Network Security

Network Security Hierarchy

Material elaborat dupa:

CISCO Security Curriculum

Kenny Paterson’s Lectures for:
M.Sc. in Information Security, Royal Holloway, University of London

Objectives of Lecture

- Understand why security should be a fundamental consideration when designing and operating networks.
- Examine the *primary enabling* threats and *fundamental* threats to security for networks.
- Introduce security *services* and *mechanisms*, and show how they can be used to counter threats.
- Study the provision of security services at different network layers in standard ISO7498-2.

Why Network Security?

- Organisations and individuals are increasingly reliant on networks of all kinds for day-to-day operations:
  - e-mail used in preference to letter, fax, telephone for many routine communications.
  - B2B and C2B e-commerce still growing rapidly.
  - the Internet is a vast repository of information of all kinds: competitors and their prices, stock markets, cheap flights,….
  - increased reliance on networks for supply chains of all kinds: from supermarkets to aircraft components.
  - utility companies control plant, banks move money, governments talk to citizens over networks.
  - growth of mobile telephony for voice and data.

Why Network Security?

- Networks are becoming increasingly inter-connected and their security consequently more complex:
  - if I send sensitive data over my internal network, then who else can see it or even alter it? My employees? My competitors?
  - can a hacker who gets into my internal network then get access to other resources (computer accounts, stored data)? Can he use my network as a stepping-off point for further attacks? I am then liable?
  - a compelling Internet presence is essential for my company, but if someone can see my website, can they alter it too?
  - how can consumers trust that a given website is that of a reputable company and not one who will miss-use their credit card details?

Why Network Security?

- Safeguarding the confidentiality, integrity and availability of data carried on these various networks is therefore essential.
- Authenticity and accountability are often also important: who did what and when?
- It’s not *only* about security of Internet-connected systems.
  - Insider threats are often more potent than threats originating on the Internet.
- It’s not *only* about TCP/IP networks
  - Many networks use special-purpose protocols and architectures
  - However TCP/IP dominates in LANs and the Internet.

Non secure wireless access, need for speed versus secure connections (secure software operates at moderate speed), IT staff shortage (more outsourcing solutions for security management) **are challenges for security**

Accessing a corporate network

Open Access: permit everything that is not explicitly denied
-Easy to implement, only basic security capabilities (passwords, server security)
- protected assets are minimal, user are trusted, threats are minimal
- isolated LANs are possible examples

Restrictive Access - Combination of restrictions and specific permissions
- configuration of specific hardware and software for security: firewalls, VPNs, IDS (Intrusion Detection System), identity servers
-LANs connected to Internet and public WANs are examples

Closed Access - that which is not explicitly permitted is denied
-All available security measures, plus extra effort for more costly H+S solutions
-Network administrators are accountable for problems

Security Policies for Networks

Standards for security

1. ISO/IEC 17799, *Information technology – Code of practice for information security management*

- common basis and practical guideline for developing organizational security standards and effective security management practices

ISO/IEC 17799 is made up of the following eleven sections:
Security policy
Organization of information security
Asset management
Human resources security
Physical and environmental security
Communications and operations management
Access control
Information systems acquisition, development and maintenance
Information security incident management
Business continuity management
Compliance

Security Policies for Networks

2. ISO7498-2

- a companion document to ISO7498-1 (the seven layer model),
- provides a useful overview of the security issues pertinent to networks
- equips us with a handy set of definitions to fix our terminology

Organizations for the Internet and IT security

CERT – Computer Emergency Readiness Team – reporting center for Internet security

SANS Institute – SysAdmin, Audit, Network, Security – documents with aspects of information security

(ISC)² – International Information System Security Certification Consortium – collection of best practices for information security and certification of conformance (System Security Certified Practitioner, Certified Information Systems Security Professional)

Common Criteria – IT security evaluation, based on security levels (Evaluation Assurance Level 4 – highest)

Security Policies for Networks

- In a secure system, the rules governing security behavior should be made explicit in the form of an *Information Security Policy*.
- Security *policy*: ‘the set of criteria for the provision of security services’
  - essentially, a set of rules
  - may be very high level or quite detailed
- Security *domain*: the scope of application of a security policy
  - where, to what information and to whom the policy applies.

Security Policies for Networks

- A *network* security policy should interpret the overall Information Security Policy in the context of the networked environment:
  - Defines what is the responsibility of the network and what is not.
  - Describes what security is to be available from the network.
  - Describes rules for using the network.
  - Describes who is responsible for the management and security of the network.

Generic Security Policy

- A generic authorization policy (from ISO 7498-2):

  ‘Information may not be given to, accessed by, nor permitted to be inferred by, nor may any resource be used by, those not appropriately authorized.’

- Possible basis for more detailed policy: needs lots of refinement to produce final document:
  - What information?
  - What resources?
  - Who is authorized and for what?
  - What about availability?

The Security Life-Cycle

- A generic model for the security life-cycle, including network security issues, is as follows:
  - define security policy,
  - analyze security threats (according to policy) and associated risks, given existing safeguards,
  - define security services to meet/reduce threats, in order to bring risks down to acceptable levels,
  - define security mechanisms to provide services,
  - provide on-going management of security.

Security Threats for Networks

- A *threat* is:
  - a person, thing, event or idea which poses some danger to an asset (in terms of confidentiality, integrity, availability or legitimate use).
  - a possible means by which a security policy may be breached.
- An *attack* is a realization of a threat.
- *Safeguards* are measures (e.g. controls, procedures) to protect against threats.
- *Vulnerabilities* are weaknesses in safeguards.

Risk

- Risk is a measure of the cost of a vulnerability (taking into account probability of a successful attack).
- Risk analysis determines whether expenditure on new or better safeguards is warranted.
- Risk analysis can be quantitative or qualitative.

Threats

Threats can be classified as:

- *deliberate* (e.g. hacker penetration);
- *accidental* (e.g. a sensitive file being sent to the wrong address).

Deliberate threats can be further sub-divided:

- *passive* (e.g. monitoring, wire-tapping);
- *active* (e.g. changing the value of a financial transaction).

In general passive threats are easier to realize than active ones.

Fundamental Threats

- Four fundamental threats (matching four ‘standard’ security goals: confidentiality, integrity, availability, legitimate use):
  - Information leakage,
  - Integrity violation,
  - Denial of service,
  - Illegitimate use.

(There are other ways to classify threats)

Primary Enabling Threats

Realization of any of these *primary enabling* threats can lead directly to a realization of a fundamental threat:

- *Masquerade*, where an entity pretends to be a different entity,
- *Bypassing controls*, where an attacker exploits system flaws or security weaknesses, in order to acquire unauthorized rights
- *Authorized violation*, where an entity authorized to use a system for one purpose uses it for another, unauthorized purpose.
- *Trojan horse*, where software contains an invisible part which, when executed, compromises the security of the system,
- *Trapdoor*, which is a feature built into a system such that the provision of specific input data allows the security policy to be violated.

First three are *penetration* threats, last two are *planting* threats.

Network Security Requirements & Problems

Network Security – ***protect data during transmissions & guarantee that data transmissions are authentic***

Security Requirements

Confidentiality – data accessed & read only by authorized parties

Integrity – data modification by authorized parties

Availability – data available to authorized parties

Network Security Problems (what to allow for):

Secrecy

Keeping information private (out of unauthorized parties)

Authentication

Proving one’s identity, before revealing info

Non-repudiation

Showing (proving) that a message was sent; use of signatures

Integrity

Showing that a message wasn't modified

Attacks on Network Security

Passive Attacks (Reconnaissance attacks)

Nature of: eavesdropping (monitoring) on transmissions

Goal: to obtain information that is being transmitted:

-information gathering: identify usernames, passwords, or … credit card numbers /sensitive personal information

-information theft (steal credit card numbers /sensitive personal information, crack a password file)

Tools Used to Perform Eavesdropping

- Network or protocol analyzers

-Packet capturing utilities on networked computers

- use of *nslookup and whois utilities* , ping command

Two **types** of passive attacks:

- Release of message contents

Outsider learns content of transmission

- Traffic analysis

By monitoring frequency and length of messages, even encrypted, nature of communication may be guessed

Passive attacks: Difficult to detect, because attacks don’t alter data; can be prevented, rather than detected; use of *encryption, switched networks, no use of protocols susceptible to eavesdropping*

Example of action: A malicious intruder typically ping sweeps the target network to determine which IP addresses are alive . After this, the intruder uses a port scanner to determine what network services or ports are active on the live IP addresses . From this information, the intruder queries the ports to determine the application type and version, as well as the type and version of operating system running on the target host. Based on this information, the intruder can determine if a possible vulnerability exists that can be exploited.

Active Attacks

Involve some data stream modification, or creation of a false stream

Masquerade

Pretending to be a different entity (manipulate TCP/IP packets by IP spoofing, falsifying the source IP address)

Replay

Capture of data unit and retransmission for an unauthorized effect

Modification of messages

Some portion of a legitimate message is altered

Denial of service

Prevents or inhibits normal use of communications facilities

Easy to detect: detection may lead to a deterrent effect (helps prevention)

Hard to prevent (requires all time physical protection)

Use of *authentication*

Security Services and Mechanisms

- A security threat is a possible means by which a security policy may be breached (e.g. loss of integrity or confidentiality).
- A security *service* is a measure which can be put in place to address a threat (e.g. provision of confidentiality).
- A security *mechanism* is a means to provide a service (e.g. encryption, digital signature).

Security Service Classification

- Security services in ISO 7498-2 are a special class of safeguard applying to a communications environment.
- Five main categories of security service:
  - Authentication (including entity authentication and origin authentication),
  - Access control,
  - Data confidentiality,
  - Data integrity,
  - Non-repudiation.
- Sixth category: “other” – includes physical security, personnel security, computer security, life-cycle controls,…

Authentication

- *Entity* authentication provides checking of a claimed identity at a point in time.
- Typically used at start of a connection.
- Addresses masquerade and replay threats.
- *Origin* authentication provides verification of source of data.
- Does not protect against replay or delay

Access Control

- Provides protection against unauthorized use of resource, including:
  - use of a communications resource,
  - reading, writing or deletion of an information resource,
  - execution of a processing resource.
- *Example: file permissions in Unix/NT file systems.*

Data Confidentiality

- Protection against unauthorised disclosure of information.
- Four types:
  - Connection confidentiality,
  - Connectionless confidentiality,
  - Selective field confidentiality,
  - Traffic flow confidentiality.
- *Example: encrypting routers as part of Swift funds transfer network.*

Data Integrity

- Provides protection against active threats to the validity of data.
- Five types:
  - Connection integrity with recovery,
  - Connection integrity without recovery,
  - Selective field connection integrity,
  - Connectionless integrity,
  - Selective field connectionless integrity.
- *Example: MD5 hashes on software*
- *Example: AH protocol in IPSec*

Non-repudiation

- Protects against a sender of data denying that data was sent (non-repudiation of origin).
- Protects against a receiver of data denying that data was received (non-repudiation of delivery).
- *Example: analagous to signing a letter and sending via recorded delivery.*
- *Example: signatures in S/MIME secure e-mail system*

Security Mechanisms

- Exist to provide and support security services.
- Can be divided into two classes:
  - Specific security mechanisms, used to provide specific security services, and
  - Pervasive security mechanisms, not specific to particular services.

Specific Security Mechanisms

- Eight types:
  - encipherment,
  - digital signature,
  - access control mechanisms,
  - data integrity mechanisms,
  - authentication exchanges,
  - traffic padding,
  - routing control,
  - notarization.

Specific Mechanisms 1

- Encipherment mechanisms = encryption algorithms.
  - Can provide data and traffic flow confidentiality.
- Digital signature mechanisms
  - signing procedure (private),
  - verification procedure (public).
  - Can provide non-repudiation, origin authentication and data integrity services.
- Both can be basis of some authentication exchange mechanisms.

Specific Mechanisms 2

- Access Control mechanisms
  - A server using client information to decide whether to grant access to resources
    - E.g. access control lists, capabilities, security labels. Data integrity mechanisms
  - Protection against modification of data.
    - Provide data integrity and origin authentication services. Also basis of some authentication exchange mechanisms.
- Authentication exchange mechanisms
  - Provide entity authentication service.

Specific Mechanisms 3

- Traffic padding mechanisms
  - The addition of ‘pretend’ data to conceal real volumes of data traffic.
  - Provides traffic flow confidentiality.
- Routing control mechanisms
  - Used to prevent sensitive data using insecure channels.
  - E.g. route might be chosen to use only physically secure network components.
- Notarization mechanisms
  - Integrity, origin and/or destination of data can be guaranteed by using a 3rd party trusted notary.
    - Notary typically applies a cryptographic transformation to the data.

Pervasive Security Mechanisms

- Five types identified:
  - – trusted functionality,
  - – security labels,
  - – event detection,
  - – security audit trail,
  - – security recovery.

Pervasive Mechanisms 1

- Trusted functionality
  - – Any functionality providing or accessing security mechanisms should be trustworthy.
  - – May involve combination of software and hardware.
- Security labels
  - – Any resource (e.g. stored data, processing power, communications bandwidth) may have security label associated with it to indicate security sensitivity.
  - – Similarly labels may be associated with users. Labels may need to be securely bound to transferred data.

Pervasive Mechanisms 2

- Event detection
  - Includes detection of
    - attempted security violations,
    - legitimate security-related activity.
  - Can be used to trigger event reporting (alarms), event logging, automated recovery.
- Security audit trail
  - Log of past security-related events.
  - Permits detection and investigation of past security breaches.
- Security recovery
  - Includes mechanisms to handle requests to recover from security failures.
  - May include immediate abort of operations, temporary invalidation of an entity, addition of entity to a blacklist.

Services Versus Mechanisms

- ISO 7498-2 indicates which mechanisms can be used to provide which services.
- Illustrative NOT definitive.
- Omissions include:
  - use of integrity mechanisms to help provide authentication services,
  - use of encipherment to help provide non-repudiation service (as part of notarization).

Service/Mechanism Table 1

Mechanism Service	Encipherment	Digital sign.	Access Control	Data integrity
Entity authentication	Y	Y		
Origin authentication	Y	Y		
Access control			Y	
Connection confidentiality	Y			
Connectionless confidentiality	Y			
Selective field confidentiality	Y			
Traffic flow confidentiality	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 of origin		Y		Y
Non-repudiation of delivery		Y		Y

Service/Mechanism Table 2

Mechanism Service	Auth. exchange	Traffic padding	Routing Control	Notarisation
Entity authentication	Y			
Origin authentication				
Access control				
Connection confidentiality			Y	
Connectionless confidentiality			Y	
Selective field confidentiality				
Traffic flow confidentiality		Y	Y	
Connection integrity with recovery				
Connection integrity without recovery				
Selective field connection integrity				
Connectionless integrity				
Selective field connectionless integrity				
Non-repudiation of origin				Y
Non-repudiation of delivery				Y

Security Services And Layers

- ISO 7498-2 lays down which security services can be provided in which of the 7 layers.
- Layers 1 and 2 may only provide confidentiality services.
- Layers 3/4 may provide many services.
- Layer 7 may provide all services.
- A set of principles dictate which services can/should be provided at which layers.

Service/Layer Table

Layer Service	Layer 1	Layer 2	Layer 3	Layer 4	Layer 5/6	Layer 7
Entity authentication			Y	Y		Y
Origin authentication			Y	Y		Y
Access control			Y	Y		Y
Connection confidentiality	Y	Y	Y	Y		Y
Connectionless confidentiality		Y	Y	Y		Y
Selective field confidentiality						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 of origin						Y
Non-repudiation of delivery						Y