Stärken und Schwächen von PKI

Johanna Cuno
Betreuer: Ralph Holz
Seminar Innovative Internettechnologien und Mobilkommunikation SS2010
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: cunoj@in.tum.de

KURZFASSUNG

Public Key Infrastructure (PKI) basiert auf den Methoden der asymmetrischen Kryptographie. Der Ansatz besitzt mehrere Vorteile, die ein Grund für die große Verbreitung von PKI sind. So unterstützt die Technologie wichtige Sicherheitskriterien wie Authentifizierung, Vertraulichkeit, Integrität und Nicht-Abstreitbarkeit. Zudem ermöglicht die am häufigsten eingesetzte PKI-Variante, die hierarchische PKI, eine zentral organisierte Administration von Zertifikaten bzw. Schlüsseln. Den Vorteilen steht eine Reihe von Nachteilen gegenüber. Ein ungelöstes Problem betrifft die Handhabung der Zertifikatsperrung. Weitere Probleme beruhen darauf, dass die der PKI zu Grunde liegenden Modelle Vertrauensbeziehungen (zum Beispiel zwischen Nutzer und Zertifizierungsstelle) modellieren, die mit den Realwelt-Bedingungen schwer vereinbar sind. Zusammengenommen überwiegen die Schwierigkeiten, die bei der Umsetzung von PKI in die Praxis auftreten.

Schlüsselworte

Public Key Infrastructure (PKI), digitales Zertifikat, digitale Signatur, Zertifizierungsstelle (engl. Certificate Authority, CA), Vertrauensmodelle, Verschlüsselungsverfahren

1. EINLEITUNG

Im globalen Wettbewerb ist es für Unternehmen von existenzieller Bedeutung, sicher kommunizieren und elektronische Transaktionen durchführen zu können. Um eine sichere Kommunikation im Unternehmensnetzwerk, aber ebenso mit Business-Partnern, Lieferanten und Kunden gewährleisten zu können, ist eine verlässliche IT-Infrastruktur notwendig. Gleichermaßen besteht ein sehr hoher Sicherheitsbedarf bei staatlichen Institutionen.

Public Key Infrastructure (PKI) wird weithin als die IT-Technologie betrachtet, die diesen Sicherheitsanforderungen gerecht wird ([1], [2]). In vielen Organisationen ist PKI zentraler Bestandteil der Sicherheitsarchitektur. Es gibt jedoch auch einige kritische Stimmen, die Schwächen von PKI aufzeigen und teilweise den gesamten Ansatz in Frage stellen [4]. Beides, Vor- und Nachteile des PKI-Ansatzes, sind Inhalt dieser Ausarbeitung.

Zu Beginn werden einige kryptographische Grundlagen behandelt. Dazu werden in Abschnitt 2 die Verfahren der symmetrischen und asymmetrischen Verschlüsselung und das Konzept der digitalen Signatur beschrieben. Im dritten Teil wird das Konzept von PKI erklärt. In den Abschnitten 4 und 5 werden schließlich die wesentlichen Stärken und Schwächen von PKI herausgestellt. Der Artikel endet mit einem kurzen Ausblick zu möglichen Alternativen in Kapitel 6 und einer abschließenden Bewertung in Kapitel 7.

2. GRUNDLAGEN

Im Folgenden werden zunächst die zwei prinzipiellen Arten der Verschlüsselung erklärt und voneinander abgegrenzt. Zudem wird der Begriff der digitalen Signatur behandelt, da dieser für das Verständnis von PKI grundlegend ist.

2.1 Symmetrische Kryptographie

Bei symmetrischen Verschlüsselungsverfahren wird ein geheimer Schlüssel verwendet. Auf der Seite des Senders wird das Dokument mit einem geheimen Schlüssel verschlüsselt. Der Empfänger kann die verschlüsselte Nachricht nur mittels desselben geheimen Schlüssels entschlüsseln. Dazu müssen die beteiligten Parteien einen sicheren Weg finden, den geheimzuhaltenden Schlüssel miteinander auszutauschen. Dies ist der wesentliche Nachteil der symmetrischen Verschlüsselung. In [2] werden diese Problematik und ein möglicher Lösungsansatz (Key Distribution Center, KDC) diskutiert.

Der große Vorteil symmetrischer Verschlüsselungsverfahren ist, dass sie im Vergleich zu den nachfolgend beschriebenen asymmetrischen Verfahren einen geringeren Rechenaufwand und kürzere Schlüssel erfordern.

In Abbildung 1 ist das Verfahren bei der symmetrischen Verschlüsselung veranschaulicht.

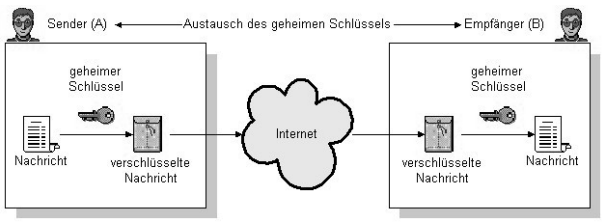

Abbildung 1: Symmetrische Verschlüsselung [11]

2.2 Asymmetrische Kryptographie

Bei den Verfahren der asymmetrischen Verschlüsselung (engl. public key encryption) verschlüsselt der Sender ein Dokument mit dem öffentlichen Schlüssel des Empfängers. Dieser wiederum entschlüsselt die Nachricht mit seinem privaten

Schlüssel (vgl. Abb. 2). Das Problem, dass ein geheimer Schlüssel ausgetauscht werden muss, entfällt damit.
Die Verteilung der öffentlichen Schlüssel ist einfach zu handhaben. Einziger Nachteil dieser Public-Key Verschlüsselungsverfahren ist, dass sie mit einem höheren Rechenaufwand verbunden sind und längere Schlüssel benötigen.
Die Methoden der asymmetrischen Kryptographie werden zudem auch zum digitalen Signieren verwendet.

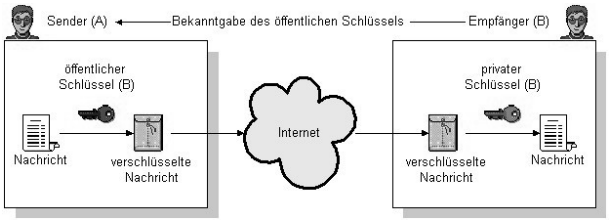

Abbildung 2: Asymmetrische Verschlüsselung [12]

2.3 Digitale Signaturen

Eine digitale Signatur hat - ähnlich wie eine handschriftliche Unterschrift - den Zweck, ein Dokument so zu kennzeichnen, dass der Ersteller des Dokuments eindeutig identifiziert und die Urheberschaft des Dokuments nicht abgestritten werden kann. Beim Signieren wird auf die Daten zunächst eine Hashfunktion angewandt. Die gehashten Daten werden mit einem privaten Schlüssel verschlüsselt. Diese Signatur wird dem Dokument angehängt und beides zusammen wird dem Empfänger übermittelt (vgl. linke Seite der Abbildung 3).
Auf der Seite des Empfängers wird die Signatur mit dem dazugehörigen öffentlichen Schlüssel entschlüsselt. Ist das Ergebnis dieses Verfizierungsprozesses derselbe Hashwert wie derjenige des ursprünglichen Dokuments, wurden die Daten während der Übermittlung nicht verändert (vgl. rechte Seite der Abbildung 3). Der Empfänger kann sich der Authentizität des Senders sicher sein und dass die Daten tatsächlich von dem angegebenen Sender stammen und unverfälscht sind.

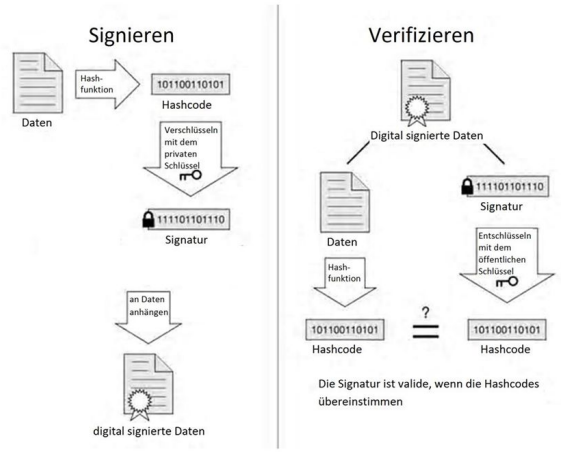

Abbildung 3: Digitales Signieren und Verifikation

3. WAS IST PKI?

Public Key Infrastructure basiert auf den Verfahren der asymmetrischen Kryptographie. Das Problem dieser Verfahren *ohne* zusätzliche Infrastruktur ist, dass beim Austausch des öffentlichen Schlüssels die Gefahr einer Man-in-the-middle-attack (MITM) besteht. Wenn zum Beispiel Person A ihren öffentlichen Schlüssel an Person B sendet und es einem Angreifer gelingt, den öffentlichen Schlüssel dabei abzufangen, kann dieser unbefugte Dritte den richtigen Schlüssel durch seinen eigenen ersetzen. Der Sender B verwendet dann beim Verschlüsseln unwissentlich den öffentlichen Schlüssel des Man-in-the-middle. Der Angreifer hat dann die Möglichkeit, die Nachricht von B an A mit seinem privaten Schlüssel zu entschlüsseln, zu lesen und sie anschließend mit dem richtigen Schlüssel von A zu verschlüsseln und an A weiterzuleiten. Das zentrale Problem hierbei ist, dass man einem öffentlichen Schlüssel per se nicht ansieht, zu wem er gehört. Die Folge ist, dass weder Person A noch Person B die MITM bemerken.
An dieser Stelle setzt das Konzept der PKI und digital signierter Zertifikate an. Ein digitales Zertifikat ist eine digital signierte Datenstruktur, die einen öffentlichen Schlüssel an die Identität seines Besitzers bindet. Der Besitzer kann dabei sowohl eine Einzelperson als auch ein Unternehmen oder eine Anwendung sein. Die digitale Signatur dient dem Nachweis der Authentizität des Zertifikateigentümers. Auf einem Zertifikat (vgl. Abb. 4) können zusätzliche Informationen wie zum Beispiel Gültigkeitsdauer und Verwendungszweck gespeichert werden.

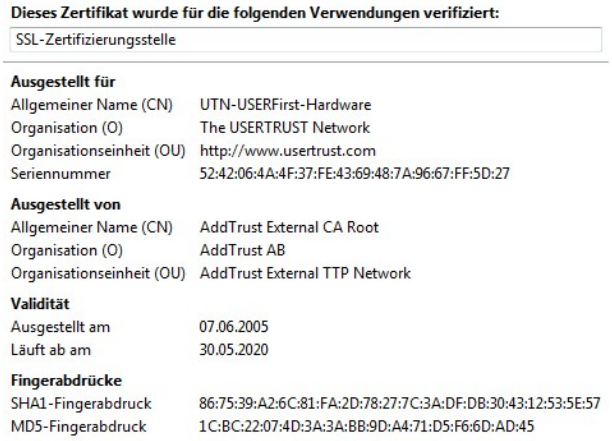

Abbildung 4: Digitales Zertifikat

PKI ist eine Infrastruktur, die sich aus verschiedenen Technologien, Verfahren und den beteiligten Anwendern zusammensetzt. Sie umfasst ein System von Hardware- und Softwarekomponenten. Wesentliche Elemente hierbei sind die Client-Software auf der Seite des Anwenders und auf der Serverseite ein *Certificate Repository*, das einen schnellen Zugriff auf gesuchte Zertifikate ermöglicht. Weiterer Bestandteil einer PKI sind sämtliche Methoden zur Erstellung, Verwaltung, Verteilung und Sperrung digitaler Zertifikate. Diese sind zumeist in einer sogenannten Policy festgelegt und variieren in Abhängigkeit des zugrundeliegenden

(Vertrauens-)Modells (vgl. nächster Abschnitt). Ausgestellt werden digitale Zertifikate von Zertifizierungsstellen (engl. Certificate Authority, CA). Eine CA kann von einer Behörde oder einem Unternehmen betrieben werden.
Es existieren verschiedene Modelle, wie eine PKI in der Praxis umgesetzt werden kann. Diese Modelle haben damit zu tun, welchem Zertifikat bzw. welcher Zertifizierungsstelle ein Benutzer vertrauen kann. Man spricht deshalb auch von *Vertrauensmodellen* (engl. trust models). Das gängigste Konzept ist das hierarchische Vertrauensmodell. Es sieht eine Wurzelinstanz, die Root CA, vor, die entweder vermittelt über weitere, untergeordnete Zertifizierungsstellen oder auf direktem Weg dem Endnutzer Zertifikate ausstellt (vgl. Abb. 5).

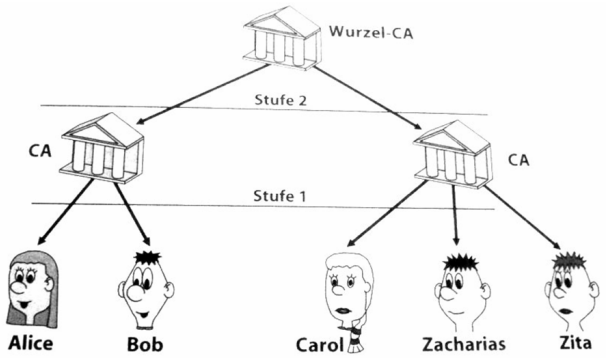

Abbildung 5: Hierarchisches Vertrauensmodell [5]

Wenn sich zwei CAs gegenseitig zertifizieren, spricht man von *Cross Certification*. Wie Abbildung 6 zeigt, können diese beiden Zertifizierungsstellen ihrerseits hierarchisch organisiert sein. Eine Cross Certification ist zum Beispiel sinnvoll, wenn Unternehmen fusionieren, die jeweils eigene Zertifizierungsstellen betreiben.

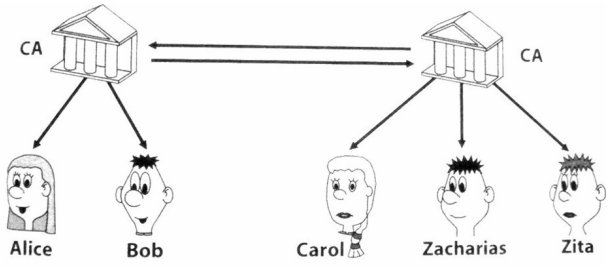

Abbildung 6: Cross Certification [5]

Ein anderer, dezentraler Ansatz der Vertrauensmodellierung wird mit dem so genannten *Web of Trust (WoT)* verfolgt. Die Grundidee ist, dass das Signieren und Ausstellen von Zertifikaten nicht mehr von zentralen Instanzen wie Certificate Authorities übernommen wird. Vielmehr kann jeder Benutzer selbst Zertifikate ausstellen und darüber individuell entscheiden, welchen potentiellen Kommunikationspartnern er vertraut. Vertrauensketten und ein "Netz des Vertrauens" entstehen, wenn Benutzer nicht nur den Personen, die sie persönlich kennen, vertrauen, sondern darüber hinaus auch deren Vertrauenspartnern (vgl. Abb. 7). Gleichwie im Modell der hierarchischen PKI wird auch im Web of Trust eine Transitivität des Vertrauens modelliert.

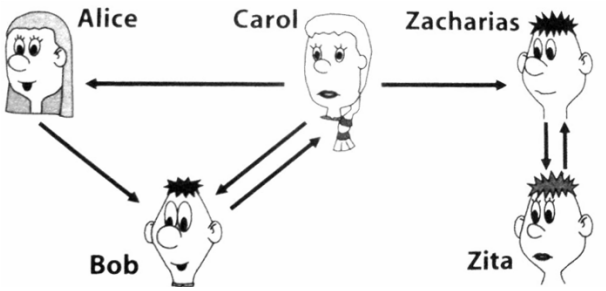

Abbildung 7: Web of Trust [5]

4. STÄRKEN VON PKI

Ein wichtiger Vorteil von PKI ist, dass das Konzept die wesentlichen Sicherheitskriterien Authentifizierung, Integrität und Vertraulichkeit unterstützt. Durch die Verwendung digitaler Signaturen wird außerdem das Kriterium der Nichtabstreitbarkeit sichergestellt, da die Urheberschaft signierter Nachrichten nicht abgestritten werden kann. In [2] sind diese Sicherheitsziele näher beschrieben.
Weiterhin erfolgt bei PKI eine zentrale Administration der öffentlichen Schlüssel. Dies ist insbesondere bei firmeninterner Umsetzung von PKI bedeutsam, da hierdurch Komplexität und Verwaltungsaufwand verringert werden.
Damit einher geht der Aspekt, dass im Rahmen einer zentral gesteuerten PKI eine Policy (vgl. z. B. [8]), die zum Beispiel Regeln zur Erneuerung und Sperrung von Zertifikaten festlegt, vergleichsweise einfacher durchzusetzen ist als beispielsweise in einem Web of Trust.

5. SCHWÄCHEN VON PKI

Bei der Umsetzung von PKI in die Praxis existieren mehrere Probleme. Neben zwei allgemeinen Schwierigkeiten bei der Anwendung von PKI, werden im Folgenden Probleme im Zusammenhang mit der Sperrung von Zertifikaten und der Rolle von Vertrauen bei der Anwendung von PKI erläutert.

5.1 Allgemeine Probleme

Eine der Schwächen von PKI ist, dass sich die Implementierung oft weit schwieriger gestaltet als vielfach propagiert wird [3]. So ist die Einrichtung von PKI meist mit aufwendigen Änderungen der Altsysteme verbunden. Zudem müssen die Nutzer ausgiebig geschult werden und zumindest am Anfang entsteht bei der Verteilung großer Mengen von Zertifikaten ein beträchtlicher Verwaltungsaufwand. Johnson und Johnson [6] berichten zum Beispiel davon, dass allein im ersten Jahr nach Einführung von PKI bei einer Mitarbeiterzahl von 110.000 insgesamt 30.000 Zertifikate gesperrt werden mussten. Diese hohe Zahl wird vor allem auf die unzureichende Schulung der Mitarbeiter im Umgang mit den Zertifikaten zurückgeführt.
Wie bei allen anderen Technologien, gilt auch für PKI, dass

ein System nur so sicher ist wie seine schwächste Komponente. Sowohl auf Seiten der beteiligten Computersysteme als auch auf Seiten der Nutzer können Sicherheitslücken entstehen. Es ist zum Beispiel denkbar, dass ein privater Schlüssel nicht ausreichend geschützt wird. Wird er gestohlen oder kopiert, können Dokumente unrechtmäßig signiert oder entschlüsselt werden.

5.2 Sperrung von Zertifikaten

Eine wichtige Anforderung an eine PKI ist, dass bereits ausgestellte Zertifikate gesperrt werden können. Dies ist zum Beispiel notwendig, wenn sich die Identität eines Zertifikatbesitzers ändert (z. B. Namenswechsel), ein Mitarbeiter das Unternehmen verlässt oder ein privater Schlüssel gestohlen oder kopiert wird. Eine unmittelbare Sperrung des entsprechenden Zertifikats ist dann von großer sicherheitskritischer Bedeutung.
Entsprechend wichtig ist es, dass sich die Nutzer einer PKI über den Status von Zertifikaten informieren können. Eine PKI muss also einen Mechanismus zur Verfügung stellen, der die Überprüfung von Zertifikaten auf ihre Gültigkeit gestattet. Dieser Vorgang wird als *Revocation Check* bezeichnet. Ein vielfach praktizierter Ansatz ist eine Art Blacklist mit gesperrten Zertifikaten, die *Certificate Revocation List (CRL)*, die in bestimmten Zeitabständen aktualisiert wird und dann durch den Nutzer von einem Server heruntergeladen werden kann.
Nach Gutmann [4] ist diese Lösung unzureichend. Das zentrale Problem dabei ist, dass CRLs nur in bestimmten Zeitabständen aktualisiert werden. Der Nutzer erhält keine Information darüber, wenn in der Zeit zwischen zwei Updates ein Zertifikat gesperrt wurde. Entsprechend problematisch ist dies, wenn ein gesperrtes Zertifikat nicht als solches erkannt wird. Notwendig wäre eine Echtzeit-Statusabfrage, welche aber mit CRLs nicht realisierbar ist. Ein zusätzliches Problem ist, dass CRLs sehr umfangreich werden können. Je häufiger eine CRL herausgegeben wird, desto größer die Netzwerk- und Serverbelastung.
Eine mögliche Alternative zu CRLs bietet OCSP (Online Certificate Status Protocol). Es erlaubt dem Nutzer, bei einem Server, dem sogenannten OCSP-Responder den Status eines Zertifikats abzufragen. Obwohl OCSP der Lösung mit CRLs überlegen ist, gibt es auch bei diesem Ansatz einige Probleme. Kritisiert wird zum Beispiel, dass der OCSP-Responder unpräzise und nicht eindeutige Informationen zum Status eines Zertifikats liefert [4]. Mögliche Antworten sind "gesperrt", "nicht gesperrt" und "unbekannt". So können sich hinter der Antwort "unbekannt" mehrere Bedeutungen verbergen. Sie wird dem Anwender übermittelt, wenn das betreffende Zertifikat nicht ausgestellt wurde, aber ebenfalls, wenn es ausgestellt, aber nicht abrufbar ist. Das Ergebnis "nicht gesperrt" bedeutet lediglich, dass das Zertifikat aktuell nicht gesperrt ist. Es beinhaltet nicht zwangsläufig, dass das Zertifikat auch valide ist, weil Kritierien wie Gültigkeitsdauer oder Verwendungszweck nicht in die Überprüfung miteinbezogen werden. Dies ist das Hauptproblem, das Gutmann [4] im Zusammenhang mit CRLs sieht und das bei OCSP gleichermaßen besteht. Beide Instrumente liefern ausschließlich Informationen darüber, ob ein Zertifikat gesperrt ist. Die Information, die der Anwender tatsächlich benötigt, ist, ob das Zertifikat auch valide ist. Für weitere Informationen zu den Vor- und Nachteilen von OCSP sei auf [4] verwiesen.

5.3 Prinzip des Vertrauens

Das Prinzip des Vertrauens und die verschiedenen Vertrauensmodelle sind für das Konzept von PKI grundlegend. Allerdings gehen damit eine Reihe weiterer Probleme einher. Bei einer hierarchischen PKI genießt die Zertifizierungsstelle an der Spitze der Hierarchie, die Root CA, unbegrenztes Vertrauen, da sie von keiner anderen CA bestätigt werden muss.
Der Nutzer an der Basis muss der Root CA in zweierlei Weise vertrauen. Zum einen muss er sich darauf verlassen, dass sie sichere und valide Verfahren beim Ausstellen von Zertifikaten verwendet, das heißt eine sorgfältige Identitätsprüfung vornimmt. Darüber hinaus muss er darauf vertrauen, dass die Root CA korrekt bei der Validierung untergeordneter oder anderer gleichberechtigter CAs (Cross Certification) vorgeht. Insbesondere bei einer mehrstufig hierarchischen PKI, aber ebenso in einem Web of Trust, wird eine Transitivität des Vertrauens modelliert, die in der realen Welt aber in keiner Weise gegeben ist. Wichtig ist, dass dies kein eigentliches Problem von PKI ist. Vielmehr bilden die Vertrauensmodelle das Geschehen in der realen Welt in ungeeigneter Weise ab.

In der Praxis kann dies erhebliche negative Folgen nach sich ziehen. Bei der Nutzung von Webdiensten, die eine verschlüsselte Kommunikation erfordern, wie zum Beispiel E-Mail-Dienste oder Online-Bankingsysteme, zeigt der Browser entweder eine Sicherheitswarnung oder ein gelbes Sicherheitsschloss an. Letzteres signalisiert dem Nutzer, dass die Seite vertrauenswürdig ist und die Kommunikation tatsächlich verschlüsselt erfolgt. Tatsächlich bedeutet das Symbol aber lediglich, dass eine Root CA oder eine untergeordnete, von der Root CA validierte CA diesen Kommunikationspartner authentifiziert hat. Ob diese CA wiederum vertrauenswürdig ist, entscheiden die Softwarehersteller. Diese entscheiden, welche Root-Zertifikate in den Browser, in den sogenannten Truststore, aufgenommen werden. Das bedeutet, dass nicht der Nutzer selber, sondern der Webbrowser darüber entscheidet, ob in die Identität eines Kommunikationspartner im WWW vertraut wird oder nicht.

5.4 Szenario

Die meisten Webbrowser sehen ein Aufnahmeverfahren für Root-Zertifizierungsstellen vor, das die Vertrauenswürdigkeit der Antragsteller überprüft (z. B. [9]). Es ist jedoch ein Szenario denkbar, nach dem einmal vom Browser als "trusted" eingestufte Root CAs ihre Macht irgendwann für kriminelle Zwecke nutzen [7]. Mittels gefälschter Zertifikate könnte der E-Mailverkehr von Nutzern abgehört oder Wirtschaftsspionage betrieben werden.
Ebenso ist es vorstellbar, dass in einem Knotenpunkt auf dem Pfad zwischen dem Rechner des Anwenders und einem Webserver (z. B. auf einem Heimrouter) neben einem echten Zertifikat ein weiteres falsches Zertifikat installiert wird. Der Webnutzer würde zum Beispiel mit Googlemail über ein falsches gmail-Zertifikat kommunizieren. Daneben läge das richtige Zertifikat, über das Google kommunizieren würde. Die gesamte Kommunikation könnte abgehört werden, ohne dass Google oder der User diese Man-in-the-middle-attack bemerken würden (vgl. Abb. 8).

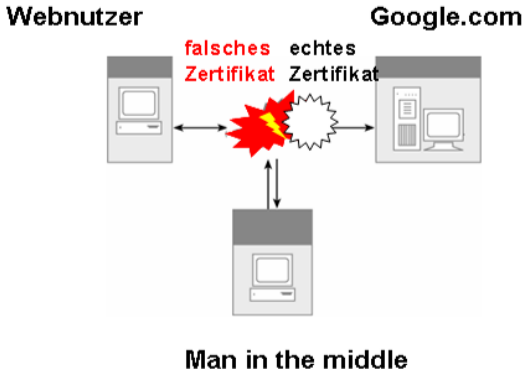

Abbildung 8: Man-in-the-middle-attack Szenario

6. ALTERNATIVEN

Vor dem Hintergrund der genannten Probleme bei der Anwendung von PKI existieren viele alternative Lösungsansätze. Nach Schmeh [5] gelten Identitätsbasierte Krypto-Systeme derzeit als die wichtigste Alternative zu PKI.
Vielfach wird auch das bereits in Abschnitt 3 beschriebene Web of Trust als bessere Variante diskutiert (vgl. z. B. [13]). Die bekanntesten Umsetzungen des Web of Trust in der Praxis ist die kommerzielle Software Pretty Good Privacy (PGP) und das OpenSource-Programm GNU Privacy Guard (GnuPG).
Das Web of Trust gilt als deutlich flexibler als die hierarchische PKI, da der Benutzer über deutlich mehr Handlungsspielraum und individuelle Kontrolle verfügt. Mit der Anwendung des WoT im WWW sind jedoch noch Probleme verbunden. Zum einen muss ein Benutzer die Vertrauenswürdigkeit und Identität potentieller Kommunikationspartner nun selbst überprüfen. Ist der betreffende Kommunikationspartner ein Webdienst im WWW, ist diese Überprüfung prinzipiell schwieriger, als wenn sie beispielsweise in einem persönlichen Treffen zwischen zwei Personen erfolgt. Zum anderen bedeuten die sehr großen Nutzerzahlen im WWW, dass das Durchsetzen von Policies nur schwer zu erreichen ist [5] und die Koordination und Administration der beteiligten Anwender eines Web of Trust schwierig zu handhaben ist [13]. In begrenzten Umgebungen allerdings, zum Beispiel im Email-Verkehr oder in Unternehmensnetzwerken hat sich das Web of Trust bereits als erfolgreiches Konzept erwiesen [10].

7. ZUSAMMENFASSUNG

Die wesentlichen Vorteile von PKI sind die Unterstützung wichtiger Sicherheitskriterien und die Reduktion von Komplexität. Die Authentifizierung und die Beweiskraft mittels digital signierter Zertifikate sind zentral für das Konzept von PKI. Positive Erfahrungsberichte gibt es vor allem, wenn PKI in einem begrenzten Rahmen, zum Beispiel unternehmensintern, angewandt wird.
Den Stärken stehen jedoch eine Reihe von ungelösten praktischen Problemen gegenüber. Dies betrifft die Sperrung von Zertifikaten und die gesamte Vertrauensproblematik, die insbesondere im WWW gravierende sicherheitsrelevante Folgen nach sich ziehen kann. Das Web of Trust ist eine interessante Alternative zur hierarchischen PKI, das aber derzeit technisch noch nicht ausgereift ist [10]. Zusammengefasst gibt es daher bislang keine Alternativen, die sich großflächig durchgesetzt haben oder das Potential haben, dies in naher Zukunft zu tun.

8. LITERATUR

[1] S. K. Katsikas, J. Lopez & G. Pernul: *Security, Trust and Privacy in Digital Business*. Second International Conference, TrustBus, Copenhagen, Denmark. Proceedings. Aug. 2005

[2] C. Adams & S. Lloyd: *Understanding PKI: Concepts, Standards and Deployment Considerations*, 2nd ed. Addison-Wesley, 2003

[3] C. Ellison & B. Schneier: Ten risks of PKI: What you're not being told about public key infrastructure. *Computer Security Journal*, 16(1): 1-7, 2000. Online verfügbar unter: `http://www.counterpane.com/pki-risks.html`

[4] P. Gutmann: PKI: It's Not Dead, Just Resting. *Computer*, vol. 35, no. 8, pp. 41-49, 2002. Online verfügbar unter: `http://csdl.computer.org/comp/mags/co/2002/08/r8toc.htm`

[5] K. Schmeh: *Kryptographie. Verfahren - Protokolle - Infrastrukturen*, 3. überarb. Aufl. dpunkt.verlag, 2007

[6] S.W. Smith: Deploying and Using Public Key Technology: Lessons Learned in Real Life. *IEEE Security Privacy*, 2004

[7] C. Soghoian & S. Stamm: *Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL*. Online verfügbar unter: `http://files.cloudprivacy.net/ssl-mitm.pdf`, 2010

[8] *Mozilla CA Certificate Policy*, `http://www.mozilla.org/projects/security/certs/policy/`

[9] Mozilla Wiki: *CA: How to apply*, `https://wiki.mozilla.org/CA:How_to_apply#Applying_for_root_inclusion_in_Mozilla_products`

[10] *Web Security Trust Models*, `http://www.freedom-to-tinker.com/blog/sjs/web-security-trust-models`

[11] A. Lauert: *Sicherheitskonzepte*, `http://ddi.cs.uni-potsdam.de/Lehre/e-commerce/elBez2-5/page05.html`, 2002

[12] A. Lauert: *Sicherheitskonzepte*, `http://ddi.cs.uni-potsdam.de/Lehre/e-commerce/elBez2-5/page06.html`, 2002

[13] G. Caronni: Walking the Web of Trust. *IEEE Computer Society Press*, 2000. Online verfügbar unter: `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.21.7392&rep=rep1&type=pdf`