GLOBAL EDITION

Corporate Computer Security

FOURTH EDITION

Randall J. Boyle | Raymond R. Panko

ALWAYS LEARNING

PEARSON

To Courtney Boyle, thank you for your patience, kindness, and perspective on what's most important in life.

—Randy Boyle

To Julia Panko, my long-time networking and security editor and one of the best technology minds I've ever encountered.

—Ray Panko

Editor in Chief: Stephanie Wall
Executive Editor: Bob Horan
Program Manager Team Lead: Ashley Santora
Program Manager: Denise Vaughn
Director of Marketing: Maggie Moylan
Executive Marketing Manager: Anne Fahlgren
Project Manager Team Lead: Judy Leale
Project Manager: Tom Benfatti
Operations Specialist: Michelle Klein
Creative Director: Jayne Conte
Head of Learning Asset Acquisition, Global Edition: Laura Dent
Assistant Acquisitions Editor, Global Edition: Debapriya Mukherjee
Project Editor, Global Edition: Amrita Naskar
Media Producer, Global Edition: Vikram Kumar
Senior Manufacturing Controller, Production, Global Edition: Trudy Kimber
Cover Designer: PreMediaGlobal
Cover Image: Devis Da Fre'/Shutterstock
Digital Production Project Manager: Lisa Rinaldi

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appear on the appropriate page within text.

Pearson Education Limited
Edinburgh Gate
Harlow
Essex CM20 2JE
England

and Associated Companies throughout the world

Visit us on the World Wide Web at: www.pearsonglobaleditions.com

ISBN 10: 1-292-06045-X
ISBN 13: 978-1-292-06045-3 (Print)
ISBN 13: 978-1-292-06659-2 (PDF)

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

10 9 8 7 6 5 4 3 2 1
14 13 12 11 10

Typeset in Times, 10/12 by Integra Software Services Pvt. Ltd

Printed and bound by Courier Westford in the United States of America

FIREWALL-FRIENDLY PROTECTION In addition, IPsec tunnel mode is firewall-friendly. Packets are only encrypted between the two IPsec gateways, so after a packet arrives, it can be filtered by a firewall placed after the IPsec gateway at each site.

NO PROTECTION WITHIN THE TWO SITES The disadvantage of tunnel mode is that it gives absolutely no protection at all to IP packets when they are traveling *within* the site networks at the two sites. This leaves packets open to attack within site networks. However, transmission within site networks generally is safer than transmission over the Internet, so the loss of protection within sites is often considered a good trade-off for the lower cost of IPsec tunnel mode operation and for IPsec's firewall friendliness.

TEST YOUR UNDERSTANDING

42. a. Distinguish between transport and tunnel modes in IPsec in terms of packet protection.
b. What are the attractions of each?
c. What are the problematic issues of each?

IPsec Security Associations (SAs)

Before two hosts or IPsec gateways communicate, they first must establish security associations. A **security association (SA)** is an agreement about what IPsec security methods and options the two hosts or two IPsec gateways will use. An SA in IPsec is reminiscent of an SSL/TLS cipher suite.

A security association (SA) is an agreement about what IPsec security methods and options the two hosts or two IPsec gateways will use.

SEPARATE SAs IN THE TWO DIRECTIONS Figure 3-31 illustrates how communicating partners negotiate security associations. Note that when two parties communicate, they must establish *two* SAs—one in each direction. If Sal and Julia communicate, there must be an SA for

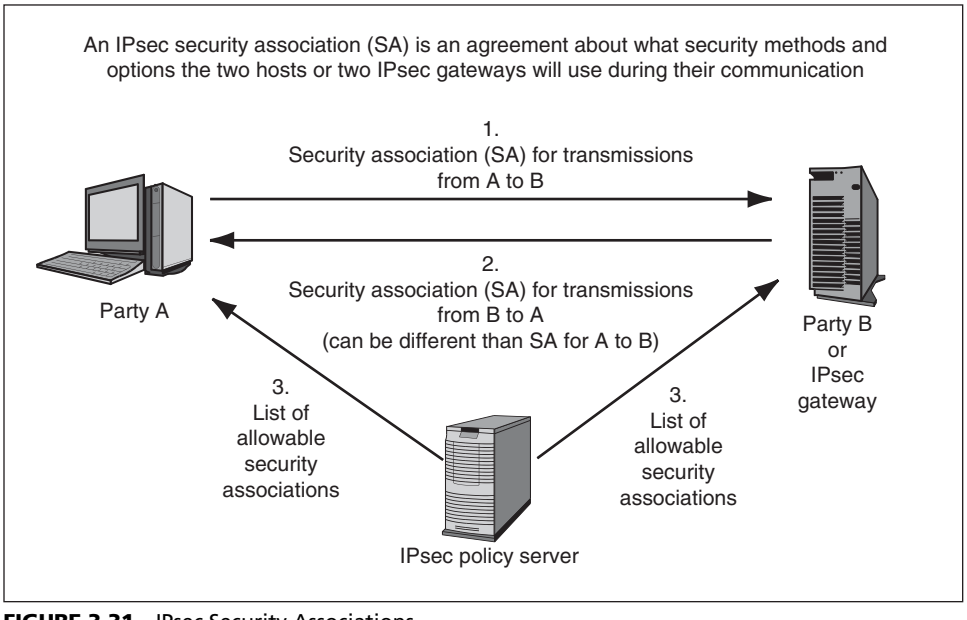

FIGURE 3-31 IPsec Security Associations

Sal to follow when sending to Julia and a separate SA for Julia to follow when sending to Sal. The use of two SAs allows a different level of protection in each direction if that is desirable.

POLICY-BASED SA As noted earlier, some allowable security methods and options in cryptographic security standards may be inadequate for a company's security needs. A company would like to set policies for acceptable security methods and options and enforce these policies on all devices that implement the standard.

SSL/TLS has no way to set and enforce policies centrally, but IPsec does. As Figure 3-31 shows, IPsec supports the use of **IPsec policy servers**, which push a list of suitable policies to individual IPsec gateway servers or hosts. From the viewpoint of security management, this is a critical capability.

TEST YOUR UNDERSTANDING

43. a. What does an SA specify? (Do not just spell SA out.)
b. When two parties want to communicate in both directions with security, how many IPsec SAs are necessary?
c. May there be different SAs in the two directions?
d. What is the advantage of this?
e. Why do companies wish to create policies for SAs?
f. Can they do so in SSL/TLS?
g. How does IPsec set and enforce policies?

3.12 CONCLUSION

In this chapter, we looked at the core cryptographic concepts that every IT security professional needs to know. We also looked at how cryptographic systems provide secured communication in a transparent and unified manner. Cryptography can be challenging. We have tried to summarize some of the key points mentioned in the chapter.

One common cryptographic protection is encryption for confidentiality, in which the original plaintext message is encrypted with a cipher (encryption/decryption method) and a key. This produces ciphertext that cannot be read by anyone intercepting it. The receiver applies the cipher in reverse with the same key or another key (depending on the cipher) to recover the original plaintext message. The chapter looked at two operations commonly used in ciphers—substitution and transposition.

In symmetric key encryption for confidentiality, the sender and receiver use the same key in both directions. In public key encryption, each party has both a public key and a private key. In public key encryption for confidentiality, the sender encrypts with the public key of the receiver. The receiver decrypts with its own private key.

For strong security, keys need to be very long to thwart cracking through exhaustive search. Symmetric key encryption ciphers need keys that are at least 100 bits long in order to be strong today. Public and private keys must be even longer to be strong. RSA keys need to be at least 1,024 bits long, and ECC keys need to be at least 512 bits long.

Another important cryptographic protection is authentication, in which a supplicant (such as a client PC) attempts to prove its identity to a verifier (typically a server) by sending credentials. Authentication typically is done both at the beginning of a communication session and also when each message is sent.

We referred frequently to three core cryptographic processes: symmetric key encryption, public key encryption, and hashing. These are easy to confuse with each other. Figure 3-32 compares how the three processes are used for confidentiality and authentication.

	Confidentiality	Authentication
Symmetric key encryption	Applicable. Sender encrypts with key shared with the receiver.	Not applicable.
Public key encryption	Applicable. Sender encrypts with *receiver's public key*. Receiver decrypts with the *receiver's own private key.*	Applicable. Sender (supplicant) encrypts with *own private key.* Receiver (verifier) decrypts with the *public key of the true party,* usually obtained from the true party's digital certificate.
Hashing	Not applicable.	Applicable. Used in MS-CHAP for initial authentication and in HMACs for message-by-message authentication.

FIGURE 3-32 Core Cryptographic Processes

- Note that only public key encryption is used for both confidentiality *and* authentication and that public–private key pairs are used *differently* in these processes.
- By contrast, symmetric key encryption is only used for confidentiality.
- Hashing, in turn, is only used for authentication. Although hashing for authentication does use a key, this does not make it symmetric key encryption, which is an entirely different process.

Cryptographic protections are rarely used alone. Rather, they are almost always packaged in cryptographic systems, which secure dialogues with a full range of protections. Cryptographic systems begin with three initial handshaking stages, then move into an ongoing communication stage.

The handshaking stages begin with the negotiation of sets of security methods and options that the communication partners will use subsequently. Corporate policies may limit which sets of methods and options can be used in order to prevent communicating partners from using weak methods and options.

Next, the two parties do initial authentication—usually mutual authentication. We specifically looked at MS-CHAP authentication, which is for users logging into Microsoft servers. MS-CHAP protects the user's login password with confidentiality. Normally, two communication partners do mutual authentication. However, MS-CHAP only authenticates the user. It does not use encryption. Rather, it uses hashing. Due to its use of reusable passwords as secrets and its lack of mutual authentication, MS-CHAP is a weak initial cryptographic method.

Finally, in the keying handshaking stage, the two parties must exchange symmetric session keys (and other secrets) securely. Session keys are only used for a single communication session. We saw how to do keying using public key distribution and Diffie–Hellman key agreement. This ends the handshaking stages.

In the ongoing communication stage, the two partners exchange many messages securely. Each message gets an electronic signature for message-by-message authentication and message integrity. There are two types of electronic signatures—HMACs and digital signatures. HMACs use hashing and a key (really, a shared secret). HMACs are inexpensive to implement and are the most widely used electronic signatures. Digital signatures use public key encryption. The

sender encrypts a message digest hash with the sender's own private key. The receiver (verifier) decrypts the message with the true party's public key—the party the supplicant claims to be.

Digital signatures give extremely strong authentication. However, digital signatures use public key encryption, which is extremely slow and therefore expensive. In addition, public key encryption for authentication normally is tested using information in the true party's digital certificate. This requires a system of trusted certificate authorities. The certificate authority gives the true party's public key, which must be used to test that the digital signature was created with the true party's private key.

This chapter included a brief section on quantum key distribution and quantum key cracking.

During the ongoing communication stage, cryptographic systems use symmetric key encryption to encrypt each message for confidentiality.

We looked at how cryptographic elements are packaged into cryptographic systems, which provide the elements of security in a single integrated package. Specific cryptographic systems use cryptographic security standards. In this chapter, we looked at some of the major cryptographic security standards.

We looked at virtual private network (VPN) which are cryptographic systems that provide secure communication over untrusted networks (the Internet, a wireless LAN, etc.). There are host-to-host, remote access, and site-to-site VPNs.

One widely used VPN standard is SSL/TLS. SSL/TLS is very popular because the client only needs a browser, and all client computers today have browsers. We saw how SSL/TLS was created for host-to-host VPNs—specifically browser–webserver VPNs. All browsers and webservers know how to set up SSL/TLS VPNs, so using them is inexpensive. We then saw how SSL/VPN gateways can turn SSL/TLS into a remote access VPN technology. However, SSL/TLS does not provide transparent protection to all applications, and setting up SSL/TLS gateways for remote access can be clumsy.

The gold standard for VPNs is IPsec. IPsec offers extremely strong security, including the requirement that both communication partners authenticate themselves using public key authentication with digital certificates. In addition, IPsec has strong policy control capabilities so that communicating partners cannot select weak security options. This policy management is centralized and therefore easy to administer.

IPsec operates in two modes. In transport mode, IPsec provides security all the way between the source and destination host. However, IPsec transport mode is expensive because of setup requirements on all clients and servers and the management of digital certificates over their life cycles. Transport mode also makes firewall filtering impossible or at least difficult. In tunnel mode, IPsec only provides security between IPsec gateways at each site. This eliminates computer setup requirements and allows firewall filtering. On the downside, tunnel mode does not provide any security within sites.

Thought Questions

1. The total processing speed of microprocessors (based on clock rate and number of circuits) is doubling roughly every year. Today, a symmetric session key needs to be 100 bits long to be considered strong. How long will a symmetric session key have to be in 30 years to be considered strong? (Hint: Consider how much longer decryption takes if the key length is increased by a single bit.)
2. Longer keys are more difficult to crack. Most symmetric keys today are 100–300 bits long. Why don't systems use far longer symmetric keys—say, 1,000-bit keys?
3. Brute force is used to crack a 100-bit key. The key is cracked in only 5,000 tries. How can this be?
4. In practice, public key authentication is used heavily for initial authentication but rarely for

message-by-message authentication. Given the intense processing power required for public key authentication and the fact that public key authentication gives the strongest authentication, explain these two usage patterns.

5. Did we see symmetric key encryption used for authentication in this chapter? If so, how was it used?
6. Describe the entries in the second row of Figure 3- 9. Comment on the strengths of the choices it uses.
   a. For the second-to-last row of Figure 3-9, comment on the strengths of its symmetric encryption cipher and of its hashing algorithm.
   b. Describe the entries in the last row of Figure 3-9. Comment on the strengths of the choices it uses.
7. Using the Internet, discuss the advisory issued by Microsoft in relation to MS-CHAP.
8. Why is ECC not as widely used as RSA?
9. Compare symmetric with public key encryption for authentication, confidentiality, and integrity of messages.
10. How does cloud computing pose security concerns in hosting digital signatures?
11. Identify potential security threats associated with authentication via digital signatures and digital certificates. Explain each and describe how you would address each threat.
12. The chapter described how public key authentication is used for message-by-message authentication in digital signatures. However, public key authentication is widely used for initial authentication. Describe the processes that the supplicant and verifier would use if public key encryption were used in initial challenge–response authentication. Draw heavily on your understanding of digital signatures, but put this information in challenge–response context.
13. If a supplicant gives you a digital certificate, should you accept it? Explain. (Think about this carefully. The answer is not obvious.)
14. Pretty Good Privacy (PGP) uses public key encryption and symmetric key encryption to encrypt long documents. How might this be possible?

Hands-on Projects

PROJECT 1

AxCrypt® is a great third-party encryption tool. You just select the files you want encrypted, enter your password, and you're done. It is even available as an option in the shortcut menu when you right-click a file. AxCrypt will automatically re-encrypt the file after you are done modifying it. It uses 128-bit AES and is completely free. Let's look at some of the functionality built into AxCrypt.

1. Download AxCrypt from http://www.axantum.com/AxCrypt.
2. Click Download.
3. Click on the appropriate version for your operating system.
4. Click Save.
5. Select your download folder.
6. If the program doesn't automatically open, browse to your download folder.
7. Right-click AxCrypt-Setup.exe.
8. Click Run as administrator.
9. Click Yes if prompted.
10. Click I Agree.
11. Click Custom Installation.
12. Deselect all the bloatware (from Amazon).
13. Click Install.
14. Deselect Register.
15. Click Finish.
16. Save all your work, exit all other programs, and reboot your computer. Once your computer is rebooted you can continue on to the next step.
17. Right-click your desktop.
18. Click New and Text Document.
19. Name the file YourName.txt. Replace YourName with your first and last name.
20. Right-click the file named YourName.txt.
21. Select AxCrypt, and Encrypt.
22. Enter the password "tiger1234" (without quotes).
23. Click OK.
24. Double-click the new YourName-txt.axx file you just created.
25. Enter the password "tiger1234" (without quotes).
26. Click OK.
27. Close the text file that you just opened.
28. Take a screenshot of your desktop showing the newly created files.