Nutzerzentrische Sicherheitsmechanismen

NEUE KONZEPTE ZUR ZUGRIFFSKONTROLLE RÜCKEN DEN MENSCHEN IN DEN VORDERGRUND

Mehr und mehr verlagern Anwender ihre täglichen Belange ins Internet. Verschiedenste digitale Ressourcen werden über Dienste und Netzwerke ausgetauscht und zugänglich gemacht. Forscher des Mind Mesh Projekts zeigen einen neuartigen Ansatz zur benutzerzentrischen Zugriffskontrolle, insbesondere in virtuellen und verteilten Forschungsumgebungen.

Während das World Wide Web in seinen Anfängen im Wesentlichen dazu diente, statische Inhalte zu verbreiten und zu konsumieren, änderte sich dieses Verhalten mit dem Aufkommen des Web 2.0 drastisch. Immer häufiger entstehen Dienste, die das Konzept des »User Generated Contents« umsetzen. Dienste wie Facebook, Twitter oder YouTube leben davon, dass Benutzer eigene Inhalte online stellen und diese mit anderen Nutzern teilen. Das neue Paradigma des Cloud Computing lässt darüber hinaus noch die Grenze zwischen der Online- und Offline-Welt immer weiter verschmelzen. So existieren etwa Speicherdienste wie Dropbox, die das Speichern und Teilen von Inhalten in der Cloud erlauben.

1

Konzepte des einfachen Informationsaustausches über Computernetze, wie sie Web 2.0- oder Clouddienste bieten, genießen allerdings auch im akademischen Umfeld immer mehr Ansehen. So genannte Virtuelle Forschungsumgebungen (Virtual Research Environments) verwalten Forschungsprojekte und Daten und setzen dabei auf Internettechnologien. So finden sich immer mehr standortübergreifende Forschungsvorhaben, in die Forscher unterschiedlicher Hochschulen, Länder oder Kontinente involviert sind. Cloud und Web 2.0 Technologien bieten dafür eine sehr komfortable Grundlage. In Wikis werden Projekte organisiert, über Twitter werden Updates kommuniziert und mit Hilfe von Dropbox werden Daten ausgetauscht. Gerade das Teilen von Daten mit anderen Projektteilnehmern stellt eine große Herausforderung für die Beteiligten dar. Häufig bieten Zugriffskontrollsysteme über Zugriffslisten die Möglichkeit bestimmten Benutzern Zugriff zu gewähren oder ihn zu verbieten (engl. access control, AC).

Der Mensch im Fokus

Während existierende AC Konzepte theoretisch für perfekte Sicherheit sorgen können, sieht die Realität häufig ganz anders aus. Zugriffslisten werden komplex und unübersichtlich, sie werden nur unregelmäßig gepflegt oder auf Validität geprüft. Auch neuere Konzepte wie etwa rollenbasierte Zugriffskontrollsysteme bieten nur unzureichende Möglichkeiten, die Komplexität von Zugriffskontrollkonfigurationen zu verringern. Aus

1 http://www.spiegel.de/netzwelt/web/0,1518,795796,00.html

diesen Bedienungsproblemen resultieren häufig Sicherheitslecks, die nicht selten zu dem ungewollten Veröffentlichen von eigentlich schützenswerten Daten führen. Erst im November 2011 führte ein mangelhaft konfiguriertes Zugriffskontrollsystem zur Veröffentlichung von 2500 Patientendaten psychisch kranker Menschen im Internet [1].

Anhand dieses Beispiels ist die Problematik aktueller Zugriffskontrollsysteme in verteilten Umgebungen gut zu erkennen. Während Sicherheit theoretisch gewährleistet werden kann, vernachlässigen aktuelle Konzepte häufig die zentrale Rolle des Menschen als Benutzer und Administrator.

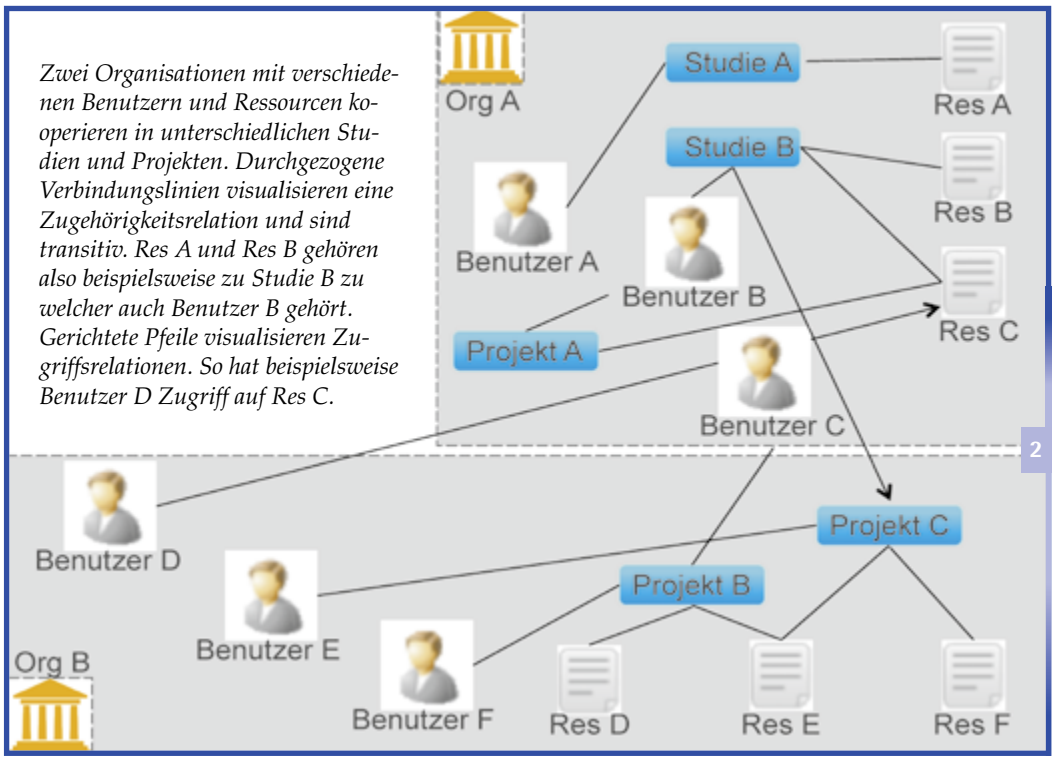
Die Probleme entstehen dabei insbesondere durch eine Kombination der folgenden Faktoren: mangelnde Instrumentierung von Arbeitsabläufen, Kontrollverlust der Datenbesitzer, fehlende Transparenz und Nachvollziehbarkeit sowie unzureichende Benutzbarkeit der vorhandenen Systeme. Gerade die Zugriffskontrolle ist ein elementarer Bestandteil beim Datenaustausch, der bisher aber immer eine Anpassung des Benutzers an die Konzepte des Systems erfordert. Bestehende AC Systeme, beispielsweise Role-based AC (RBAC) oder Attribute-based AC (ABAC), erfordern eine bestimmte Methodik beim Definieren von Zugriffsrechten. So muss ein Benutzer zum Beispiel festlegen, dass die Rolle »Projektpartner« auf alle projektbezogenen Ressourcen zugreifen darf. Soll nun aber eine einzelne andere Datei zur Verfügung gestellt werden, die anderen Benutzern in der Rolle Projektpartner nicht zugänglich sein soll, muss eine weitere Rolle speziell angelegt werden. Außerdem ist eine solche Konfiguration meistens nur von einem Systemadministrator durchführbar, welcher aber unter Umständen gerade keine Zeit hat oder gar nicht existiert. Insgesamt sind die bestehenden Zugriffskontrollmodelle mit einem Fokus auf Sicherheit und Ausdrucksstärke erdacht worden, kümmern sich aber nur selten um die Fähigkeiten und Anforderungen desjenigen, der die Konfiguration des Systems vornehmen muss. In modernen Forschungsumgebungen kann aufgrund der speziellen individuellen Bedürfnisse diese Konfiguration eigentlich nur vom jeweiligen Benutzer selbst vorgenommen werden.

Somit können Sicherheitslösungen nur erfolgreich eingesetzt werden, wenn Sicherheitskonzepte den Benutzer von Anfang an integrieren und sie so gut es geht bei der zu erledigenden Aufgabe unterstützen. Im Rahmen der Forschung des noch jungen Gebiets der *Usable Security* beschäftigen wir uns mit Konzepten für benutzerzentrische Zugriffskontrollsysteme, unter anderem für verteilte Forschungsumgebungen.

Benutzerzentrische Zugriffskontrolle für verteilte Forschungsumgebungen

Im Mind Mesh Projekt erarbeiten wir einen neuartigen Ansatz zur benutzerzentrischen Zugriffskontrolle, insbesondere in virtuellen und verteilten Forschungsumgebungen. Zugriffsregeln auf im System verwaltete Daten werden nicht mehr von Administratoren definiert, sondern jeder Benutzer bekommt für ihn benutzbare Werkzeuge zur Verfügung gestellt, um selbst zu entscheiden, welche Zugriffe erlaubt sind und welche nicht.

Im ersten Schritt zu einem solchen System muss der Benutzer zunächst in die Lage versetzt werden, den aktuellen Zustand des Systems zu



Zwei Organisationen mit verschiedenen Benutzern und Ressourcen kooperieren in unterschiedlichen Studien und Projekten. Durchgezogene Verbindungslinien visualisieren eine Zugehörigkeitsrelation und sind transitiv. Res A und Res B gehören also beispielsweise zu Studie B zu welcher auch Benutzer B gehört. Gerichtete Pfeile visualisieren Zugriffsrelationen. So hat beispielsweise Benutzer D Zugriff auf Res C.

Abbildung 1
Das neue Paradigma des Cloud-Computing lässt die Grenze zwischen der Online- und der Offline-Welt immer weiter verschmelzen.
Quelle: © bannosuke/Fotolia.com

Abbildung 2
Beispielhafter MindMesh Kontext in grafischer Darstellung

erfassen und zu überblicken, sowie anschließend darauf basierend Entscheidungen zu treffen. Um diese Entscheidungsgrundlage so intuitiv wie möglich zu gestalten, verwendet das Mind Mesh Konzept, in Anlehnung an Concept- und Mind Maps, eine interaktive Graph-Struktur zur Darstellung des Kontexts.

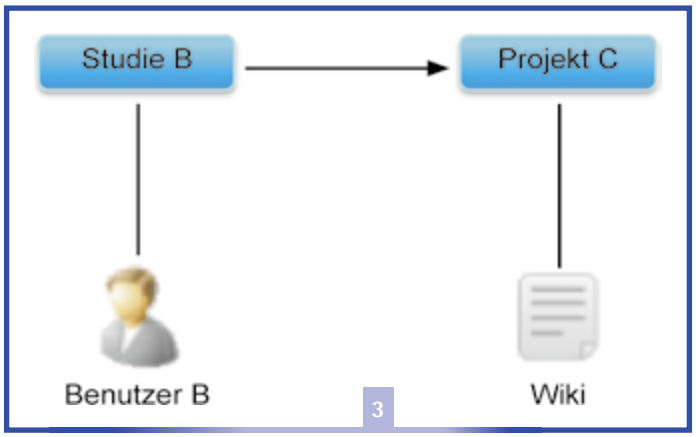


Abbildung 3
In einer Detailansicht kann anhand der Graph-Struktur erklärt und dargestellt werden, warum ein gewisser Benutzer Zugriff erhalten hat.

Kontext bezeichnet in diesem Fall Objekte, mit deren Hilfe der Benutzer Zugriffskontrolle definieren können soll, also beispielsweise Dateien, Projekte, andere Benutzer, Organisationen oder Ressourcen. Kanten zwischen Objekten zeigen Zusammenhänge an, die entlang verschiedener Dimensionen (Farbe, Stärke, Beschriftung, Muster) weitere Informationen darstellen können (vgl. Abbildung 1). Möchte nun ein Benutzer einem Kollegen in einer Partnerorganisation Zugriff auf seinen neuesten Datensatz gewähren, kann er einfach dessen Knoten im Graph auf die entsprechende Datei »ziehen«. Die Mind Mesh Infrastruktur sorgt dann im Hintergrund dafür dass auf den entsprechenden Endsystemen Berechtigungen gesetzt werden.
Die Erstellung der Zugriffsregeln, die letztendlich definieren, welche Objekte von welchen Benutzern zugegriffen werden dürfen, profitiert auch von einer grafischen Repräsentation der Umgebung. Der Benutzer kann zum Beispiel intuitiv das Szenario »Diese drei Kollegen sollen Zugriff auf diese Daten erhalten« konfigurieren, indem er die entsprechenden Knoten im Graph markiert. Unter Einbeziehung des enthaltenen Kontexts kann die Software dann Regeln vorschlagen, die zum Beispiel die ausgewählten Benutzer anhand gewisser Attribute (Organisationszugehörigkeit, Status, Projektmitarbeit …) identifiziert, und damit potenziell auch zukünftige Benutzer abdeckt, oder direkt anhand von identifizierenden Merkmalen genau diese Benutzergruppe modelliert. Das Benutzerinterface kann dabei direkt die Effekte einer Regel grafisch darstellen.

Sind verschiedene Berechtigungen im System gesetzt, soll der Benutzer außerdem erkennen können, wer genau Zugriff auf die von ihm verwalteten Ressourcen hat. Es könnte beispielsweise sein, dass zu Projektstart festgelegt wurde, dass alle Projektpartner und ihre Mitarbeiter Zugriff auf ein Projektwiki haben. Zudem wurden noch Ausnahmeregeln für weitere Berater und Beobachter hinzugefügt. Betrachtet ein Projektmitarbeiter, der mit der Verwaltung des Wikis betraut wurde, nun nach einiger Zeit die Berechtigungssituation, kommt es oft dazu, dass nicht nachvollziehbar ist, warum eine gewisse Person Zugriff hat. Nutzt man die Berechtigungserstellung anhand der Graph-Struktur aus, kann durch Rückgriff auf selbige dem Benutzer verdeutlicht werden, wie es zu einer Entscheidung kam. Fungiert der unbekannte Benutzer B etwa seit kurzem als Berater in der zu Projekt C gehörenden Studie B, erklärt diese Beziehung, warum automatisch auch Zugriff auf das Wiki gewährt wurde (vgl. Abbildung 2).

Ein weiterer wichtiger Aspekt ist die Berücksichtigung von Datenschutzrichtlinen. Insbesondere bei transnationalen Kooperationen können die Anforderungen sehr vielfältig sein. Eine Formalisierung dieser Anforderungen in Kombination mit einer Markierung von zu teilenden Informationen kann unter Verwendung von Logikformalismen eine automatische Prüfung ermöglichen. So kann in einer Mind Mesh-gestützten Infrastruktur beispielsweise automatisiert eine Anonymisierung von personenbezogenen Daten in einem Dokument vorgenommen werden. Derart gesichert kann und darf das Dokument dann weitergegeben werden.

Auf ähnliche Art und Weise könnte eine Richtlinie festlegen, dass eine Ethikkommission angerufen werden muss, bevor Daten weitergegeben werden können. Die Entscheidung, ob ein Zugriff auf eine Datei gewährt wird, hängt also unter anderem von der Entscheidung eines Gremiums ab. Existierende Zugriffskontrollmodelle sehen solche Anwendungsfälle nicht vor.

Fazit

Usable Security gewinnt zunehmend an Bedeutung. Unsere Arbeit im Rahmen der benutzbaren Zugriffskontrolle ebnet dabei den Weg für innovative Dienste im Future Internet, die die Sicherheit von digitalen Ressourcen nicht vernachlässigen. Zentrale Herausforderungen im Rahmen dieser Forschung präsentieren sich hauptsächlich in der Entwicklung von für IT-ferne Benutzer verständlichen Interaktionsmodellen. Wir arbeiten derzeit an Prototypen zur interaktiven und intuitiven Visualisierung von großen Graph-Strukturen. Es gilt dabei immer, die kognitiven Grenzen des Benutzers zu berücksichtigen.

Wir glauben, dass eine Verlagerung des Fokus von den Bedürfnissen der Maschine auf die Bedürfnisse des Benutzers insbesondere bei Sicherheitsmechanismen ein wichtiger Teil zukünftiger Internetanwendungen sein muss. Das Mind Mesh Projekt wird zeigen, wie die Kernaufgabe Sicherheit hiervon profitieren kann.

Literatur

- L.F. Cranor and S. Garfinkel. Security and Usability: Designing Systems that People Can Use. O'Reilly Media, 2005.
- M. Harbach and M. Smith. Visual Access Control for Research Ecosystems. In 5th IEEE International Conference on Digital Ecosystems and Technologies, pages 101–108, 2011.
- M. Smith, M. Harbach, S. Mertins, A. Lewis, and L. Griffiths. Towards a Translational Medicial Research Ecosystem. In Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies, pages 120–126, 2011.

Dipl.-Inf. Sascha Fahl
Jahrgang 1985, ist seit Anfang 2011 wissenschaftlicher Mitarbeiter in der Arbeitsgruppe *Distributed Computing and Security*. Seine Schwerpunkte liegen im Bereich der Usable Security, leichtgewichtiger Kryptografie und Zugriffskontrolle in verteilten Infrastrukturen. Kontakt: fahl@dcsec.uni-hannover.de

Dipl.-Inf. Marian Harbach
Jahrgang 1985, ist seit Herbst 2010 wissenschaftlicher Mitarbeiter in der Arbeitsgruppe *Distributed Computing and Security*. Seine Schwerpunkte liegen im Bereich der Usable Security und Zugriffskontrolle. Weitere Forschungsinteressen sind verteilte Forschungsinfrastrukturen und ihre Anwendungen. Kontakt: harbach@dcsec.uni-hannover.de

Prof. Dr. Matthew Smith
Jahrgang 1978, ist der Leiter der Arbeitsgruppe *Distributed Computing and Security* und Mitglied im Forschungszentrum L3S. Er forscht im Spannungsfeld von komplexen verteilten Systemen, deren Sicherheit und einfacher Benutzbarkeit. Kontakt: smith@dcsec.uni-hannover.de