

Secure Communication Overview

Segurança Informática em Redes e Sistemas
2024/25

Ricardo Chaves, David R. Matos

Ack: Carlos Ribeiro, André Zúquete,
Miguel P. Correia, Miguel Pardal

Roadmap

- Goals
- Basic approximations
 - Link security *versus* end-to-end security
- Acting layers

Goals of secure communication

- Provide security mechanisms and protocols for communication assuring:
 - **Confidentiality** of the exchanged data
 - **Integrity** verification of the exchanged data
 - **Authenticity** of the communicating parties
 - Machines, services, users

Secure channel functionalities

- Trustworthy **authentication** between parties
- Negotiation/computation of **session keys**
 - Session key: secret shared between the communicating parties
 - Support secure communication
 - Session key establishment often integrated with the authentication (above)
- Secure **data exchange**
 - Leveraging secure channels using the session keys

Basic approximations

- **Link security**
 - Security is assured between a pair of machines
 - Is not scalable / not adaptable to the Internet
 - We would have to trust each “hop” in the network path
- **End-to-end security**
 - Security is assured by end-point software exchanging the messages
 - Scalable and adaptable to the Internet

End-to-end principle

- Formulated by Saltzer, Reed and Clark in 1981, applied to **reliability**
- IP assumes this principle for correcting errors
 - It is easier to obtain reliability beyond a certain margin by mechanisms in the end hosts of a network rather than in the intermediary nodes
 - Especially when the intermediary nodes are beyond the control of, and not accountable to the end hosts
- End-to-end principle can be applied to **security**
 - By implementing security in the lower levels, all channels must bear its cost
 - Even if not necessary
 - Hard to verify
 - By implementing security in the higher levels, the channel endpoints can implement the functionalities tailored to the application's needs
 - Avoid redundancies

Acting layers:

Actions and solutions

Layers		Responsibility	Approach	Solutions	
	Transaction	Local data manipulation applications	End-to-end security	PGP, PEM, S/MIME	
OSI Layers	Application	Applications for remote data exchange		End-to-end security	HTTPS, IMAPS SSH
	Presentation				
	Session				
	Transport	Operating Systems			TLS
	Network				IPsec
	Link	Devices	Link security		IEEE 802.11*
Physical					

Choosing the correct layer (1/2)

- **Transaction layer solution**
 - Allows the secure exchange of objects
 - e.g., mail messages, documents, files
 - Allows to assure **non-repudiation** of object authorship
- **Application and transport layer solution**
 - Allows security to adapt to the needs of distributed applications
 - Requires the applications to be modified to use these protocols
 - It is not easy to design a solution that is simultaneously:
 - **Generic** – to be used by many applications and
 - **Powerful** – to address the requirements of all applications

Choosing the correct layer (2/2)

- **Network and link layer solution**
 - Requires modification of the operating system or device
 - Tend to be simpler and more generic
 - Independent of the applications
 - Allow the applications to remain unchanged
 - but may not cover all their security requirements
 - Requires extra-application control
 - Definition of minimum security requirements
 - Selecting policy of security mechanisms

Acting layers

- Advantages of acting at **upper layers**
 - Better fit to the application's requirements
 - Possible to enforce non-repudiation
 - Awareness of the entities involved: users, services
 - Awareness of session and connection that allows
 - Different key management protocols
 - Different ways of exploring security mechanisms
- Advantages of acting at **lower layers**
 - Simplicity of use, coverage
 - No need to modify applications and higher layer infra-structures

Secure communication:

Data Link layer and below

Layers		Responsibility	Approach	Solutions	
	Transaction	Local data manipulation applications	End-to-end security	PGP, PEM, S/MIME	
OSI Layers	Application	Applications for remote data exchange		End-to-end security	HTTPS, IMAPS SSH
	Presentation				
	Session				
	Transport	Operating Systems			TLS
	Network				IPsec
	Link	Devices	Link security	IEEE 802.11*	
	Physical				

Secure communication:

Network layer

Layers		Responsibility	Approach	Solutions
	Transaction	Local data manipulation applications	End-to-end security	PGP, PEM, S/MIME
OSI Layers	Application	Applications for remote data exchange		HTTPS, IMAPS SSH
	Presentation			
	Session			
	Transport	Operating Systems		
	Network			IPsec
	Link	Devices	Link security	IEEE 802.11*
	Physical			

Secure communication: Transport layer and above

Layers		Responsibility	Approach	Solutions
OSI Layers	Transaction	Local data manipulation applications	End-to-end security	PGP, PEM, S/MIME
	Application	Applications for remote data exchange		HTTPS, IMAPS SSH
	Presentation			
	Session			
	Transport	Operating Systems		TLS
	Network	Systems		IPsec
	Link	Devices	Link security	IEEE 802.11*
	Physical			