



**Institut für Telematik**

unter Betreuung der  
**Fraunhofer Management GmbH**



**Preprint 00-14**

**Integration der Schleusentechnologie Lock-Keeper  
in moderne Sicherheitsarchitekturen\***

Ernst-Georg Haffner  
Thomas Engel  
Christoph Meinel

\*In Proc. "Informatik aktuell: Sicherheit in Netzen und Medienströmen". M. Schumacher, R. Steinmetz, Springer-Verlag, 2000.  
ISSN 1431-472-X, S. 17-26



Authors	Ernst-Georg Haffner Thomas Engel Christoph Meinel
Copyright	© 2000 Institut für Telematik e.V., Trier
Trademarks	Use of a term in this paper should not be regarded as affecting the validity of any trademark and service mark. The product or brand names are trademarks of their respective owners.
Printing	09/2000
Document status	Version 1.0
	Printed in Germany All rights reserved
	The documentation was accomplished through the Institut für Telematik. The information contained in this document represents the current view of the authors on the issues discussed as of the date of publication. Because the mentioned enterprises must respond to changing market conditions, the results of this paper should not be interpreted to be a commitment on the part of the authors. Any information presented after the date of publication are subject to change. The right to copy this documentation is limited by copyright law. Making unauthorised copies, adaptations or compilation works without permission of the authors or institutions mentioned above is prohibited and constitutes a punishable violation of the law.

Moderne Sicherheitsarchitekturen sind darauf ausgerichtet, die diversen Kommunikationsanforderungen von Abteilungen und Unternehmensstrukturen nach außen und untereinander durch geeignete, adäquate Maßnahmen gegen unbefugten Missbrauch zu schützen. Hierzu werden unterschiedliche *Security Level* mit den jeweilig erlaubten Anwendungen definiert und zum Einsatz gebracht. Auf den niedrigsten Leveln sind alle Protokolle erlaubt, während eine Erhöhung der Sicherheitsanforderungen zugleich eine Restriktion an möglichen Anwendungen nach sich zieht, die gewöhnlich durch *Firewalls* kontrolliert werden. Am oberen Ende der Sicherheitsskala sind die kommunizierenden Netze physikalisch getrennt und die zugelassenen Protokolle entsprechend eingeschränkt. Die *Lock-Keeper™ Architektur* als eine Möglichkeit für hochsicheren Datenaustausch wird hier vorgestellt und seine Integration in komplexe Sicherheitsstrukturen aufgezeichnet.

## **Integration der Schleusentechnologie Lock-Keeper™ in moderne Sicherheitsarchitekturen**

Ernst-Georg Haffner  
Thomas Engel  
Christoph Meinel

### **Einleitung**

Mit der weltweit wachsenden Vernetzungsdichte von Computern über das Internet und den sich daraus ergebenden Möglichkeiten zum Datentransfer zu den unterschiedlichsten Zwecken steigen auch die betrieblichen Anforderungen an die Rechnerkommunikation. Kaum ein Unternehmen kann es sich heutzutage leisten, ohne Zugriff auf den gigantischen Datenspeicher des Internets auszukommen und selbst der Datenaustausch zwischen Filialen eines Konzerns erfolgt nicht selten - zumeist verschlüsselt - über das Netz der Netze.

Dabei steigt ebenfalls der Anspruch an die Qualität der Datenformate. Moderne Medien verbessern jedoch nicht allein die Brauchbarkeit der dargestellten Informationen, sondern erfordern überdies Transferkanäle hoher Bandbreite.

Allerdings wachsen mit den vielen Chancen des heutigen Informationsaustausches ebenso die Risiken. Anbindungen von Institutionen, Behörden und Unternehmen an das Internet über Standleitungen generieren gefährliche Angriffsmöglichkeiten für Attacken. Die Integrität der unternehmenseigenen Daten zu schützen, die Authentizität der Kommunikationspartner zu gewährleisten und die Abhör- und Manipulationssicherheit während eines Datenaustausches zu garantieren wird in den sogenannten *Security Policies* geregelt. Je nach Sicherheitsbedürfnis der betroffenen Stellen sind unterschiedliche Maßregeln für den elektronischen Datenverkehr sowie Verhaltensvorschriften für die Mitarbeiter Bestandteil dieser Dokumente. Allerdings sind für große Konzerne keineswegs gleiche Anforderungen aller Abteilungen vorauszusetzen. Vielmehr sehen die Sicherheitsvorschriften komplexer Sicherheitsarchitekturen unterschiedliche *Security Levels* vor, wobei im Einzelnen zu klären ist, welche Kommunikationsziele - unter welchen Sicherheitsbedingungen - zu erreichen sind. Nicht selten müssen hier schwerwiegende Entscheidungen gefällt und Kompromisse eingegangen werden.

Als Werkzeuge zur Realisierung der angestrebten Ziele dienen im Bereich der Sicherheitsinfrastrukturen für den elektronischen Informationsaustausch zumeist *Firewalls*. Der Zweck dieser Systeme besteht in einer Art Filterfunktion: nur berechnete Zugriffe für authentifizierte Benutzer<sup>1</sup> mittels der erlaubten Protokolle dürfen zugelassen werden. In diesem Artikel werden wir darüber hinaus Einsatzmöglichkeiten der Schleusentechnik des *Lock-Keeper™* vorstellen, einer Entwicklung des Instituts für Telematik, die vermittels physikalischer Trennung der kommunizierenden Netzwerke in der Lage ist, höhere Sicherheitsanforderungen zu gewährleisten und bestimmte Attacken von Angreifern auszuschließen.<sup>2</sup> Wir werden

---

<sup>1</sup> Zumeist wird anstatt der Überprüfung der Authentizität des Benutzers auch eine solche des Quellrechner-Systems als statthaft empfunden.

<sup>2</sup> Das Patentverfahren der *Lock-Keeper™*-Architektur ist unter der Patentnummer 198 38 253.7-31 geführt.

weiterhin aufzeigen, an welchen Stellen der Sicherheitsarchitekturen eine geeignete Analyse eingehender und ausgehender Daten erfolgen kann.

In den folgenden Abschnitten wollen wir zunächst die Gefährdungspotentiale von Angriffen gegen firmeneigene Netze aufzeigen und hier ebenfalls grundlegende Fragestellungen der Security Policies berücksichtigen (Abschnitt: „Angriffe gegen Datennetze“). In einem weiteren Abschnitt folgen dann diverse Ansätze zur Abwehr derartiger Angriffe, die zu komplexen Sicherheitsarchitekturen führen (Abschnitt: „Abwehrmaßnahmen gegen Angriffe“). Im Vordergrund wird dabei die Funktionsweise des Lock-Keeper™ stehen. Eine Zusammenfassung mit Ausblick auf künftige Aktivitäten beschließt die Ausführungen.

## Angriffe gegen Datennetze

**Die Bedeutung der Security Policy.** Um Technologien gegen Angreifer auf Datennetze geeignet beurteilen und bewerten zu können, werden wir zunächst die wesentlichen Aspekte moderner Sicherheitskonzepte aufzeigen.

Wir unterscheiden hierbei zwischen einem inneren Computer-Netzwerk (IN) und einem äußeren (ON). Das IN beinhaltet jedwede Art vertraulicher und zu schützender Information eines Unternehmens, einer Behörde oder sonstigen Institution. Das ON ist ein Netzwerk oder ein Verbund von Netzen, über das Datenaustausch mit Kommunikationspartnern erfolgen soll. Ein prominentes Beispiel eines ON ist das *Internet*. Firmeneigene Intranets stellen INs dar. Allerdings können die Netzwerkstrukturen auch komplexer sein. Innerhalb größerer Unternehmen und Konzerne kann auch der Datenaustausch untereinander mittels INs und ONs modelliert werden.

Ein wesentlicher, allerdings nicht der einzige Sicherheitsaspekt konzentriert sich hierbei auf die Frage, wie der Datenaustausch zwischen IN und ON gegen mögliche Angriffe von außen (aus dem ON) geschützt werden kann. Allerdings darf hierbei nicht vergessen werden, dass de facto die meisten Attacken gegen Netze aus den INs selbst erfolgen [1].

Mögliche Risiken im Datenaustausch sind nicht-gewährleistete Authentizität von Sender und Empfänger, Abhör- und Manipulationsmöglichkeiten von Seiten Dritter und das unbefugte Eindringen in das IN, während gerade ein Datentransfer zwischen den Netzen erfolgt. Auch die Daten selbst können das Computernetzwerk gefährden. „Viren“, „Würmer“ und andere sogenannte „Beastware“ stellen eine Bedrohung des INs dar.

Aufgrund dieser komplexen und umfangreichen Gefährdungspotentiale sollte ein Unternehmen zunächst eine *Security-Policy* [2] aufstellen, die im Detail die wichtigsten Sicherheitsfragen beantworten muss. Wie bereits in der Einleitung erwähnt, geht das größte Sicherheitsrisiko im Umgang mit elektronischem Datentransfer mit dem höchsten *Quality of Service* (QoS) einher. Wenn alle Arten von Programmen und Protokollen zu Verfügung stehen, wächst die Begeisterung des Anwenders mit dem Missfallen der Sicherheitsexperten. Typische moderne Internet-Protokolle und -Anwendungen wie *http*, *ftp*, *telnet*, *rlogin* [3], *smtp* und *sendmail* [4] stellen ebenfalls enorme Risiken dar<sup>3</sup>.

**Klassifikation von Attacken.** Zum Erstellen einer spezifischen Security-Policy, die als Grundlage zur Absicherung gegen Angriffe von innen oder außen dient, ist es erforderlich, die möglichen Arten von Attacken zu klassifizieren und dabei festzuhalten, welche Abwehrmaßnahmen geeignet sind, den Bedürfnissen des jeweiligen Unternehmens bzw. der entsprechenden Abteilungen zu genügen.

Die nachfolgende Tabelle 1 gibt einen kurzen Überblick über die möglichen Klassen von Attacken und zeigt, ob es sich hierbei um einen „Online-Angriff“ handelt, bei dem der Angreifer interaktiv über das Netz auf die Systeme im IN gelangt (vgl. [2]).

Diese Klassifikation zeigt auf, dass zahlreiche Möglichkeiten für den Angriff gegen ein IN existieren. Rein zahlenmäßig gehören die Offline-Angriffe mittels Beastware inzwischen zu den meistverbreiteten Angriffstypen, jedoch gelten die Online-Angriffe als die gefährlichsten, da die gesamte Integrität des inneren Netzwerks potentiell in Frage gestellt wird.

**Psychologische Faktoren.** Interessanterweise spielen für den Einsatz von Sicherheitswerkzeugen neben der technischen Relevanz zunehmend psychologische Faktoren eine zentrale Rolle. Das „Gefühl der Sicherheit“ ist kein bloßer Zusatz oder gar ein Nebeneffekt in der informations- und kommunikationsbetonten Arbeitswelt. Ein aus sicherheitstechnischer Sicht objektiv überzeugendes System kann – wenn die Security-Policy in dieser Frage noch Lücken aufweist – durchaus verunsichernd auf die

<sup>3</sup> Zu generellen Sicherheitsrisiken von UNIX siehe [5].

betroffenen Personen wirken. Eine zentrale Rolle spielt hierbei die Klarheit und Überschaubarkeit des Sicherheitskonzepts, die sich in der Security Policy offenbart.

Klasse	Beschreibung der Quelle	On-line
Passwort-Diebstahl	Passwörter befinden sich in Klartext-Dateien oder werden abgehört auf IP-Ebene. Dictionary-Attacks raten Passwörter systematisch.	✓
„Social engineering“	Passwörter werden durch menschliche Interaktion bewusst oder unbewusst übermittelt (z.B. telefonisch).	✓
Bugs und Hintertüren	Fehlverhalten von Software; bewusste Abweichung von der Programmspezifikation durch den Programmierer; oder Viren und Würmer schaffen neue „Hintertüren“.	✓
Authentifikationsfehler	Programme zeigen Einwahlmasken im IN und senden die Passwörter ins ON.	✓
Fehler auf Protokollebene	Sicherheitslücken im TCP-Protokoll, etwa „TCP sequence number attack“; Tunneling; „message encapsulating“; „tiny fragment attack“; „overlapping fragment attack“ [6].	✓
Offline-Angriff (meist „Denial-of-service“)	Würmer, Trojanische Pferde und Viren („Beastware“) können das IN in seiner Funktion beeinträchtigen oder gar zerstören. Daten des IN können ins ON gelangen.	--

Tabelle 1: Klassifizierung von Angriffsmöglichkeiten gegen Computernetze

**Beastware.** Wie Tabelle 1 aufweist, stellen Attacken über Inhalte der Daten selbst, die Viren, Würmer, Trojanische Pferde und andere „Beastware“ ([7],[8]) enthalten können, grundsätzlich hohe Risiken dar [9]. Hierzu ist jedoch die Frage zu klären, worin sich das hohe Gefährdungspotential dieser Daten äußert. Inzwischen existieren zwar eine Reihe von Werkzeugen und Analysetools, die einen gewissen Anteil wohlbekannter Beastware erkennen und eliminieren können (Virens Scanner, Mail-Analyser etc.), allerdings sollte dies nicht darüber hinwegtäuschen, dass ein Großteil des Sicherheitsrisikos grundsätzlich für ausführbaren Code bestehen bleibt.

Es handelt sich jedoch informationstheoretisch de facto um ein unentscheidbares Problem, dass ein Programm prinzipiell nicht herausfinden kann, welche Handlungen eine bestimmte Software auszuführen in der Lage ist. Und dies gilt nicht nur für eine automatische Analyse der Beastware: wie sollte ein menschlicher Administrator alle Wirkungen eines Programms mit den verschiedensten Eingabewerten ermitteln (z.B. wenn eine unendliche Testmenge erforderlich ist)?

Deshalb sind es durchaus berechtigte Sorgen, die Sicherheitsexperten von Unternehmen dazu veranlassen, keine unbekannte Software von außen in das firmeneigene Netz aufzunehmen und sehr restriktive Maßnahmen anstrengen, damit nicht durch diverse Kompilations-, Umwandlungs- oder Dekodierprozesse aus einfachem ASCII-Text ein Stück Software wird. Im Rahmen einer klar definierten Security-Policy lassen sich derartige Maßnahmen für gewöhnlich, insbesondere in Hochsicherheitsbereichen, als völlig legitim vertreten.

### Abwehrmaßnahmen gegen Angriffe

**Firewalls.** Als ein sehr wichtiges Werkzeug zur Gewährleistung von Netzwerksicherheit hat sich in den vergangenen Jahren die bereits erwähnte *Firewall* etabliert. Eine Firewall ist eine Sammlung von Komponenten zwischen zwei Netzwerken, die zusammen folgende Eigenschaften erfüllen.

- Der Datenverkehr zwischen den beiden Netzen muss in beiden Richtungen die Firewall passieren.
- Nur autorisierter Datenverkehr - gemäß der jeweiligen Security-Policy - darf die Firewall passieren.
- Die Firewall selbst kann nicht angegriffen werden. (vgl. [2])

Die meisten modernen Firewalls sind Paketfilter. Sie analysieren TCP/IP<sup>4</sup>-Pakete, indem sie Sender und Empfänger gemäß der IP-Adresse verifizieren; sie kontrollieren den TCP-Port um sicherzustellen, dass der gewählte Dienst auch in Anspruch genommen werden darf. Allerdings gibt es zahlreiche Methoden, mit denen die Analysemechanismen einer Firewall hintergangen werden können. Mängel und

<sup>4</sup> Transmission Control Protocol/Internet Protocol

Sicherheitslücken in der Konstruktion einer Firewall versuchen die Hersteller schnellstmöglich zu schließen. Es gibt jedoch keine absolute Sicherheit, dass sich Unbefugte nicht trotz Absicherung durch eine Firewall aus dem ON in das IN Zugang verschaffen.

Die Ursache hierfür liegt in der prinzipiellen Aufgabenstellung dieser Sicherheitsmaßnahme: eine Firewall muss erlaubte Anfragen von nicht-autorisierten unterscheiden und hierbei erstere ermöglichen, während letztere abzuwehren sind. Angriffe mit hoher krimineller Energie basieren in der Regel darauf, dass die Kriterien für den berechtigten Zugriff durch den unberechtigten Angreifer gefälscht werden, und somit die Firewall ungehindert passiert werden kann. Es besteht hier demnach durch die prinzipielle Funktionsweise dieses Systems ein inhärentes Sicherheitsrisiko.

**Die Lock-Keeper™ Architektur.** Bei sehr hohen Sicherheitsanforderungen von Unternehmen und wenn nicht alle Dienste zwischen den Netzen bereitgestellt werden müssen, stellt das Datenaustauschverfahren des *Lock-Keeper™* (LK) eine echte Alternative oder Ergänzung zu klassischen Firewalls dar.

Der LK operiert dabei wie eine Schleuse. Zu keinem Zeitpunkt besteht eine direkte Verbindung zwischen den Netzen IN und ON, statt dessen werden die Daten zunächst in ein Vermittlungsnetz, das LKN transferiert, um nach Abtrennung vom jeweiligen Quellnetz eine Verbindung zum Zielnetz aufzubauen (vgl. Abb. 1).

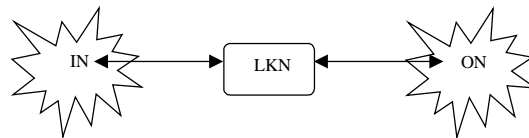


Abbildung 1: Topologie der Schleusentechnologie des Lock-Keeper™

Die Abbildung 1 stellt eine abstrakte Darstellung der Netzwerktopologie des LK dar. Zentral für die Funktionsweise des LK ist dabei, dass die Trennung der beiden Netze auf einer *physikalischen Ebene* stattfindet. Damit wird es auch für den Systemadministrator kaum möglich, die Funktionsweise des Lock-Keeper™ auch nur vorübergehend zu umgehen. Somit kann zwar eine fehlerhafte Software-Komponente oder eine falsche oder unzureichende Konfiguration dazu führen, dass der Datenaustausch beeinträchtigt wird (*denial-of-service*), allerdings wird die Integrität der Daten des IN dabei nicht beeinträchtigt. Die dynamische Verbindung der jeweiligen Netze basiert dabei auf *PPP*<sup>5</sup>, so dass hierüber Datentransfers und Mailübergabe stattfinden kann. Eine symbolische Darstellung der Funktionsweise des LK findet sich in Abbildung 2.

Eine Schleusentechnologie, wie die des Lock-Keeper™, bleibt für die möglichen Online-Angriffe immun (vgl. 2.2), da das zugehörige Sicherheitskonzept nicht etwa berechnete von nicht-erlaubten Anfragen trennt (wie bei einer Firewall, 3.1), sondern grundsätzlich – unabhängig von einer optionalen Analyse – jedweden Datenverkehr zwischen IN und ON zwischenspeichert und hierdurch alle direkten Angriffsmöglichkeiten unterbindet. In der Umkehrung bedeutet dies natürlich ebenfalls, dass bestimmte Dienste, die eine direkte und unmittelbare Verbindung zwischen den Computer-Netzwerken erfordern, durch den Lock-Keeper™ nicht bereitgestellt werden können. Im Ausblick wird auf künftige Entwicklungen in diesem Bereich hingewiesen.

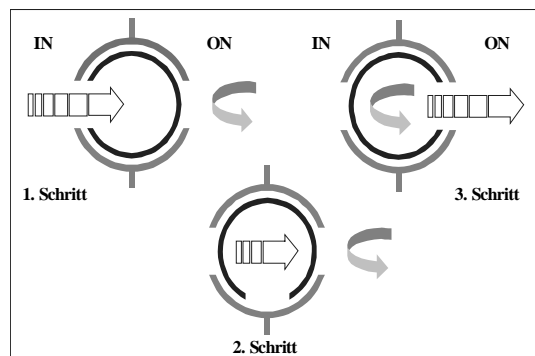


Abbildung 2: Funktionsweise des Lock-Keeper™

<sup>5</sup> Point to Point Protocol

Die oben angesprochenen psychologischen Aspekte einer Sicherheitsarchitektur sprechen aufgrund der Klarheit des Schleusenverfahrens für den Einsatz eines Lock-Keeper™. Ohne genaue Kenntnis der (TCP)-Protokoll-Spezifikationen lassen sich die prinzipiellen Sicherheitscharakteristika vermitteln. Sowohl Software-Fehler als auch versehentliche oder absichtliche Misskonfigurationen des Systems gestatten aufgrund des hardwarenahen Aufbaus keine direkte Verbindung der Netze durch die Schleuse.

Der Preis für eine sichere Abwehr von Online-Attacken muss jedoch durch Einbußen im *Quality of Service* gezahlt werden. So ist beispielsweise ein klassisches Browsen im Internet nicht möglich, wenn die Netze mittels Lock-Keeper™ verbunden sind. Einen Ausweg aus diesem Dilemma bieten hier mehrschichtige Sicherheitsarchitekturen. So kann ein Unternehmen das eigene Netz in mehrere Subnetze aufteilen, wobei – je nach Sicherheitslevel – diese Netze untereinander mittels einer Firewall oder eines Lock-Keeper™ gesichert sind. Selbstverständlich können Firewall und Lock-Keeper™ auch kombiniert eingesetzt werden (vgl. 3.3).

Die theoretische Funktionsweise des Lock-Keeper™ als Schleuse für sicheren Datenaustausch kann auf mehrere unterschiedliche Arten implementiert und realisiert werden. Entscheidend für die Einhaltung der Sicherheitscharakteristika ist dabei die Trennung zwischen der Schleusen-steuernden Software und der Trennung der beiden Netze. Jedwedes – absichtliches oder unbeabsichtigt-fahrlässiges – Fehlverhalten der Software darf keinesfalls dazu führen, dass die beiden zu trennenden Netze verbunden werden.

Im einfachsten Falle, wo der LK nur aus einem einzigen Rechnersystem besteht, kann dies zum Beispiel dadurch realisiert werden, dass die Verbindungen zwischen den Netzen über den Lock-Keeper™ mit ISDN-Leitungen realisiert werden. Schließt man den LK und die beiden zu verbindenden Systeme an *denselben* NTBA<sup>6</sup> an, so ist stets gewährleistet, dass jeweilig maximal 2 Leitungen belegt werden können. Da jede Verbindung zwischen dem Lock-Keeper™ und einem der beiden Netze (IN oder ON) jedoch bereits 2 Leitungen beansprucht, kann keinesfalls per Software eine direkte Verbindung zwischen IN und ON hergestellt werden; selbst dann nicht, wenn der LK durch eine erfolgreiche Attacke von außen kompromittiert worden wäre. Wie leicht zu sehen ist, verlagert sich die Sicherheitsanforderung an den Lock-Keeper™ selbst somit auf die bereitgestellte Infrastruktur. Eine Sicherheitsbeurteilung eines solchen Verfahrens ist deswegen günstig zu beurteilen, weil auch durch Eingriffe des Systemadministrators (ohne die Infrastruktur zu verändern) die Systemcharakteristik nicht gefährdet wird. Die Möglichkeit für Denial-of-Service Attacken bleibt jedoch bestehen; allerdings sind die Daten im IN stets geschützt vor direkten (online-)Angriffen aus dem ON.

Eine alternative Implementierung besteht in einer hardwareseitigen Lösung, die per se den LK stets nur *entweder* mit dem IN *oder* dem ON verbindet. Wiederum ist eine solche Lösung gegen mögliche Software-Attacken gefeit. Allerdings muss gewährleistet bleiben, dass die Umschaltzeit zwischen den Netzen nicht so niedrig gewählt wird, dass sie für das robuste IP-Protokoll transparent wird.

**Kombinierte Sicherheitsarchitekturen.** Typischerweise beinhalten die IT-Architekturen von Unternehmen mit Internet-Standleitungszugängen neben der Absicherung durch eine Firewall (FW) ebenfalls Virens Scanner (VS) und Mail-Analysetools (MA).

Der LK operiert dabei wie eine Schleuse. Zu keinem Zeitpunkt besteht eine direkte Verbindung zwischen den Netzen IN und ON, statt dessen werden die Daten zunächst in ein Vermittlungsnetz, das LKN transferiert, um nach Abtrennung vom jeweiligen Quellnetz eine Verbindung zum Zielnetz aufzubauen (vgl. Abb. 1).

Router (R) und Bridge-Router (BR) sind ebenfalls in der Lage, durch sogenannte Access-Listen verschiedene Segmente interner Netze voneinander zu trennen. Dazwischen entsteht eine „demilitarisierte Zone“ (DMZ). In diese komplexe Architektur lassen sich ebenfalls Schleusenkomponenten des Lock-Keeper™ (LK) für Hochsicherheitsanwendungen einflechten. Eine mögliche Ausbaustufe skizziert die Abbildung 3.

---

<sup>6</sup> Network Termination Basic Access

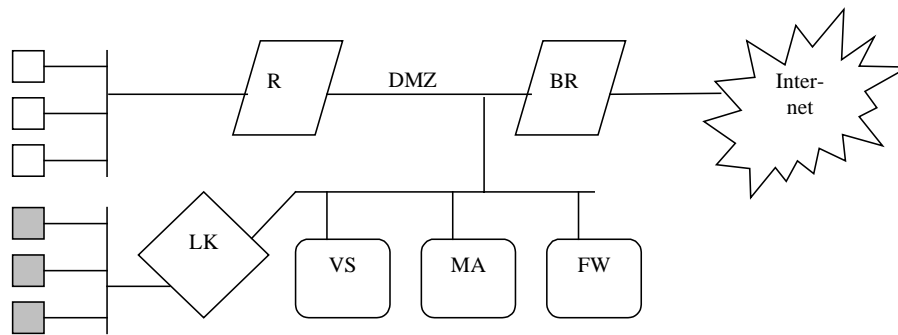


Abbildung 3: Moderne Sicherheitsarchitekturen mit Schleusenkomponenten

Die Schleusentechnologie lässt sich jedoch ebenso mit dem Internet direkt verbinden. Dann werden für derartig abgesicherte Netzsegmente allerdings typische Internet-Dienste (wie z.B. das Browsen) grundsätzlich unterbunden, oder zumindest nur mit starken Einbußen in den Antwortzeiten ermöglicht (über Cache-Proxies).

Die physikalische Trennung von Netzwerken hat eine längere Historie. Woodward erwähnt den Begriff des „Security-Guard“ als ein Verbindungsstück zwischen einem unsicheren und einem vertrauenswürdigen Rechnersystem bereits 1979 [10]. Hier spielt jedoch die menschliche Kontrollkomponente eine entscheidende Rolle. Außerdem wird der Datentransfer zunächst nur in einer Richtung betrachtet. Dieser Gedanke wurde schließlich erneut aufgegriffen und erweitert von Denning, lange bevor das *World Wide Web* das Internet populär gemacht hat [11].

**Reduktion des Zeitversatzes.** Ein prinzipielles Phänomen beim Einsatz der Schleusentechnologie ergibt sich durch den zwingenden Zeitversatz, den wir auch *Zyklus* nennen. Selbst wenn Daten mit optimaler Geschwindigkeit bis zum zentralen Schleusenserver gelangen, müssen sie spätestens hier auf das nächste Öffnen des Schleusentores warten. Im schlechtesten Falle jedoch gelangen die Daten nicht einmal ohne Zeitversatz bis zur Schleusenzentrale. Dann ist ein zusätzlicher Zyklus bis zur Auslieferung der Daten ins Zielnetz erforderlich.

Eine Erweiterungslösung des Lock-Keeper™ sieht hierbei vor, durch ein Klonen des Schleusensystems einen kompletten Zyklus zu reduzieren. Dabei ergeben sich nun unterschiedliche Restriktionen, was die möglichen Öffnungsperioden der Schleusentore angeht. Nur die Tore  $IS_1$  und  $OS_2$  sowie  $IS_2$  und  $OS_1$  dürfen gleichzeitig eine Verbindung der Netze ermöglichen (vgl. Abbildung 4).

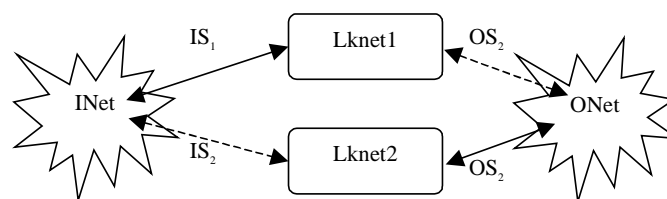


Abbildung 4: Zyklusreduktion durch Lock-Keeper™-Verdopplung

### Zusammenfassung und Ausblick

Moderne Sicherheitsarchitekturen müssen sich am wandelnden und wachsenden Bedarf an elektronischem Datenaustausch orientieren. Vielfältiger und multimedialer Transfer von Informationen zieht jedoch ebenso vielfältig ausgeprägte Angriffsmöglichkeiten nach sich. Durch unterschiedliche Sicherheitslevel lassen sich Anforderungen an die *Quality-of-Service* mit den jeweiligen Sicherheitsbedürfnissen in Einklang bringen. Hierzu ist eine möglichst breit angelegte Palette einsetzbarer Sicherheitskomponenten zu berücksichtigen. Neben klassischen Firewalls stellen so auch Lock-Keeper™ Infrastrukturen bereit, die Datenaustausch ermöglichen.

Neben der prinzipiellen Funktionsweise dieser Systeme wurde in der vorliegenden Arbeit zudem die Integration in komplexe Sicherheitsarchitekturen gezeigt. Zur Überwindung von zeitlichen Engpässen oder Beschränkungen von Diensten wurden darüber hinaus komplexe Erweiterungsmöglichkeiten skizziert.

Für künftige Ausbaustufen der Schleusentechnologie wird derzeit daran gearbeitet, zeitverzögert auch solche Dienste bereitzustellen, die für gewöhnlich eine unmittelbare Verbindung zwischen den datenaustauschenden Netzen erfordern. Die Einschränkungen im Bereich des Quality-of-Service könnten damit vermindert werden.

## Literatur

- [1] Morrie Gasser: Building a secure Computer System, Van Nostrand Reinhold, 1988
- [2] William R. Cheswick, Steven M. Bellovin: Firewalls and Internet Security, Addison-Wesley, 5<sup>th</sup> printing April, 1995
- [3] P. Gulbins, UNIX Version 7, bis System V.3, Springer-Verlag, 1988
- [4] B. Costales, E. Allmann: sendmail, O'Reilley and Associates, 2<sup>nd</sup> edition, 1997
- [5] David A. Curry: UNIX System Security: A Guide for Users and System Administrators, Addison-Wesley, 1992
- [6] G. Paul Ziemba et al.: Request for Comments: 1858, Security Considerations – IP Fragment Filtering, October 1996
- [7] Klaus Brunnstein: Beastware (Viren, Würmer, trojanische Pferde) Paradigmen Systemischer Unsicherheit, Sichere Daten, sichere Kommunikation, Springer-Verlag, 1994, 44-60
- [8] F. Cohen: Computer Viruses: Theory and Experiments”, proceedings of the 7<sup>th</sup> National Computer Security Conference, Gaithersburg 1984, 240-263
- [9] P. A. Karger: Limiting the Potential Damage of Discretionary Trojan Horses, Proceedings of the 1987 Symposium on Security and Privacy, IEEE Computer Society, 1987, 32-37
- [10] J. P. L. Woodward: Applications for Multilevel Secure Operating Systems, proceedings of the NCC 48, 1979, 319-328
- [11] D. E. Denning: Cryptographic Checksums for Multilevel Database Security, Proceedings of the 1984 Symposium on Security and Privacy, Silver Spring 1984, 52-61