Nutzung von Sozialen Netzwerk-Plattformen für die Verteilung von Public Keys

Malte Hülder · Vincent Wolff-Marting · Volker Gruhn

Professur für Angewandte Telematik/e-Business, Institut für Informatik,
Universität Leipzig
{huelder, wolff-marting, gruhn}@ebus.informatik.uni-leipzig.de

Zusammenfassung

Public Key Infrastrukturen (PKI) sind schon seit einigen Jahren bekannt, jedoch setzen sie sich nur sehr zögerlich durch, insbesondere im privaten Bereich. In diesem Artikel werden einige Hürden für die existierenden Ansätze (besonders das Web-of-Trust) beschrieben und es wird ein Lösungsansatz vorgestellt, der auf der Integration von sozialen Netzwerk-Plattformen mit den bestehenden Schlüssel-Servern beruht. Eine prototypische Umsetzung der genannten Ansätze zeigt, dass diese praktisch einsetzbar sind und die Usability von PKI verbessern können.

1 Einleitung

Public Key Infrastrukturen (PKI) können auf zwei verschiedene Arten umgesetzt werden [FeSc03]: Hierarchisch oder als Netzwerk. Beim hierarchischen Ansatz werden die Schlüssel zentral verwaltet und eine Certification Authority (CA) bestätigt die Authentizität der Schlüssel [CSFB+08, Caro00]. Als dezentrale Alternative wurde das Vertrauensnetzwerk (Web-of-Trust) entwickelt, in dem die Benutzer die Authentizität der Schlüssel wechselseitig bestätigen [Zimm95, Ecke04]. Das Vertrauensnetzwerk baut darauf, dass die Funktion „Vertrauen“ in gewisser Weise transitiv ist. Wenn beispielsweise ein Benutzer A einem Benutzer B vertraut, und B wiederum Vertrauen in einen dritten Benutzer C hat, dann kann A allein deswegen auch ein gewisses Vertrauen in C setzen [Maur96a].

Zur Verteilung und Authentifizierung öffentlicher Schlüssel existieren zwei zueinander nicht kompatible Standards, X.509 [CSFB+08] und OpenPGP [CDFT07]. Beide Standards definieren Formate zur Speicherung und zum Austausch von kryptographischem Schlüsselmaterial, zur Beglaubigung (Zertifizierung/Signierung) dieser Schlüssel sowie zum Widerruf von Schlüsseln oder Beglaubigungen. Mit den Schlüsseln können jeweils auch weitere Angaben zum Inhaber der Schlüssel zusammengefasst werden. Die Verbreitung und das vornehmliche Anwendungsgebiet beider Standards unterscheiden sich, was jedoch im Rahmen dieser Arbeit keine Auswirkungen hat. Insgesamt ist X.509 eher für ein hierarchisches Modell geeignet, OpenPGP vor allem für das Web-of-Trust entwickelt. Das äußert sich darin, das X.509 Zertifikate durch exakt eine Signatur beglaubigt sind, während OpenPGP Schlüsseln beliebig viele Signaturen zugeordnet werden können. Tatsächliche Implementierungen zeigen jedoch, dass eine X.509 Hierarchie

P. Horster (Hrsg.) · D•A•CH Security 2008 · syssec (2008) 1-10.

auch auf ein Vertrauensnetz aufbauen kann (siehe z.B. CAcert[1] , Thawte[2]). Umgekehrt lässt sich eine Hierarchie auch mit OpenPGP abbilden. So ist es zum Beispiel beim Einsatz von PGP in Unternehmen sinnvoll und üblich, dass alle Mitarbeiterschlüssel durch eine zentrale Stelle des Unternehmens signiert werden. CAcert bietet diesen Service ebenfalls an.

Während der letzten Jahre hat sich gezeigt, dass PKI – egal nach welchem Standard – von privaten Benutzern nur zögerlich angenommen werden. Wir sehen verschiedene Gründe für diese träge Entwicklung: Hierarchische PKI sind recht kostenintensiv. An den professionellen Betrieb einer CA werden von den Kunden besondere Anforderungen bezüglich Verfügbarkeit und Datenschutz gestellt, die sich in hohen Betriebskosten niederschlagen. Das gilt insbesondere, wenn der Anbieter fortgeschrittene oder qualifizierte Lösungen im Sinne der EU Signaturrichtlinie [PaRa00] anbietet. Dezentrale Web-of-Trust Strukturen basieren auf einem Peer-to-Peer Ansatz, sie können kostengünstiger realisiert werden, aber Verfügbarkeit und Datenschutz liegen im Verantwortungsbereich der Nutzer. Die geringeren monetären Kosten werden gewissermaßen durch eine höhere Zeitinvestition des Benutzers erkauft. Schließlich erfordern beide Ansätze in hohem Maße Benutzerinteraktion, die die Fähigkeiten eines unerfahrenen Nutzers leicht übersteigen. Zum Beispiel kann das Web-of-Trust in den gängigen E-Mail Programmen Outlook und Thunderbird erst nach der Installation von Zusatzprogrammen genutzt werden [CDFT07]. Hierarchische PKI erfordern die manuelle Installation von Zertifikaten und fehlende Zertifikate werden durch generische Fehlermeldungen bemängelt (siehe Abb. 1).

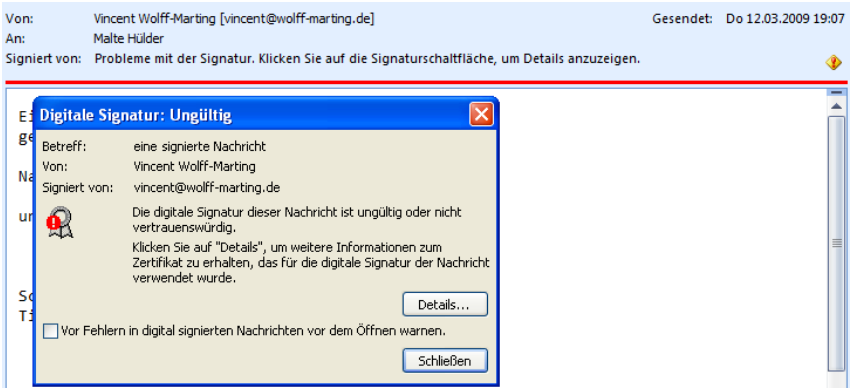

Abb. 1: Fehlermeldung für nicht installierte Zertifikate in MS Outlook.

Im folgenden Abschnitt 2 werden die Hürden, die insbesondere private Nutzer von der scheinbar kostenlosen Nutzung des Web-of-Trust abhalten, weiter ausgeführt. In Abschnitt 3 werden Möglichkeiten zur Überwindung dieser Hürden vorgestellt, die sich aus der Kombination des Web-of-Trust mit den sozialen Netzwerk-Plattformen des sogenannten „Web 2.0“ ergeben. Der Zusammenhang zu ähnlichen Ansätzen wird in Abschnitt 4 erläutert. Abschnitt 5 schließlich stellt die prototypische Umsetzung des Konzeptes vor.

2 Hürden der bisherigen Ansätze

Wenn „Vertrauen“, so wie angenommen, transitiv funktioniert, dann sollte sich ein eng vermaschtes Vertrauensnetz relativ schnell aufbauen lassen, da jeder einer gewissen Anzahl von

[1] http://www.cacert.org
[2] http://www.thawte.com/secure-email/web-of-trust-wot/index.html

Personen traut und diese Personen wiederum (teilweise disjunkte) Gruppen von Vertrauten benennen können. Bereits 1967 hat Milgram [Milg67] dargelegt, dass zwei beliebige Personen nicht weiter als 6 Bekannte voneinander entfernt sind. 2003 wurde diese Hypothese mit E-Mail-Benutzern bestätigt [Watt03]. Ein vertrauenswürdiger Pfad von einer Person zu einer anderen sollte also durchschnittlich nicht mehr als 6 Knoten beinhalten. Dennoch bestehen existierende Vertrauensnetze oft nur aus einzelnen Inseln und sind weit davon entfernt, ein weltumspannendes Netz zu bilden [GGADG+02].

Ein Grund für dieses Phänomen mag darin liegen, dass die Bedeutung von „Vertrauen“ in einem Vertrauensnetz für viele Benutzer nicht ganz klar ist. Denn dahinter verbirgt sich einerseits die Aussage, dass die Authentizität der Bekanntschaft und des Schlüssels geprüft wurde, aber auch die Aussage, dass dieser Person zugetraut wird, ihrerseits mit hinreichender Sorgfalt die Angaben in Bezug auf Dritte zu machen. Sobald das Vertrauen in die Sorgfalt der Bekanntschaft unklar ist, kann nicht mehr von einer Transitivität ausgegangen werden.

Ein weiteres Hindernis ist die teils umständliche Handhabung der Implementierungen. Zwar existieren zwischenzeitlich Erweiterungen für die etablierten E-Mail Programme, jedoch erfordern sie eine manuelle Installation. Empfänger einer signierten Nachricht, die ihrerseits die notwendigen Erweiterungen nicht installiert haben, werden durch die für sie unleserliche Signatur leicht verunsichert. Um diese Verunsicherung zu vermeiden, verzichten erfahrene Benutzer mitunter sogar auf eine Signatur ihrer Nachrichten, wenn sie nicht absolut sicher sind, dass der Empfänger sie verstehen kann.

Der Austausch von Schlüsseln schließlich ist ebenfalls kompliziert. Wenn zwei Benutzer wechselseitig ihre Identität und die Authentizität der öffentlichen Schlüssel geprüft haben, sollen sie die Schlüssel des jeweils anderen elektronisch signieren. Die derart behandelten Schlüssel werden dann wieder veröffentlicht, sodass Dritte die Authentizität (und Vertrauenswürdigkeit) durch Prüfung von bereits vertrauten Signaturen feststellen können. Der ganze Vorgang kann zu einer ernsten Geduldsprobe für den Benutzer werden, wenn jeder der Schritte manuell durchgeführt werden muss.

Der Nachfolgend beschriebene Ansatz soll den gesamten Umgang mit Schlüsseln für den Benutzer einfacher und vor allem verständlicher gestalten.

3 Kombination sozialer Netzwerke mit PKI

In den letzten Jahren sind soziale Netzwerk-Plattformen im World Wide Web entstanden, die sich rasch einer wachsenden Beliebtheit erfreuen konnten. Ausgehend von Milgrams Theorie der „kleinen Welt“ [Milg67], verbinden einige dieser Netzwerke Leute mit ähnlichen Interessen oder Vorlieben (z.B. Flickr[3] oder Last.fm[4]), während andere im Wesentlichen die Bekanntenkreise der realen Welt nachbilden (z.B. MySpace.com[5] , Facebook[6] oder XING[7]).

Insbesondere die letzteren bilden eine Art zwischenmenschlicher Beziehungen ab, die einen gewissen Bekanntheitsgrad und Vertrauen zwischen den Mitgliedern des Netzwerks voraussetzt, wie sie auch in einem Web-of-Trust existieren. Soziale Netzwerk-Platformen, die ihre Mit-

[3] http://www.flickr.com
[4] http://last.fm
[5] http://www.myspace.com
[6] http://www.facebook.com
[7] http://www.xing.com

glieder nur aufgrund gemeinsamer Interessen miteinander verbinden, zeigen diese Eigenschaft wahrscheinlich nicht. Daher soll der Begriff „soziales Netzwerk“ im Folgenden nur für Netzwerke verwendet werden, die eine Repräsentation der realen Welt darstellen. Solche Netzwerke können auf verschiedene Weisen für die Verwaltung von Public Keys genutzt werden, die auf einander aufgebaut werden können:

1. Eine Soziale Netzwerk-Plattform unterstützt lediglich das Verknüpfen von Nutzerprofilen mit öffentlichen Schlüsseln, die auf herkömmlichen Web-of-Trust Schlüssel-Servern [KuLa07] gespeichert werden.

2. Das Netzwerk unterstützt zusätzlich aktiv das wechselseitige Signieren von öffentlichen Schlüsseln durch Kontakte.

3. Das Netzwerk bietet weitergehende Funktionen im Umfeld um die Schlüsselverwaltung an.

Die Vorteile dieser Möglichkeiten werden in den folgenden Abschnitten diskutiert. Ein zentrales Anliegen ist es dabei, die Usability zu verbessern und die notwendigen Schritte für den Endbenutzer einfach und verständlich darzustellen. Der vorgestellte Ansatz ist grundsätzlich zu den beiden Standards X.509 und OpenPGP kompatibel. Zwar stützt er sich auf ein Vertrauensnetzwerk, doch, wie die in der Einleitung genannten Beispiele zeigen, ist das keine zwingende Festlegung. Diese Abschnitt ist daher allgemein gefasst, wo nötig werden die Unterschiede oder Gemeinsamkeiten im Detail erläutert.

3.1 Schlüsselverwaltung

Die elementarste Unterstützung der Schlüsselverwaltung (bzw. Zertifikatsverwaltung) besteht darin, Public Keys wie andere persönliche Daten in der Plattform zu speichern – Benutzer können ihre eigenen Schlüssel hoch laden und die Schlüssel anderer Nutzer herunter laden. Im Vergleich zu existierenden Schlüssel-Servern [KuLa07] bedeutet dies zunächst nur erhöhten Komfort. Die Suche und Identifikation von Schlüsseln und deren Eigentümern ist leichter und bequemer, da Netzwerk-Plattformen üblicherweise mehr persönliche Informationen über ihre Benutzer vorhalten als traditionelle Schlüssel-Server. Darüber hinaus könnten die einfache Verwendung die aktuelle Popularität von sozialen Netzwerken das öffentliche Interesse in elektronischen Signaturen als Nebeneffekt verstärken.

Da der Eigentümer eines Schlüssels in der Regel nicht sicher von der Plattform authentifiziert wird, wenn er einen Schlüssel hoch lädt, kann aber auch keine Zusicherung in Bezug auf die Authentizität des Schlüssels gegeben werden. Anders als traditionelle Schlüssel-Server werden soziale Netzwerke aktiv für die Kommunikation zwischen ihren Mitgliedern genutzt und ermöglichen so eine weitere Form der multilateralen Authentifizierung: Während es meist relativ leicht ist, eine gefälschte Identität in einem sozialen Netzwerk anzulegen, ist es schon wesentlich schwieriger, ein Netzwerk von Bekannten aufzubauen und zu unterhalten, das mit dem realen Netzwerk der imitierten Person übereinstimmt. Übliche Interaktionen mit Hilfe der Plattform, insbesondere im Kontext realer Aktivitäten (z.B. gemeinsamer Treffen) können ein gewisses Vertrauen in das Benutzerkonto rechtfertigen. Ein Teil dieses Vertrauens könnte auf die Public Keys übertragen werden, die mit diesem Benutzerkonto verbunden wurden – speziell, wenn diese Verbindung schon seit einiger Zeit besteht. Allerdings gilt dies nur für direkte Kontakte, ein solches indirektes Vertrauen kann nicht als transitiv angenommen werden. Insbesondere ist hier kein Schutz gegen ausgeklügelte Angriffe wie Man-in-the-Middle-Angriffe (MITM), die Übernahme eines fremden Kontos [FeSc03] gegeben. Auch besteht kein Schutz vor Angriffen, bei denen die soziale Struktur des Opfers aus einer Plattform einfach in einer

Anderen nachgebildet wird (Profil-Imitation). Zusammenfassend muss davon abgeraten werden, einem Schlüssel zu vertrauen, der nicht auch auf andere Weise verifiziert worden ist.

3.2 Authentifizierung und Schlüsselsignatur

Um den Web-of-Trust-Charakter eines virtuellen sozialen Netzwerks explizit zu verbessern, ist die Implementierung eines Protokolls zur Nutzerauthentifizierung und zur Schlüsselsignatur erforderlich. Richtig angewandt bietet so ein Protokoll auch vor der im letzten Abschnitt beschriebenen Profil-Imitation einen gewissen Schutz. Wie beschrieben, signieren die Benutzer von OpenPGP ihre Schlüssel gegenseitig [Caro00], während bei X.509 sämtliche Signaturen von wenigen zentralen Instanz getätigt werden [CSFB+08]. Traditionell benötigt der Prozess der Schlüsselsignatur in einem Web-of-Trust mehrere Nutzerinteraktionen. Zunächst muss der Benutzer den Schlüssel erhalten und unter Nutzung eines möglichst sicheren Kommunikationskanals prüfen, ihn schließlich signieren und dann die neue Signatur veröffentlichen.

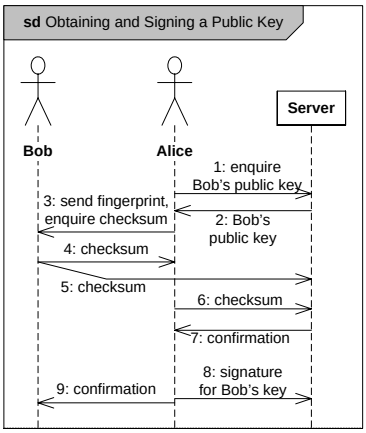

Abb. 2: UML Sequenz-Diagramm: Bezug und Signatur eines Public Key

Abb. 2 beschreibt einen möglichen Ablauf von Schlüsselprüfung und -signatur. Der Ablauf erfordert eine direkte Kommunikation zwischen Nutzern (Schritte 3, 4 und 9). Diese Kommunikation sollte niemals mit Mitteln des sozialen Netzwerks, sondern über einen unabhängigen Kommunikationskanal erfolgen. Ein Telefonanruf wäre hier beispielsweise empfehlenswert, da der Klang der Stimme und die beiläufige Unterhaltung eine recht verlässliche Authentifizierung zwischen Bekannten ermöglichen [Zimm95]. Ein persönliches Treffen ermöglicht wahrscheinlich die größte Sicherheit gegen vorgetäuschte Identitäten („Identitätsdiebstahl“), während E-Mail, Instant Messaging, Chat oder andere digitale Kanäle dies nicht leisten. Je nach der gewünschten Zuverlässigkeit kann eine Plattform Richtlinien vorgeben, welche Kommunikationskanäle für diesen Zweck vorgeschrieben oder verboten sind – die Plattform kann den genutzten Kommunikationskanal ggf. zusammen mit den Signaturen in Schritt 8 erfassen und diese Information zur Gewichtung der Signaturen bei einer Vertrauensberechnung heranziehen. Das OpenPGP Nachrichtenformat definiert verschiedene „Signaturtypen“, um unterschiedliche Gewissenhaftigkeit bei der Nutzerverfikation abzubilden [CDFT07, Kap. 5.2.1.].

Die Prüfsumme, die in den Schritten 4-6 genutzt wird, sollte für jeden Nutzer separat berechnet werden; sie darf nicht mit dem „Fingerabdruck“ verwechselt werden, der traditionell zur Schlüsselprüfung eingesetzt wird. Eine eindeutige Prüfsumme erzwingt die direkte Kommunikation und dadurch die implizite Authentifizierung des Schlüsseleigentümers: Ein Zufallswert

könnte hier bereits ausreichend sein. Der traditionelle Fingerabdruck kann leicht von jedermann berechnet werden und daher kann die direkte Kommunikation möglicherweise umgangen werden. Die Plattform sollte keine Signaturen akzeptieren (Schritt 8), solange sie die zugehörigen Prüfsummen nicht erhalten hat (Schritte 5 und 6). Dadurch wird die Gefahr reduziert, einem vorher eingeschleusten, gefälschten Schlüssel zusätzliche Glaubwürdigkeit zu verleihen. Eine Ausnahme muss möglicherweise für den Schlüsseleigentümer gemacht werden, der wahrscheinlich nicht bereit sein wird, Signaturen die auf anderen Plattformen oder Wegen durchgeführt wurden, noch einmal zu wiederholen. Es kann sinnvoll sein, zwischen Signaturen, die mit Hilfe dieser sozialen Netzwerk-Plattform erzeugt wurden, und anderen Signaturen zu unterscheiden. Beispielsweise könnten die letzteren von Vertrauensberechnungen ausgeschlossen werden. In jedem Fall sollte aber der Schlüssel spezifische Fingerabdruck zusammen mit der Anfrage in Schritt 3 übertragen werden, um sicherzustellen, dass der im vorhergehenden Schritt übermittelte Schlüssel nicht kompromittiert wurde.

Die Nachricht in Schritt 5 sollte mit dem zu prüfenden Schlüssel signiert werden, um MITM Angriffe zu verhindern; falls Schritt 4 auch elektronisch durchgeführt wird, sollte er ebenfalls signiert werden. Um die Nutzerakzeptanz zu erhöhen, sollte das Protokoll möglichst weitgehend automatisiert durchgeführt werden können.

Falls dieses Protokoll mit X.509 Zertifikaten durchgeführt werden soll, kann in Schritt 8 ein Zertifikat generiert und vom Server signiert werden. Dafür kann der Server eine gewisse Anzahl von Beglaubigungen voraussetzen (vgl. CAcert[8] , Thawte[9]).

In bestimmten Situationen muss die Signatur eines Schlüssels (bzw. ein Zertifikat) widerrufen und für ungültig erklärt werden. OpenPGP und X.509 stellen Mittel für einen solchen Widerruf bereit [CDFT07, CSFB+08]. Der Widerruf eines Zertifikats ist eine dauerhafte Maßnahme, die weitere Nutzung des Zertifikats verbietet. Sie wird in der Regel notwendig, wenn der private Schlüssel bekannt geworden ist oder wenn ein Zertifikat fehlerhaft ausgestellt wurde.

In einem Web-of-Trust kann ein Public Key mittels des zugehörigen privaten Schlüssels oder eines vorher autorisierten Widerufsschlüssels widerrufen werden. Zertifikate können ganz ähnlich mit dem Schlüssel, mit dem sie veröffentlicht wurden oder einem vorher autorisierten Widerufsschlüssel widerufen werden. In einer Hierarchie wird der Widerruf von der CA durchgeführt. Eine soziale Netzwerk-Plattform muss den Eigentümern sowie den Signierern eines Schlüssels die Möglichkeit geben, Widerrufsschlüssel in eine Web-of-Trust Umgebung zu laden, sowie für hierarchische Umgebungen ein Protokoll zum Widerruf von Zertifikaten als Antwort auf Beschwerden definieren. Außerdem könnten einzelne Nutzer anderen Nutzern aus persönlichen Gründen explizit misstrauen wollen, was aber noch keinen Widerruf rechtfertigen würde – beispielsweise könnten sie die anderen Nutzer verdächtigen, das Authentifizierungsprotokoll aus Unkenntnis oder absichtlich nicht korrekt durchzuführen und stattdessen ungeprüfte Zertifikate auszustellen. Verschiedene Autoren haben sich dieses Themas bereits angenommen und Berechnungsgrundlagen für Vertrauensberechnungen vorgestellt, die auch das Konzept des Misstrauens berücksichtigen [GoPH03, RiAD03, GKRT04]. Eine soziale Netzwerk-Plattform, die Vertrauensberechungen durchführt, sollte diesen Aspekt ebenfalls berücksichtigen.

[8] http://www.cacert.org

[9] http://www.thawte.com/secure-email/web-of-trust-wot/index.html

3.3 Weitere Unterstützungen zur Schlüsselverwaltung

Eine wichtige Eigenschaft von Public Key Infrastructures ist die Möglichkeit, Vertrauen anhand eines Vertrauenspfades auf unbekannte Signaturen zu übertragen [Caro00]. Derzeit scheint es jedoch für OpenPGP keine benutzerfreundlichen Möglichkeiten zu geben, einen solchen Pfad zu finden; es existieren allenfalls experimentelle Ansätze [McDo05, Darx02]. Soziale Netzwerk-Plattformen bieten oftmals bereits die Möglichkeit, Pfade zu anderen Mitgliedern des Netzwerks zu finden. Einen Vertrauenspfad innerhalb des Netzwerks zu finden, kann daher ebenfalls leicht angeboten werden, wenn die Informationen über Public Keys in die Plattform integriert werden. Für X.509 Zertifikate ist diese Funktion nicht relevant, da diese Zertifikate alle zur Verifikation nötigen Informationen bereits enthalten sollten.

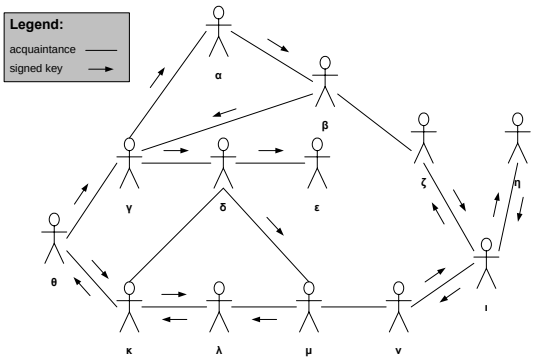

Abb. 3: Ein Web-of-Trust in einem sozialen Netzwerk

Außerdem kann die Plattform Lücken im Web-of-Trust finden und Nutzer ermuntern, diese Lücken zu schließen. Abb. 3 zeigt ein einfaches soziales Netzwerk, das ein Web-of-Trust enthält. Die Verbindungslinien zeigen Bekanntschaften an, die Pfeile zeigen von einem Schlüsselsignierer zu einem Schlüsseleigentümer. Zwar ist das Netzwerk ist zusammenhängend, nicht jedoch das Web-of-Trust. Um beide Zusammenhangskomponenten zu verbinden, kann die Plattform vorschlagen, dass β und ζ oder μ und ν ihre Schlüssel austauschen und gegenseitig signieren. Darüber hinaus gibt es ein paar Brücken, die das Web-of-Trust trennen, falls sie entfernt würden. Daher sollten auch δ und κ (sowie die meisten einseitigen Verbindungen) animiert werden, ihre Schlüssel auszutauschen und gegenseitig zu signieren. Aus praktischen Gründen sollten immer beide Nutzer aufgefordert werden, ihre Schlüssel gegenseitig zu prüfen und zu signieren. In einem realistischen (also wesentlich komplexeren) Szenario, können die kritischen Kanten mit Hilfe der Graphentheorie gefunden werden.

Nutzer könnten ihre Schlüssel mit ihrer virtuellen Identität im sozialen Netzwerk verknüpfen und umgekehrt. Auf diese Weise kann klargestellt werden, dass ein bestimmter Schlüssel zur Nutzung im Kontext des sozialen Netzwerks bestimmt ist. Ohne eine solche Verknüpfung könnte ein Angreifer seiner gefälschten Identität im sozialen Netzwerk den realen Public Key eines Opfers hinzufügen. Zwar kann er mit diesem Schlüssel weder Nachrichten signieren oder entschlüsseln, jedoch könnte er Dritte verleiten, dieser virtuellen Identität zusätzliches Vertrauen zu schenken. Ein OpenPGP-Schlüssel kann mit einer virtuellen Identität im sozialen Netzwerk verknüpft werden, indem ein zusätzliches „User ID Package“ hinzugefügt und mit dem eigenen Schlüssel signiert wird. Per Konvention sollte die User ID als E-Mail-Adresse gemäß RFC 2822 angegeben werden, aber es ist auch jede andere UTF-8 Zeichenkette erlaubt

[CDFT07]. Eine vernünftige Namenskonvention für soziale Netzwerke zu finden, sollte kein besonders schwieriges Problem darstellen.

Ein X.509 Zertifikat sollte über das „SubjectAltName“ Attribut mit der virtuellen Identität im sozialen Netzwerk verknüpft werden. An dieser Stelle sind verschiedene Formate erlaubt, einschließlich E-Mail-Adressen und URIs [CSFB+08]. Alternativ könnte auch das „Subject“ Attribut genutzt werden, allerdings würde dies die Verwendung eines „X.500 distinguished name“ [ITUT05] erfordern, der ggf. nicht gut zu den bestehenden Namenskonventionen eines sozialen Netzwerks passen würde. Da die X.509 Zertifikate, die wir in diesem Artikel angesprochen haben, ausschließlich von der sozialen Netzwerk-Plattform ausgegeben werden, erscheint eine Verknüpfung zu der jeweiligen virtuellen Identität notwendig.

4 Verwandte Arbeiten

Khan und Shaikh schlagen eine „Relationship Algebra“ vor, die die Übertragung aus einem sozialen Beziehungsnetzwerk in eine generische Algebra ermöglicht [KhSh06]. Dann kann eine Menge von Nebenbedingungen definiert werden, die genutzt werden kann, um bestimmte Fragen durch Anwendung von algebraischen Operationen zu beantworten. Khan und Shaikh liefern zwei Beispiele: Eins ist die Auswahl eines Gutachters für eine wissenschaftliche Konferenz oder ein Journal. Das zweite Beispiel betrachtet die Gabe von Impfstoffen und Immunisierung. Der Ansatz lässt sich auch auf Vertrauen in einem sozialen Beziehungsnetzwerk erweitern.

Ries, Kangasharju und Mühlhäuser bieten einen Überblick über Vertrauenssysteme [RiKM06]. Jeder der vorgestellten Ansätze bietet ein eigenes Modell und es ist schwierig, sie direkt zu vergleichen. In [RiKM06] wird eine Reihe von Kriterien vorgestellt, mit denen die verschiedenen Systeme analysiert werden, und es wird festgestellt, dass eine gewisser Grad an Unsicherheit oder Konfidenz in dem Modell enthalten sein muss, um nützliche Aussagen in virtuellen sozialen Netzwerken treffen zu können.

Maurer erläutert, dass Vertrauen nicht durch ein binäres System beschrieben werden kann, sondern einer kontinuierlichen Skala bedarf [Maur96a]. Er schlägt dafür das Intervall zwischen 0 und 1 vor, so dass die Werte als Wahrscheinlichkeiten interpretiert werden können. Er beschreibt, wie Vertrauen über einen Pfad von Empfehlungen berechnet werden kann und kommt zu dem Schluss, dass das Vertrauen relativ schnell abnimmt. In [Maur96b] werden umfassende Berechnungen zu der Betrugswahrscheinlichkeit einer einseitigen Nachrichtenauthentifizierung angestellt. Diese Berechnungen ließen sich zum Vergleich der Wahrscheinlichkeiten auf den Web-Of-Trust Ansatz übertragen.

Das PGP Web-Of-Trust wurden von Guardiola u. a. untersucht [GGADG+02]. Sie haben entdeckt, dass es sich eher um eine Menge von stark verknüpften Clustern handelt als um einen verknüpften Graphen. Ferner haben sie festgestellt, dass dieser Graph recht robust gegen absichtliche Angriffe ist.

Golbeck, Parsia und Hendler haben einen Algorithmus für die Berechnung von Vertrauen in sozialen Netzwerken als Proof of Concept entwickelt [GoPH03]. Sie schlagen vor, ihn zur Klassifizierung der Glaubwürdigkeit von Ressourcen, etwa Dokumenten oder Nachrichten, in semantischen Netzen zu verwenden. Sie betonen speziell den Unterschied zwischen der Kenntnis des Ursprungs einer Ressource und dem Vertrauen in deren Inhalt. Ferner berücksichtigt der Algorithmus explizit auch Misstrauen. Richardson, Agrawal und Domingos verfolgen einen ähnlichen Ansatz [RiAD03]. Sie betonen besonders, dass Vertrauensberechnungen in

Abhängigkeit vom Startpunkt, also dem Benutzer, dessen Vertrauen berechnet werden soll, zu unterschiedlichen Ergebnissen führen können. Beide Artikel gehen nicht explizit auf Soziale Netzwerk Plattformen ein – zum Zeitpunkt der Veröffentlichungen waren diese Systeme auch noch nicht besonders verbreitet. Dennoch sind die Algorithmen dafür gut geeignet. Eine weitergehende Untersuchung des Konzeptes „Misstrauen“ findet sich in [GKRT04].

Victor u.a. haben die Bedeutung von Schlüsselfiguren für Netzwerke beschrieben, in denen Nutzern Produkte oder Webseiten auf der Basis von Bewertungen durch andere Nutzer empfohlen werden [VCTDC08]. Die untersuchte Art von Netzen ist eher vergleichbar mit den zu Beginn von Abschnitt 3 genannten Netzwerken, die Personen mit ähnlichen Interessen verknüpfen, und daher nicht direkt auf diese Arbeit übertragbar. Trotzdem kann es im Sinne eines stark verknüpften Web-of-Trusts interessant sein, Schlüsselfiguren zu finden, die viele andere Nutzer verifiziert haben und besonders vertrauenswürdig sind, um durch die plattformseitige Empfehlung, seinen Schlüssel mit einer solchen Schlüsselfigur auszutauschen, auch Neulingen schnell zu einem gesteigerten Nutzen des Web-of-Trusts durch verkürzte Vertrauenspfade zu verhelfen.

Datta, Hauswirth und Aberer führen eine „quorum based decentralized PKI“ als Alternative zum Web-Of-Trust ein [DaHA03]. Sie basiert auf einer massiv-redundanten Schlüsselspeicherung in einem Peer-to-Peer Netzwerk. Dieser Ansatz richtet sich vor allem auf die Authentifizierung von Benutzerkonten. Er bietet keine Verknüpfung zwischen Personen und den Konten. Existierende Bekanntschaften und Vertrauen zwischen realen Personen wird daher bei diesem Ansatz nicht in Betracht gezogen.

5 Validation

Um die Realisierbarkeit der in diesem Artikel genannten Möglichkeiten zu zeigen und deren Praktikabilität zu erproben, wurde ein Prototyp implementiert, der die Verwaltung von Public Keys in einem sozialen Netzwerk ermöglicht. Der Prototyp wurde auf Basis von OpenSocial[10] erstellt, einer gemeinsamen Schnittstelle für soziale Netzwerke, die von Google entwickelt wurde und von verschiedenen namhaften Betreibern sozialer Netzwerke unterstützt wird. Es sollte daher relativ leicht fallen, diesen Prototyp später in bestehende soziale Netzwerke zu integrieren, wenn die Entwicklung ausgereift ist.

In der derzeitigen Ausbaustufe erlaubt es der Prototyp, Public Keys, die auf einem Schlüssel-Server abgelegt sind, mit einem Nutzerkonto zu verbinden. Bei Besichtigung des Nutzerprofils kann dann jeder erkennen, dass die Person einen Public Key besitzt und diesen auch über die Plattform beziehen. Dabei betreibt die Plattform keinen eigenen Schlüssel-Server, sondern nutzt die bereits vorhandene Infrastruktur.

Der Prototyp ermöglicht es ebenfalls, einen Vertrauenspfad von einem Mitglied des soziale Netzwerks zu einem anderen zu ermitteln (Abb. 4). Auf diese Weise kann ein Nutzer feststellen, wie lang der Pfad zu einer ihm nicht direkt bekannten Person ist und überlegen, ob er dessen Public Key anhand des Vertrauenspfads ein gewisses Vertrauen zubilligen möchte oder nicht. Dabei kann der Prototyp die sog. „Signaturtypen“ [CDFT07, Kap. 5.2.1] auslesen und insbesondere die Information über die Gewissenhaftigkeit bei der Nutzerverfikation zu einer Signatur (0x10-0x13) interpretieren und anzeigen. Diese Daten bilden einen Grundbaustein der Vertrauensberechnung für einen Vertrauenspfad.

Der vorgestellte Prototyp hat noch keinen produktiven Stand erreicht. Hierfür gilt es, zunächst

[10] http://www.opensocial.org

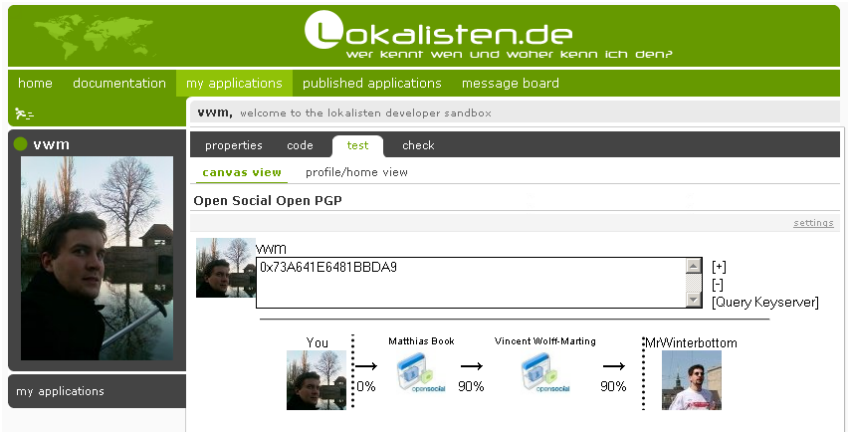

Abb. 4: Screenshot des Prototyps

noch die Performanz und Stabilität zu verbessern, außerdem sollen auch die in Abschnitt 3 genannten erweiterten Maßnahmen umgesetzt werden.

6 Zusammenfassung und Ausblick

In den vorherigen Kapiteln wurde gezeigt, wie virtuelle soziale Netzwerk-Plattformen helfen können, Hürden bei der Verteilung von öffentlichen Schlüsseln zu überwinden. Dazu wurde ein einfaches Protokoll zur wechselseitigen Authentifizierung und zum Signieren der Schlüssel für Mitglieder eines solchen Netzwerkes vorgestellt. Anstelle einer vollständig neuen technologischen Lösung wurden Verbesserungen der Usability und Automatisierungen vorgeschlagen. Die Lösung ist uneingeschränkt kompatibel zu vorhandenen Systemen und kann parallel zu ihnen betrieben werden. Das vorgestellte Web-of-Trust kann verschiedene unabhängige, sogar zueinander im Wettbewerb stehende Plattformen überspannen.

Die vorgestellten Mechanismen wurden zu einen gewissen Teil bereits prototypisch realisiert. Der Prototyp verbindet die beiden Welten der sozialen Netzwerke und OpenPGP-Schlüssel-Server, sodass das Auffinden von Schlüsseln deutlich vereinfacht wird. Der Prototyp ist jedoch noch in einem frühen Stadium; bevor er in einem produktiven System eingesetzt werden kann, müssen Stabilität und Performanz verbessert werden.

Diese Arbeit betrachtet vor allem den Schlüsselaustausch zwischen Individuen. In großen Organisationen und Unternehmen wird der hierarchische Ansatz sinnvoller sein als ein Web-of-Trust, da ein Web-of-Trust auf Veränderungen wie zum Beispiel Einstellungen und Entlassungen nur langsam reagiert. Eine virtuelle soziale Netzwerk Plattform wird keine neuen Funktionen zur existierenden Authentifizierung innerhalb der Organisation beitragen. Kleine und mittlere Unternehmen können durchaus von dem beschriebenen Ansatz profitieren, da er kostengünstiger umzusetzen sein kann, als die Implementierung einer eigenen PKI.

Für die Kommunikation zwischen den Mitgliedern verschiedener Organisationen kann der beschriebene Ansatz – unabhängig von der Größe der Organisation – eine nützliche Abkürzung darstellen, wenn keine direkte Authentifizierung, wie etwa wechselseitig signierte Root-Zertifikate, vorgesehen ist.

In Zukunft wollen wir die Vertrauensberechnung von Vertrauenspfaden im Netzwerk genauer betrachten. Beiträge von Jøsang u.a. [JøHP06, JøBh08] zur „Subjective Logic“ bieten eine

gute Grundlage für diese Arbeit. Dabei soll aber Einbindung eines Algorithmus zur Vertrauensberechnung möglichst offen gestaltet werden, sodass auch andere Algorithmen genutzt und miteinander verglichen werden können.

Außerdem sollen weitergehende Maßnahmen untersucht werden, die die Nutzung von Signaturen und Verschlüsselung in sozialen Netzwerken voran bringen können. Beispielsweise kann ein Browser-Plugin ermöglichen, dass die Kommunikation zwischen Mitgliedern des sozialen Netzwerks auch bei Nachrichtenfunktionen innerhalb des Netzwerks signiert oder verschlüsselt werden kann. Auf diese Weise könnte dann durch Verschlüsselung sichergestellt werden, dass die Nachrichten in einem geschlossenen Forum tatsächlich nur für den festgelegten Nutzerkreis zugänglich sind. Selbst wenn durch Sicherheitslücken Nachrichten für Dritte zugänglich werden, wie es in der Vergangenheit bereits passiert ist, bleiben die Inhalte durch die Verschlüsselung geschützt. Eine solche Funktionalität kann insbesondere auch für Unternehmen interessant sein, die vertrauliche Informationen nur mit ausgewählten Kommunikationspartnern teilen möchten. Bei einer Umsetzung ist entscheidend, dass private Schlüssel bei deren Eigentümer verbleiben und allenfalls für das lokale Browser-Plugin zugänglich sind, aber niemals über das Netzwerk übertragen oder gar in der Netzwerk-Plattform gespeichert werden.

7 Danksagung

Die Professur für Angewandte Telematik/e-Business ist eine Stiftungsprofessur der Deutschen Telekom AG.

Literatur

[Caro00] G. Caronni: Walking the Web of Trust. IEEE Computer Society, Los Alamitos, CA, USA (2000), Bd. 00, 153.

[CDFT07] J. Callas, L. Donnerhacke, H. Finney, R. Thayer: OpenPGP Message Format. RFC 4880. (2007), `http://tools.ietf.org/html/rfc4880`.

[CSFB+08] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280. (2008), `http://tools.ietf.org/html/rfc5280`.

[DaHA03] A. Datta, M. Hauswirth, K. Aberer: Beyond "web of trust": Enabling P2P E-commerce. In: *Proceedings of the IEEE International Conference on E-Commerce* (2003), 303–313.

[Darx02] Darxus: GPG/PGP Signature Path Tracing (2002), `http://www.chaosreigns.com/code/sigtrace/`.

[Ecke04] C. Eckert: IT-Sicherheit. Oldenbourg Verlag, 3. Aufl. (2004).

[FeSc03] N. Ferguson, B. Schneier: Practical Cryptography. Wiley (2003).

[GGADG+02] X. Guardiola, R. Guimera, A. Arenas, A. Diaz-Guilera, D. Streib, L. A. N. Amaral: Macro- and micro-structure of trust networks. In: *ArXiv Condensed Matter e-prints* (2002), `http://arxiv.org/abs/cond-mat/0206240`.

[GKRT04] R. Guha, R. Kumar, P. Raghavan, A. Tomkins: Propagation of trust and distrust. *In: WWW '04: Proceedings of the 13th international conference on World Wide Web*, ACM Press, New York, NY, USA (2004), 403–412.

[GoPH03] J. Golbeck, B. Parsia, J. Hendler: Cooperative Information Agents VII, Springer, Berlin, Heidelberg, *Lecture Notes in Computer Science*, Bd. 2782, Kap. Trust Networks on the Semantic Web (2003), 238–249.

[ITUT05] ITU-T: Recommendation X.500, The Directory: Overview of Concepts, Models and Service (2005), `http://www.itu.int/rec/T-REC-X.500-200508-I/en`.

[JøBh08] A. Jøsang, T. Bhuiyan: Optimal Trust Network Analysis with Subjective Logic. In: *Emerging Security Information, Systems, and Technologies, The International Conference on*, 0 (2008), 179–184.

[JøHP06] A. Jøsang, R. Hayward, S. Pope: Trust network analysis with subjective logic. *In: ACSC '06: Proceedings of the 29th Australasian Computer Science Conference*, Australian Computer Society, Inc., Darlinghurst, Australia, Australia (2006), 85–94.

[KhSh06] J. I. Khan, S. Shaikh: Relationship Algebra for Computing in Social Networks and Social Network Based Applications. In: *Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence (WI'06)* (2006).

[KuLa07] C. Kuethe, R. Laager: OpenPGP Public Key Server (2007), `http://pks.sourceforge.net`.

[Maur96a] U. Maurer: Modelling a Public-Key Infrastructure. *In: ESORICS'96* (1996).

[Maur96b] U. Maurer: A Unified and Generalized Treatment of Authentication Theory. *In: STACS: Annual Symposium on Theoretical Aspects of Computer Science* (1996), *LNCS*, Bd. 1046, 387–398.

[McDo05] J. McDowell: Experimental PGP key path finder (2005), `http://the.earth.li/~noodles/pathfind.html`.

[Milg67] S. Milgram: The small world problem. In: *Psychology Today*, 2 (1967), 60–67.

[PaRa00] E. Parlament, E. Rat: Richtlinie 1999/93/EC des Europäischen Parlamentes und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. In: *Amtsblatt der Europäischen Gemeinschaften*, L 13 (2000), 12–20.

[RiAD03] M. Richardson, R. Agrawal, P. Domingos: The SemanticWeb –ISWC 2003, Springer, Berlin / Heidelberg, *Lecture Notes in Computer Science*, Bd. 2870, Kap. Trust Management for the Semantic Web (2003), 351–368.

[RiKM06] S. Ries, J. Kangasharju, M. Mühlhäuser: A Classification of Trust Systems. *In: R. Meersman, Z. Tari, P. Herrero, (Hrsg.), OTM Workshops 2006*, LNCS 4277, Springer-Verlag Berlin Heidelberg (2006), 894–903.

[VCTDC08] P. Victor, C. Cornelis, A. M. Teredesai, M. De Cock: Whom Should I Trust? The Impact of Key Figures on Cold Start Recommendations. *In: SAC '08: Proceedings of the 2008 ACM symposium on Applied computing*, ACM, New York, NY, USA (2008), 2014–2018.

[Watt03] D. J. Watts: Six degrees: The Science of a Connected Age. Norton (2003).

[Zimm95] P. R. Zimmermann: The Official PGP User's Guide. MIT Press, Boston, Massachusetts, U.S.A. (1995).