Sicherheit im Cyberspace

Information ist alles in der Informationsgesellschaft: Überall sofort verfügbar, aber auch leicht zu manipulieren oder spurlos zu vernichten. Je mehr Bereiche von den Informationstechnologien abhängen, desto effizienter, aber auch desto verwundbarer wird die Informationsgesellschaft. Damit wird die Kryptographie zu einer grundlegenden Sicherheitstechnologie.

VON RETO KOHLAS UND UELI MAURER

Informationstechnologien durchdringen unser tägliches Leben mehr und mehr. Sie sind die treibende Kraft einer grundlegenden gesellschaftlichen, wirtschaftlichen und politischen Entwicklung, die zur Informationsgesellschaft führen wird. Information wird zur bestimmenden Ressource, die effiziente Verarbeitung und Verteilung, der Besitz und der Schutz von Information zum erfolgsentscheidenden Wirtschaftsfaktor. Information unterscheidet sich von konventionellen Ressourcen durch die Möglichkeit, sie in kürzester Zeit beliebig oft zu vervielfältigen, sie mit Lichtgeschwindigkeit zu übertragen und sie zu vernichten, ohne Spuren zu hinterlassen.

Informationssicherheit

Von der Entwicklung zur Informationsgesellschaft sehen wir heute erst den Anfang, und wo sie hinführt, ist schwierig abzuschätzen. Sicher scheint, dass diese Entwicklung grosse Auswirkungen auf die globale Gesellschaft haben wird, ob wir dies wollen oder nicht. Es stehen noch beträchtliche Hindernisse im Weg, mit denen sich die Politik, die Ethik, die Wirtschaft und die Forschung befassen muss. Dazu gehören insbesondere die Verwundbarkeit der Informationsgesellschaft, Aspekte des Datenschutzes (das viel diskutierte Privacy-Problem), die Kontrolle der enormen Komplexität der Systeme, die Benutzbarkeit für alle Menschen und die Anpassung des traditionell schwerfälligen Rechtssystems. Die Informationstechnologien werden wegen ihres gesellschaftlichen und wirtschaftlichen Veränderungspotenzials voraussichtlich zu ähnlichen Grundsatzdiskussionen führen wie zuvor die Nuklear- und zur Zeit die Gentechnologie.

Mit zunehmender Digitalisierung wächst das Risiko, dass durch Ausfall oder Fehlfunktion eines oder mehrerer Informationssysteme Schaden entsteht. Die Komplexität der Systeme macht es zunehmend schwierig, Risikofaktoren für Fehlverhalten zu identifizieren und deren Gefahrenpotenziale abzuschätzen.

Informationsrisiken

Grundsätzlich lässt sich unterscheiden zwischen Risiken, die unbeabsichtigt entstehen (durch Einflüsse der Umgebung wie Stromausfall oder Brand, fehlerhafte Soft- oder Hardware oder Bedienungsfehler), und Risiken, die auf einer Absicht beruhen. Angriffe können von Hackern, Kriminellen, Wirtschaftsspionen, Geheimdiensten und anderen unternommen werden, zum Beispiel mit dem Ziel, Zugang zu geheimer Information zu erlangen, Information zu verändern oder zu löschen oder ein System zu sabotieren. Der Angreifer versucht dabei, den schwächsten Punkt eines Systems auszunützen. Verschiedene Aufsehen erregende Ereignisse haben in letzter Zeit das Schadenspotenzial von Attacken gegen Informationssysteme aufgezeigt. Der «I love you»-Virus zum Beispiel, der sich in kürzester Zeit in Mailservern in der ganzen Welt festsetzte, verursachte einen Schaden in zweistelliger Milliardenhöhe. Ein anderes Beispiel sind Denial-of-Service-Attacken, welche die Webserver bekannter Internetfirmen wie Yahoo und Amazon.com lahm gelegt haben.

Das Internet muss als völlig unsicher betrachtet werden. Hacker können relativ einfach eine Kommunikation abhören, falsche Daten einspeisen oder Systeme für eine gewisse Zeit lahm legen. Offensichtliche Sicherheitsanforderungen sind deshalb die Geheimhaltung, die Authentizität und die Verfügbarkeit von Information. Darüber hinaus gibt es aber viel komplexere Aspekte der Informationssicherheit, die man zum Teil erst mit der technologischen Entwicklung und dem Aufkommen von neuen Anwendungen erkennen wird. Als einfaches Beispiel sei die Beweisbarkeit digitaler Transaktionen erwähnt, was beispielsweise bei einem digital abgeschlossenen Vertrag von Bedeutung ist.

Das Thema Informationssicherheit fasziniert durch seine Vielschichtigkeit: nebst technischen spielen organisatorische, wirtschaftliche, benutzerbezogene und rechtliche Aspekte eine Rolle. Wichtige Technologien sind biometrische Verfahren und physische Schutzmechanismen im Mikrobereich (beispielsweise Smart Cards) wie im Makrobereich (zum Beispiel Gebäudesicherheit). Eine Schlüsseltechnologie ist die Kryptographie.

Unterschriften, Geld und Wahlen digital

Die Kryptographie ist eine Wissenschaft, die sich mit mathematischen und algorithmischen Aspekten der Informationssicherheit befasst. Bis zur Mitte dieses Jahrhunderts war die Kryptogra-

Reto Kohlas ist Assistent am Institut für Theoretische Informatik der ETH Zürich. Dr. Ueli Maurer ist Professor für Informatik an der ETH Zürich.

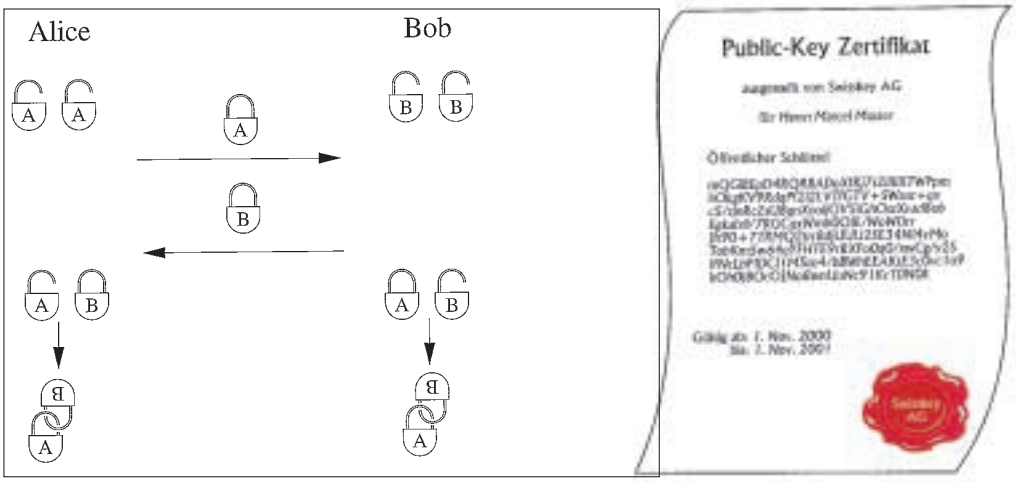

Abbildung 2: Beispiel eines Public-Key-Zertifikats

Abbildung 1:
Mechanisches Analogon des Diffie-Hellmann-Protokolls
Das Ziel des Diffie-Hellman-Protokolls ist die Erzeugung eines geheimen Schlüssels durch zwei Kommunikationspartner Alice und Bob, die zu Beginn keine gemeinsame geheime Information besitzen und lediglich über einen vom Gegner abgehörten Kanal verbunden sind. In der Abbildung entspricht dem geheimen Schlüssel das Paar ineinander verschlossener Vorhängeschlösser. Der Schlüssel ist geheim, weil der Gegner nur die beiden verschlossenen Schlösser zu sehen bekommt und deshalb nicht die ineinander verschlossene Konfiguration erzeugen kann.

Das Vorhängeschloss symbolisiert eine so genannte Einwegfunktion, also eine Funktion f, die für ein gegebenes Argument x einfach zu berechnen ist (f(x) aus x zu berechnen, entspricht dem Schliessen des Schlosses). Das Invertieren dieser Funktion (entspricht dem Öffnen des Schlosses) ist hingegen in der Praxis unmöglich. (Das Invertieren einer Funktion f bedeutet, für einen gegebenen Wert y einen Wert x mit y=f(x) zu finden.)

Alice und Bob wählen je zufällig einen Wert x_A resp. x_B (d. h. ein Schloss in geöffnetem Zustand) und berechnen daraus den Wert $f(x_A)$ resp. $f(x_B)$ (d. h. das Schloss im geschlossenen Zustand). Diese Werte werden über den unsicheren Kanal ausgetauscht. Anschliessend können Alice wie auch Bob die Konfiguration der ineinander verschlossenen Schlösser unter Verwendung des jeweiligen offenen Schlosses einfach erzeugen.

phie aber weniger eine Wissenschaft, sondern mehr eine Sammlung von Techniken für den Entwurf und das Brechen von Chiffrierverfahren, die fast ausschliesslich im militärischen Bereich Anwendung fanden. Heute wird die Kryptographie als mathematische Wissenschaft betrieben und ist von zentraler Bedeutung für die weitere Entwicklung der Informationstechnologie.

Ein aktuelles Thema mit unmittelbarer praktischer Bedeutung sind digitale Unterschriftenverfahren. Digitale Unterschriften sind das digitale Analogon der herkömmlichen Unterschrift. Jemand kann ein digitales Dokument so unterschreiben, dass jedermann (beispielsweise ein Richter) die Unterschrift verifizieren kann, aber niemand die Unterschrift fälschen oder von einem Dokument auf ein anderes übertragen kann.

Mit digitalem Geld kann man die Funktionalität des Papiergeldes nachbilden, insbesondere die Unfälschbarkeit des Geldes und die Anynomität des Zahlungsvorgangs. Diese Unfälschbarkeit schliesst mit ein, das mehrfache Ausgeben einer digitalen Münze zu verhindern. Die Anonymität ist für den Datenschutz wichtig, wobei aber gleichzeitig Geldwäscherei, Steuerhinterziehung und andere Formen der Kriminalität verhindert werden müssen.

So genannte Zero-Knowledge-Beweisverfahren erlauben, die Kenntnis eines bestimmten Geheimnisses zu beweisen, ohne jegliche Information darüber preiszugeben. Eine Anwendung ist, dass ein Benutzer die Kenntnis eines Passwortes gegenüber einem System beweisen und sich somit ausweisen kann, ohne dem möglicherweise nicht vertrauenswürdigen System das Passwort zu zeigen, ja sogar ohne darüber irgendwelche Information wegzugeben.

Eine weitere Thematik sind Methoden zur sicheren Berechnung einer Funktion der Inputs mehrerer Parteien, so dass am Schluss nur das Resultat bekannt wird, aber alle Inputs der Parteien geheim bleiben, und zwar selbst dann, wenn ein Teil der Parteien eine beliebige gemeinsame Betrugsstrategie anwendet. Hoch aktuell sind digitale Abstimmungen, bei denen das Wahlergebnis unverfälschbar berechnet werden soll, während die einzelnen Stimmen geheim bleiben.

Public-Key-Kryptographie

Die beschriebene Entwicklung der Kryptographie wurde ermöglicht durch eine sensationelle Erfindung, die Entdeckung der so genannten Public-Key-Kryptographie durch Diffie und Hellmann Mitte der Siebzigerjahre. Ohne diese geniale Entdeckung wären moderne Sicherheitsanwendungen im Internet undenkbar.

Bei der Anwendung der Public-Key-Kryptographie generiert

sich jede kommunizierende Person ein Public-Key-Paar, bestehend aus einem privaten und einem öffentlichen Schlüssel (deshalb der Begriff Public-Key-Kryptographie oder asymmetrische Kryptographie). Praktisch kann man sich diese beiden Schlüssel als grosse Zahlen vorstellen. Der private Schlüssel wird von jedem Benutzer geheim gehalten und beispielsweise auf einer Smartcard gespeichert, der öffentliche Schlüssel wird, wie der Name sagt, publiziert, in einem Directory Service und/oder auf einem Webserver. Ein Public-Key-Verschlüsselungssystem ist dadurch charakterisiert, dass man zwar mit Kenntnis des öffentlichen Schlüssels eine Nachricht verschlüsseln, aber nur mit dem privaten Schlüssel wieder entschlüsseln kann. Ein digitales Signaturverfahren, wie schon weiter oben erwähnt, erlaubt einem Benutzer, eine Nachricht mit seinem privaten Schlüssel zu signieren. Eine solche Signatur kann mit dem entsprechenden öffentlichen Schlüssel überprüft werden. Da nur die Kenntnis des privaten Schlüssels das Signieren erlaubt, kann eine digitale Signatur Beweiskraft besitzen.

Das Public-Key-Verfahren von Diffie und Hellmann basiert wie alle heute breit verwendeten Public-Key-Verfahren auf algebraischen und zahlentheoretischen Konzepten. Das Verfahren wird in Abbildung 1 abstrakt anhand von Schlössern erklärt, ohne auf die zum präzisen Verständnis notwendige Mathematik einzugehen.

Public-Key-Infrastrukturen

Die sichere Anwendung der Public-Key-Kryptographie bedingt, dass die verwendeten öffentlichen Schlüssel authentisch sind. Möchte zum Beispiel eine Kundin Alice eine Tele-Banking-Transaktion verschlüsselt an eine Bank senden, so muss sie sicher sein, den öffentlichen Schlüssel der Bank zu verwenden. Gelingt es einem Gegner, seinen eigenen Schlüssel als denjenigen der Bank auszugeben (zum Beispiel durch eine gefälschte Antwort auf die Anfrage des Kunden an einen Schlüsselserver), so könnte er die Nachricht an Stelle der Bank lesen. Enthält die Nachricht den Sicherheitscode des Kunden, so ist anschliessend ein Betrug für den Gegner einfach.

Im Kontext des Internets muss man oft öffentliche Schlüssel von Benutzern oder Organisationen verwenden, die man vorher nie getroffen hat. Um sicherzustellen, dass ein öffentlicher Schlüssel echt ist, kann man so genante Public-Key-Zertifikate verwenden. Ein Public-Key-Zertifikat ist eine digital unterschriebene Bescheinigung für die Authentizität eines bestimmten Schlüssels zu einer bestimmten Person. Dies ist vergleichbar mit einem Reisepass, in welchem die Bindung zwischen gewissen Personalien und einem Foto bezeugt wird. Zweck einer so genannten Public-Key-Infrastruktur (PKI) ist die Herausgabe, Verwaltung, Verteilung und Annulierung von Public-Key-Zertifikaten.

Ein Public-Key-Zertifikat ist genau dann Evidenz für die Authentizität des zertifizierten Schlüssels, wenn erstens der öffentliche Schlüssel der Zertifizierungsinstanz authentisch bekannt ist und wenn zweitens die Instanz vertrauenswürdig ist. Wenn man den öffentlichen Schlüssel der Zertifizierungsinstanz nicht schon besitzt, so stellt sich also das neue Problem, diesen Schlüssel zu erhalten und zu authentisieren. Dies geschieht in der Regel wiederum anhand eines Zertifikates, das von einer noch höheren Zertifizierungsinstanz ausgestellt ist. Dadurch entstehen ganze Pfade von Zertifikaten. Um einen solchen Pfad verwenden zu können, muss man erstens den öffentlichen Schlüssel der ersten Zertifizierungsinstanz authentisch besitzen (zum Beispiel fest im Browser codiert haben) und zweitens allen Zertifizierungsinstanzen auf dem Pfad vertrauen. Aus diesem und anderen Gründen ist Vertrauen eine grundlegende Ressource in der Informationssicherheit. Der Aufbau vertrauenswürdiger Instanzen (so genannter Trusted Third Parties) ist ein interessantes Forschungsgebiet und ein attraktives Geschäftsfeld innerhalb des e-Commerce.

Obwohl ein intuitives Verständnis für die Bedeutung und Benutzung von Public-Key-Infrastrukturen vorhanden ist, gibt es einige Unklarheiten und Zweideutigkeiten. So ist es nicht klar, was eine Zertifizierungsinstanz mit dem Zertifikat bezeugt. Es ist ein Unterschied, ob ein Benutzer einen bestimmten öffentlichen Schlüssel als seinen eigenen deklariert hat, ob er auch bewiesen hat, dass er den privaten Schlüssel tatsächlich kennt, oder ob er sich sogar in einem rechtlich bindenden Sinn verpflichtet hat, digitale Signaturen als gleichbedeutend mit seiner eigenen Unterschrift zu akzeptieren. Ein aktuelles Forschungsprojekt der Autoren hat zum Ziel, die im Kontext der Public-Key-Infrastrukturen atomaren Evidenzstücke und Schlussfolgerungen in logischen Regeln formal zu beschreiben.

Forschungsinformation

Die Forschungsgruppe für Informationssicherheit und Kryptographie im Departement für Informatik befasst sich mit einem breiten Spektrum von theoretischen und angewandten Fragestellungen der Kryptographie, insbesondere mit den Themen Public-Key-Kryptographie, digitale Signaturen, Public-Key-Infrastrukturen, digitale Zahlungssysteme, sichere digitale Wahlverfahren, Sicherheit in verteilten Systemen und speziell mit dem Thema der mathematisch beweisbaren Sicherheit.

Kontakt: Prof. U. Maurer,
E-Mail: maurer@inf.ethz.ch
Web: http://www.inf.ethz.ch/department/TI/um/index.html