Segurança da Informação

Conceitos Básicos

Principais Referências

- Capítulo 1 do Stallings
- RFC 2828: Internet Security Glossary
- Modelo de Redes
  - ISO/IEC 7498-1:1994 e ITU-T Recommendation X.200. INFORMATION TECHNOLOGY -- OPEN SYSTEMS INTERCONNECTION -- BASIC REFERENCE MODEL: THE BASIC MODEL
  - ISO 7498-2:1989 e Recommendation X.800. INFORMATION PROCESSING SYSTEMS -- OPEN SYSTEMS INTERCONNECTION -- BASIC REFERENCE MODEL -- PART 2: SECURITY ARCHITECTURE
- NIST SP 800-12 Rev. 1: An Introduction to Information Security

Definições Básicas

Nomenclaturas diversas para a própria área

- Segurança da Informação
  - Nome histórico, associado ao primeiro objeto protegido por meio de técnicas "criptográficas" – a informação
  - Ainda é o termo mais usado - podemos entender que extrapola para Segurança de Sistemas de Informação
- Segurança de Sistemas de Informação
  - Usado explicitamente por algumas agências (e.g. ANSSI)
- Segurança de Computadores
  - Remete não apenas à Informação mas aos aspectos "computacionais" a serem protegidos
- Segurança Cibernética
  - Geralmente usado no ambiente de Defesa, remete ao "espaço cibernético" como um ambiente a ser protegido e explorado
- Segurança da Informação e Criptografia (SIC)
  - Termo frequentemente usado pela Inteligência no Brasil

Definição de segurança de computadores

- Segurança de computadores: A proteção oferecida a um sistema de informação automatizado para atingir os **objetivos** apropriados de preservação da integridade, disponibilidade e confidencialidade de ativos de sistemas de informação (incluindo hardware, software, firmware, informações/dados e telecomunicações).
- Origem: An Introduction to Computer Security: the NIST Handbook, de 1995, versão anterior ao "An Introduction to Information Security"
- É apenas uma das definições possíveis...

Definição da SP 800-12 R1

- Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure **confidentiality**, **integrity**, and **availability**.

Definição da RFC 2828

- $ computer security (COMPUSEC)
  - (I) Measures that implement and assure security services in a computer system, particularly those that assure access control service.
  - (C) Usually understood to include functions, features, and technical characteristics of computer hardware and software, especially operating systems.

- "I" identifies a RECOMMENDED Internet definition.
- "N" identifies a RECOMMENDED non-Internet definition.
- "O" identifies a definition that is not recommended as the first choice for Internet documents but is something that authors of Internet documents need to know.
- "D" identifies a term or definition that SHOULD NOT be used in Internet documents.
- "C" identifies commentary or additional usage guidance.

Definição da RFC 2828

- $ computer security (COMPUSEC)
  - (I) Measures that implement and assure security services in a computer system, particularly those that assure access control service.
  - (C) Usually understood to include functions, features, and technical characteristics of computer hardware and software, especially operating systems.

- "I" identifies a RECOMMENDED Internet definition.
- "N" identifies a RECOMMENDED non-Internet definition.
- "O" identifies a definition that is not recommended as the first choice for Internet documents but is something that authors of Internet documents need to know.
- "D" identifies a term or definition that SHOULD NOT be used in Internet documents.
- "C" identifies commentary or additional usage guidance.

RFC 2828

- $ security service
  - (I) A processing or communication service that is provided by a system to give a specific kind of protection to system resources.
    (See: access control service, audit service, availability service, data confidentiality service, data integrity service, data origin authentication service, non-repudiation service, peer entity authentication service, system integrity service.)
  - (O) "A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or the data transfers." [I7498 Part 2]
  - (C) Security services implement security policies, and are implemented by security mechanisms.
- "I" identifies a RECOMMENDED Internet definition.
- "N" identifies a RECOMMENDED non-Internet definition.
- "O" identifies a definition that is not recommended as the first choice for Internet documents but is something that authors of Internet documents need to know.
- "D" identifies a term or definition that SHOULD NOT be used in Internet documents.
- "C" identifies commentary or additional usage guidance.

X.800 (e ISO 7498-2)

- Não propõe definição para segurança de computadores
  - Trata o conceito central de *serviços de segurança* e o conceito relacionado de *mecanismos de segurança*
- 3.3.51 security service.
  - A service, provided by a **layer of communicating open systems**, which ensures adequate security of the systems or of data transfers.
  - Curiosamente, o padrão não define "rigorosamente" segurança ou mecanismo (embora trate estes assuntos)

Serviços e Mecanismos de Segurança X.800

- 5.1 Overview
  - **Security services that are included in the OSI security architecture and mechanisms which implement those services** are discussed in this section. The security services described below are basic security services. In practice they will be invoked at appropriate layers and in appropriate combinations, usually with non-OSI services and mechanisms, to satisfy security policy and/or user requirements. Particular security mechanisms can be used to implement combinations of the basic security services. Practical realizations of systems may implement particular combinations of the basic security services for direct invocation.
- 5.2 Security services
  - The following are considered to be the security services which can be provided optionally within the framework of the OSI Reference Model. The authentication services require authentication information comprising locally stored information and data that is transferred (credentials) to facilitate the authentication.
- 5.3 Specific security mechanisms
  - The following mechanisms may be incorporated into the appropriate (N)-layer in order to provide some of the services described in § 5.2.

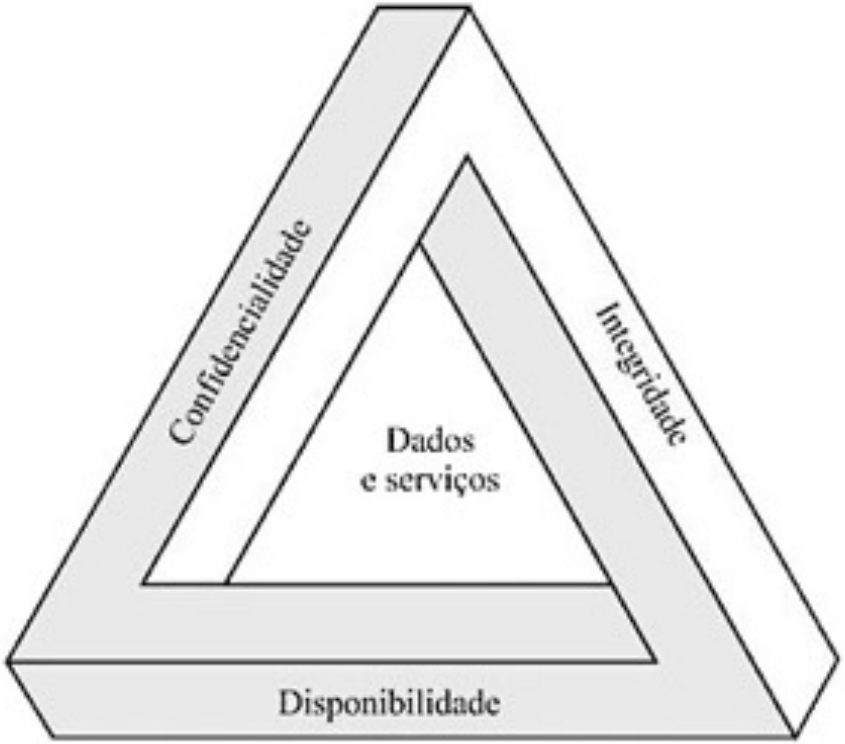
Serviços e Mecanismos de Segurança X.800

Service \ Mechanism	Encipherment	Digital signature	Acces control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y	·	·	Y	·	·	·
Data origin authentication	Y	Y	·	·	·	·	·	·
Access control service	·	·	Y	·	·	·	·	·
Connection confidentiality	Y	·	·	·	·	·	Y	·
Connectionless confidentiality	Y	·	·	·	·	·	Y	·
Selective field confidentiality	Y	·	·	·	·	·	·	·
Traffic flow confidentiality	Y	·	·	·	·	Y	Y	·
Connection Integrity with recovery	Y	·	·	Y	·	·	·	·
Connection integrity without recovery	Y	·	·	Y	·	·	·	·
Selective field connection integrity	Y	·	·	Y	·	·	·	·
Connectionless integrity	Y	Y	·	Y	·	·	·	·
Selective field connectionless integrity	Y	Y	·	Y	·	·	·	·
Non-repudiation. Origin	·	Y	·	Y	·	·	·	Y
Non-repudiation. Delivery	·	Y	·	Y	·	·	·	Y

Analisando as definições

- Todas elas remetem a um conjunto de "objetivos" ou "requisitos" de segurança que permitem proteger recursos: **confidencialidade**, **integridade** e **disponibilidade**
- Especialistas convergem para um conjunto básicos de objetivos/requisitos de segurança:
  - Essa abordagem é bem clara nos padrões NIST, e reverberada por vários especialistas

Tríade CID (CIA)



Tríade CID (CIA)

- **Confidencialidade**: Preservar restrições autorizadas ao acesso e revelação de informações, incluindo meios para proteger a privacidade pessoal e as informações proprietárias. Uma perda de confidencialidade consiste na revelação não autorizada de informações.
- **Integridade**: Defender contra a modificação ou destruição imprópria de informações, garantindo a irretratabilidade (ou não repúdio) e a autenticidade das informações. Uma perda de integridade consiste na modificação ou destruição não autorizada de informações.
- **Disponibilidade**: Assegurar que o acesso e o uso das informações seja confiável e realizado no tempo adequado. Uma perda de disponibilidade consiste na disrupção do acesso ou da utilização de informações ou de um sistema de informação.

Detalhando os três objetivos fundamentais

- Confidencialidade
  - Confidencialidade de dados: Garante que informações privadas ou confidenciais não fiquem disponíveis nem sejam reveladas a indivíduos não autorizados.
  - Privacidade: Garante que os indivíduos controlem ou influenciem quais informações sobre eles podem ser coletadas e armazenadas, e por quem e para quem tais informações podem ser reveladas.
- Integridade
  - Integridade de dados: Garante que informações e programas sejam alterados somente de maneira especificada e autorizada.
  - Integridade de sistemas: Garante que um sistema desempenhe sua função pretendida de maneira incólume, livre de manipulação não autorizada do sistema, seja deliberada, seja inadvertida.
- Disponibilidade
  - Garante que os sistemas e recursos estejam prontamente disponíveis e que não haja negação de serviço a usuários autorizados.

Dois "possíveis" objetivos adicionais

- **Autenticidade**: A propriedade de ser genuína e poder ser verificada e confiável; confiança na validade de uma transmissão, de uma mensagem ou do originador de uma mensagem. Isso significa verificar que os usuários são quem dizem ser e que cada dado que chega ao sistema veio de uma fonte confiável.
- **Determinação de responsabilidade**: O objetivo de segurança que leva à exigência de que as ações de uma entidade sejam rastreadas e atribuídas unicamente àquela entidade. Isso dá suporte à irretratabilidade, à dissuasão, ao isolamento de falhas, à detecção e prevenção de intrusões, e à recuperação e à ação judicial após uma ação.

Riscos, Ameaças e Ataques

Definições-chave (adaptado da RFC 2828)

- **Política de segurança.** Conjunto de regras e práticas que especificam ou regulamentam como um sistema ou organização provê serviços de segurança para proteger ativos sensíveis e críticos de um sistema.
- **Vulnerabilidade.** Falha, defeito ou fraqueza no projeto, implementação ou operação e gerenciamento de um sistema que poderia ser explorada para violar a política de segurança do sistema.
- **Ameaça.** Um potencial para violação de segurança, que existe quando há circunstância, capacidade, ação ou evento que poderia infringir a segurança e causar dano.
- **Adversário (agente fonte de ameaça).** Entidade que ataca um sistema ou é uma ameaça para ele.
- **Ataque.** Tentativa de violação da segurança do sistema que deriva de ameaça inteligente, isto é, um ato inteligente que é uma tentativa deliberada para burlar serviços de segurança e violar a política de segurança de um sistema.
- **Contramedida (controle).** Ação, dispositivo, procedimento ou técnica que reduz uma ameaça, uma vulnerabilidade ou um ataque, eliminando-o ou prevenindo-o, minimizando o dano que ele pode causar ou descobrindo-o e relatando-o de modo a possibilitar uma ação corretiva.
- **Risco.** Expectativa de perda de segurança expressa como a probabilidade de que uma ameaça particular explorará uma vulnerabilidade particular com resultado danoso particular.

Originais da RFC 2828

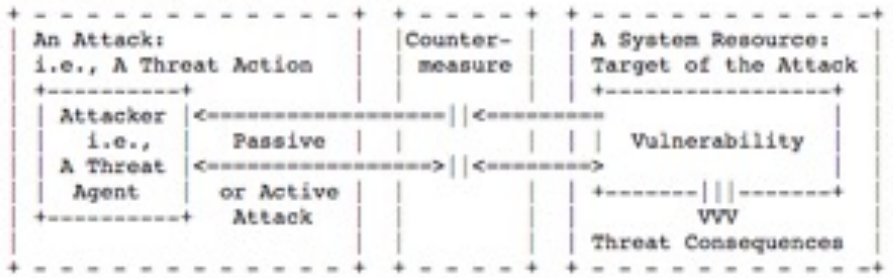
- $ vulnerability
  - (I) A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.
  - (C) Most systems have vulnerabilities of some sort, but this does not mean that the systems are too flawed to use. Not every threat results in an attack, and not every attack succeeds. Success depends on the degree of vulnerability, the strength of attacks, and the effectiveness of any countermeasures in use. If the attacks needed to exploit a vulnerability are very difficult to carry out, then the vulnerability may be tolerable. If the perceived benefit to an attacker is small, then even an easily exploited vulnerability may be tolerable. However, if the attacks are well understood and easily made, and if the vulnerable system is employed by a wide range of users, then it is likely that there will be enough benefit for someone to make an attack.

Originais da RFC 2828

- $ adversary
  - (I) An entity that attacks, or is a threat to, a system.
- $ threat
  - (I) A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. (See: attack, threat action, threat consequence.)
  - (C) That is, a threat is a possible danger that might exploit a vulnerability. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminalorganization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of an "act of God" such as an earthquake, a fire, or a tornado).
  - (C) In some contexts, such as the following, the term is used narrowly to refer only to intelligent threats:
  - (N) U. S. Government usage: The technical and operational capability of a hostile entity to detect, exploit, or subvert friendly information systems and the demonstrated, presumed, or inferred intent of that entity to conduct such activity.

Originais da RFC 2828

- $ attack
  - (I) An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. (See: penetration, violation, vulnerability.)
    - - Active vs. passive: An "active attack" attempts to alter system resources or affect their operation. A "passive attack" attempts to learn or make use of information from the system but does not affect system resources. (E.g., see: wiretapping.)
    - - Insider vs. outsider: An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization. An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.
  - (C) The term "attack" relates to some other basic security terms as shown in the following diagram:



Originais da RFC 2828

- $ countermeasure
  - (I) An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by **eliminating or preventing** it, by **minimizing the harm** it can cause, or by **discovering and reporting** it so that corrective action can be taken.
  - (C) In an Internet protocol, a countermeasure may take the form of a protocol feature, an element function, or a usage constraint.

Ataque ativo vs passivo

- Passivo: não há interação, interferência ou efeito no sistema atacado
  - Exemplo: Leitura de mensagem em um canal de comunicação
- Ativo: baseia-se na interação, interferência ou efeito no sistema atacado
  - Exemplo: Modificação de uma mensagem em um canal de comunicação
  - Exemplo: Exploração de uma vulnerabilidade (exemplo, injeção de SQL) em uma aplicação web

Ataque interno vs externo

- Externo: realizado por indivíduo desprovido de credenciais ou informações privilegiadas em relação aos sistemas atacados; realizado a partir de redes públicas
  - Exemplo: invasão de uma rede corporativa a partir da Internet.
- Interno: realizado a partir de redes restritas ou beneficiado por credenciais e informações privilegiadas
  - Exemplo: invasão de um sistema corporativo por empregado a partir de uma Intranet
  - Exemplo (interno-equivalente): ataque realizado por visitante com acesso físico a um ponto de rede de uma empresa
  - Exemplo (interno-equivalente): acesso a uma VPN usando credenciais obtidas por meio de engenharia social

Contramedidas (abordagens)

- Prevenção
  - Ataque não é bem-sucedido
  - Exemplo: cifrar dados em trânsito
- Redução de Impacto
  - Ataque gera impacto reduzido
  - Exemplo: destruição automática de dados críticos
- Detecção
  - Ataque é detectado
  - Exemplo: detecção de presença de usuário não-autorizado
- Resposta
  - Sistema reage contra ataque
  - Exemplo: shutdown de sistema violado
- Recuperação
  - Sistema se recupera após ataque
  - Exemplo: sistema de backup

Arquiteturas de Segurança

O Padrão 7498

INTERNATIONAL STANDARD

ISO/IEC 7498-1

Second edition
1994-11-15

Corrected and reprinted
1996-06-15

Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model

Technologies de l'information — Modèle de référence de base pour l'interconnexion de systèmes ouverts (OSI): Le modèle de base

Contents

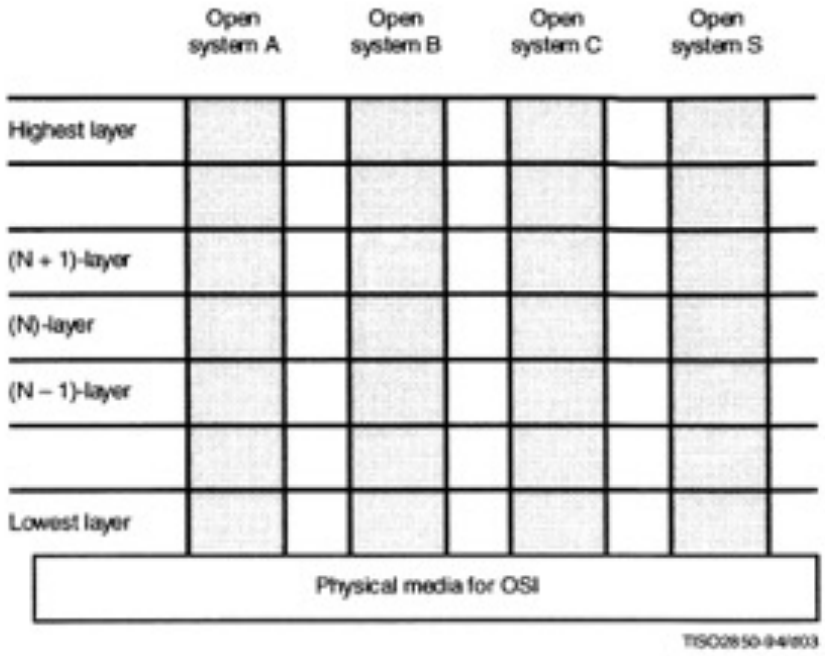


Figure 3 – Layering in cooperating open systems

INTERNATIONAL STANDARD

ISO 7498-2

First edition
1989-02-15

Information processing systems — Open Systems Interconnection — Basic Reference Model —

Part 2 : Security Architecture

Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Modèle de référence de base —

Partie 2 : Architecture de sécurité

Information processing systems — Open Systems Interconnection — Basic Reference Model —

Part 2 :
Security Architecture

0 Introduction

ISO 7498 describes the Basic Reference Model for Open Systems Interconnection (OSI). That part of ISO 7498 establishes a framework for coordinating the development of existing and future standards for the interconnection of systems.

The objective of OSI is to permit the interconnection of heterogeneous computer systems so that useful communication between application processes may be achieved. At various times, security controls must be established in order to protect the information exchanged between the application processes. Such controls should make the cost of obtaining or modifying data greater than the potential value of so doing, or make the time required to obtain the data so great that the value of the data is lost.

This part of ISO 7498 defines the general security-related architectural elements which can be applied appropriately in the circumstances for which protection of communication between open systems is required. It establishes, within the framework of the Reference Model, guidelines and constraints to improve existing standards or to develop new standards in the context of OSI in order to allow secure communications and thus provide a consistent approach to security in OSI.

A background in security will be helpful in understanding this document. The reader who is not well versed in security is advised to read annex A first.

This part of ISO 7498 extends the Basic Reference Model to cover security aspects which are general architectural elements of communications protocols, but which are not discussed in the Basic Reference Model.

1 Scope and field of application

This part of ISO 7498:

a) provides a general description of security services and related mechanisms, which may be provided by the Reference Model; and

b) defines the positions within the Reference Model where the services and mechanisms may be provided.

This part of ISO 7498 extends the field of application of ISO 7498, to cover secure communications between open systems.

Basic security services and mechanisms and their appropriate placement have been identified for all layers of the Basic Reference Model. In addition, the architectural relationships of the security services and mechanisms to the Basic Reference Model have been identified. Additional security measures may be needed in end-systems, installations and organizations. These measures apply in various application contexts. The definition of security services needed to support such additional security measures is outside the scope of this standard.

OSI security functions are concerned only with those visible aspects of a communications path which permit end systems to achieve the secure transfer of information between them. OSI Security is not concerned with security measures needed in end systems, installations, and organizations, except where these have implications on the choice and position of security services visible in OSI. These latter aspects of security may be standardized but not within the scope of OSI standards.

This part of ISO 7498 adds to the concepts and principles defined in ISO 7498; it does not modify them. It is not an implementation specification, nor is it a basis for appraising the conformance of actual implementations.

Conteúdo da 7498-2

DATA COMMUNICATION NETWORKS: OPEN SYSTEMS INTERCONNECTION (OSI); SECURITY, STRUCTURE AND APPLICATIONS

INTERNATIONAL TELECOMMUNICATION UNION

SECURITY ARCHITECTURE FOR OPEN SYSTEMS INTERCONNECTION FOR CCITT APPLICATIONS

CCITT

THE INTERNATIONAL TELEGRAPH AND TELEPHONE CONSULTATIVE COMMITTEE

X.800

3.3.51 **security service**

A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

5 General description of security services and mechanisms

5.1 *Overview*

Security services that are included in the OSI security architecture and mechanisms which implement those services are discussed in this section. The security services described below are basic security services. In practice they will be invoked at appropriate layers and in appropriate combinations, usually with non-OSI services and mechanisms, to satisfy security policy and/or user requirements. Particular security mechanisms can be used to implement combinations of the basic security services. Practical realizations of systems may implement particular combinations of the basic security services for direct invocation.

Serviços de Segurança

- Autenticação
  - Autenticação de Entidade e Autent. de Origem de Dados
- Controle de acesso
- Confidencialidade de dados
  - Confidencialidade com conexão, sem conexão, seletiva por campos e de fluxo de tráfego
- Integridade de dados
  - Integridade com conexão com recuperação, sem recuperação e seletiva por campos; sem conexão e sem conexão seletiva por campos
- Irretratabilidade
  - Com prova de origem e com prova de entrega
- Disponibilidade

Mecanismos de Segurança Específicos

- Criptografia
- Assinatura Digital
- Controle de acesso
- Integridade de dados
- Troca de autenticações
- Preenchimento de tráfego
- Controle de roteamento
- Notarização

Mecanismos de Segurança Pervasivos

- Funcionalidade confiável
- Rótulo de segurança
- Detecção de evento
- Trilha de auditoria de segurança
- Recuperação de segurança

Relação entre serviços e mecanismos

Mechanism / Service	Encipherment	Digital signature	Acces control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y	·	·	Y	·	·	·
Data origin authentication	Y	Y	·	·	·	·	·	·
Access control service	·	·	Y	·	·	·	·	·
Connection confidentiality	Y	·	·	·	·	·	Y	·
Connectionless confidentiality	Y	·	·	·	·	·	Y	·
Selective field confidentiality	Y	·	·	·	·	·	·	·
Traffic flow confidentiality	Y	·	·	·	·	Y	Y	·
Connection Integrity with recovery	Y	·	·	Y	·	·	·	·
Connection integrity without recovery	Y	·	·	Y	·	·	·	·
Selective field connection integrity	Y	·	·	Y	·	·	·	·
Connectionless integrity	Y	Y	·	Y	·	·	·	·
Selective field connectionless integrity	Y	Y	·	Y	·	·	·	·
Non-repudiation. Origin	·	Y	·	Y	·	·	·	Y
Non-repudiation. Delivery	·	Y	·	Y	·	·	·	Y

Posicionamento dos serviços

Service	Layer						
	1	2	3	4	5	6	7*
Peer entity authentication	·	·	Y	Y	·	·	Y
Data origen authentication	·	·	Y	Y	·	·	Y
Access control service	·	·	Y	Y	·	·	Y
Connection confidentiality	Y	Y	Y	Y	·	Y	Y
Connectionless confidentiality	·	Y	Y	Y	·	Y	Y
Selective field confidentiality	·	·	·	·	·	Y	Y
Traffic flow confidentiality	Y	·	Y	·	·	·	Y
Connection Integrity with recovery	·	·	·	Y	·	·	Y
Connection integrity without recovery	·	·	Y	Y	·	·	Y
Selective field connection integrity	·	·	·	·	·	·	Y
Connectionless integrity	·	·	Y	Y	·	·	Y
Selective field connectionless integrity	·	·	·	·	·	·	Y
Non-repudiation Origin	·	·	·	·	·	·	Y
Non-repudiation. Delivery	·	·	·	·	·	·	Y