Segurança da Informação, Parte 2: Conceitos Básicos

2.1: Visão Geral de Segurança da Informação baseada no Stallings Cap.1

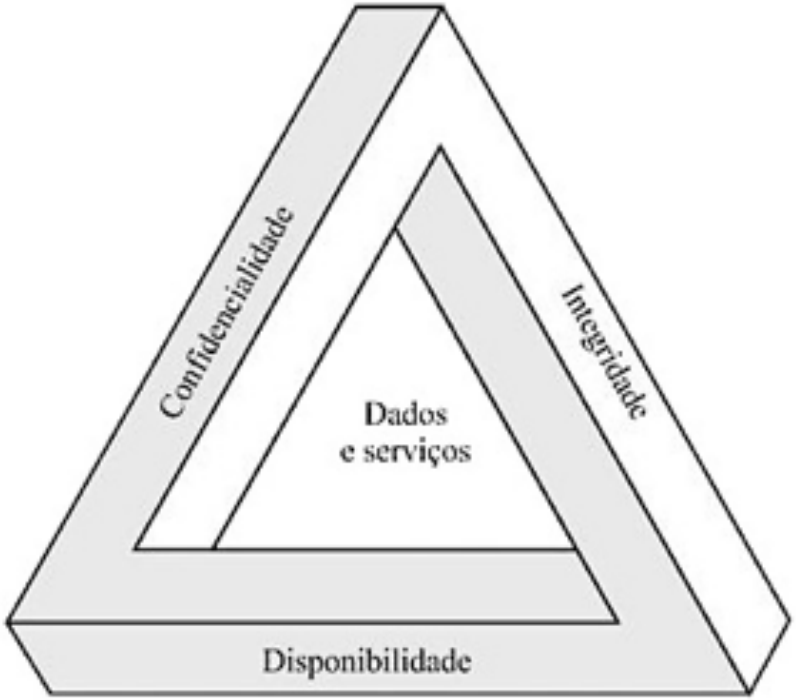
Definição de segurança de computadores

- 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).
- É apenas uma das definições possíveis...

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 funcionem prontamente e que não haja negação de serviço a usuários autorizados.

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.

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.

Terminologia RFC 2828

- **Adversário (agente fonte de ameaça).** Entidade que ataca um sistema ou é uma ameaça para ele.
- **Ameaça.** Um potencial para violação de segurança, que existe quando há circunstância, capacidade, ação ou evento que poderia infringir a segurança e causar dano.
- **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.

Terminologia 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.
- **Recurso de sistema (ativo).** Dados contidos em um sistema de informação; serviço provido por um sistema; capacidade do sistema, como poder de processamento ou largura de banda de comunicação; item de equipamento do sistema; instalação que abrigue operações e equipamentos de sistema.
- **Risco.** Expectativa de perda de segurança expressa como a probabilidade de que uma ameaça particular explorará uma vulnerabilidade particular com resultado danoso particular.
- **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.

Ataques e contramedidas

- Ataque ativo vs passivo
- Ataque interno vs externo
- Contramedidas
  - impedir (isolamento físico, firewall, zeroization)
  - detectar (lacre, IDS)
  - recuperar (seguro, backup)

Ações e consequências de ameaças

- Revelação não-autorizada
  - Exposição
  - Interceptação
  - Inferência
  - Intrusão
- Fraude
  - Personificação
  - Falsificação
  - Retratação/Repúdio
- Disrupção
  - Incapacitação
  - Corrupção
  - Obstrução
- Usurpação
  - Apropriação indevida
  - Utilização indevida

Ameaças a ativos

	Disponibilidade	Confidencialidade	Integridade
Hardware	O equipamento é roubado ou desabilitado e, por consequência, há negação de serviço.		
Software	Programas são removidos, negando acesso a usuários.	Uma cópia não autorizada do software é feita.	Um programa instalado é modificado, seja para fazê-lo falhar durante a execução, seja para obrigá-lo a executar alguma tarefa não pretentida.
Dados	Arquivos são removidos, prevenindo seu acesso por usuários.	É realizada leitura não autorizada de dados. Uma análise estatística de dados revela dados subjacentes.	Arquivos existentes são modificados ou novos arquivos são fabricados.
Enlaces de comunicação	Mensagens são destruídas ou eliminadas. Enlaces ou redes de comunicação tornam-se indisponíveis.	Mensagens são lidas. O padrão de tráfego de mensagens é observado.	Mensagens são modificadas, atrasadas, reordenadas ou duplicadas. Mensagens falsas são fabricadas.

Requisitos Funcionais de Segurança

- Controle de acesso
- Conscientização e treinamento
- Auditoria e responsabilidade
- Avaliações de certificação, credenciamento e segurança
- Gerenciamento de configuração
- Planejamento de contingência
- Resposta a incidentes
- Manutenção
- Proteção da mídia
- Proteção física e ambiental
- Planejamento
- Segurança de pessoal
- Avaliação de risco
- Aquisição de sistemas e serviços
- Proteção de sistemas e comunicações
- Integridade de sistemas e informações

Arquitetura de Segurança (X.800)

- **Ataque à segurança**: Qualquer ação que comprometa a segurança de informações que uma organização possui.
- **Mecanismo de segurança**: Um mecanismo projetado para detectar, impedir ou recuperar-se de um ataque à segurança.
- **Serviço de segurança**: Um serviço que aprimora a segurança dos sistemas de processamento de dados e das transferências de informações de uma organização. (?!=)

Serviços de Segurança

- Autenticação
- Controle de acesso
- Confidencialidade de dados
- Integridade de dados
- Irretratabilidade
- 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 Disseminados (?!=)

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

Estratégias para a Segurança: Política de Segurança

- Fatores
  - O valor dos ativos que estão sendo protegidos
  - As vulnerabilidades do sistema.
  - Ameaças potenciais e probabilidade de ataques
- Compromissos (tradeoffs)
  - Facilidade de uso versus segurança
  - Custo de segurança versus custo de falha e recuperação

Estratégias para a Segurança: Implementação de Segurança (abordagens)

- Prevenção
  - Ataque não é bem-sucedido
  - Exemplo: cifrar dados em trânsito
- Detecção
  - Ataque é detectado
  - Exemplo: 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

Garantia e Avaliação

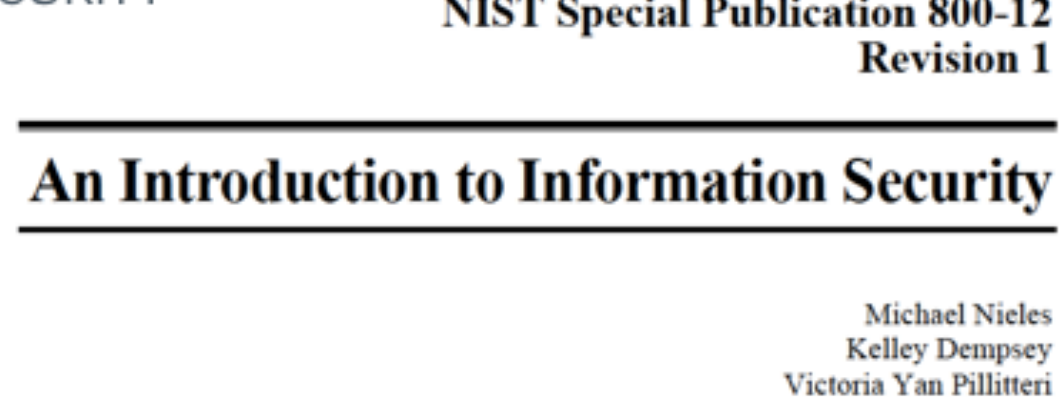
- Garantia: "grau de confiança que o consumidor tem de que as medidas de segurança técnicas, bem como operacionais, funcionam como pretendido para proteger o sistema e as informações que ele processa"
- Exemplos de questões:
  - O projeto do sistema de segurança cumpre seus requisitos?
  - A implementação do sistema de segurança está de acordo com suas especificações?
- Avaliação é o processo de examinar um produto ou sistema de computador em relação a certos critérios.

Segurança da Informação, Parte 2: Conceitos Básicos

2.2: Introdução à Segurança da Informação baseada no NIST SP 800-12 Rev. 1

Objetivo

- Apresentar de maneira formal e estruturada conceitos de segurança da informação
- Ter contato comum exemplo de ”padrão”
  - Basearemo-nos em um ”padrão nacional” que possui reconhecimento internacional
  - NIST SP 800-112 Rev. 1: AN INTRODUCTION TO INFORMATION SECURITY


NIST Special Publication 800-12
Revision 1

An Introduction to Information Security

Michael Nieles
Kelley Dempsey
Victoria Yan Pillitteri

Terminologia Básica

- *The term Information System is defined by 44 U.S.C., Sec. 3502 as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."*
- *For this publication, the term system is used in lieu of the term information system to reflect the broader applicability of information resources of any size or complexity, organized expressly for the collection, processing, use, sharing, dissemination, maintenance, or disposition of data or information.*

Terminologia Básica – outros termos

- *Information – (1) Facts or ideas, which can be represented (encoded) as various forms of data; (2) Knowledge (e.g., data, instructions) in any medium or form that can be communicated between system entities.*
- *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.*

Terminologia Básica – outros termos

- *Confidentiality – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*
- *Integrity – Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.*
  - *Data Integrity – The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.*
  - *System Integrity – The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.*

Terminologia Básica – outros termos

- *Availability – Ensuring timely and reliable access to and use of information.*
- *Security Controls – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, availability, and integrity of the system and its information.*
  - *In this document, the terms security controls, safeguards, security protections, and security measures have been used interchangeably.*

Oito conceitos de segurança da informação

1. Information security supports the mission of the organization.

2. Information security is an integral element of sound management.

3. Information security protections are implemented so as to be commensurate with risk.

4. Information security roles and responsibilities are made explicit.

5. Information security responsibilities for system owners go beyond their own organization.

6. Information security requires a comprehensive and integrated approach.

7. Information security is assessed and monitored regularly.

8. Information security is constrained by societal and cultural factors.

Papéis e Responsabilidades (cap.3)

- Risk Executive Function (Senior Management)
- Chief Executive Officer (CEO)
- Chief Information Officer (CIO)
- Information Owner/Steward
- Chief Information Security Officer (CISO)
- System Owner
- System Security Officer
- Information Security Architect
- System Security Engineer (SSE)
- Security Control Assessor
- System Administrator
- User
- Supporting Roles
  - Auditor, Physical Security Staff, Disaster Recovery/Contingency Planning Staff, Quality Assurance Staff, Procurement Office Staff, Training Office Staff, Human Resources, Risk Management/ Physical Plant Staff, Planning Staff, Privacy Office Staf

Ameaças e Vulnerabilidades (cap.4)

- Vulnerabilidades
  - *A vulnerability is a weakness in a system, system security procedure, internal controls, or implementation that could be exploited by a threat source*
- Fontes de Ameaça
  - *Threat Source – The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.*

Fontes de ameaças

- Adversárias e não-adversárias
  - *A threat source can be adversarial or non-adversarial. Adversarial threat sources are individuals, groups, organizations, or entities that seek to exploit an organization's dependence on cyber resources. Even employees, privileged users, and trusted users have been known to defraud organizational systems. Non-adversarial threat sources refer to natural disasters or erroneous actions taken by individuals in the course of executing their everyday responsibilities.*

Eventos de Ameaça

- Fontes de ameaça levam a eventos de ameaça
  - *If the system is vulnerable, threat sources can lead to threat events. A threat event is an incident or situation that could potentially cause undesirable consequences or impacts. An example of a threat source leading to a threat event is a hacker installing a keystroke monitor on an organizational system.*

Medidas de segurança "custo-efetivas"

- Compreender ameaças e vulnerabilidades ajuda a implementar medidas de segurança custo-efetivas
  - *In order to protect a system from risk and to implement the most cost-effective security measures, system owners, managers, and users need to know and understand the vulnerabilities of the system as well as the threat sources and events that may exploit the vulnerabilities. When determining the appropriate response to a discovered vulnerability, care should be taken to minimize the expenditure of resources on vulnerabilities where little or no threat is present.*

Exemplos de fontes e eventos de ameaça

- Adversariais
  - *Fraud and Theft*
  - *Insider Threat*
  - *Malicious Hacker*
  - *Malicious Code*
- Não-adversariais
  - *Errors and Omissions*
  - *Loss of Physical and Infrastructure Support*
  - *Impacts to Personal Privacy of Information Sharing*

Política de Segurança da Informação (cap.5)

- Política: regras que especificam o comportamento "correto" ou "esperado"
- São as regras e diretrizes para manter a segurança da informação
  - *Information security policy is defined as an aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information*

Padrões, guias e procedimentos

- Padrões organizacionais
  - *Organizational standards (not to be confused with American National Standards, FIPS, Federal Standards, or other national or international standards) specify uniform use of specific technologies, parameters, or procedures when such uniform use will benefit an organization.*
  - Exemplo: crachás de identificação
- Guias
  - *Guidelines assist users, systems personnel, and others in effectively securing their systems. The nature of guidelines, however, immediately recognizes that systems vary considerably, and imposition of standards is not always achievable, appropriate, or cost-effective.*
  - Exemplo: guia para criação de procedimentos de sistema
- Procedimentos
  - *Procedures describe how to implement applicable security policies, standards, and guidelines. They are detailed steps to be followed by users, system operations personnel, or others to accomplish a particular task*
  - Exemplo: guia para criação de contas de usuário

Três ”níveis” de política de segurança

- Vários níveis de decisão gerencial
  - *Managers at all levels make choices that can affect policy, with the scope of the policy's applicability varying according to the scope of the manager's authority.... To differentiate various kinds of policy, this chapter categorizes them into three basic types...*
- Políticas de Programa organizacional
  - Cria um programa de segurança na organização
- Política de Tema Específico
  - Abordam áreas específicas de relevância para a organização
- Política de Sistema Específico
  - Aplicam-se a conjuntos particulares de sistemas

Seg.Info. e Gerenciamento de Riscos (cap.6)

- Risco é uma medida da ameaça a que uma entidade está sujeita por ocasião de um evento potencial
- Tipicamente, função do impacto do evento (caso ocorra) e da probabilidade de que o evento ocorra

* Muitas outras definições podem ser encontradas na literatura

Gerenciamento de Riscos no Cotidiano

- Usar cinto de segurança
- Carregar guarda-chuva
- Anotar os itens de uma lista de compras
- Escolher o caminho mais longo, porém sem trânsito
- Fazer um plano de previdência

... no limite, tudo o que fazemos pode se enquadrar no arcabouço do gerenciamento de riscos...

Riscos em Segurança da Informação

- Minimizar riscos relacionados à operação de sistemas
  - *With respect to information security, risk management is the process of minimizing risks to organizational operations (e.g., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation of a system.*
- Quatro etapas
  - Enquadramento
  - Avaliação
  - Resposta
  - Monitoração

Framework de riscos de sistemas

- Gerenciamento de sistemas no nível de sistemas de informação
- Etapas
  - Categorização de Sistemas
  - Seleção de Controles de Segurança
  - Implementação de Controles de Segurança
  - Avaliação de Controles de Segurança
  - Autorização de Sistemas
  - Monitoramento de Controles de Segurança

The RMF promotes the concepts of near real-time risk management and ongoing system authorization through the implementation of robust continuous monitoring processes. The RMF also provides senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational systems supporting their core missions and business functions, and integrates information security into the enterprise architecture and system development life cycle (SDLC).


FIPS 199 / SP 800-60
FIPS 200 / SP 800-53
Multiple NIST Publications*
*e.g., SP 800-34, SP 800-61, SP 800-128
SP 800-53A
SP 800-37
SP 800-137 / SP 800-37 / SP 800-53 A
Starting Point
Categorize System
Select Controls
Implement Controls
Assess Controls
Authorize System
Monitor Controls
Organization-wide Risk Management SP 800-39

Garantias (cap.7)

- Garantia da informação: grau de confiança na segurança da informação
  - *Information assurance is the degree of confidence one has that security measures protect and defend information and systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of systems by incorporating protection, detection, and reaction capabilities.*
- Categorias dos métodos e ferramentas de garantia
  - Projeto (e Implementação)
  - Operacional (subdividido em auditoria e monitoramento)

Suporte e operações de sistemas

- Refere-se a todos os aspectos envolvidos na execução de um sistema.
  - Inclui administração do sistema e tarefas externas (ex. ”manutenção da documentação”)
  - Não inclui ”projeto” ou ”planejamento”
- Exemplos de atividades/categorias
  - *User support;*
  - *Software support;*
  - *Configuration management;*
  - *Backups;*
  - *Media controls;*
  - *Documentation; and*
  - *Maintenance*

Segurança em suporte e operações

- Segurança deve ser considerada em todas as atividades de suporte e operações de sistemas
- Exemplos de problemas
  - Documentação imprecisa ou incompleta
  - Contas antigas de usuários
  - Conflitos de configuração de software
- Segurança está intimamente relacionada a S&O
- Pessoal de S&O deve ter conhecimento de Segurança
  - Exemplo: problemas no log in de um usuário podem indicar conta desabilitada após tentativa de ataque

Criptografia (cap.9)

- Área da Matemática dedicada à transformação de dados para segurança da informação
- Criptografia é uma ferramenta central em Segurança – mas pode (deve) ser combinada com outras
- Usos da criptografia
  - Proteção de dados armazenados
  - Proteção de dados em trânsito ”interno”
  - Proteção de dados em trânsito ”externo”
    - Possivelmente, a criptografia será a única ferramenta de proteção, neste caso

Aplicações da criptografia

- Cifração – proteção da confidencialidade
- Autenticação de Mensagem – proteção da integridade
- Assinatura Digital – autenticidade e irrefutabilidade
- Autenticação de usuário – identificação

Controles de segurança (cap. 10)

Controles de segurança são ferramentas que organizações podem implementar para aumentar a segurança de informações e sistemas

- *Access Control (AC)*
- *Awareness and Training (AT)*
- *Audit and Accountability (AU)*
- *Assessment, Authorization, and Monitoring (CA)*
- *Configuration Management (CM)*
- *Contingency Planning (CP)*
- *Identification and Authentication (IA)*
- *Individual Participation (IP)*
- *Incident Response (IR)*
- *Maintenance (MA)*
- *Media Protection (MP)*
- *Privacy Authorization (PA)*
- *Physical and Environmental Protection (PE)*
- *Planning (PL)*
- *Program Management (PM)*
- *Personnel Security (PS)*
- *Risk Assessment (RA)*
- *System and Services Acquisition (SA)*
- *System and Communications Protection (SC)*
- *System and Information Integrity (SI)*

Segurança da Informação, Parte 2: Conceitos Básicos

2.3: Arquiteturas de Redes e Segurança: os padrões ISO/IEC 7498 partes 1 e 2

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

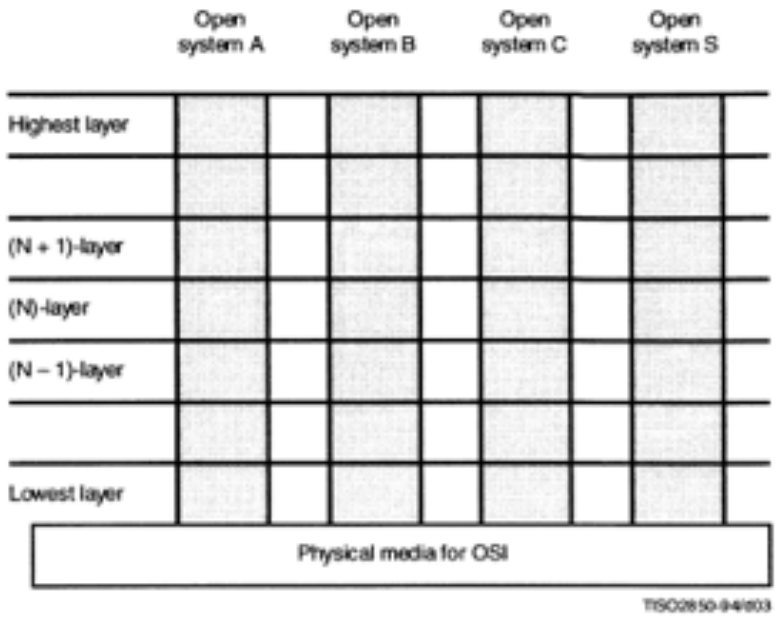


Figure 3 – Layering in cooperating open systems

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.

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

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