COMPUTER SECURITY

Chapter 6: Network Security

SECURITY IN COMPUTING, FIFTH EDITION

Chapter 6: Networks (cont.)

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Rise of the Hackers

- [Rise of the Hackers]

ENCRYPTION FOR NETWORKS

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Secret Key vs. Public Key Encryption

	Secret Key (Symmetric)	Public Key (Asymmetric)
Number of keys	1	2
Key size (bits)	56–112 (DES), 128–256 (AES)	Unlimited; typically no less than 256; 1000 to 2000 currently considered desirable for most uses
Protection of key	Must be kept secret	One key must be kept secret; the other can be freely exposed
Best uses	Cryptographic workhorse. Secrecy and integrity of data, from single characters to blocks of data, messages and files	Key exchange, authentication, signing
Key distribution	Must be out-of-band	Public key can be used to distribute other keys
Speed	Fast	Slow, typically by a factor of up to 10,000 times slower than symmetric algorithms

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Digital Signatures

- Tool to demonstrate authenticity
  - similar to a paper signature
- A way by which a person or organization can affix a bit pattern to a file
  - implies confirmation,
  - pertains to that file only
  - cannot be forged

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Digital Signatures

- A digital signature often uses asymmetric or public key cryptography
  - public key cryptographic protocols involve several sequences of messages and replies
    - Time consuming if both parties are not immediately available
  - In this situation, a technique that could authenticate a party even if it is inactive would be useful
    - Similar to a paper signature

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Digital Signatures

- Properties required of digital signatures:
  - It must be unforgeable
    - If person S signs message M with signature Sig(S,M), no one else can produce the pair [M,Sig(S,M)].
  - It must be authentic
    - If a person R receives the pair [M, Sig(S,M)] purportedly from S, R can check that the signature is really from S.
    - Only S could have created this signature
      - the signature is firmly attached to M.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Digital Signatures

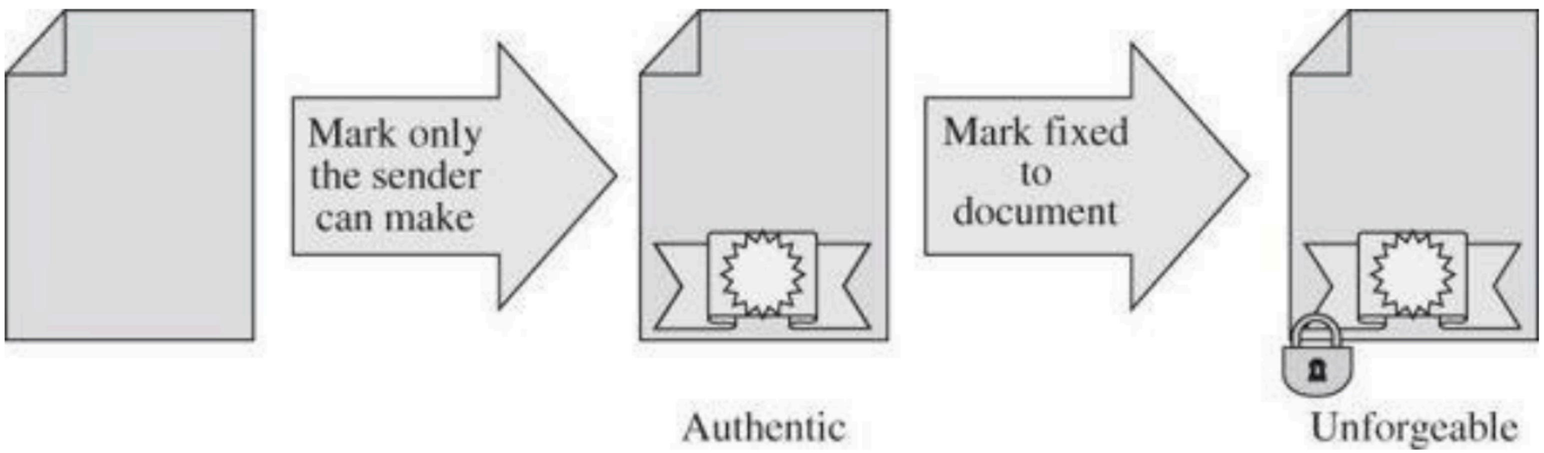


FIGURE 2-26 Digital Signature Requirements

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Public Key for Signatures

- Let's assume that:
  - Public key encryption for user U is E(M,KU)
  - Private key transformation for U is written as D(M,KU)
- How do we prove authenticity?

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Public Key for Signatures

- Authenticity:
  - Sender S sends D(M, KS) to R
    - Using his private key
  - R decodes the message with the public key transformation
    - Computing E(D(M, KS), KS) = M
  - Since only S can create that message the message must genuinely have come from S
    - Only S has the private key

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Public Key for Signatures

- Unforgeability (integrity):
  - R will save D(M, KS)
  - R can show at a later date M and D(M, KS)
    - If S tries to change message M, claim forgery
  - Anyone can verify M since D(M, KS) is transformed to M with the public key transformation of S
    - E(D(M, KS), KS) = M
  - => public key satisfies unforgeability

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Cryptographic Tools

Cryptographic primitive / Security Goal	Hash	MAC	Digital signature
Integrity	Yes	Yes	Yes
Authentication	No	Yes	Yes
Non-repudiation	No	No	Yes
Kind of keys	none	symmetric keys	asymmetric keys

https://crypto.stackexchange.com/questions/5646/what-are-the-differences-between-a-digital-signature-a-mac-and-a-hash

Encryption for networks

- Link encryption
- End-to-end encryption,
- Tools that are commonly used for implementing network encryption

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Link Encryption

- In link encryption data packets are encrypted just before system places them on the physical communications link
  - Traffic is encrypted and decrypted at each network routing point
    - Switch, node, etc.
- Data packets are decrypted just as they arrive at the destination system.
- The repeated decryption and encryption allows the routing information contained in each transmission to be read and employed further to direct the transmission toward

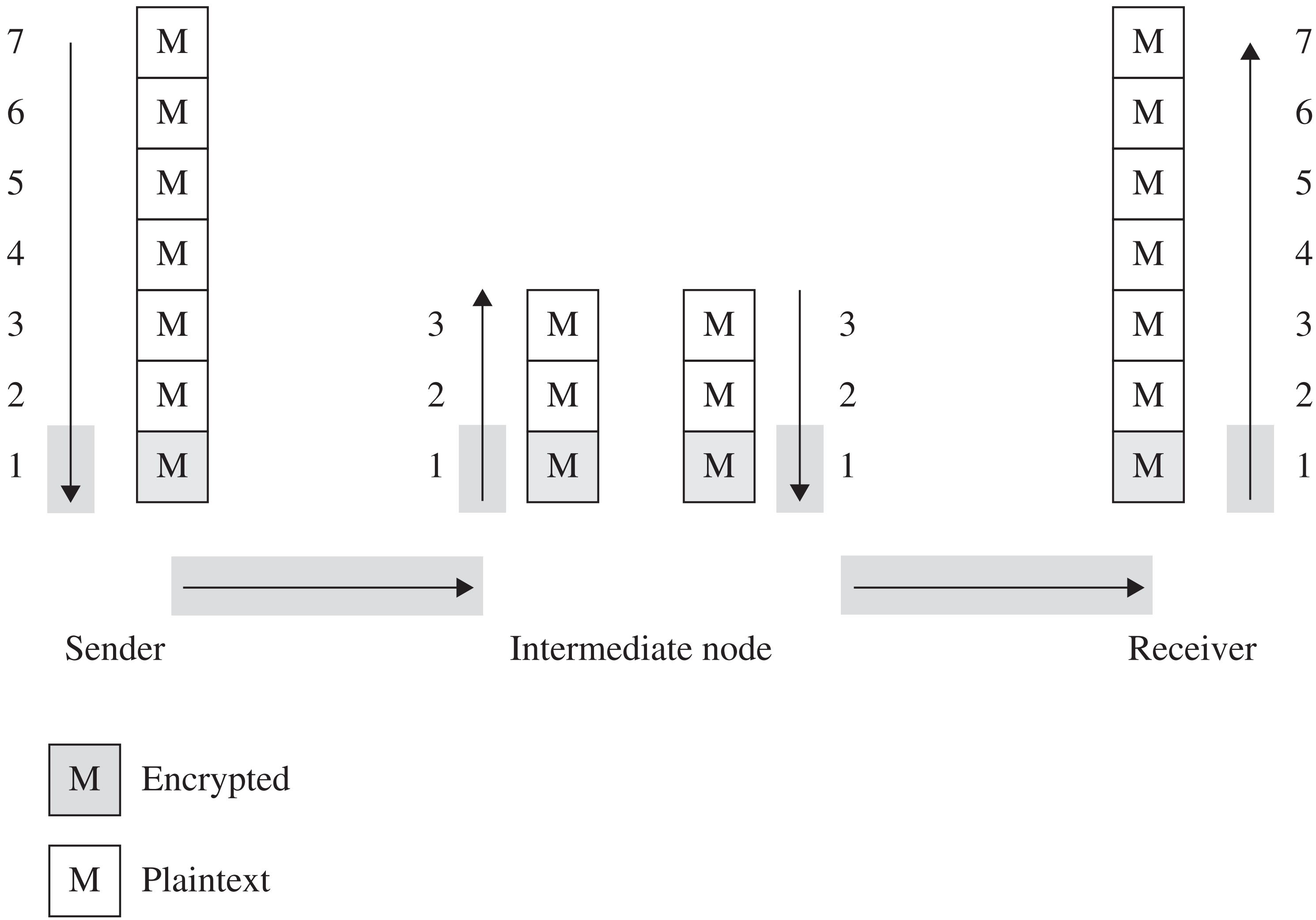
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Link Encryption

- Typically a host has only one link to the network
  - All traffic sent from this host will be encrypted by it
- However, receiving hosts need to decrypt data
  - All hosts must share keys
- If message is encrypted along some links and not others, the encryption advantages may be lost
    - Intermediate hosts may see message
  - => link encryption is usually performed on all links of a network

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

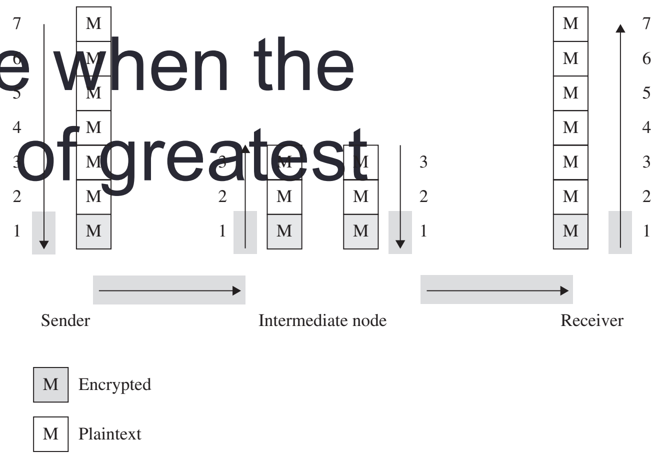
Link Encryption Example



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Link Encryption Example

- Data is encrypted only at layer 1 OSI stack.
- If data is communicated through an intermediate node:
  - The intermediate node will decrypt the data when it arrives
  - May re-encrypt it for the next link.
- Link encryption is appropriate when the transmission line is the point of greatest vulnerability
  - such as in wireless scenarios



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Link Encryption

- Useful when transmission line is vulnerable
  - i.e., if network hosts are secure but communication medium shared with other users
- Desirable when all communications on a single line needs to be protected
  - i.e., protecting internal communication between two offices of same company
- Can be used to implement a private network by using public resources

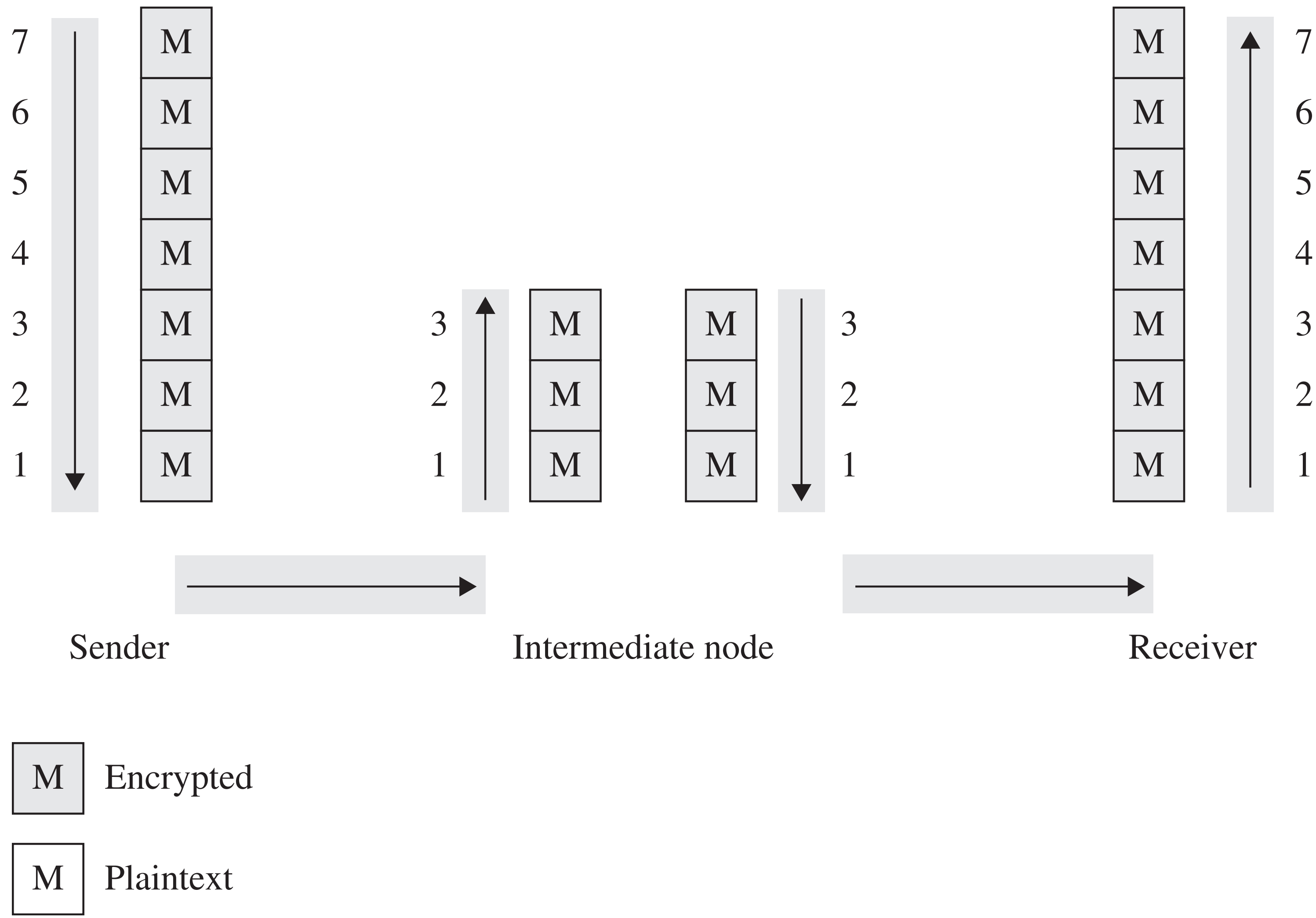
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

End-to-End Encryption

- Data is encrypted all the way up to OSI layer 7, the application layer
  - In contrast with link encryption
  - In real-world end-to-end encryption, the data often isn't encrypted all the way to layer 7
    - such as encryption that use SSL,
- Important: intermediate nodes cannot decrypt the data.
- End-to-end encryption is appropriate whenever sending sensitive data through untrustworthy intermediate nodes
  - such as over the Internet

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

End-to-End Encryption



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

End-to-End Encryption

- Advantage: Provides a virtual cryptographic channel between each pair of users
- Disadvantage: Each pair of users should share a unique cryptographic key
  - Number of keys required = $\frac{n*(n-1)}{2}$
    - Increases rapidly as network grows
- => link encryption is faster and uses fewer keys

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

End-to-End Encryption

- Advantages:
  - More flexible then link encryption
  - Can be used selectively
  - Done on user level
  - Can be integrated into application
- Both encryptions can be applied simultaneously
  - End-to-end can be applied on top of link encryption

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Link vs. End-to-End

Link Encryption	**End-to-End Encryption**
Security within hosts	
Data partially exposed in sending host	Data protected in sending host
Data partially exposed in intermediate nodes	Data protected through intermediate nodes
Role of user	
Applied by sending host	Applied by user application
Invisible to user	User application encrypts
Host administrators select encryption	User selects algorithm
One facility for all users	Each user selects
Can be done in software or hardware	Usually software implementation; occasionally performed by user add-on hardware
All or no data encrypted	User can selectively encrypt individual data items
Implementation considerations	
Requires one key per pair of hosts	Requires one key per pair of users
Provides node authentication	Provides user authentication

From S

End-to-End Encryption

- Whatsapp incorporated end-to-end encryption
  - Whatsapp End-to-End Encryption

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

BROWSER ENCRYPTION

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

BROWSER ENCRYPTION

- Browsers can encrypt data for protection during transmission
- The browser and the server negotiate a common encryption key
  - => if an attacker does hijack a session at the TCP or IP protocol level, the attacker cannot join the application data exchange

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Secure Shell (SSH)

- Originally developed for UNIX but now available on most OSs
- Provides an authenticated, encrypted path to the OS command line over the network
- Replacement for insecure utilities such as Telnet, rlogin, and rsh
- Protects against spoofing attacks and modification of data in communication

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SSH Secure Interactive Command Session

- The client connects to the server via a TCP session.
- The client and server exchange information on administrative details
  - such as supported encryption methods and their protocol version, each choosing a set of protocols that the other supports.

https://www.hostinger.com/tutorials/ssh/basic-ssh-commands

SSH Secure Interactive Command Session (cont.)

- The client and server initiate a secret-key exchange to establish a shared secret session key
  - Used to encrypt their communication (but not for authentication).
  - Session key is used in conjunction with a chosen block cipher (typically AES, 3DES) to encrypt all further communications.
- The server sends the client a list of acceptable forms of authentication
  - Such as public key based algorithms
  - The client tries these in sequence

https://www.hostinger.com/tutorials/ssh/basic-ssh-commands

SSH Secure Interactive Command Session

- The most common mechanism is to use a password or the following public-key authentication method:
  - If public-key authentication is the selected mechanism, the client sends the server its public key.
  - The server checks if this key is stored in its list of authorized keys.
    - If so, the server encrypts a challenge using the client's public key and sends it to the client.
  - The client decrypts the challenge with its private key and responds to the server, proving its identity.

https://www.hostinger.com/tutorials/ssh/basic-ssh-commands

A secure interactive command session (cont.):

- Once authentication has been successfully completed, the server lets the client access appropriate resources
  - such as a command prompt.

https://www.hostinger.com/tutorials/ssh/basic-ssh-commands

SSH

- SSH - Secure Shell

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SSL and TLS

- Secure Sockets Layer (SSL) was designed in the 1990s
  - to protect communication between a web browser and server
- In a 1999 upgrade to SSL, it was renamed Transport Layer Security (TLS)
- TLS is the modern, and much more secure, protocol
  - Although protocol is still commonly called SSL
- SSL is implemented at OSI layer 4 (transport) and provides:
  - Server authentication

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SSL Cipher Suites

- At the start of an SSL session, the client and server negotiate encryption algorithms, known as the “cipher suite”
- The server sends a list of cipher suite options, and the client chooses an option from that list
- The cipher suite consists of
  - A digital signature algorithm for authentication
  - An encryption algorithm for confidentiality
  - A hash algorithm for integrity

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SSL Cipher Suites

- Cipher suite negotiation is at the center of a very common SSL configuration vulnerability
- It is very common for servers to be configured to offer as many cipher suites as possible
  - to provide broad compatibility
- Cipher suite options may have significant known vulnerabilities (many actually do)
  - presents the opportunity for a man-in-the-middle to negotiate on the client's behalf for a weak cipher suite that the attacker can break

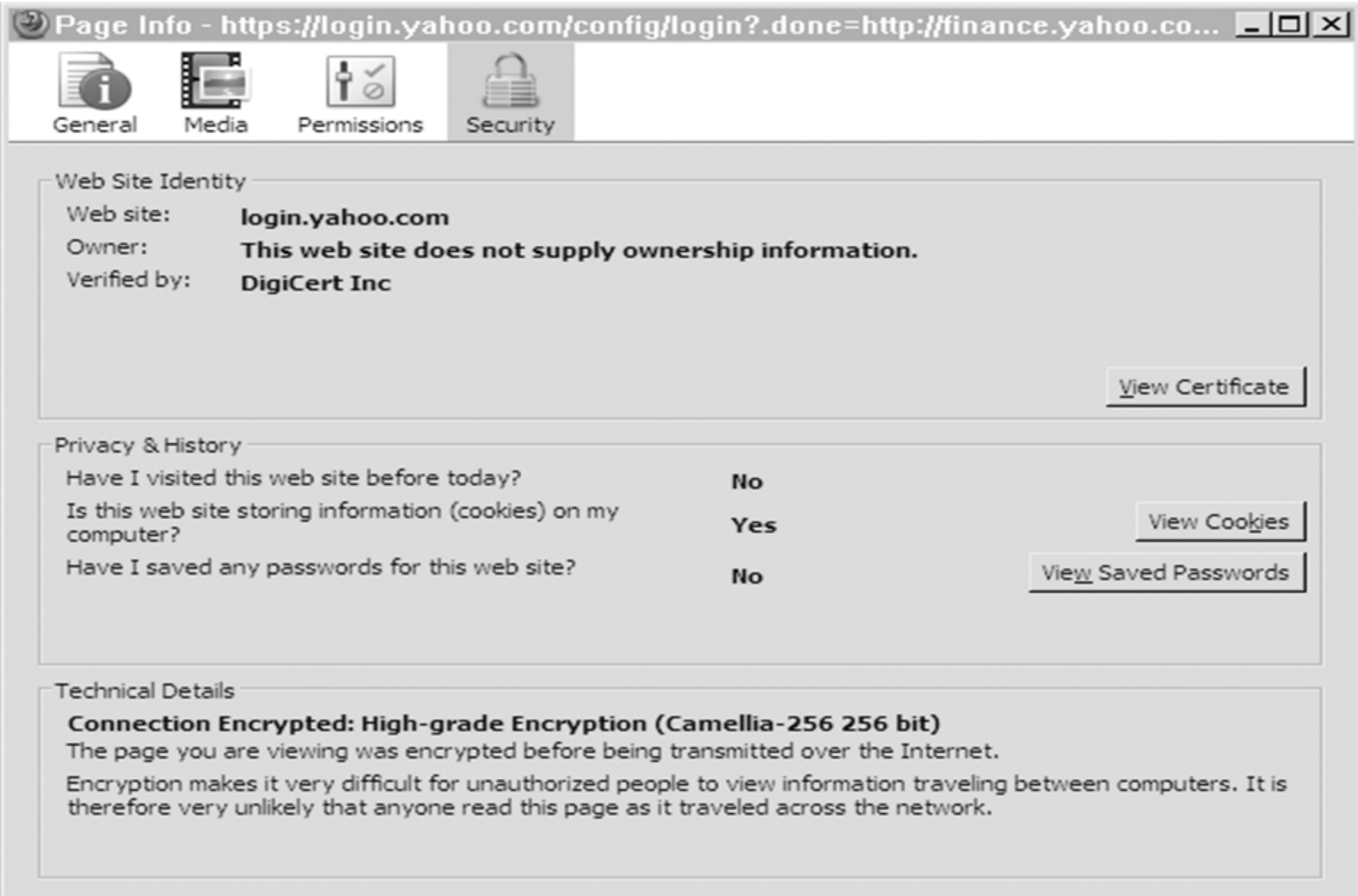
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SSL Cipher Suites (Partial List)

Cipher Suite Identifier	**Algorithms Used**
TLS_NULL_WITH_NULL_NULL	No authentication, no encryption, no hash function
TLS_RSA_WITH_NULL_MD5	RSA authentication, no encryption, MD5 hash function
TLS_RSA_EXPORT_WITH_RC4_40_MD5	RSA authentication with limited key length, RC4 encryption with a 40-bit key, MD5 hash function
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA authentication, triple DES encryption, SHA-1 hash function
TLS_RSA_WITH_AES_128_CBC_SHA	RSA authentication, AES with a 128-bit key encryption, SHA-1 hash function
TLS_RSA_WITH_AES_256_CBC_SHA	RSA authentication, AES with a 256-bit key encryption, SHA-1 hash function
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA authentication, AES with a 128-bit key encryption, SHA-256 hash function
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA authentication, AES with a 256-bit key encryption, SHA-256 hash function
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	Diffie-Hellman digital signature standard, triple DES encryption, SHA-1 hash function
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA http://www.iana.org/go/rfc5932	RSA digital signature, Camellia encryption with a 256-bit key, SHA-1 hash function
TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384	Elliptic curve cryptosystem digital signature algorithm, Aria encryption with a 256-bit key, SHA-384 hash function

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

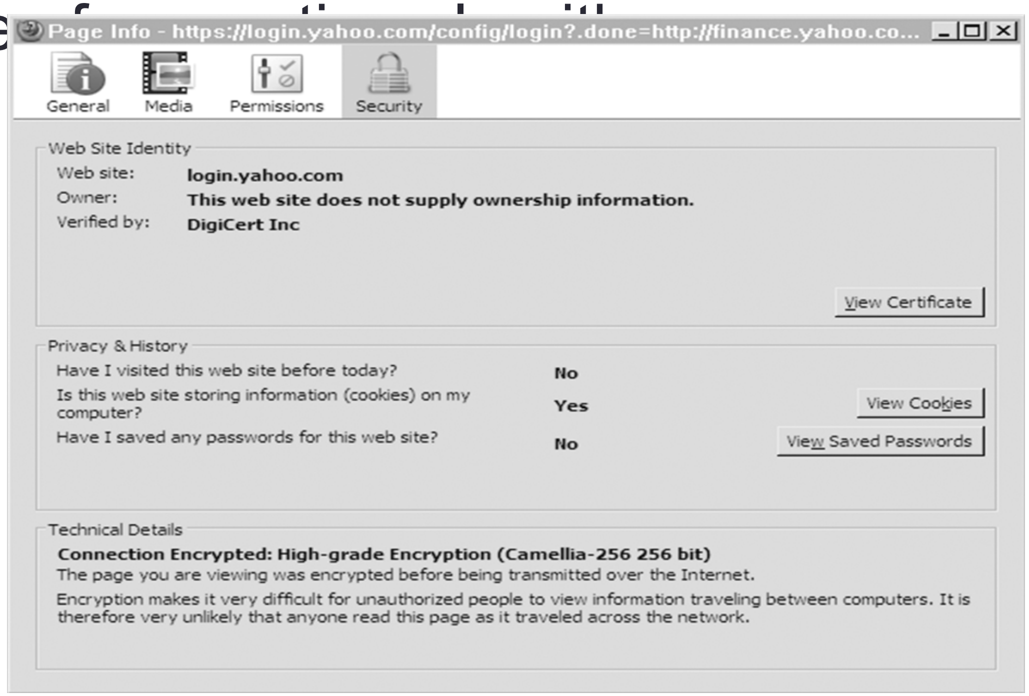
SSL Session Established



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SSL Session Established

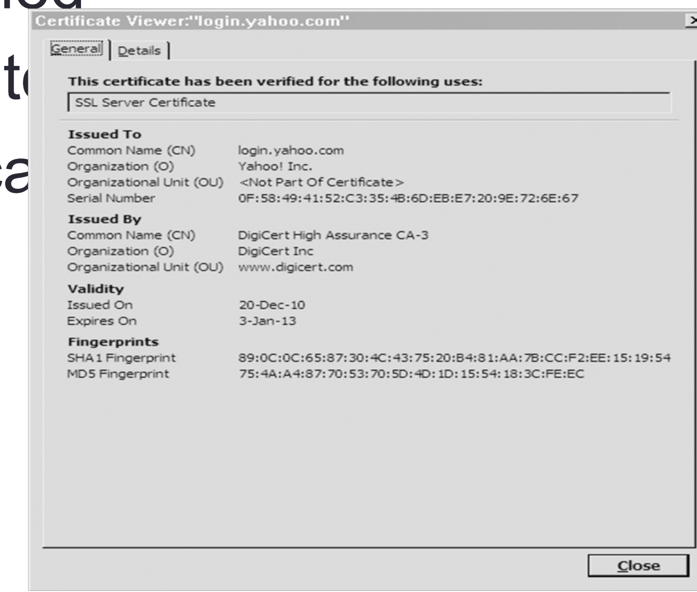
- SSL session dialog includes the following:
  - Site that is verified
  - The certificate authority
  - The choice



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

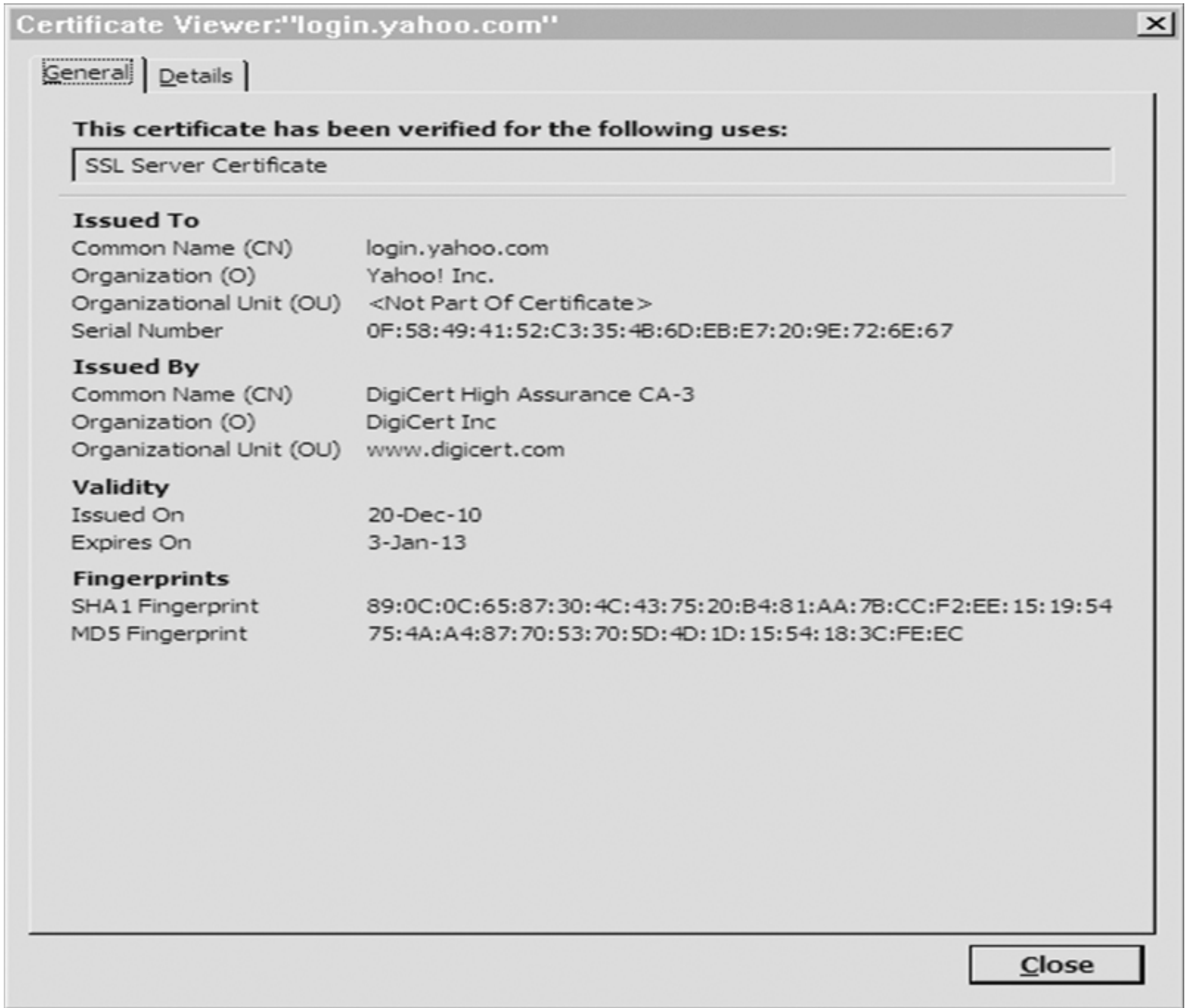
SSL Certificate

- Certificate details:
  - The domain name being certified
  - The company that owns the site
  - The CA that issued the certificate
  - The relevant dates



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

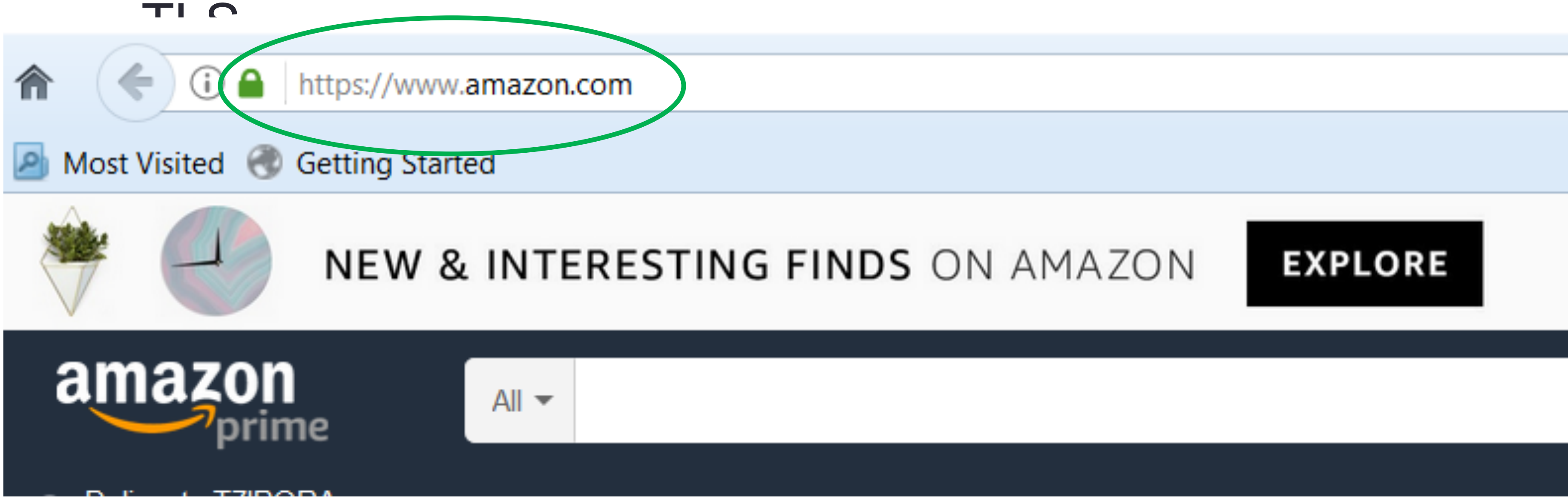
SSL Certificate



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

TLS/SSL

- HTTPS (HTTP Secure) is an adaptation of HTTP for secure communication
  - In HTTPS, the communication protocol is encrypted by



HTTPS/SSL

- https://www.youtube.com/watch?v=hExRDVZHhig

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Onion Routing

- Both in link and end-to-end encryption, data is secured by addressing data is not
  - Volume may be visible to eavesdropping
- A technique for anonymous communication over a computer network
  - Enables untraceable data transmission
- Messages are encapsulated in layers of encryption, analogous to layers of an onion

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Onion Routing

- Onion routing prevents an eavesdropper from learning source, destination, or content of data
  - in transit in a network
- This is particularly helpful for evading authorities
  - such as when users in oppressive countries want to communicate freely with the outside world

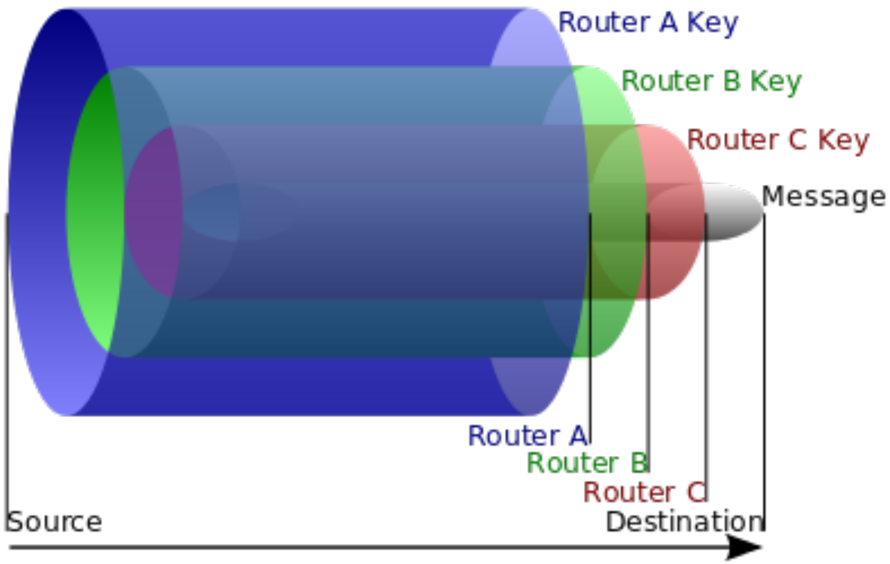
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Onion Routing

- Uses asymmetric cryptography, as well as layers of intermediate hosts, so that:
  - The intermediate host that sends the message to the ultimate destination cannot determine the original sender
  - The host that received the message from the original sender cannot determine the ultimate destination

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Onion Routing Example



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Onion Routing Example

- The source of the data sends the onion to Router A
- Router A removes a layer of encryption to learn only where to send it next and where it came from
  - Router A does not know if sender is the origin or just another node
- Router A sends it to Router B, which decrypts another layer to learn its next destination.
- Router B sends it to Router C, which re the final layer of encryption
- Router C transmits the original message to its destination

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Tor (The Onion Router) Project

- Uses onion routing to protect again network analysis
- Transfers communications around a distributed network
  - Run by volunteers around world
- Prevents outsiders from learning what sites users visit
- Prevents sites from learning user's physical location
- https://www.youtube.com/user/TheTorProject/

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Virtual Private Networking (VPN)

- Link encryption can give a network's users the sense that they are on a private network
  - even when it is part of a public network.
- When applied at the link level, the encrypting and decrypting are invisible to users
- This approach is called a **virtual private network** (or **VPN**)

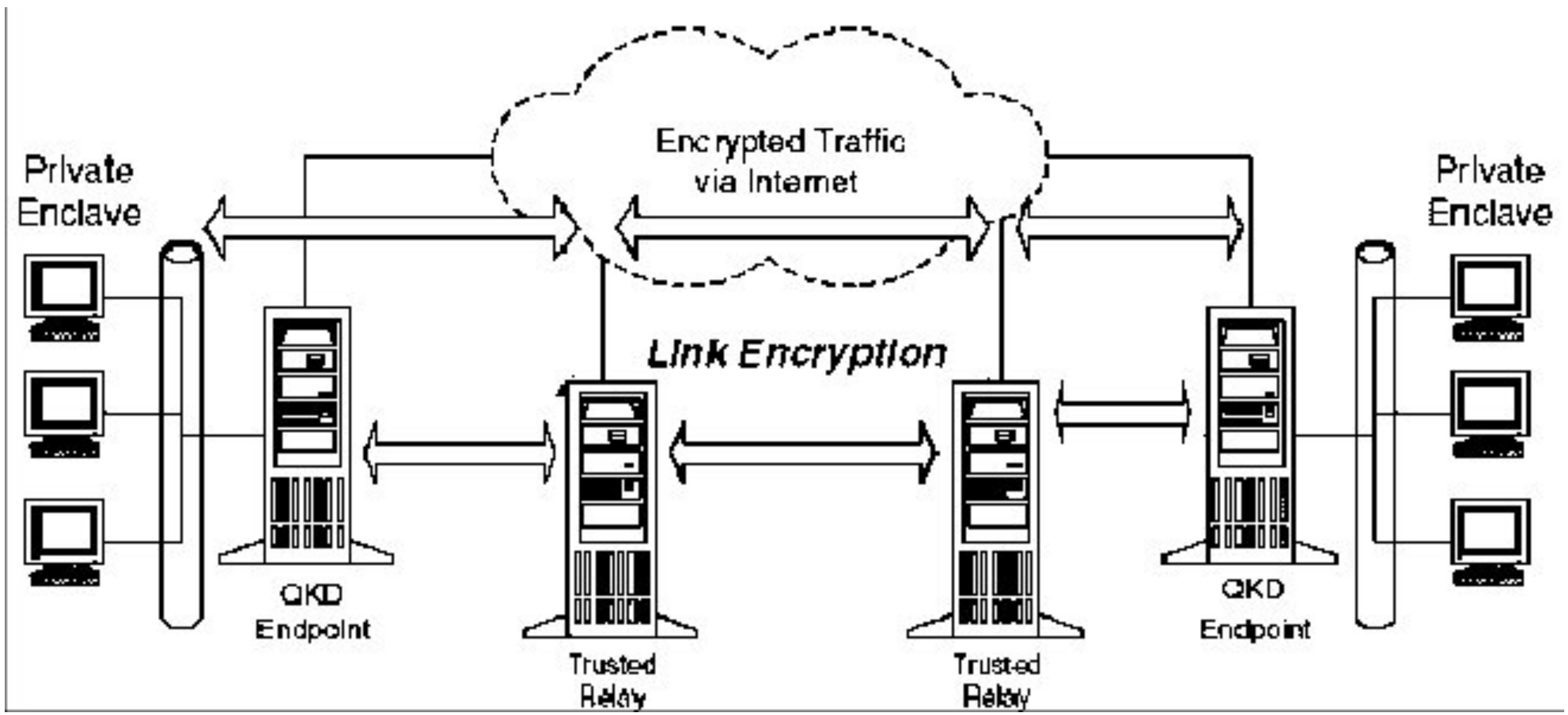
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Link Encryption

- In link encryption data packets are encrypted just before system places them on the physical communications link
- Data packets are decrypted just as they arrive at the destination system.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Link Encryption



https://www.researchgate.net/figure/QKD-network-with-trusted-relays-and-link-encryption_fig2_51893133

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Virtual Private Networking (VPN)

- A technology that allows private networks to be safely extended over long physical distances
  - making use of a public network, such as the Internet, as a means of transport.
- VPN provides guarantees of data confidentiality, integrity, and authentication
  - despite the use of an untrusted network for transmission.
- There are two primary types of VPNs, **remote access VPN** and **site-to-site VPN.**

https://www.techsupportalert.com/content/best-vpn-services.htm

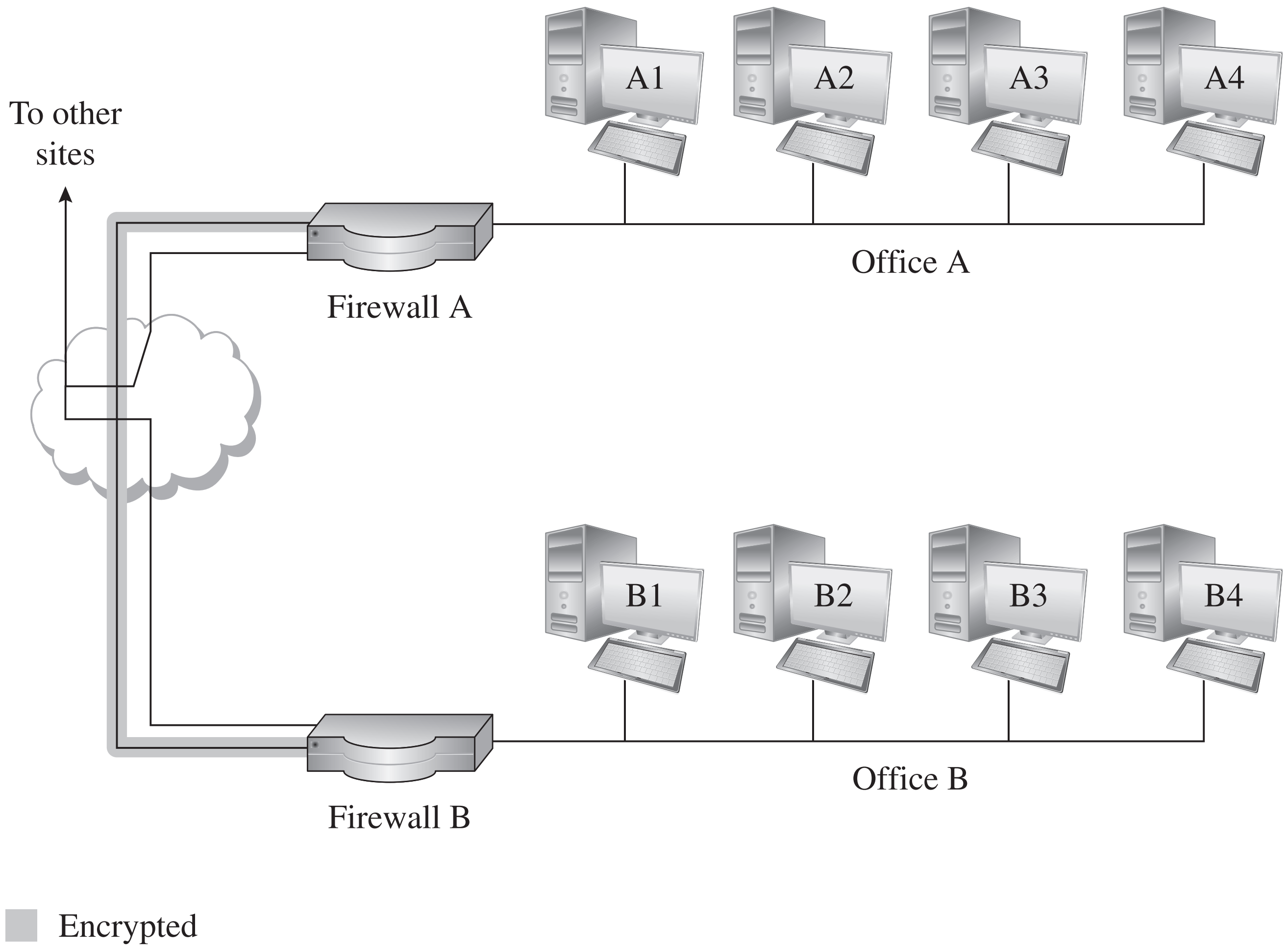
Types of VPNs

- **Remote access** VPNs allow authorized clients to access a private network that is referred to as an **intranet.**
  - For example, an organization may wish to allow employees access to the company network remotely
    - but make it appear as though they are local to their system and even the Internet itself.
  - To accomplish this, the organization sets up a VPN endpoint, known as a **network access server, or NAS**
    - Clients typically install VPN client software on their machines
    - Software handles negotiating a connection to the NAS and facilitating communication.

Types of VPNs

- **Site-to-site** VPN solutions are designed to provide a secure bridge between two or more physically distant networks.
  - Before VPN, organizations wishing to safely bridge their private networks purchased expensive leased lines
    - to directly connect their intranets with cabling.

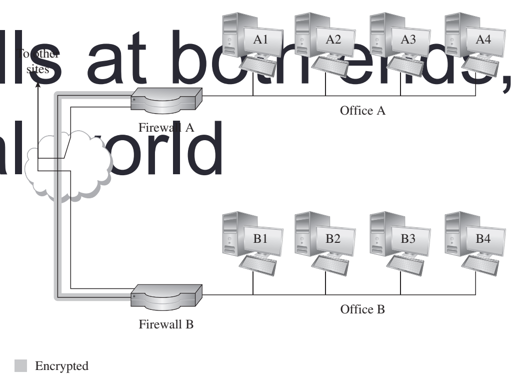
Virtual Private Networks (VPN) Example



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

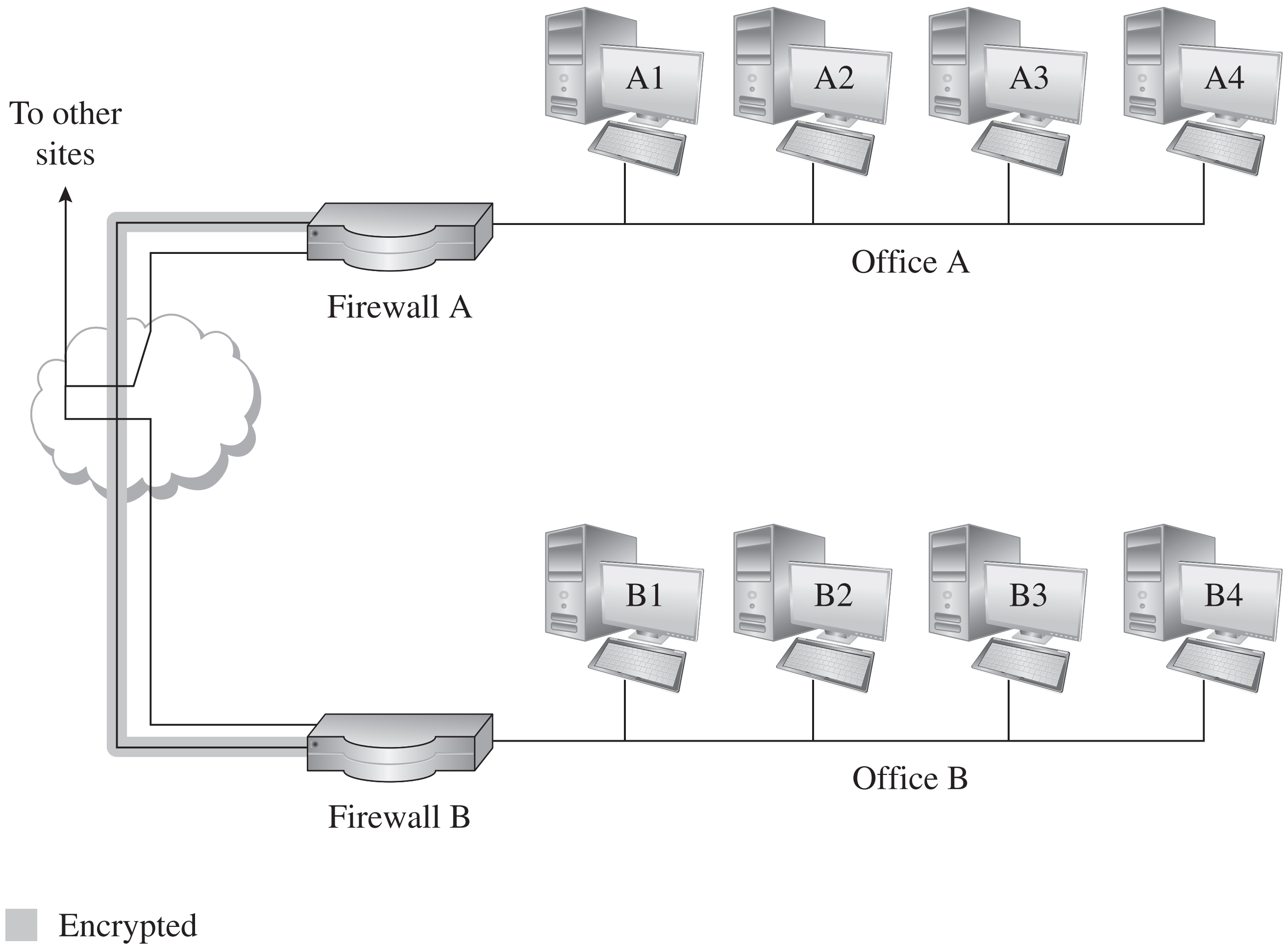
Virtual Private Networks (VPN) Example

- An encrypted tunnel provides confidentiality and integrity for communication between two sites
  - over public networks
- Connects Office A to Office B over the Internet so they appear to their users as one seamless, private network.
- The VPN is terminated by firewalls at both ends, which is often the case in the real world



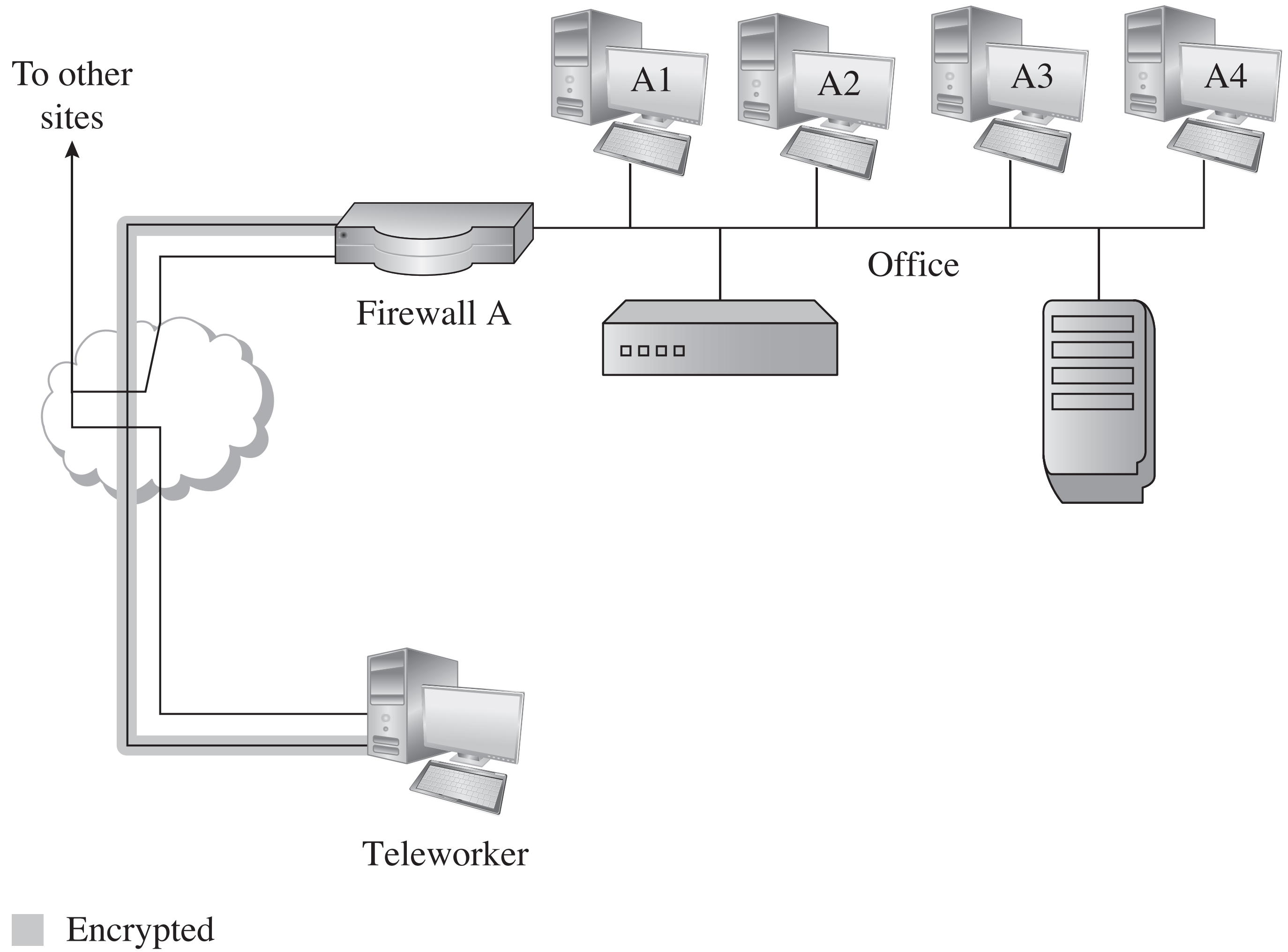
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Virtual Private Networks (VPN) Example



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

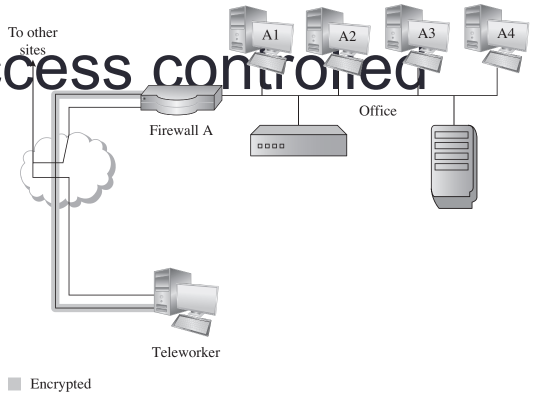
VPN (cont.) – Example 2



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

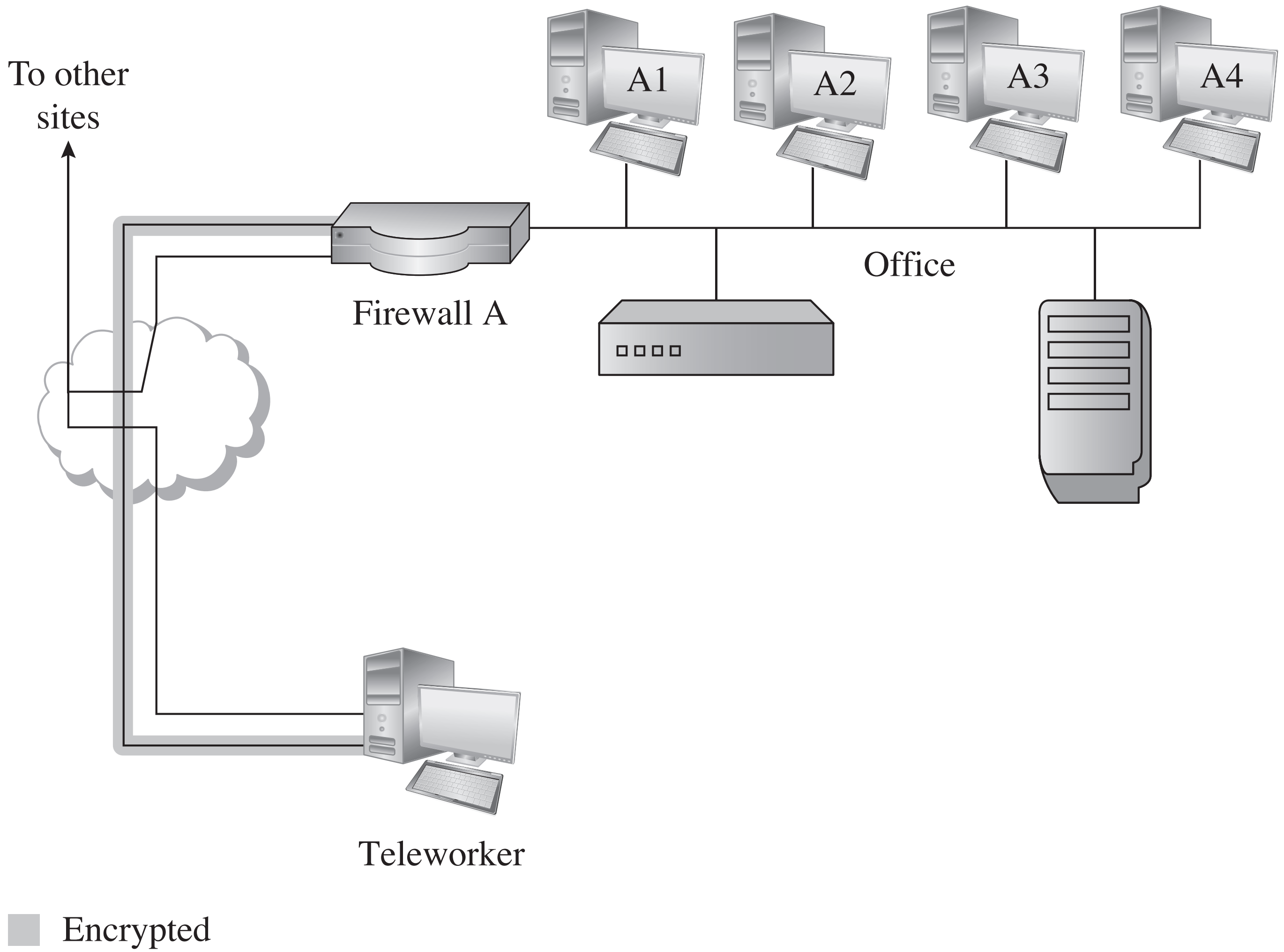
VPN (cont.) – Example 2

- A teleworker uses a VPN to connect to a remote office.
- The teleworker authenticates to the firewall
  - The firewall is acting as a VPN server
- The firewall passes that authentication information to the servers in the office
  - so teleworker can be appropriately access controlled data



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

VPN (cont.) – Example 2



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

- Questions?