Authentifikations- und Schlüsselverteilsysteme

Rolf Oppliger

Institut für Informatik und angewandte Mathematik (IAM), Universität Bern, Neubrückstrasse 10, CH-3012 Bern

Zusammenfassung In Computernetzen und verteilten Systemen werden Authentifikations- und Schlüsselverteilsysteme eingesetzt, um auf der Anwendungsschicht Sicherheitsdienste anbieten zu können. In diesem Beitrag werden die Authentifikations- und Schlüsselverteilsysteme Kerberos (OSF DCE), NetSP, SPX, TESS und SESAME vorgestellt, diskutiert und miteinander verglichen.

1 Einleitung

In Computernetzen und verteilten Systemen werden Authentifikations- und Schlüsselverteilsysteme eingesetzt, um auf der Anwendungsschicht Sicherheitsdienste, wie Authentifikations-, Datenvertraulichkeits- und -integritäts-, Zugriffskontroll- und Verbindlichkeitsdienste [1], anbieten zu können. Im Gegensatz zu sicheren Nachrichtenvermittlungssystemen, wie Privacy Enhanced Mail (PEM) oder Pretty Good Privacy (PGP), sind Authentifikations- und Schlüsselverteilsysteme nicht auf eine Anwendung beschränkt. Stattdessen bieten sie eine Programmierschnittstelle (API) an, über die sich Sicherheitsdienste selektiv in Anwendungen integrieren lassen. In diesem Beitrag werden die Authentifikations- und Schlüsselverteilsysteme Kerberos (OSF DCE), NetSP, SPX, TESS und SESAME vorgestellt, diskutiert und miteinander verglichen. Auf die kryptographischen Grundlagen und die speziellen Probleme, mit denen sich die Authentifikation und Schlüsselverteilung in Computernetzen und verteilten Systemen zu befassen hat, wird im Rahmen dieses Beitrages nicht eingegangen; sie werden als bekannt vorausgesetzt [2, 3, 4].

Im folgenden wird ein Schlüssel aus einem symmetrischen Kryptosystem als K, und ein Schlüsselpaar aus einem asymmetrischen Kryptosystem als (k, k^{-1}) notiert. Dabei stellt k den öffentlichen und k^{-1} den privaten Schlüssel dar. Indizes werden verwendet, um Prinzipale, d.h. Benutzer, Clients und Server, zu referenzieren. Der Ausdruck $\{m\}K$ steht für eine Nachricht m, die mit K chiffriert worden ist. Für die Entschlüsselung wird derselbe Schlüssel K verwendet, so dass $\{\{m\}K\}K$ wieder m ergibt. Demgegenüber steht $\{m\}k$ ($\{m\}k^{-1}$) für eine Nachricht m, die mit k (k^{-1}) chiffriert worden ist. Für die Entschlüsselung wird k^{-1} (k) verwendet, so dass $\{\{m\}k\}k^{-1}$ ($\{\{m\}k^{-1}\}k$) wieder m ergibt.

2 Kerberos

Das Authentifikations- und Schlüsselverteilsystem Kerberos ist im Rahmen des Projekts Athena am Massachusetts Institute of Technology (MIT) entwickelt worden [5]. Kerberos ist innerhalb einer Verwaltungseinheit (Realm) zentral, und zwischen verschiedenen Realms hierarchisch organisiert. In jedem Realm ist ein Authentifikationsserver (AS) für die Authentifikation von Prinzipalen, sowie für die Generierung und Verteilung von Sitzungsschlüsseln zuständig. Der AS teilt mit jedem Prinzipal P einen Schlüssel K_p. Dieser Schlüssel ist entweder mit Hilfe einer Einweg-Hashfunktion aus einem Passwort abgeleitet, oder er ist explizit gegeben. Hat der AS einen Benutzer authentifiziert, dann stellt er ihm ein Ticket Granting Ticket (TGT) aus. Mit diesem TGT kann der Benutzer dann während einer definierten Zeitspanne bei einem Ticket Granting Server (TGS) Tickets für die Beanspruchung von Dienstleistungen beziehen, die von einem Server angeboten werden.

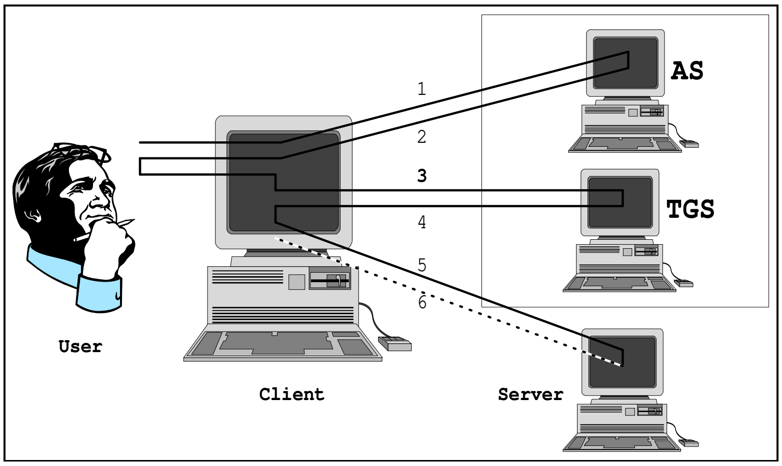

Abbildung1. Kerberos

Wenn ein Client C im Auftrag eines Benutzers U auf einen Server S zugreifen will, dann hat er das folgende Protokoll zu durchlaufen (vgl. Abbildung 1):

$$
\begin{array}{llll}
1: \mathrm{C} & \longrightarrow \mathrm{AS} & : \mathrm{U} \\
2: \mathrm{AS} & \longrightarrow \mathrm{C} & : T_{c,tgs}, \{TGS, K, T_{start}, T_{expire}\}K_u \\
3: \mathrm{C} & \longrightarrow \mathrm{TGS} & : S, T_{c,tgs}, A_{c,tgs} \\
4: \mathrm{TGS} & \longrightarrow \mathrm{C} & : T_{c,s}, \{S, K', T'_{start}, T'_{expire}\}K \\
5: \mathrm{C} & \longrightarrow \mathrm{S} & : T_{c,s}, A_{c,s} \\
6: \mathrm{S} & \longrightarrow \mathrm{C} & : \{T'\}K'
\end{array}
$$

In Schritt 1 kontaktiert C den AS. Der AS konstruiert ein TGT $T_{c,tgs} = \{U, C, TGS, K, T_{start}, T_{expire}\}K_{tgs}$ und stellt dieses im 2. Schritt zusammen mit $\{TGS, K, T_{start}, T_{expire}\}K_u$ C zu. C muss nun U auffordern, sein Passwort einzugeben. Kommt U dieser Aufforderung nach, dann kann C mit Hilfe einer Einweg-Hashfunktion h den Schlüssel $K_u = h(pwd)$ rekonstruieren, damit $\{TGS, K, T_{start}, T_{expire}\}K_u$ dechiffrieren und den für die Kommunikation mit dem TGS einzusetzenden Sitzungsschlüssel K extrahieren. Man beachte, dass $T_{c,tgs}$ mit dem geheimen Schlüssel des TGS chiffriert ist, und von C nicht entschlüsselt werden kann. $T_{c,tgs}$ kann im Wesentlichen nur dazu eingesetzt werden, beim TGS ein Ticket für einen Server S zu beantragen. Im 3. Schritt stellt C dem TGS den Namen des Servers S, $T_{c,tgs}$, sowie einen mit Hilfe von K konstruierten Authentikator $A_{c,tgs} = \{C, T\}K$ zu. $A_{c,tgs}$ enthält einen Zeitstempel T, der die Frische der Nachricht zu sichern hat. Der TGS dechiffriert $T_{c,tgs}$, überprüft dessen Gültigkeit, extrahiert K, dechiffriert $A_{c,tgs}$ und überprüft die Frische von T. Akzeptiert er das TGT, dann konstruiert er ein Ticket $T_{c,s} = \{U, C, S, K', T'_{start}, T'_{expire}\}K_s$, und stellt dieses zusammen mit $\{S, K', T'_{start}, T'_{expire}\}K$ im 4. Schritt C zu. C kann mit Hilfe von K $\{S, K', T'_{start}, T'_{expire}\}K$ entschlüsseln und daraus K' extrahieren. K' ist der neue, für die Kommunikation mit S einzusetzende Sitzungsschlüssel. C konstruiert einen neuen Authentikator $A_{c,s} = \{C, T'\}K'$, und stellt im 5. Schritt $T_{c,s}$ und $A_{c,s}$ S zu. S kann $T_{c,s}$ dechiffrieren, dessen Gültigkeit prüfen, K' extrahieren, $A_{c,s}$ dechiffrieren und die Frische des Zeitstempels T' prüfen. Akzeptiert S sowohl $T_{c,s}$ als auch $A_{c,s}$, dann nimmt er C als authentisch im Auftrag von U handelnd an. Ist eine gegenseitige Authentifikation erforderlich, dann gibt S im 6. Schritt $\{T'\}K'$ an C zurück.

Offenbar teilen C und S ab Schritt 5 den Sitzungsschlüssel K', und können damit Datenauthentifikations-, -vertraulichkeits- und -integritätsdienste anbieten. Kerberos sieht als symmetrisches Kryptosystem den Data Encryption Standard (DES) und als Einweg-Hashfunktionen DES-CBC, MD4 und MD5 vor.

3 NetSP

Die Tatsache, dass aus den USA Kryptosysteme nur dann ohne aufwendige Verfahren exportiert werden dürfen, wenn sie ausschliesslich für Authentifikationszwecke eingesetzt werden können, hat IBM veranlasst, eine Familie von Authentifikations- und Schlüsselverteilprotokollen zu entwickeln, die auf dem alleinigen Einsatz von Einweg-Hashfunktionen zur Bildung von Nachrichtenauthentifikationscodes (MAC) basiert [6]. Die Protokolle sind zuerst in einem Prototypen namens KryptoKnight und danach in NetSP (Network Security Program) eingesetzt worden. Im Zentrum der Familie steht ein 2-Parteien Authentifikationsprotokoll (2PAP), dessen Resistenz gegenüber bestimmten Angriffen formal gezeigt worden ist:

$$\begin{aligned}
1 &: \mathrm{A} \longrightarrow \mathrm{B} : N_a \\
2 &: \mathrm{B} \longrightarrow \mathrm{A} : N_b, MAC_{ba}(N_a, N_b, B) \\
3 &: \mathrm{A} \longrightarrow \mathrm{B} : MAC_{ab}(N_a, N_b)
\end{aligned}$$

A fordert B in Schritt 1 mit einer Zufallsmarke N_a heraus. In Schritt 2 antwortet B mit einer Zufallsmarke N_b und einem MAC, den er aus N_a, N_b and B bildet. A kann diesen MAC verifizieren, um B zu authentifizieren. Um sich auch gegenüber B zu authentifizieren, hat A in Schritt 3 noch einen MAC über N_a und N_b bilden und B zustellen. Dieser Schritt ist optional und nur für eine gegenseitige Authentifikation erforderlich. Man beachte, dass die Schlüssel zur Bildung von $MAC_{ba}(N_a, N_b, B)$ in Schritt 2 und $MAC_{ab}(N_a, N_b)$ in Schritt 3 nicht notwendigerweise gleich sein müssen. Sie sind gleich, wenn A und B ein symmetrisches Kryptosystem einsetzen und einen entsprechenden Sitzungsschlüssel teilen. 2PAP lässt sich aber auch mit einem asymmetrischen Kryptosystem betreiben. MAC_{ba} (MAC_{ab}) stellt dann einen MAC dar, der von B (A) gebildet und von A (B) verifiziert werden kann.

Ein 2-Parteien Schlüsselverteilprotokoll (2PKDP) ergibt sich aus 2PAP, wenn man B durch eine Schlüsselverteilzentrale (KDC) ersetzt:

$$\begin{array}{llll} 1: \mathrm{A} & \longrightarrow \mathrm{KDC} & : & N_a \\ 2: \mathrm{KDC} & \longrightarrow \mathrm{A} & : & N_k, MAC_a(N_a, N_k, KDC) \oplus K'_a \\ 3: \mathrm{A} & \longrightarrow \mathrm{KDC} & : & MAC_a(N_a, N_k) \end{array}$$

Schritt 1 ist identisch mit 2PAP. In Schritt 2 stellt die KDC A eine frische Zufallsmarke N_k und einen MAC zu, den sie mit dem neuen Schlüssel für A, d.h. mit K'_a, bitweise modulo 2 addiert. Nach Erhalt dieser Nachricht konstruiert A zunächst den MAC und rekonstruiert dann K'_a. Hat A den Empfang von K'_a zu bestätigen, dann gibt sie in Schritt 3 $MAC_a(N_a, N_k)$ zurück. Wiederum ist dieser Schritt optional. Man beachte, dass A nach dem Empfang von N_k und $MAC_a(N_a, N_k, KDC) \oplus K'_a$ in Schritt 2 keine Möglichkeit hat, die Authentizität der Nachricht zu prüfen. 2PAKDP ist eine Version von 2PKDP, bei der dieses Problem bereinigt ist. Bei einem 3-Parteien Schlüsselverteilprotokoll (3PKDP) teilen A und B mit der KDC jeweils einen Schlüssel, und die KDC moderiert einen Schlüsselaustausch zwischen A und B. Verschiedene 3PKDP lassen sich aus 2PAP und 2PKDP, bzw. 2PAKDP, konstruieren. Dasselbe gilt für ein Single Sign-On (SSO), das im Wesentlichen einem 2PAKDP mit Vorauthentifikation entspricht. Um im Rahmen von NetSP Datenvertraulichkeitsdienste anbieten zu können, sieht NetSP den Einsatz von CDMF (Commercial Data Masking Facility) vor.

4 SPX

Mit dem Distributed Authentication Security Service (DASS) hat DEC im Rahmen der Digital Distributed System Security Architecture (DSSA) einen Authentifikationsdienst vorgeschlagen. Der Dienst ist in RFC 1507 spezifiziert und im Rahmen von SPX als Prototyp implementiert [7].

Im Gegensatz zu Kerberos und NetSP verfolgt SPX einen hybriden Ansatz, d.h. es werden sowohl ein symmetrisches Kryptosystem (DES) als auch ein asymmetrisches Kryptosystem (RSA) eingesetzt. Die Architektur von SPX ist stark an der ITU-T (früher CCITT) Empfehlung X.509 orientiert. Öffentliche und private Schlüssel werden von rinrm Certificate Distribution Center (CDC) verwaltet und verteilt, und für die Authentifikation der Benutzer ist eine Login

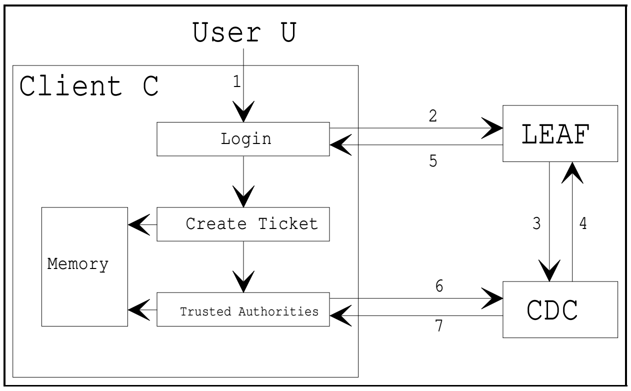

Abbildung2. SPX Benutzerinitialisierung

Enrollment Agent Facility (LEAF) zuständig. Abbildung 2 zeigt, wie sich ein Benutzer U in SPX über einen Client C in ein System einzuführen hat. Die Benutzerinitialisierung lässt sich folgendermassen beschreiben:

$$
\begin{array}{lll}
1 : \mathrm{U} & \longrightarrow \mathrm{C} & : \mathrm{U}, pwd' \\
2 : \mathrm{C} & \longrightarrow \mathrm{LEAF} & : \{U, T, N, h_1(pwd')\}k_{leaf} \\
3 : \mathrm{LEAF} & \longrightarrow \mathrm{CDC} & : \mathrm{U} \\
4 : \mathrm{CDC} & \longrightarrow \mathrm{LEAF} & : \{\{k_u^{-1}\}h_2(pwd), h_1(pwd), U\}K, \{K\}k_{leaf} \\
5 : \mathrm{LEAF} & \longrightarrow \mathrm{C} & : \{\{k_u^{-1}\}h_2(pwd), U\}N \\
6 : \mathrm{C} & \longrightarrow \mathrm{CDC} & : \mathrm{U} \\
7 : \mathrm{CDC} & \longrightarrow \mathrm{C} & : \{U, TA_u, L, k_{TA_u}\}_{k_u^{-1}}
\end{array}
$$

Dabei stellen h_1 und h_2 Einweg-Hashfunktionen, pwd' ein von U eingegebenes Passwort, pwd das von der CDC für U registrierte Passwort, T ein Zeitstempel, N eine Zufallsmarke, TA_u eine vertrauenwürdige Autorität für U und $\{U, TA_u, L, k_{TA_u}\}_{k_u^{-1}}$ ein Zertifikat für den öffentlichen Schlüssel von TA_u dar.

Will sich C im Auftrag von U gegenüber einem Server S authentifizieren, dann hat er das folgende Authentifikationsprotokoll zu durchlaufen:

$$
\begin{array}{lll}
1 : \mathrm{C} & \longrightarrow \mathrm{CDC} & : S \\
2 : \mathrm{CDC} & \longrightarrow \mathrm{C} & : \{TA_u, S, L_1, k_s\}k_{TA_u}^{-1} \\
3 : \mathrm{C} & \longrightarrow \mathrm{S} & : \{T\}K, \{U, L_2, k_d\}k_u^{-1}, \{K\}k_s, \{k_d^{-1}\}K \\
4 : \mathrm{S} & \longrightarrow \mathrm{CDC} & : U \\
5 : \mathrm{CDC} & \longrightarrow \mathrm{S} & : \{TA_s, U, L_3, k_u\}k_{TA_s}^{-1} \\
6 : \mathrm{S} & \longrightarrow \mathrm{C} & : \{T+1\}K
\end{array}
$$

Dabei stellen L_1, L_2 und L_3 Gültigkeitsdauern dar. Nach Ablauf des Protokolls teilen C und S einen symmetrischen Schlüssel K und ein asymmetrisches Schlüsselpaar (k_d, k_d^{-1}). Damit lassen sich sowohl Datenvertraulichkeits- als auch

-integritätsdienste anbieten. Im Hinblick auf einen möglichen Einsatz von SPX muss mit besonderem Nachruck darauf hingewiesen werden, dass sich DEC strategisch auf OSF DCE ausgerichtet hat, und dass die Entwicklungsarbeiten an SPX zwischenzeitlich eingestellt worden sind. SPX ist heute frei verfügbar.

5 TESS

Am Europäischen Institut für Systemsicherheit (E.I.S.S.) der Universität Karlsruhe ist das Sicherheitssystem TESS (The Exponential Security System) entwickelt worden [8]. TESS umfasst das Authentifikations- und Schlüsselverteilsystem SELANE (Secure Local Area Network Environment) und das digitale Unterschriftensystem EES (Exponential Electronic Signature).

In TESS ist eine SKIA (Secure Key Issuing Authority) sowohl für die Registrierung der Benutzer, als auch für die Generierung, Zertifizierung und Verteilung von persönlichen Token in Form von Chip- oder PCMCIA-Karten zuständig. Mit Hilfe dieser Token können sich zwei Benutzer auf einen geheimen und authentischen Sitzungsschlüssel einigen. Der bilaterale Einsatz dieses Schlüssels impliziert Authentizität, und mit Hilfe des Schlüssels können Datenvertraulichkeits- und -integritätsdienste angeboten werden. Verbindlichkeitsdienste werden über EES realisiert.

6 SESAME

Auf der Basis der OSI-Sicherheitsarchitektur hat die European Computer Manufacturer Association (ECMA) ein Security Framework erarbeitet, das im Rahmen des Projekts SESAME (A Secure European System for Applications in a Multi-vendor Environment) implementiert worden ist [9]. Seit Version 2 wird in SESAME Kerberos V5 eingesetzt. Erweitert wird Kerberos um digitale Unterschriften und Mechanismen zur Zugriffskontrolle. SESAME verfolgt einen hybriden Ansatz und stellt damit eine echte Erweiterung von Kerberos V5 dar.

Die Arbeitsweise von SESAME ist in Abbildung 3 schematisch dargestellt. Ein Benutzer kontaktiert einen lokalen User Sponsor (US). Im Zusammenspiel mit dem Authentication and Privilege Attribute (APA) Client und dem AS werden dem Benutzer ein TGT ausgestellt. Es ist die Aufgabe des Secure Association Context Managers (SACM) auf der Seite des Clients, das TGT zu verwalten, und beim Privilege Attribute Server (PAS) die Ausstellung eines Privilege Attribute Certificates (PAC) zu beantragen. Dieses ist zusammen mit dem TGT bei einem Key Distribution Server (KDS) einzureichen, um ein Ticket für einen bestimmten Server zu erhalten. Ein PAC ist in SESAME digital unterschrieben, und seine Gültigkeit ist zeitlich befristet. Auf der Serverseite stellt ein SACM die Verbindung der Applikation zu SESAME sicher. Für die Verifikation von PACs und Tickets ist eine PAC Validation Facility (PVF) zuständig. Die PVF arbeitet ebenfalls mit dem KDS zusammen. Die PVF kommt auch dann zum Einsatz, wenn sich der Server im Rahmen einer gegenseitigen Applikation gegenüber dem

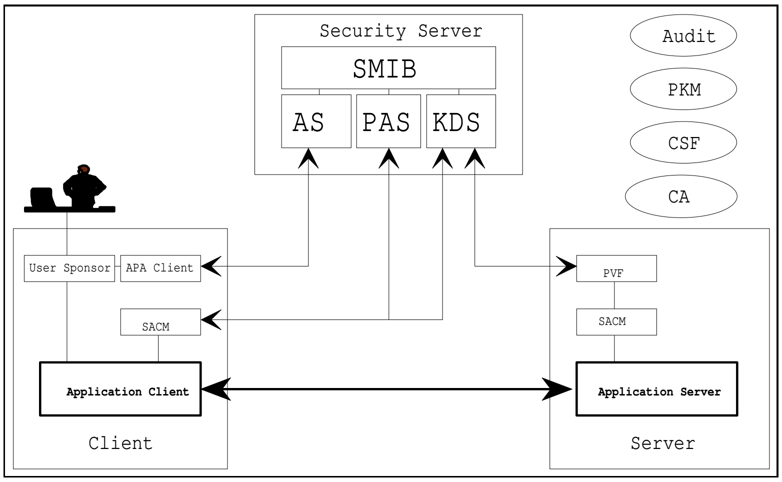

Abbildung3. SESAME

Client zu authentifizieren hat. Damit die an SESAME beteiligten Komponenten ihre Aufgaben erfüllen können, sind eine Certifiaction Authority (CA), eine Cryptographic Support Facility (CSF), ein Public Key Management (PKM) und eine Systemüberwachungskomponente (Audit) im Hintergrund aktiv.

7 Schlussfolgerungen

Die in diesem Beitrag vorgestellten Authentifikations- und Schlüsselverteilsysteme unterscheiden sich in vielerlei Hinsicht.

Sicherheitsdienste: Alle Systeme bieten Authentifikations-, Datenvertraulichkeits- und -integritätsdienste an (NetSP mit der Einschränkung einer auf 40 Bit beschränkten Schlüssellänge). Zusätzlich bietet TESS noch Verbindlichkeits- und SESAME noch Zugriffskontrolldienste an.

Kryptographische Verfahren: NetSP beschränkt sich auf den Einsatz von Einweg-Hashfunktionen zur Bildung von MACs. Kerberos setzt ein symmetrisches Kryptosystem ein. Alle anderen Systeme verfolgen einen hybriden Ansatz.

Konformität mit Standards: Kerberos und SPX sind als RFC spezifiziert. Mit Ausnahme von TESS bieten alle Systeme als Programmierschnittstelle das Generic Security Service API (GSS-API) an, wie es von der IETF CAT WG erarbeitet und in den RFCs 1508 und 1509 spezifiziert worden ist. Für die Verteilung von Zertifikaten setzen SPX und SESAME Verfahren ein, die mit ITU-T X.509 kompatibel sind.

Vertrieb: Kerberos ist das einzige System, bei dem sowohl frei verfügbare als auch kommerziell vertriebene Versionen erhältlich sind. NetSP und SESAME werden kommerziell vertrieben, wobei bei zweiterem die Frage des Vertriebs noch nicht endgültig geklärt ist. SPX und TESS sind frei verfügbar.

Exportierbarkeit: Die Frage der Exportierbarkeit stellt sich in erster Linie für die in den USA entwickelten Systeme Kerberos, NetSP und SPX. Während Kerberos und SPX den Exportrestriktionen unterliegen, darf NetSP aus den USA exportiert werden.

Die Bedeutung eines Authentifikationsdienstes für die verteilte Verarbeitung ist auch von der Open Software Foundation (OSF) erkannt worden. Für den Release 1 der OSF Distributed Computing Environment (DCE) ist Kerberos V5 mit SESAME-spezifischen Erweiterungen übernommen worden [10].

Danksagung

Ich danke Prof. Dr. D. Hogrefe, Dr. A. Greulich und A. Grossmann von der Universität Bern, D. Bleichenbacher von der ETH Zürich, sowie P. Trachsel und M. Frauenknecht vom schweizerischen Bundesamt für Informatik (BFI) für die Mitarbeit und Unterstützung bei der Entstehung dieses Beitrages.

References

1. ISO/IEC, "Information Processing Systems — Open Systems Interconnection Reference Model — Part 2: Security Architecture", ISO/IEC 7498-2, 1989.
2. R. Oppliger, *Computersicherheit — Eine Einführung*, Vieweg-Verlag, 1992.
3. B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc., New York, 1994.
4. C. Kaufman, R. Perlman, and M. Spenciner, *Network Security: Private Communication in a Public World*, Prentice Hall, Englewood Cliffs, N.J., 1995.
5. J.I. Schiller, "Secure Distributed Computing", *Scientific American*, pp. 72 – 76, November 1994.
6. R. Bird, I. Gopal, A. Herzberg, P.A. Janson, S. Kutten, R. Molva, and M. Yung, "The KryptoKnight Family of Light-Weight Protocols for Authentication and Key Distribution", *IEEE/ACM Transactions on Networking*, vol. 3, pp. 31 – 41, February 1995.
7. J.J. Tardo and K. Alagappan, "SPX: Global Authentification Using Public Key Certificates", *in Proceedings of the IEEE Symposium on Security and Privacy*, pp. 232 – 244, Los Alamitos, California, 1991. IEEE Computer Society Press.
8. Th. Beth and D. Gollmann, "Security Systems Based on Exponentiation Primitives: TESS — The Exponential Security System", *in Proceedings of the IFIP TC11 Tenth International Conference on Information Security, IFIP SEC'94*, 1994, Curacao, May 23 – 27, 1994.
9. P.V. McMahon, "SESAME V2 Public Key and Authorisation Extensions to Kerberos", *in Proceedings of the Internet Society Symposium on Network and Distributed System Security*, pp. 114 – 131, February 1995.
10. A. Grossmann, "Analyse und Beurteilung des OSF DCE Sicherheitssystems", Diplomarbeit, Universität Bern, 1995.