Sicherheitsaspekte in AMBIX

Ein Directory-Service des DFN-Vereins

Dr. Ralf Schneider, Karl-Peter Gietz, Dr. Kurt Spanier

Das DFN-Projekt AMBIX[1] ermöglicht Organisationen aus dem Bereich der Forschung in Deutschland, bequem und datenschutzkonform Personendaten im X.500 zu veröffentlichen und aktuell zu halten. Die Einhaltung datenschutzrechtlicher Vorgaben erfordert die Berücksichtigung verschiedener Sicherheitsaspekte.

AMBIX und X.500

Die Speicherung und Veröffentlichung von Personen- und Organisationsdaten bei AMBIX erfolgt Mithilfe der X.500-Technologie [1], einer von internationalen Normierungsgremien (ISO und ITU) standardisierten, weltweit verteilbaren Datenbank.

Im X.500 können beliebige, hierarchisch darstellbare Informationen gespeichert werden. Alle Daten werden in Servern, den *Directory System Agents* (DSAs), lokal abgelegt und verwaltet. Mittels *Directory User Agents* (DUAs) können über spezielle Protokolle Informationen gesucht, abgefragt und angezeigt sowie verändert oder gelöscht werden. Eines der wichtigsten DUA/DSA-Protokolle, das *Lightweigth Directory Access Protocol* (LDAP) [2], hat sich mittlerweile als Internet-Standard etabliert und wird von vielen führenden Software-Herstellern unterstützt.

Die vom DSAs gespeicherten Informationen sind im *Directory Information Tree* (DIT) hierarchisch strukturiert angeordnet, wobei jeweils ein sog. Master-DSA für die Verwaltung eines definierten Teilbereiches dieses Baumes zuständig ist.

Alle Informationen eines Eintrags werden in Attributen abgelegt, welche sich aus einem Attribut-Typ und einem oder mehreren Attribut-Werten zusammensetzen. Bestimmte Attribut-Werte bilden den, innerhalb einer Hierarchieebene eindeutigen, *Relative Distinguished Name* (RDN) eines Eintrags. Zusammen mit den im DIT hierarchisch übergeordneten RDNs ergibt sich daraus der im gesamten DIT eindeutige *Distinguished Name* (DN). Als eine Hauptanwendung des X.500 ist die Speicherung von Organisations- und Personendaten zu nennen. Alle hierfür benötigten Attribute werden vom Standard zur Verfügung gestellt.

Bereits bei der Konzeption des Projekts AMBIX wurden die Aspekte der deutschen Datenschutzgesetzgebung berücksichtigt. Grundlage hierfür bildete eine vom DFN-Verein in Auftrag gegebene Datenschutzexpertise [3]. Kernpunkte der Expertise besagen: Werden die erfaßten Personendaten auf ein Minimalset aus Name, Vorname, akademischer Titel, Telefon- und Faxnummer, E-Mail-Adresse sowie Organisationszugehörigkeit beschränkt, genügt vor deren Veröffentlichung im AMBIX-Verzeichnis die Einhaltung einer angemessenen Widerspruchsfrist (6 Wochen), nachdem die Betroffenen über die Datenlieferung informiert und ihre Rechte aufgeklärt worden sind. Dafür dürfen diese Personendaten nur an Länder mit adäquaten Datenschutzbestimmungen weitergegeben werden.

Zukünftig werden auch öffentliche Schlüssel von asymmetrischen Verschlüsselungsverfahren im AMBIX-Verzeichnis abgelegt. Bei der hierfür notwendig gewordenen Erweiterung des bestehenden Minimalsets, wurde dieses um öffentliche Schlüssel und zusätzliche, freiwillige Angaben wie Arbeitsgebiet und URL ergänzt.

Mit diesem erweiterten Minimalset können nun auch die Daten der Teilnehmer von WiNShuttle aufgenommen werden, einem Internet-Provider-Dienst des DFN-Vereins für Angehörige von Einrichtungen aus dem öffentlichen bzw. bildungs- und forschungsorientierten Bereich. Da WiNShuttle-Benutzer nur nach einer expliziten Zustimmung zur Veröffentlichung Ihrer Daten im Verzeichnis aufgenommen werden, unterliegen diese Daten nicht den oben genannten Beschränkungen der Datenschutzexpertise.

Organisationsdaten unterliegen keinen datenschutzrechtlichen Beschränkungen und können mit allen relevanten Informationen in der hierarchischen Struktur des X.500 abgebildet und frei zur Verfügung gestellt werden.

[1] (A)ufnahme von (M)ail-(B)enutzern (i)n das (X).500 Directory. Dieses DFN-Projekt wird gefördert aus Mitteln des BMBF.

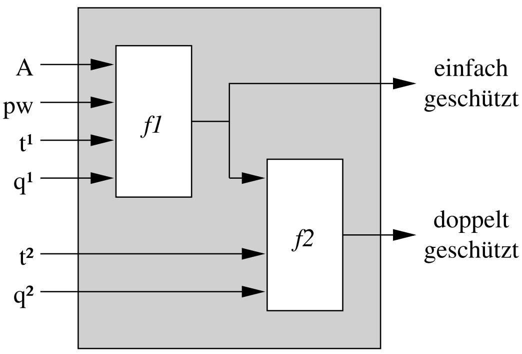
Für die Verarbeitung der Datenlieferungen von Organisationen und den Reaktionen der Betroffenen wurde eine netzwerkfähige *remote procedure call* (RPC) basierende Client-Server Maschine entwickelt [4]. Um alle Vorgaben der Datenschutzexpertise zu erfüllen, werden die Daten zuerst in einer projektinternen Datenbank gespeichert und alle Vorgänge protokolliert, wodurch die Chronologie eines Eintrags jederzeit nachvollzogen werden kann.

TWEB (Tübinger Web-Gateway), ein WWW-X.500-Gateway, ermöglicht einen komfortablen Zugang zu den Daten. Hierin wurden speziell für AMBIX ein Mechanismus zur Realisierung der datenschutzrechtlich vorgegebenen Zugriffsbeschränkung sowie ein Mechanismus zum Selbsteintrag ins AMBIX-Verzeichnis implementiert.

Sicherheit in AMBIX und im X.500

Die Einhaltung der datenschutzrechtlichen Vorgaben erfordert die Berücksichtigung verschiedener Sicherheitsmaßnahmen. So kommt der Authentifizierung der Benutzer und der Bestimmung des Landes, aus dem der Zugriff erfolgt, eine wichtige Rolle zu.

Da nicht davon ausgegangen werden kann, daß alle Benutzer des Dienstes auch im Verzeichnis eingetragen sind, können die im X.509 [5] definierten Authentifizierunsmechanismen nicht für die Autorisierung des Anfragenden herangezogen werden.



A = DN des Benutzers
pw = Paßwort von A
t = Zeitangabe
q = Zufallszahl (optional)
f = gerichtete Funktion

Abb. 1: Einfache geschützte Authentifizierung

Beim AMBIX-DSA sind daher die Zugriffsrechte so eingestellt, daß Personendaten prinzipiell nur an das AMBIX-TWEB weitergegeben werden, welches sich beim DSA durch Angabe von Paßwort und DN mittels *protected simple bind* authentifiziert (siehe Abb. 1).

Hierbei werden Paßwort und DN eines für TWEB eingerichteten Eintrags zusammen mit einer Zufallszahl (q^1) und/oder einer Zeitangabe (t^1) mittels einer gerichteten Funktion (*f1*) geschützt. Die so geschützte Information kann sofort übertragen werden (einfach geschützt) oder vor der Übertragung mittels einer weiteren gerichteten Funktion (*f2*) sowie einer weiteren Zeitangabe (t^2) und/oder Zufallszahl (q^2) geschützt werden (doppelt geschützt).

Mit einer Anfrage beim *Domain Name Service* (DNS) ermittelt das TWEB die Top-Level Domain des abfragenden Rechners. Ist diese nicht in der Liste der erlaubten Top-Level Domains aufgeführt bzw. existiert kein DNS Eintrag, werden keine Personendaten angezeigt. In diesem Fall werden, wie auch bei der Anfrage anderer DUAs oder DSAs, nur Organisationsdaten herausgegeben und angezeigt.

Neben der Möglichkeit *robots exclusion protocol* (REP) konforme Suchroboter vom Zugriff auf die Daten auszuschließen, werden von TWEB weitere Mechanismen zur Zugriffskontrolle bereitgestellt. So lassen sich für ein beliebiges Zeitintervall die Anzahl der Zugriffe aus einem definierbaren IP-Adressbereich aufzeichnen. Werden dabei regelmäßige oder besonders häufige Zugriffe registriert, wird dieser Bereich automatisch für eine gewisse Zeit gesperrt, hierbei sind IP-Adressbereich, Zahl der Zugriffe und die Zeitintervalle frei konfigurierbar.

Schließlich können durch einen entsprechenden Eintrag in der Konfigurationsdatei einzelne Rechner oder Domains vom Zugriff auf Personendaten oder gänzlich vom Zugriff auf die AMBIX-Daten ausgeschlossen werden.

Bei Datenlieferungen von Organisationen und Benutzern muß deren Authentizität sichergestellt sein. Für alle am Projekt beteiligten Organisationen wurde mindestens ein Administrator bestimmt und diesem ein Paßwort übermittelt. E-Mail-Adresse und Paßwort sind im DS-Manager-Eintrag der betreffenden Organisation im X.500 abgelegt. Datenlieferungen werden nur dann akzeptiert, wenn am Anfang der Datei die E-Mail-Adresse und das Paßwort des Administrators angegeben wurden und diese Angaben mit den im X.500 gespeicherten übereinstimmen.

Im Verzeichnis eingetragene Personen erhalten an die registrierte E-Mail-Adresse ein Datenänderungsformular zugesandt, welches eine mit einer komplexen Prüfsumme versehene Personenidentifikationsnummer (PIN) enthält. Datenänderungen sind für die Benutzer nur mit einem durch diese PIN authentifizierten Formular möglich. Um einen Mißbrauch des Formulars zu verhindern, werden die Daten soweit möglich auf formaler Konsistenz geprüft sowie bestimmte Einschränkungen realisiert, z.B. ist eine gleichzeitige Änderung von Vor- und Nachname nur über den Administrator möglich. Durch zurückschicken einer Mail mit den aktuellen Daten an alle gespeicherten E-Mail-Adressen sowie der automatischen Auswertung der Fehlerrückmeldungen wird die Funktionsfähigkeit der Adressen verifiziert. Aufgrund der Transparenz der Vorgänge und der Information der einzelnen Benutzer wird eine zusätzliche Sicherheit gewährleistet.

Sowohl bei den Organisationslieferungen als auch bei den Benutzer-Formularen ist für die Zukunft eine sicherere Kommunikation durch Verschlüsselung und Authentifizierung der Daten mittels eines asymmetrischen Verfahrens (vgl. nächstes Kapitel) vorgesehen. Die Einrichtung der dafür erforderlichen Infrastruktur ist in Vorbereitung.

Einen gewissen Schwachpunkt bildet die Möglichkeit des Selbsteintrags, die erst geschaffen wurde, nachdem sich herausgestellt hatte, daß nur ein kleiner Teil der angeschriebenen Organisationen zur aktiven Lieferung von Personendaten bereit war. Die Selbsteinträgerdaten können vom Projekt nur formal geprüft werden, werden jedoch vor dem Eintrag ins Verzeichnis den zuständigen Administratoren zur inhaltlichen Überprüfung geschickt.

Nicht zuletzt müssen direkte Angriffe auf die AMBIX-Rechner als unberechtigter Zugriff auf die Personendaten in Betracht gezogen und abgewehrt werden. Da für die verwendete Plattform (HP-UX) kein *Secure-RPC* zur Verfügung steht, wurde für die RPC-Schnittstelle ein eigener Authentifizierungsmechanismus implementiert. Alle Zugriffe auf TCP- und RPC-Dienste werden überwacht, protokolliert (*TCPwrapper* bzw. *portmapper*) und ausschließlich den projekteigenen Rechnern gewährt. Um ein sicheres Login übers Netz zu gewährleisten, wird *Secure Shell* (ssh) eingesetzt, welches eine verschlüsselte Datenübertagung und eine Authentifizierung mit dem RSA-Algorithmus [6] ermöglicht.

Die Quellen der oben erwähnten Programme können z.B. unter ftp://ftp.cert.dfn.de/pub/ gefunden werden.

AMBIX und Verschlüsselungstechnik

In der elektronischen Kommunikation ist ein zunehmender Einsatz von kryptographischen Verfahren zu verzeichnen. Hier sind vor allem *public key cryprosystems* (PKCS) zu nennen.

Bei PKCS wird für die Verschlüsselung der Daten ein Schlüsselpaar benötigt, welche einem Benutzer (X) zugeordnet ist. Diese sind ein geheimer Schlüssel (X_S) und ein öffentlich zugänglicher Schlüssel (X_P) der aus X_S berechnet wird. Aus der Kenntnis von X_P kann jedoch nicht auf X_S zurückgeschlossen werden. Den öffentlichen Schlüssel können andere Benutzer zur Verschlüsselung von Daten heranziehen, die sich dann nur noch mit dem komplementären geheimen Schlüssel entschlüsseln lassen.

Solche Verfahren eignen sich auch zum Erstellen digitaler Signaturen, mit denen sowohl die Unversehrtheit des Inhalts wie auch die Urheberschaft einer digitalen Nachricht geprüft und bestätigt werden können. Auch die im X.509 definierte strenge Authentifizierung (*strong bind*) basiert auf der Anwendung eines PKCS.

Für eine sinnvolle Anwendung von PKCS ist eine vertrauenswürdige Quelle erforderlich, von der zuverlässig der öffentliche Schlüssel einer Person bezogen werden kann.

In Zusammenarbeit mit dem Projekt DFN-PCA [7] (PCA - *policy certification authority*) an der Universität Hamburg wird von AMBIX eine Infrastruktur aufgebaut mit dem Ziel eine solche Quelle zur Verfügung zustellen.

Eine Zertifizierungs-Instanz (CA - *certification authority*) stellt die Identität eines Benutzers fest, signiert dessen öffentlichen Schlüssel und erzeugt so ein mit einer Gültigkeitsdauer versehenes Zertifikat. Die für die Abbildung einer CA im X.500 benötigten Attribute werden im X.509 definiert. Ist eine CA in einer im Verzeichnis abgebildeten Organisation angesiedelt, werden diese Attribute zusätzlich zu den bereits vorhandenen Attributen eines Organisationseintrags im Verzeichnis gespeichert, ansonsten wird ein neuer Organisationseintrag für diese CA angelegt.

CAs sind hierarchisch im DIT organisiert, so daß eine weiter unten angesiedelte CA von der darüberliegenden CA zertifiziert werden kann. An der Spitze eines solchen Zertifizierungsbaumes steht eine PCA (hier DFN-PCA), welche auch die gemeinsame Sicherheitspolitik dieser CAs definiert.

Eine weiter Aufgabe der CAs ist es, ungültig oder zurückgezogene Zertifikate in regelmäßigen Abständen in sog. *certificate revocation lists* (CRLs) herauszugeben.

Zertifikate und CRLs müssen jederzeit öffentlich zugänglich sein. Dem X.500 kommt dabei eine zentrale Bedeutung zu, da anhand des DNs eine eindeutige Zugehörigkeit eines Zertifikats zu einer Person gewährleistet werden kann. Hierfür übermitteln PCA und CAs die von ihnen erstellten Zertifikate und herausgegebenen CRLs über einen sicheren Kommunikationskanal an AMBIX, wonach diese im Verzeichnis veröffentlicht werden.

Ausblick

Die DFN-PCA hat vor kurzem mit der Zertifizierung von CAs begonnen, so daß in nächster Zeit mit der Übermittlung der ersten Zertifikate zu rechnen ist.

Das Ablegen nach X.509 zertifizierter Schlüssel im Verzeichnis ist mit den dort definierten Attributen problemlos möglich. Für die Schlüssel eines weiteren augenblicklich gängigen PKCS, *pretty good privancy* (PGP), existiert derzeit noch kein standardisierter Attribut-Set, sondern nur proprietäre Definitionen, wie sie z.B. im Tübinger Telefon- und Mitarbeiterverzeichnis [8] verwendet werden.

Notwendige Änderungen und Ergänzungen der AMBIX-Software, zur Verarbeitung und Darstellung der Zertifikate, sind teilweise abgeschlossen bzw. in Arbeit. Hierbei wurde darauf geachtet, daß auch von der DFN-PCA für die nahe Zukunft geplante Zertifikate für *SSL*, zur Absicherung des WWW, und *S/MIME* aufgenommen werden können.

Im Augenblick wird an einem Gesetzesentwurf zur rechtlichen Regelung digitaler Signaturen [9] gearbeitet. Auch ist in Deutschland eine Diskussion über eine Kryptoregulierung im Gange. Inwieweit diese beiden Entwicklungen Auswirkungen auf die weitere Projektarbeit haben werden bleibt abzuwarten.

Literatur

[1] The Directory: Overview of Concepts, Models and Services - CCITT Recommendation X.500 ISO/ICE 9594-1 / Information Technology; Open System Interconnection (1993)

[2] W. Yeong, T. Howes und S. Kille, Lightweight Directory Access Protocol, RFC 1777, Performance Systems International, Universität Michigan, ISODE Consortium, März 1995

[3] Dr. Jürgen W. Goebel und Jürgen Scheller, Datenschutzrechtliche Probleme bei der Einrichtung und dem Betrieb von X.500-Directories im Rahmen des Deutschen Forschungsnetzes, Frankfurt 1993

[4] K.-P.Gietz, Dr. R. Schneider, Dr. K. Spanier, X.500 für Alle - Das DFN-Projekt AMBIX, DFN-Mitteilungen, Heft 42, Nov. 1996, S. 23 ff.

[5] The Directory: Authentication Framework - CCITT Recommendation X.509 ISO/ICE 9594-8 / Information Technology; Open System Interconnection (1993)

[6] R.L. Riverst, A. Shamir und L.A. Adleman, Method of obtaining Digital Signatures and Public-key Cryptosystems, Communications of the ACM, Vol. 21, No. 2 (February 1978)

[7] Projekt DFN-PCA, http://www.cert.dfn.de/dfnpca/

[8] Telefon- und Mitarbeiterverzeichnis der Universität Tübingen, http://x500.uni-tuebingen.de:8889/

[9] SiG, Artikel 3, IuKDG, Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz) BT-Drs. 13/7934 vom 11.06.1997

Kontakt:

Universität Tübingen
Zentrum für Datenverarbeitung
DFN-Projekt AMBIX
Brunnenstraße 27
72074 Tübingen
Tel. 07071 29-77539
Fax. 07071 26-5912
E-Mail: ambix-d@mail500.uni-tuebingen.de
URL: http://ambix.uni-tuebingen.de/