NETWORKS AND TELECOMMUNICATIONS SERIES

Network Security

André Perez

ISTE WILEY

Network Security

Network Security

André Perez

ISTE

WILEY

First published 2014 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

Library of Congress Control Number: 2014945531

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-84821-758-4

Contents

Preface

This book introduces the security mechanisms deployed in Ethernet, wireless-fidelity (Wi-Fi), Internet Protocol (IP) and Multi-Protocol Label Switching (MPLS) networks. These mechanisms are grouped according to the four functions below:

– data protection;

– access control;

– network isolation;

– data monitoring.

Data protection is supplied by data confidentiality and integrity control services:

– confidentiality consists of ensuring that data can only be read by authorized individuals. This service is obtained using a mechanism that encrypts the relevant data;

– integrity control consists of detecting modifications in transferred data. This service is obtained via a hash function or an encryption algorithm that generates a seal.

Access control is provided by a third-party authentication service. This service consists of verifying the identity of the

person wishing to access a network. This service is generally obtained with a hash function, as for integrity control.

Network isolation is supplied by the Virtual Private Network (VPN) service. This service makes it possible to create closed user groups and authorize communication solely between users belonging to the same group. Note that access control also implicitly enables network isolation.

Data monitoring consists of applying rules to data in order to authorize its transfer or detect attacks. The service is supplied by analyzing the fields of the various protocols making up the data structure.

Network

The role of the network is to transport data between two hosts. The network is composed of two entities (Figure P.1):

– the Local Area Network (LAN) is the network on which the hosts connect. This is usually a private network deployed by businesses;

– the Wide Area Network (WAN) is the network that ensures the interconnection of the LAN networks. It is usually a public network deployed by Internet access and transit operators.

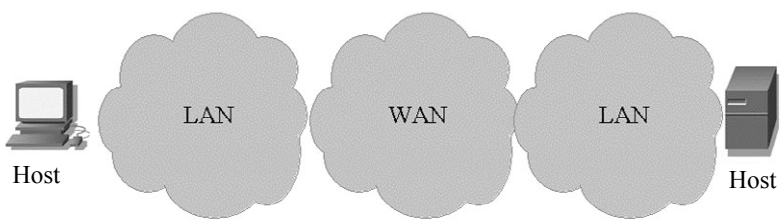

Figure P.1. *Network architecture*

The LAN network is constructed of two types of blocks: the access block and the core block (Figure P.2):

– the access block connects the network's hosts. Access blocks can be dedicated to different types of hosts:

- computers, telephones,
- application servers,
- network and security management system,
- WAN network;

– the core block enables the networking of access blocks.

The Internet access provider's WAN network is structured in three units (Figure P.3):

– access network: it corresponds to the connection of the LAN network with the operator's primary technical site;

– aggregation network: it collects the traffic generated by access networks. It generally has regional coverage;

– core network: this connects the different aggregation networks. It generally has national coverage and also provides the interface between operators.

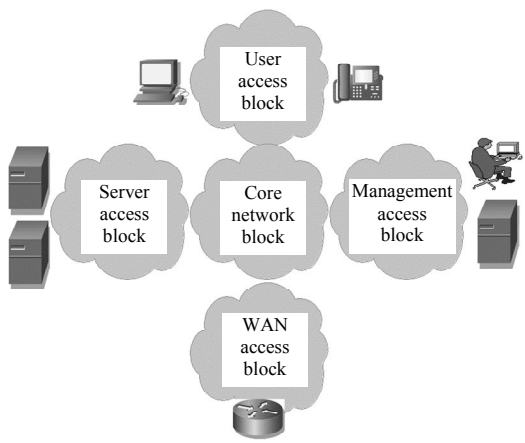

Figure P.2. *Architecture of LAN network*

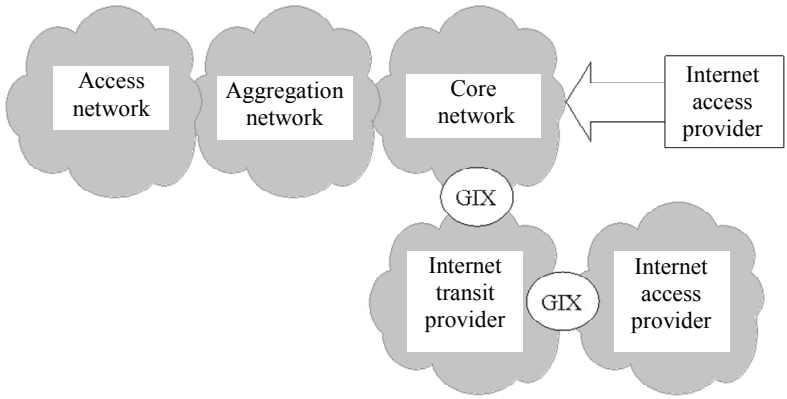

Figure P.3. *Architecture of WAN network*

The interconnection of the WAN networks of different Internet access providers takes place in the core network, in two different ways:

– the connection is direct, when the Internet access providers are operating in the same territory;

– the connection is established by an Internet transit provider, in the opposite case. Internet transit networks have an architecture similar to that of the core network of the Internet access provider.

A Global Internet eXchange (GIX) point enables different Internet access and transit providers to exchange traffic using mutual agreements called peering, generally based on the balancing of the volumes of data transmitted and received (Figure P.3).

Introduction to cryptography

Chapter 1 introduces the fundamental concepts of cryptography. Cryptography addresses aspects related to communications security, in order to provide confidentiality, integrity control and third-party authentication services.

Confidentiality service is implemented by encryption mechanisms. There are two main families of cryptographic algorithms: secret-key symmetrical algorithms and public- and private-key asymmetrical algorithms.

Symmetrical algorithms are well adapted to data encryption but pose the issue of establishing a secret key. Two frequently used methods are generation using the Diffie–Hellman algorithm and transport of the secret key via asymmetrical algorithms. Encryption is provided, for example, by the Advanced Encryption Standard (AES) algorithm or the Triple Data Encryption Standard (3DES) algorithm.

Asymmetrical algorithms are applied in the transportation of secret keys and digital signatures. In the former case, the secret key is encrypted by the public key and decrypted by the private key. In the latter case, the inverse occurs. Encryption is provided by algorithms based on modular exponentiation, such as the RSA (named after the initials of its three inventors, Rivest, Shamir and Adleman) algorithm or the Elliptic Curve Cryptography (ECC) algorithm.

The hash function is another type of cryptographic function. It converts a string of any length (the data to be protected) into a smaller chain, generally of fixed size (a digest). The hash function can be supplied by the two algorithms below:

– Message Digest 5 (MD5), which calculates a 128-bit digest;

– Secure Hash Algorithm (SHA), which calculates a digest of between 160 and 512 bits.

Sealing is based on the secret key and provides the data integrity control service. Seals can be calculated in two different ways:

– the symmetrical encryption algorithm is applied to the data; therefore, the seal is the last block of the cryptogram;

– the hash function is applied to a set comprised of data and a secret key, the association of which is defined, for example, by the Hashed Message Authentication Code (HMAC) calculation function.

The signature is based on the encryption of the digest by a private key and its decryption by a public key. It provides the service of integrity and non-repudiation by the source of the data received by the recipient.

The distribution of public keys is associated with the display of a certificate. This is a data structure signed by a certification authority that guarantees that the issuer of the public key is actually its holder.

802.1x mechanism

Chapter 2 introduces the 802.1x access control mechanism, deployed in the LAN network and implementing the following technologies:

– Ethernet technology, in the case of access to a switch;

– Wi-Fi technology, in the case of connection to an Access Point (AP).

The 802.1x mechanism has three components (Figure P.4):

– the supplicant is the device (for example, the computer) wishing to access the Ethernet or Wi-Fi network;

– the authenticator is the device (Ethernet switch or Wi-Fi AP) that controls the supplicant's access to the LAN network;

– the authentication server is the device that authenticates the supplicant and authorizes access to the LAN network.

The 802.1x mechanism is based on a series of protocols (Figure P.4):

– the Extensible Authentication Protocol (EAP) Over LAN (EAPOL) protocol, exchanged between the supplicant and the authenticator;

– the EAP protocols exchanged between the supplicant on one hand, and the authenticator or authentication server on the other. The EAP protocol is carried by the EAPOL protocol on the interface between the supplicant and the authenticator;

– the Remote Authentication Dial-In User Service (RADIUS) protocol exchanged between the authenticator and the authentication server. The RADIUS protocol carries the EAP protocol on the interface between the authenticator and the authentication server;

– the EAP-Method protocol exchanged between the supplicant and the application server. The EAP-Method protocol is carried by the EAP protocol.

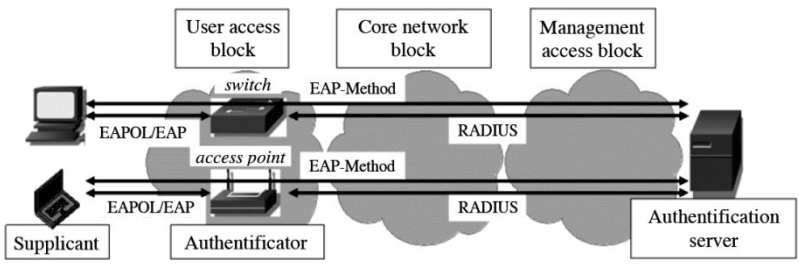

Figure P.4. *802.1x mechanism*

The EAP-Method protocol offers several types of authentication:

– the EAP-MD5 method: the client is authenticated using a password. This method is similar to the

Challenge-Handshake Authentication Protocol (CHAP), which is based on the Point-to-Point Protocol (PPP) used for point-to-point connections;

– the EAP-Transport Layer Security (TLS) method: authentication is mutual between the supplicant and the authentication server using certificates;

– the EAP-Tunneled-TLS (TTLS) method: authentication is mutual between the supplicant and the authentication server by means of an authentication server-side certificate, while the supplicant can use a password.

As a complement to authentication, the EAPOL protocol participates in the generation of keys for encryption and in the integrity control used by the Wi-Fi Protected Access (WPA) and WPA2 mechanisms described in Chapter 3.

WPA mechanisms

Chapter 3 introduces the WPA1 and WPA2 security mechanisms applied to Wi-Fi networks. Wi-Fi technology is originally a LAN private network access technology using radio transmission. It has the distinctive characteristic of using free frequency bands. It is also used in WAN public networks to establish hotspots.

WPA1 and WPA2 security mechanisms are used only in private networks. The security used in the case of hotspots generally involves the transport security described in Chapter 5.

Radio interface security began with the Wired Equivalent Privacy (WEP) mechanism. Due to its weaknesses, it was supplanted by the WPA1 mechanism and then by the WPA2 mechanism. These three mechanisms specifically implement third-party access control and data protection services.

For the WEP mechanism, third-party access control is based on the rivest cipher 4(RC4) algorithm. Access control