E-mail

- Chapter 5

Learning Objectives

- Understand the need for secure e-mail
- Outline benefits of PGP and S/MIME
- Understand e-mail vulnerabilities and how to safeguard against them
- Explain the dangers posed by e-mail hoaxes and spam, as well as actions that can be taken to counteract them

FORESEC

Challenges to Utility and Productivity Gains Offered by E-mail

- E-mail security
- Floods of spam
- Hoaxes

FORESEC

E-mail Security Technologies

- Two main standards
  - Pretty good privacy (PGP)
  - Secure/Multipurpose Internet Mail Extension (S/MIME)
- These competing standards:
  - Seek to ensure integrity and privacy of information by wrapping security measures around e-mail data itself
  - Use public key encryption techniques (alternative to securing communication link itself, as in VPN)

FORESEC

Secure E-mail and Encryption

- Secure e-mail
  - Uses cryptography to secure messages transmitted across insecure networks
- Advantages of e-mail encryption
  - E-mail can be transmitted over unsecured links
  - E-mail can be stored in encrypted form
- Key cryptography concepts
  - Encryption
  - Digital signatures
  - Digital certificates

FORESEC

Main Features of Secure E-mail

- Confidentiality
- Integrity
- Authentication
- Nonrepudiation

Encryption

- Passes data and a value (key) through a series of mathematical formulas that make the data unusable and unreadable
- To recover information, reverse the process using the appropriate key
- Two main types
  - Conventional cryptography
  - Public key cryptography

Encryption

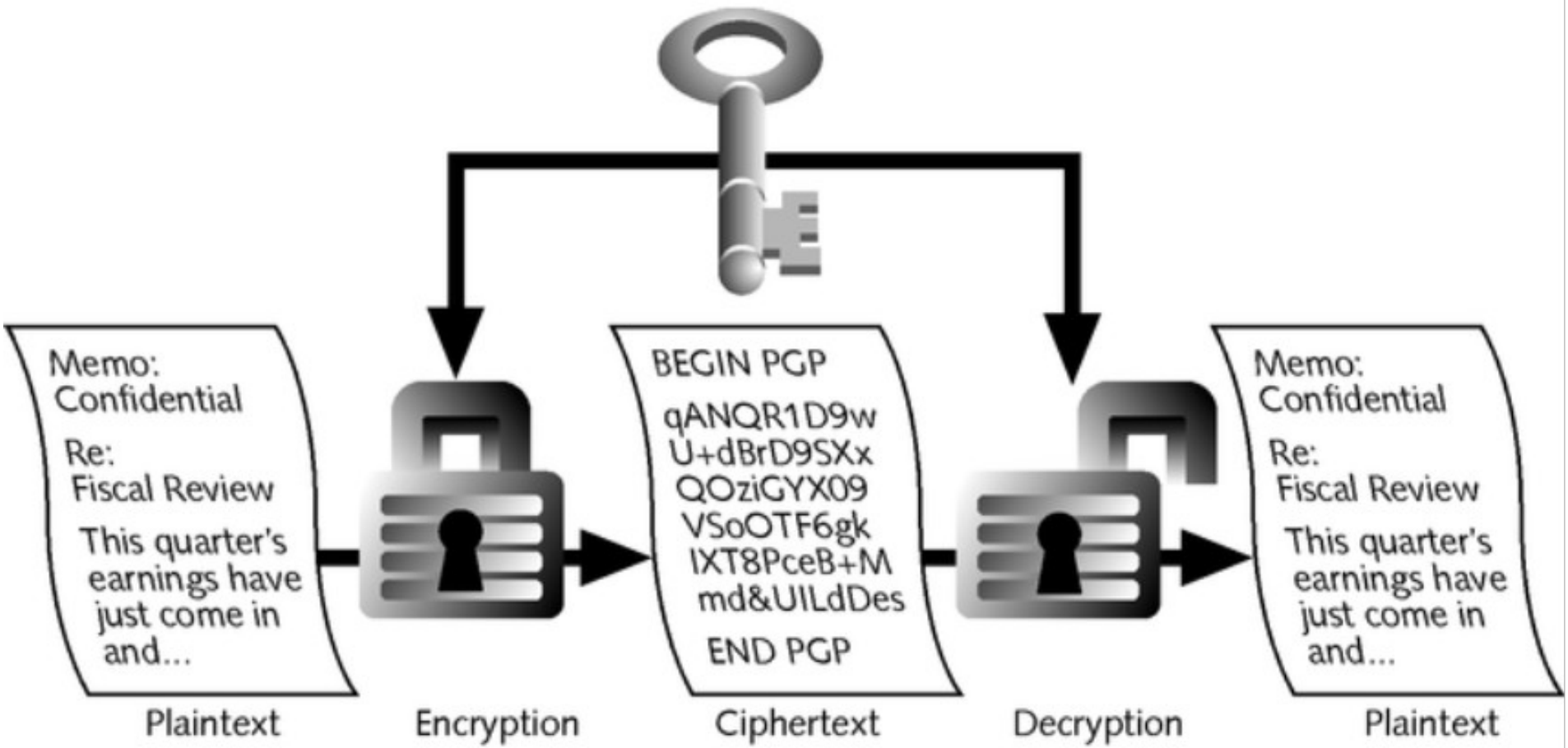

Figure 5-1 How conventional encryption works

FORESEC

Hash Functions

- Produce a message digest that cannot be reversed to produce the original
- Two major hash functions in use
  - SHA-1 (Secure Hash Algorithm 1)
  - MD5 (Message Digest algorithm version 5)

Digital Signatures

- Electronic identification of a person or thing created by using a public key algorithm
- Verify (to a recipient) the integrity of data and identity of the sender
- Provide same features as encryption, except confidentiality
- Created by using hash functions

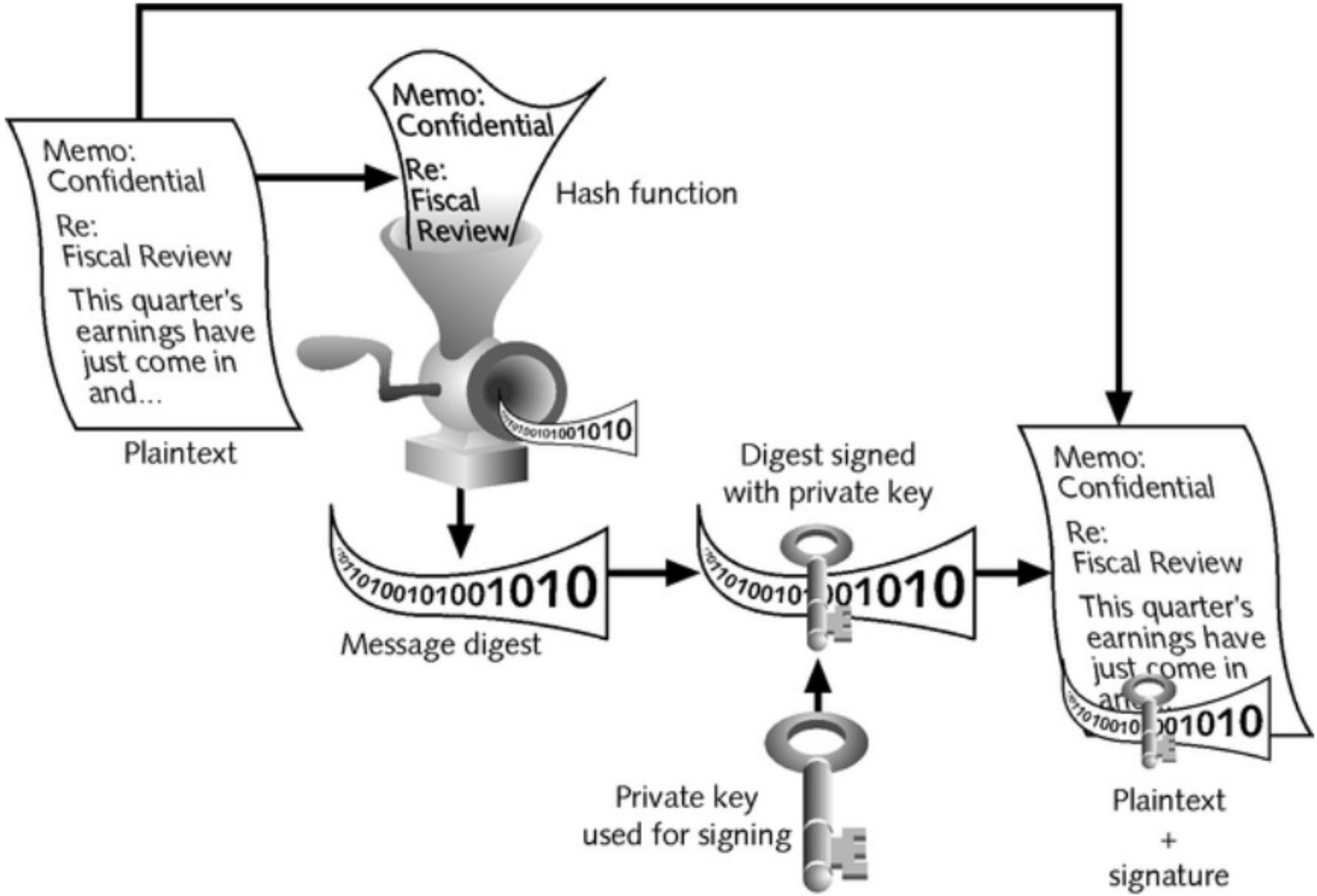

Figure 5-2 How digital signatures are created

FORESEC

Digital Certificates

- Electronic document attached to a public key by a trusted third party
- Provide proof that the public key belongs to a legitimate owner and has not been compromised
- Consist of:
  - Owner's public key
  - Information unique to owner
  - Digital signatures or an endorser

FORESEC

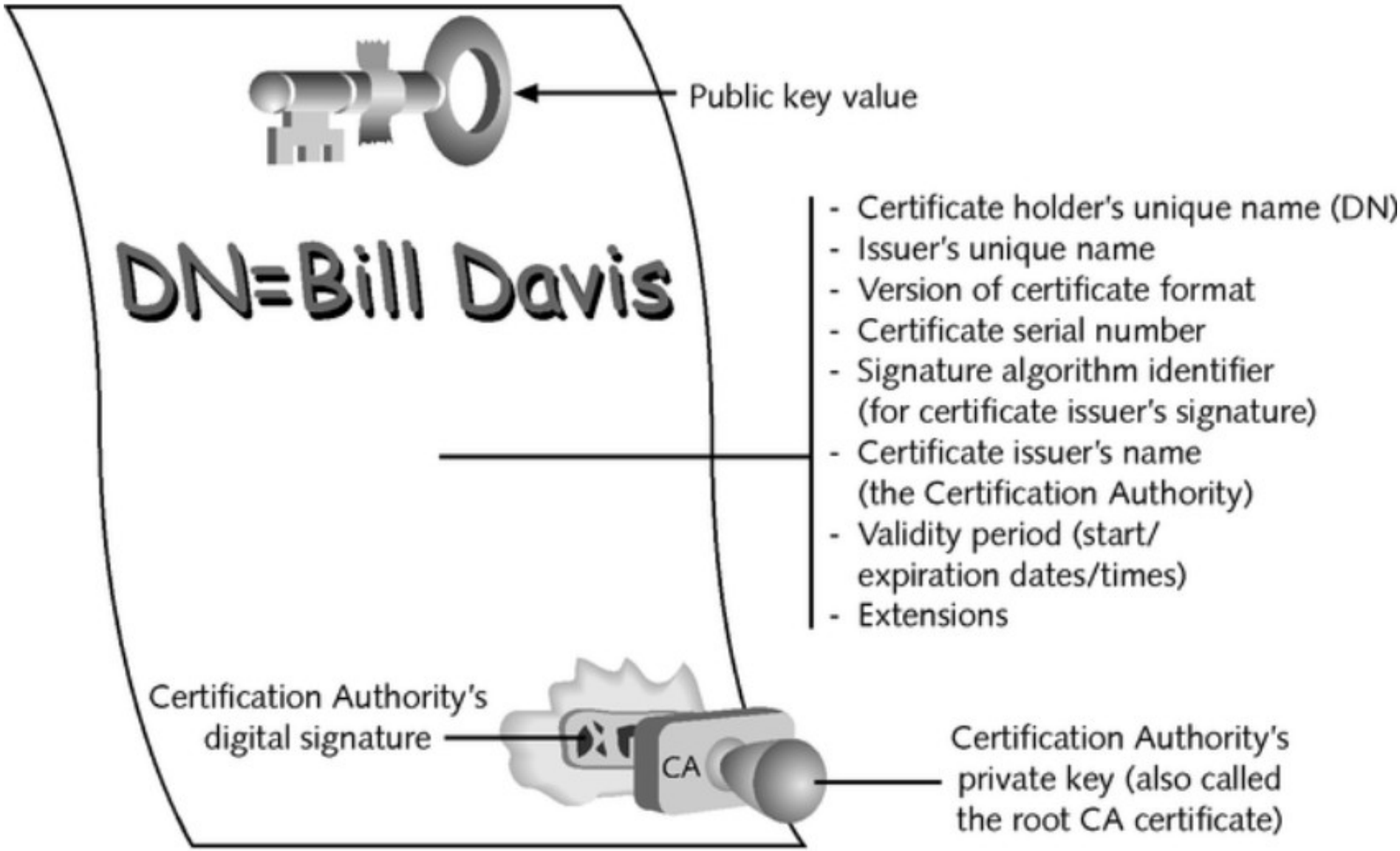

Figure 5-3 A digital certificate

FORESEC

Combining Encryption Methods

- Hybrid cryptosystems
  - Take advantage of symmetric and public key cryptography
  - Example: PGP/MIME
- Conventional encryption
  - Fast, but results in key distribution problem
- Public key encryption
  - Private key and public key

Public Key Encryption

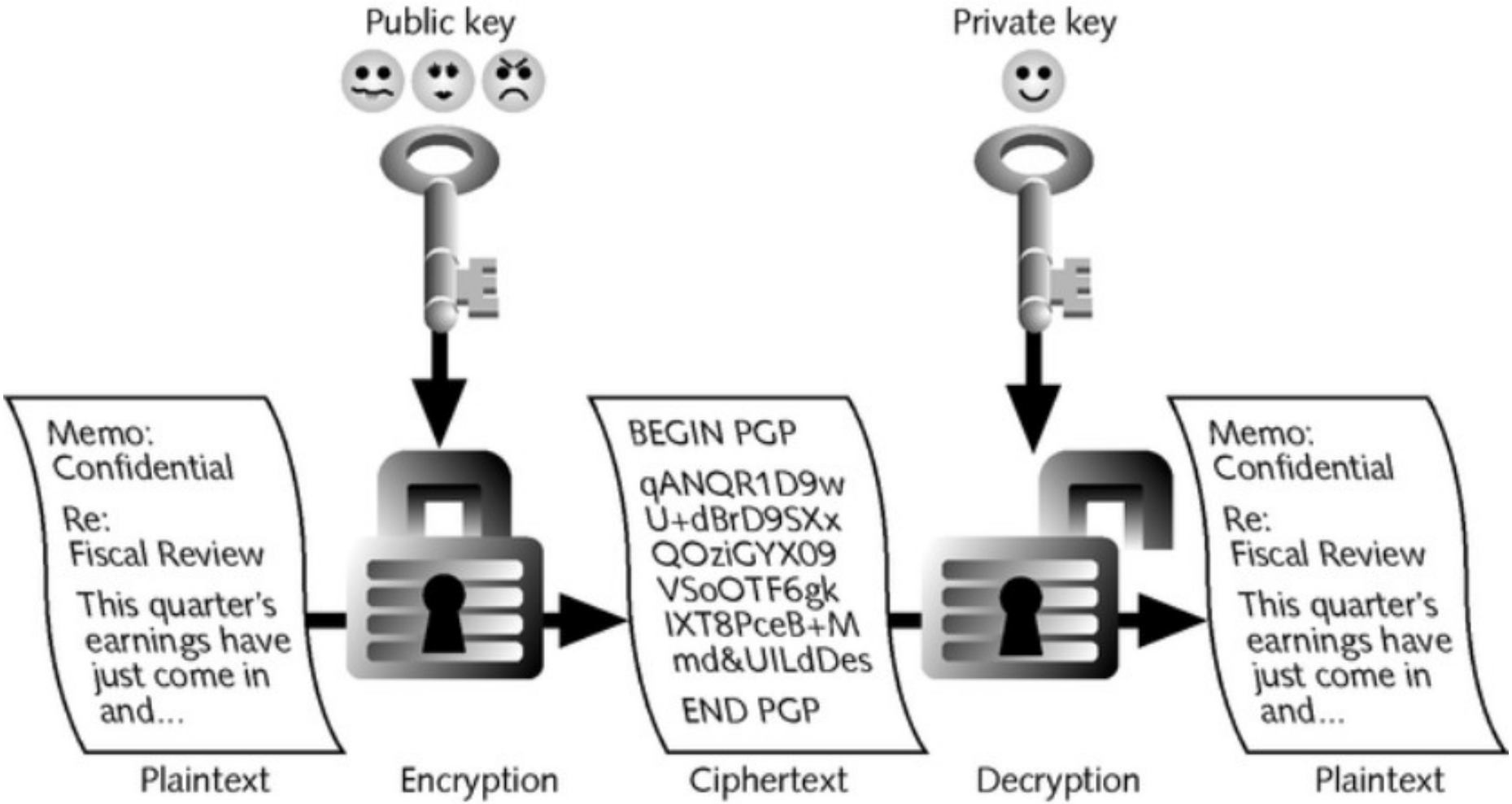

Figure 5-4 How public key encryption works

FORESEC

How Secure E-mail Works

- Encryption
  1. Message is compressed
  2. Session key is created
  3. Message is encrypted using session key with symmetrical encryption method
  4. Session key is encrypted with an asymmetrical encryption method
  5. Encrypted session key and encrypted message are bound together and transmitted to recipient
- Decryption: reverse the process

FORESEC

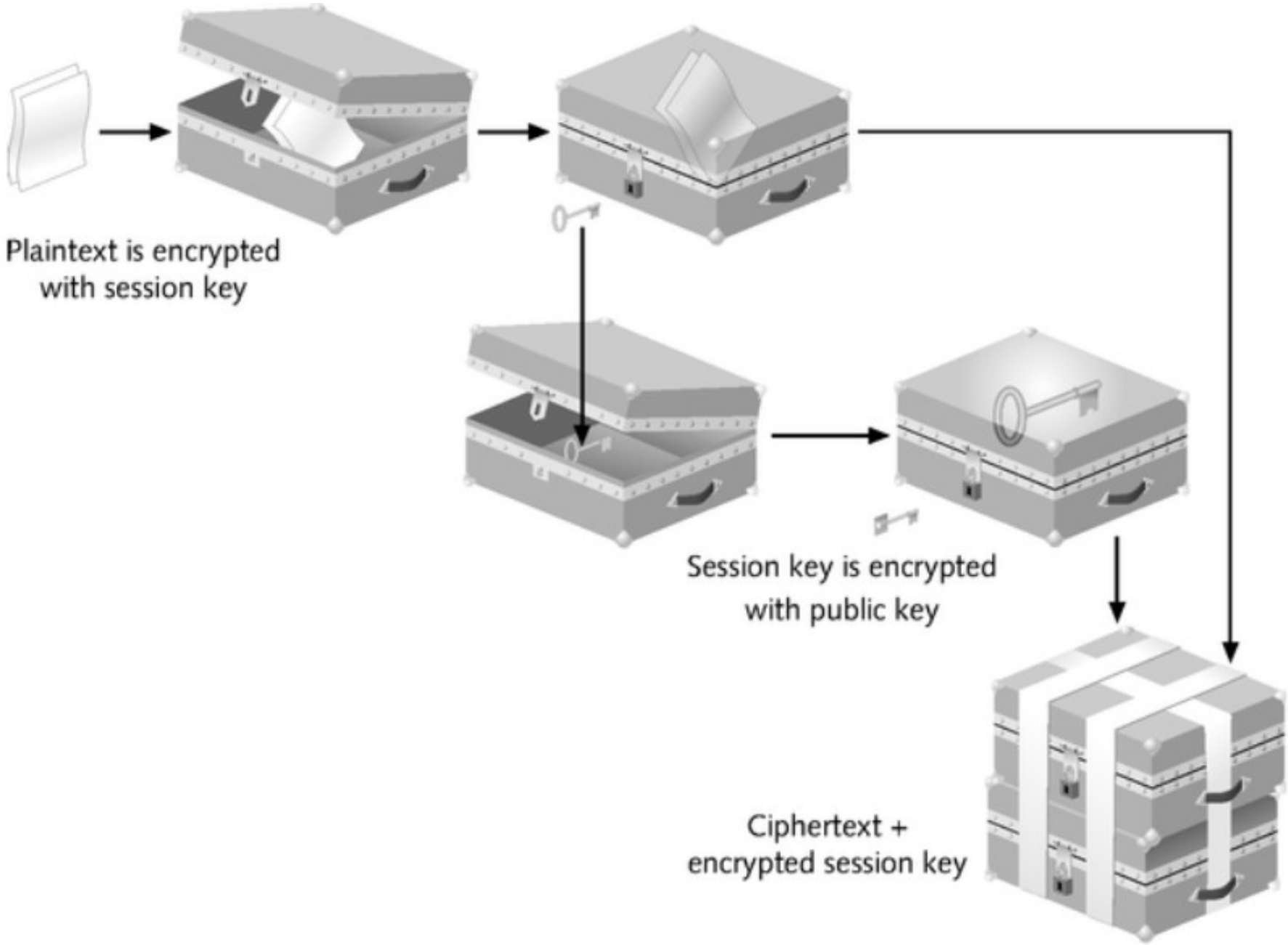

Figure 5-5 How secure email encryption works

FORESEC

Secure E-mail Decryption

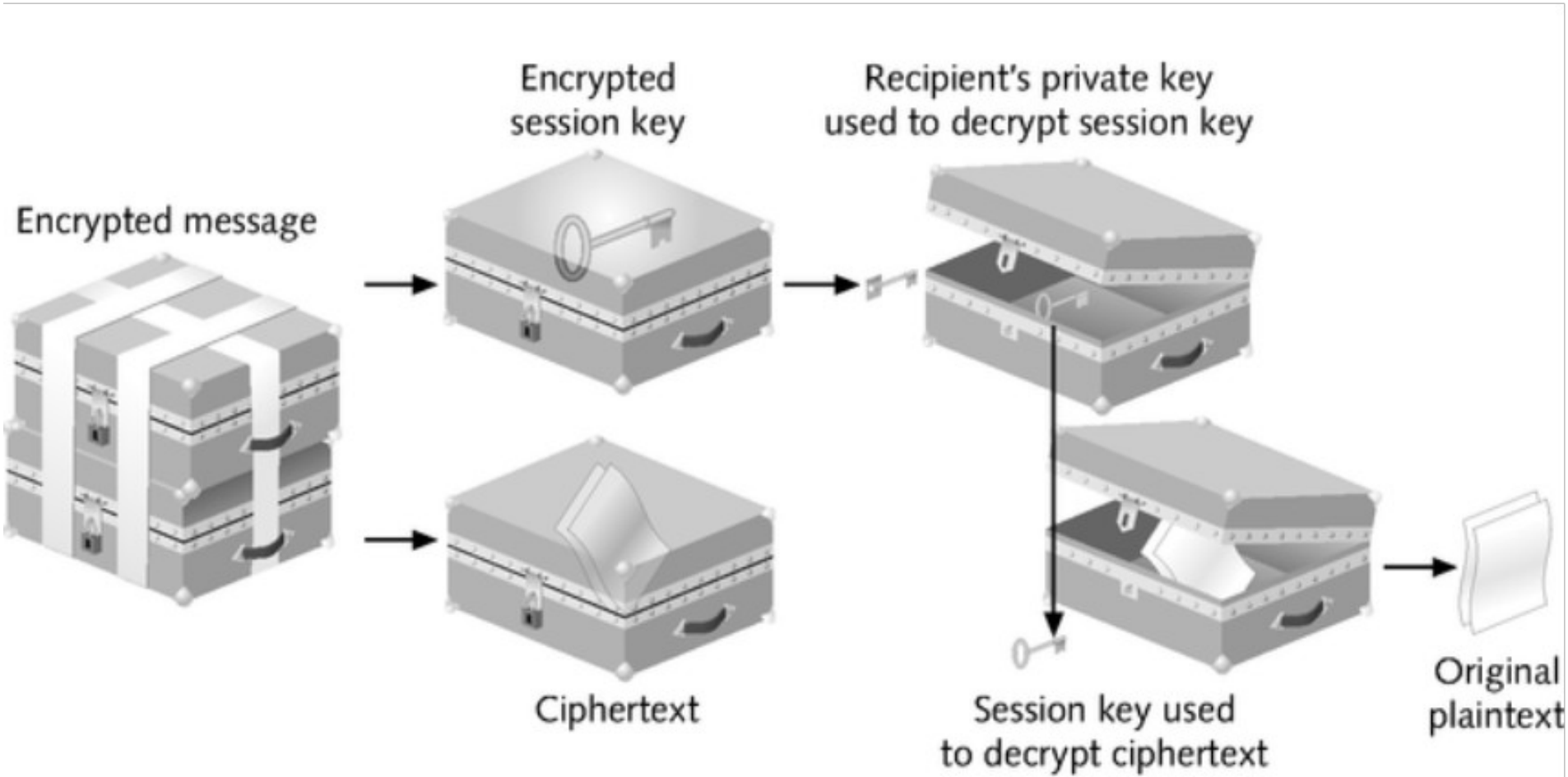

Figure 5-6 How secure email decryption works

Background on PGP

- Current de facto standard
- Written by Phil Zimmerman 1991
- Supports major conventional encryption methods
  - CAST
  - International Data Encryption Algorithm (IDEA)
  - Triple Data Encryption Standard (3DES)
  - Twofish

PGP Certificates

- More flexible and extensible than X.509 certificates
- A single certificate can contain multiple signatures

PGP Certificate Format

Table 5-1 PGP certificate format

Certificate	Certificate Format
PGP version number	Version of PGP, which was used to create the key associated with the certificate
Certificate holder's public key	Public portion of your key pair, together with the algorithm of the key, which is either RSA, RSA Legacy, DH), or **Digital Signature Algorithm (DSA)**
Certificate holder's information	Identity information about the user, such as his or her name, user ID, e-mail address, ICQ number, photograph, etc.
Digital signature of the certificate owner	Signature created with the private key corresponding to the public key associated with this certificate
Certificate's validity period	Start date/time and expiration date/time; indicates when the certificate will expire
Preferred symmetric encryption algorithm for the key	Encryption algorithm to which the certificate owner prefers to have information encrypted; the supported algorithms are CAST, IDEA, 3DES, and Twofish

FORESEC

S/MIME

- Specification designed to add security to e-mail messages in MIME format
- Security services
  - Authentication (using digital signatures)
  - Privacy (using encryption)

FORESEC

What S/MIME Defines

- Format for MIME data
- Algorithms that must be used for interoperability
  - RSA
  - RC2
  - SHA-1
- Additional operational concerns
  - ANSI X.509 certificates
  - Transport over the Internet

S/MIME Background

- Four primary standards
  - RFC 2630
    - Cryptographic Message Syntax
  - RFC 2633
    - S/MIME version 3 Message Specification
  - RFC 2632
    - S/MIME version 3 Certificate Handling
  - RFC 2634
    - Enhanced Security Services for S/MIME

S/MIME Encryption Algorithms

- Three symmetric encryption algorithms
  - DES
  - 3DES
  - RC2
- PKCS (Public Key Cryptography Standards)
- S/MIME prevents exposure of signature information to eavesdropper
  - Applies digital signature first; then encloses signature and original message in an encrypted digital envelope

X.509 Certificates

- Rather than define its own certificate type (like PGP), S/MIME relies on X.509
- Issued by a certificate authority (CA)

Table 5-2 X.509 certificate format

Certificate	Certificate Format
X.509 version	Identifies which version of the X.509 standard applies to this certificate, which in turn determines what information can be specified in it
Certificate holder's public key	Public key of the certificate holder, together with an algorithm identifier that specifies which cryptosystem the key belongs to and any associated key parameters
Serial number of the certificate	Unique serial number to distinguish it from other certificates issued. This information is used in numerous ways; for example, when a certificate is revoked, its serial number is placed on a certificate revocation list (CRL).
Certificate holder's distinguished name (DN)	Intended to be unique across the Internet, a DN consists of multiple subsections and may look something like this: CN=Jonathan Public, EMAIL=jonathanpublic@hotmail.com, OU=Security Team, O=Consulting Inc., C=US (These refer to the subject's Common Name, Organizational Unit, Organization, and Country.)
Certificate's validity period	Start date/time and expiration date/time
Unique name of the certificate issuer	Unique name of the entity that signed the certificate. This is normally a CA. Using the certificate implies trusting the entity that signed this certificate.
Digital signature of the issuer	Signature using the private key of the entity that issued the certificate
Signature algorithm identifier	Algorithm used by the CA to sign the certificate

FORBSEC

S/MIME Trust Model: Certificate Authorities

- Purely hierarchical model
- Line of trust goes up the chain to a CA, whose business is verifying identity and assuring validity of keys or certificates

FORESEC

Differences Between PGP and S/MIME

Features	***S/MIME3***	***OpenPGP***
Structure of messages	Binary, based on CMS	PGP
Structure of digital certificates	X.509	PGP
Algorithm: symmetric encryption	3DES	3DES
Algorithm: digital signature	Diffie-Hellman	ElGamal

continued…

Differences Between PGP and S/MIME

Features	***S/MIME3***	***OpenPGP***
Algorithm: hash	SHA-1	SHA-01
MIME encapsulation for signed data	Choice of multipart/signed or CMS format	Multipart/signed with ASCII armor
MIME encapsulation for encrypted data	Application/ PKCS#7-MIME	Multipart/ encrypted
Trust model	Hierarchical	Web of trust

continued…

Differences Between PGP and S/MIME

Features	***S/MIME3***	***OpenPGP***
Marketplace adoption	Growing quickly	Current encryption standard
Marketplace advocates	Microsoft, RSA, VeriSign	Some PGP, Inc. products absorbed into McAfee line
Ease of use	Configuration not intuitive; must obtain and install certificates; general use straight-forward	Configuration not intuitive; must create certificates; general use straight-forward

continued…

Differences Between PGP and S/MIME

Features	***S/MIME3***	***OpenPGP***
Software	Already integrated in Microsoft and Netscape products	PGP software must be downloaded and installed
Cost of certificates	Must be purchased from CA; yearly fee	PGP certificates can be generated by anyone; free
Key management	Easy, but you must trust CA	Harder; user must make decisions on validity of identities

continued…

Differences Between PGP and S/MIME

Features	***S/MIME3***	***OpenPGP***
Compatibility	Transparently works with any vendor's MIME e-mail client, but not compatible with non-MIME e-mail formats	Compatible with MIME and non-MIME e-mail formats, but recipient must have PGP installed
Centralized management	Possible through PKI	Status is in doubt

E-mail Vulnerabilities

Table 5-4 E-mail vulnerabilities

Attack	Vulnerability	Solution
Eavesdropping	Lack of confidentiality; because e-mail is sent in clear text, it can be read in transit	E-mail encryption for communications that require confidentiality; note that encrypted messages cannot be effectively scanned for viruses until they reach the desktop and are decrypted
Spoofing and masquerading	Lack of authentication; dummy e-mail accounts can be set up to pose as trusted businesses and trick users into giving over credit card numbers and other types of information	Digital certificates issued by a trusted certificate authority prove to the customer that the sender of an e-mail really is who he or she says it is
Man-in-the-middle attack, session hijacking	Lack of authentication; by tricking e-mail servers to send their data through a third node, an attacker can pose as one or both people in an e-mail exchange	By digitally signing their data, the two parties can authenticate each other and be sure of the sender's identity; they also gain the same certainty by encrypting their e-mails

FORESEC

continued…

E-mail Vulnerabilities

Table 5-4 E-mail vulnerabilities (continued)

Attack	Vulnerability	Solution
Data manipulation	Lack of integrity; because e-mail data is sent as plaintext, it can be modified or changed in transit	E-mail encryption stops both the reading and manipulation of e-mails; digital signatures on e-mails ensure that if the data is changed in transmission, the recipient will know
Malware	Malicious software; viruses, Trojan horses, backdoors, and worms can spread through e-mail, destroy data, and be part of a DoS attack on e-mail servers	Virus filtering software on desktops, servers, and Internet gateways
Social engineering	Repudiation; because a variety of e-mail attacks are possible, users can claim that they did not send a given message	E-mail encryption and digital signatures provide nonrepudiation, because the sender must have their own digital certificate and passphrase to use them
Password guessing	A wide variety of password guessing attacks can be used against a PGP key or X.509 digital certificate	Choose a strong passphrase for your certificate or key
Information leaks	Users can send sensitive company data to other untrusted networks or to untrusted parties	Train users on acceptable use of e-mail; use an e-mail content filtering solution

FORESEC

Spam

- Act of flooding the Internet with many copies of the same message in an attempt to force the message on people who would not otherwise choose to receive it
- Unrequested junk mail

E-mail Spam

- Targets individual users with direct mail messages
- Creates lists by:
  - Scanning Usenet postings
  - Stealing Internet mailing lists
  - Searching the Web for addresses
- Uses automated tools to subscribe to as many mailing lists as possible

Hoaxes and Chain Letters

- E-mail messages with content designed to get the reader to spread them by:
  - Appealing to be an authority to exploit trust
  - Generating excitement about being involved
  - Creating a sense of importance/belonging
  - Playing on people's gullibility/greed
- Do not carry malicious payload, but are usually untrue or resolved

FORESEC

Costs of Hoaxes and Chain Letters

- Lost productivity
- Damaged reputation
- Relaxed attitude toward legitimate virus warnings

FORRESTER

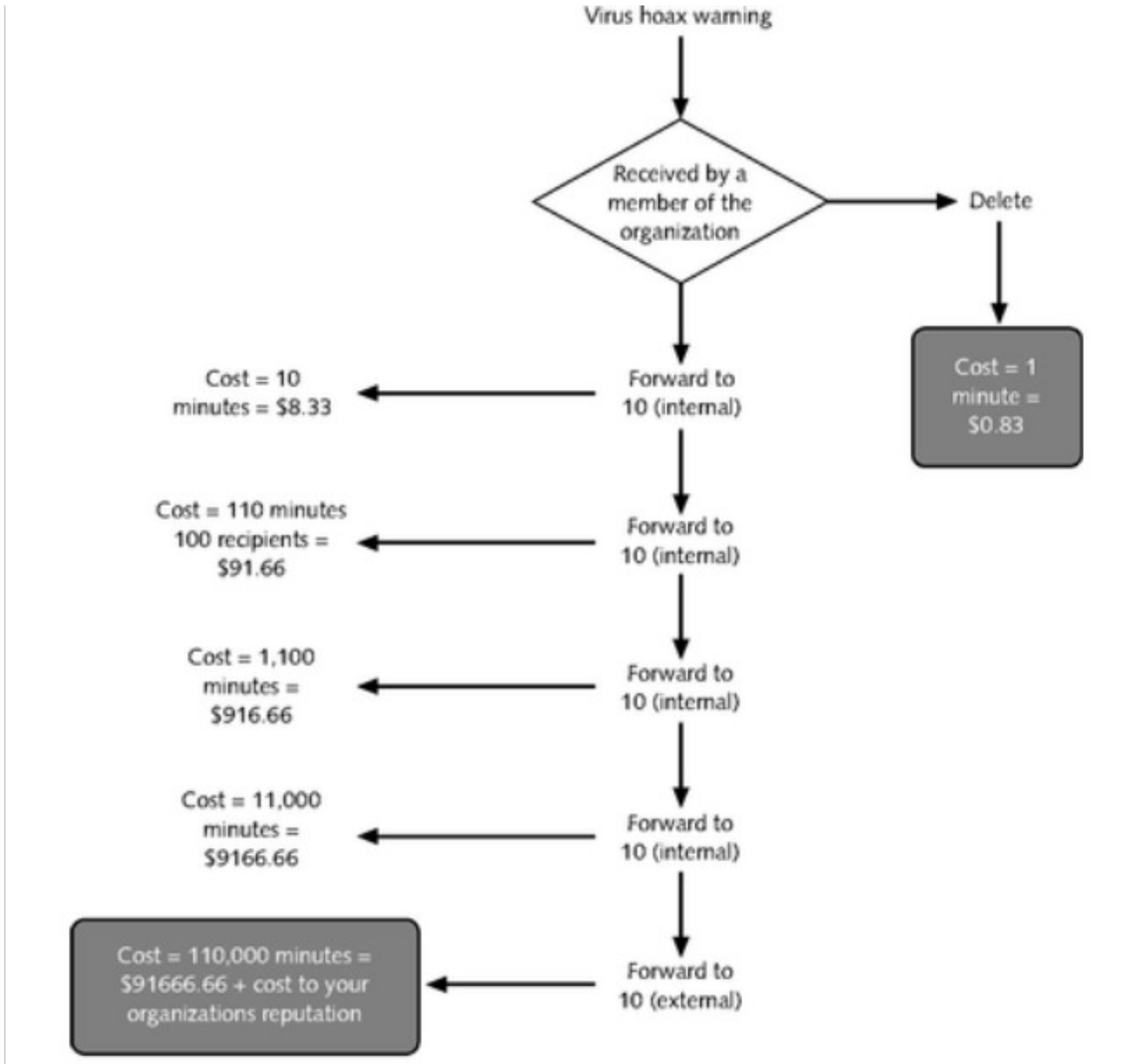

Figure 5-7 What hoaxes and chain letters really cost

FORBSEC

Nuclear Strike Hoax

```
PLEASE FORWARD THIS TO EVERYONE YOU KNOW. THIS IS VERY IMPORTANT.

Virus Update, 1/22/00

Symantec Virus Alert Center

Hello Subscriber,

...A new, deadly type of virus has been detected in the wild. You
should not open any message entitled "LAUNCH NUCLEAR STRIKE NOW",
as this message has been programmed to access NORAD computers in
Colorado and launch a full-scale nuclear strike on Russia and the
former Soviet states. Apparently, a disgruntled ex-Communist
hacker has designed a pernicious VBScript that actually bypasses
the U.S. arsenal's significant security system and takes command
of missiles and bombers directly. By opening the e-mail, you may
be causing Armageddon. Needless to say, Armageddon will wipe out
your hard drive and damage your computer.

Again, we warn you, PLEASE, DO NOT OPEN ANY E-MAIL ENTITLED
"LAUNCH NUCLEAR STRIKE NOW". YOU MAY CAUSE A FULL-SCALE
NUCLEAR HOLOCAUST.
…
VIRUS NAME: ArmaGeddyLee, HappyOrMaybeNot00, OopsWrongButton00
TRANSMITTAL METHOD: VBScript attached to e-mail
HAZARD: Extremely Super High
AREA OF INFECTION: Detected in wild
CHARACTERISTICS: Destroys life on earth via nuclear armageddon

Please forward this warning to everyone you can.
```

Figure 5-8 Nuclear strike virus

FORBSEC

Countermeasures for Hoaxes

- Effective security awareness campaign
- Good e-mail policy
- E-mail content filtering solutions

Guidelines for Hoax Countermeasures

- Create a policy and train users on what to do when they receive a virus warning
- Establish the intranet site as the only authoritative source for advice on virus warnings
- Ensure that the intranet site displays up-to-date virus and hoax information on the home page
- Inform users that if the virus warning is not listed on the intranet site, they should forward it to a designated account

FORESEC

Chapter Summary

- PGP
  - Current de facto e-mail encryption standard
  - Basis of OpenPGP standard
- S/MIME
  - Emerging standard in e-mail encryption
  - Uses X.509 certificates used by Microsoft and Netscape browser and e-mail client software
- E-mail vulnerabilities and scams, and how to combat them
  - Spam
  - Hoaxes and e-mail chain letters

FORESEC