichkeit den Versuch im Rahmen der Computer- Arbeitsge-

meinschaft (AG) der 1. Klasse oder der 3. Klasse durchzuführen. Da die AG der 1. Klasse nur aus Mädchen bestand, fiel die Entscheidung auf die gemischte AG der 3. Klasse. So konnten mögliche Unterschiede zwischen Jungen und Mädchen mit in die Auswertungen einfließen. Des Weiteren findet der Unterricht der ausgewählten 3. Klasse mit Tablet-PCs und einem digitalem Whiteboard statt. Es wurde also vermutet, dass die Kinder eine gewisse Erfahrung im Umgang mit Computern und Technik haben. Insgesamt 13 Kinder, darunter 8 Jungen und 5 Mädchen, der AG der 3. Klasse nahmen an dem Versuch teil. Die Kinder waren im Alter von 8 bis 9 Jahren und alle deutsche Muttersprachler. Vorbereitend wurde eine Einverständniserklärung mit einem Begleitschreiben der Schulleitung an die Eltern gegeben und sich der Klasse vorgestellt. Dabei wurde den Kindern erklärt, dass ihre Hilfe benötigt wird und sie ein Programm auf dem iPhone testen sollen. Es wurde nicht erwähnt, dass es beim dem Test um Warnmeldungen geht, um eine Beeinflussung zu verhindern. Der Versuch wurde an drei aufeinanderfolgenden Tagen mit jeweils 4 bis 5 Kindern einzeln durchgeführt. Der Versuch bestand aus drei Phasen Einführung, Bedienung des Prototypen und Fragebogen. Für die Einführung waren etwa fünf Minuten, für den Versuch fünfzehn Minuten und für das Ausfüllen des Fragebogens fünfzehn Minuten geplant. Insgesamt sollte die Länge des Versuchs eine Schulstunde (ca. 45 min.) nicht überschreiten, um die Konzentration der Kinder nicht zu überbeanspruchen.

3.3 Auswertung

Die Auswertung soll klären, ob die nutzerspezifischen Smartphone-Securitywarnungen für Grundschulkinder angemessen konzipiert sind. Dafür wurden verschiedene Forschungsfragen untersucht. Zum Einen sollte geklärt werden, wie verständlich die - speziell für Grundschulkinder entwickelten - Securitywarnungen sind. Zur Beantwortung dieser Forschungsfrage muss das Konstrukt „Verständlichkeit der Warnmeldung“ operationalisiert werden. Zur Operationalisierung werden folgende 3 Instrumente herangezogen: Reaktion (angemessene und unangemessene Reaktion erfasst im Protokoll und Logfile), Interpretation der Warnmeldung aus Sicht des Kindes (erfasst im Fragebogen), Häufigkeit der Nutzung des „Warum? “-Buttons (erfasst im Logfile). Für jede angezeigte Warnmeldung wurden die drei Instrumente ausgewertet. Interessant war hierbei die Diskrepanz zwischen Interpretation und Reaktion beim Warnen bzw. Installieren eines infizierten Updates. So interpretierten die meisten Kinder die Warnmeldung zwar richtig, die Hälfte der Kinder handelte aber unangemessen (installierten das infizierte Update). Dies könnte, neben dem Verständnis der Warnmeldung, auch an weiteren Faktoren liegen. Mögliche Ursachen der unangemessenen Reaktionen könnten Unsicherheit der Kinder, der Aufforderungscharakter des Update-Hinweises und mangelndes Bewusstsein bezüglich IT-Sicherheit auf Smartphones sein. Bei zwei weiteren Warnmeldungen: Angriff über Bluetooth (angemessene Reaktion ist Deaktivieren des Bluetooth) und über das Senden einer infizierten Datei an das Smartphone (angemessene Reaktion ist das Blockieren dieser Datei) gab es ebenfalls interessante Ergebnisse. So reagierten die meisten (92 bzw. 100 Prozent) Kinder angemessen. Jedoch ergab die Interpretation im Fragebogen und die Methode des Lauten Denkens (erfasst im Protokoll), dass die Mehrheit der Kinder die Warnmeldungen nicht

verstanden hat. So gab es eine intuitiv richtige Reaktion auf die Warnmeldungen trotz der fehlenden oder fehlerhaften Interpretation. Des Weiteren wurde untersucht, wie ansprechend das gewählte Design der Securitywarnungen für Grundschulkinder gestaltet ist. Die Evaluation des Designs wurde mithilfe des Fragebogens durchgeführt. Insgesamt beurteilten 9 Kinder (69 Prozent) die Warnmeldung und die Comic-Figur auf einer Skala von 1 (sehr gut) bis 6 (ungenügend) als sehr gut. Beim Text bewerteten alle Kinder die Schrittgröße, sowie 11 Kinder (83 Prozent) die Textlänge als angemessen. Die meisten Kinder empfanden die verwendeten Wörter verständlich. Jedoch hatten einige Kinder während des Versuchs Verständnisprobleme mit englischen Begriffen, wie „Update“ oder „Bluetooth“. Insgesamt kann daraus geschlussfolgert werden, dass der Text vom Inhalt, in Schrittgröße und Textlänge ansprechend gestaltet wurde. Jedoch sollte auf englische Begriffe verzichtet werden. Darüber hinaus sollte geklärt werden, wie Zeit und Reihenfolge der Präsentation von Securitywarnungen die Reaktion der Probanden beeinflussen. Mithilfe des Logfiles, indem gespeichert wurde wie lange eine Warnmeldung geöffnet war und des schriftlichen Protokolls in dem eine Vermutung, ob eine Warnmeldung gelesen wurde, vermerkt wurde, kann geschätzt werden ob eine Warnmeldung gelesen wurde oder nicht. Vergleicht man diese Schätzung mit der zeitlichen Abfolge der Warnmeldungen, ergibt sich eine Tendenz, dass mit fortschreitender Versuchszeit die Wahrscheinlichkeit für das Durchlesen der Warnmeldung abnimmt (siehe Abb. 3). Dieses könnte an einer Gewöhnung an die Warnmeldung, dem Habituationseffekt, liegen und deckt sich mit der Nutzung des „Warum? “-Buttons, die ebenfalls mit der Zeit nachlässt.

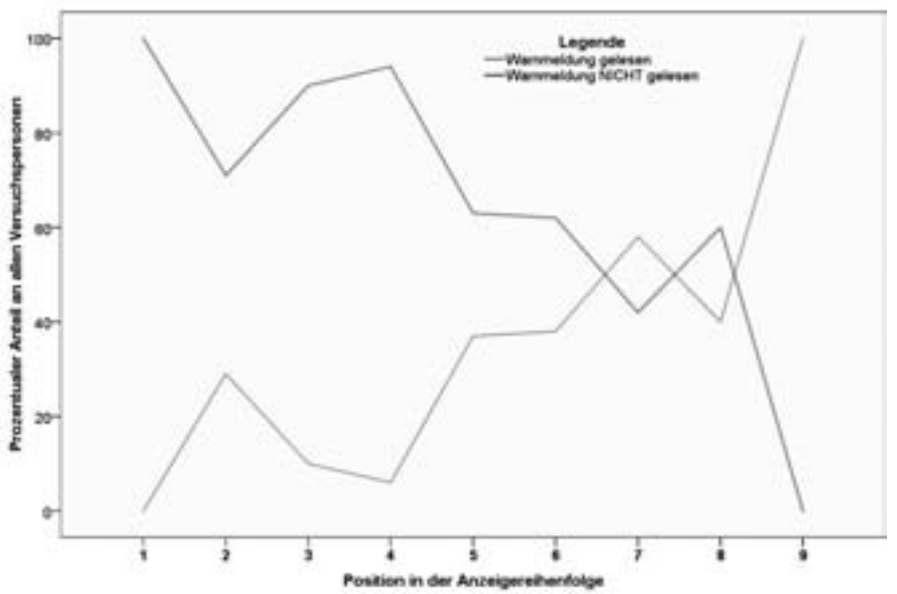

Abbildung 3: Einfluss der Versuchszeit auf das Leseverhalten aller Warnmeldungen

4 Fazit

Die Nutzerstudie mit anschließender Evaluation lässt darauf schließen, dass die erarbeiteten Designkriterien gut gewählt sind. So kann die Empfehlung ausgesprochen werden, dass das Design im Comic- bzw. Zeichentrickstil, unterstützt durch - für Grundschulkinder - bekannte Symbole und mit altersgerechtem Textinhalten, gestaltet wird. Wobei der Text keine englischen Begriffe enthalten sollte. Die Nutzung einer Comic- bzw. Zeichentrick-Figur, die über Text in einer Sprechblase mit den Grundschulkindern „spricht“, ist also für das Design von Securitywarnungen für Smartphones für Grundschulkinder geeignet. Auch kann eine Farbkodierung entsprechend einer Ampel (grün, gelb, rot) genutzt werden. Die Evaluation hat gezeigt, dass Grundschulkinder die entsprechend gefärbte Figur mit der Warnmeldung in Verbindung bringen, die sie als erstes gesehen haben. Eventuell könnte dies genutzt werden, indem zum Beispiel verschiedene Figuren bzw. Charaktere entwickelt werden, die jeweils eine bestimmte Bedrohung repräsentieren. Dieses müsste allerdings in weiteren Nutzerstudien evaluiert werden. Die Evaluationsergebnisse lassen vermuten, dass die meisten Grundschulkinder wenig sensibilisiert im Bezug auf Sicherheit von Smartphones sind. Dem könnte entgegengewirkt werden, indem im Unterricht oder zum Beispiel in Computer-AGs der Schulen Sicherheitsaspekte und Bedrohungen erläutert werden. Darüber hinaus könnten entsprechende Tutorial-Programme zum spielerischen Lernen im Kontext von Security- Ereignissen und die Reaktion darauf entwickelt werden. Des Weiteren sollten Handlungsmöglichkeiten an die Eltern übertragen werden. So könnte, wenn ein Kind ein Update installieren will oder das Smartphone aufgrund eines Virus ausgeschaltet werden sollte, eine SMS oder eMail an die Eltern geschickt werden. Den Eltern würde so die Möglichkeit gegeben aus der Ferne dem Update zuzustimmen bzw. das Smartphone auszuschalten. Bei weiterer Entwicklung von Securitywarnungen sollten die unterschiedlichen Einstellungsmöglichkeiten von Smartphones (Ton bzw. Vibration deaktivieren) mit implementiert werden. Darüber hinaus könnten unterschiedliche Modi für verschiedene Altersstufen bzw. Erfahrungen der Kinder entwickelt werden. Zu betonen ist, dass die Nutzerstudie nur mit einer kleinen Testgruppe von 13 Grundschulkindern im Alter von acht bis neun Jahren durchgeführt wurde. Somit ist die Aussagekräftigkeit aufgrund der Größe der Testgruppe und der geringen Altersdifferenz der Probanden eingeschränkt. Es ist also zu empfehlen die Testergebnisse, die auf für Grundschulkinder angemessen entwickelte Designkriterien schließen lassen, mit einer größeren Testgruppe mit größerer Altersspanne zu überprüfen.

5 Acknowledgements

Die Arbeit von Dr. Sven Tuchscheerer ist Teil des ViERforES II Projektes, welches vom Deutschen Ministerium für Bildung und Forschung (BMBF) finanziert wird. Teile dieser Arbeit entstanden im Rahmen der Bachelorarbeit von Wiebke Menzel im Sommersemester 2011 an der Otto-von-Guericke-Universität Magdeburg (FIN/ITI/AMSL).

Literatur

[Bol98] D. Boles. Vorlesungsskript Mulimedia-Systeme, 12 1998. Letzter Aufruf: 20.04.2011.

[BSI10] Bundesamt für Sicherheit in der Informationstechnik. Jahresbericht 2010, 2010. Letzter Aufruf: 29.09.2011.

[iPha] Webseite Heise.de. Technische Daten iPhone 3G. Letzter Aufruf: 28.07.2011.

[iPhb] Webseite Apple.com. Technische Daten iPhone 4. Letzter Aufruf: 28.07.2011.

[Jür03] S. Jürgens. Evaluation von world-wide-web basierten Benutzungsschnittstellen für Kinder. Diplomarbeit, Fachbereich Informatik, Universität Hamburg, September 2003.

[kik] Webseite KIKA.de. Aktuelles Fernsehprogramm. Letzter Aufruf: 20.04.2011.

[KIM11] KIM-Studie 2010 - Kinder + Medien, Computer + Internet - Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger in Deutschland. Februar 2011. Letzter Aufruf: 29.09.2011.

[Sad] Quellecode zu „Das große iPhone Enwicklerbuch: Rezepte für Anwendungsprogrammierung mit dem iPhone SDK“ von Erica Sadun. Letzter Aufruf: 28.08.2011.

[SEA+09] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri und Lorrie Faith Cranor. Crying wolf: an empirical study of SSL warning effectiveness. In *Proceedings of the 18th conference on USENIX security symposium*, SSYM'09, Seiten 399–416, Berkeley, CA, USA, 2009. USENIX Association.

[WL02] S. Wink und K. Lindner. *Kids und Computerspiele: Eine pädagogische Herausforderung*. Logophon, 2002. ISBN: 3-922514-83-9.