Information Security Management

Chapter 9
Protection Mechanisms

Webster University
Scott Granneman

“People are the missing link
to improving Information Security.
Technology alone can’t solve
the challenges of Information Security.”

-- The Human Firewall Council

Upon completion of this chapter, you should be able to:

Know and understand access control approaches,
including authentication, authorization,
& biometric access controls

Define and identify the various types of firewalls
& the common approaches to firewall implementation

Discuss the current issues in dial-up access & protection

Identify & describe types of intrusion detection systems
& the 2 strategies on which they are based

Discuss cryptography & the encryption process,
& compare & contrast
symmetric & asymmetric encryption

InfoSec is an emerging discipline

Combines efforts of
people, policy, procedures,
education, training, awareness,
& technology
to improve the CIA of
an organization’s information assets

Technical controls alone
cannot ensure a secure IT environment

They’re essential, but
they must be combined
with sound policy
& education, training, & awareness efforts

Some of the most powerful
& widely used
technical security mechanisms
include:

✓ Access controls
✓ Firewalls
✓ Dial-up protection
✓ Intrusion detection systems
✓ Scanning & analysis tools
✓ Encryption systems

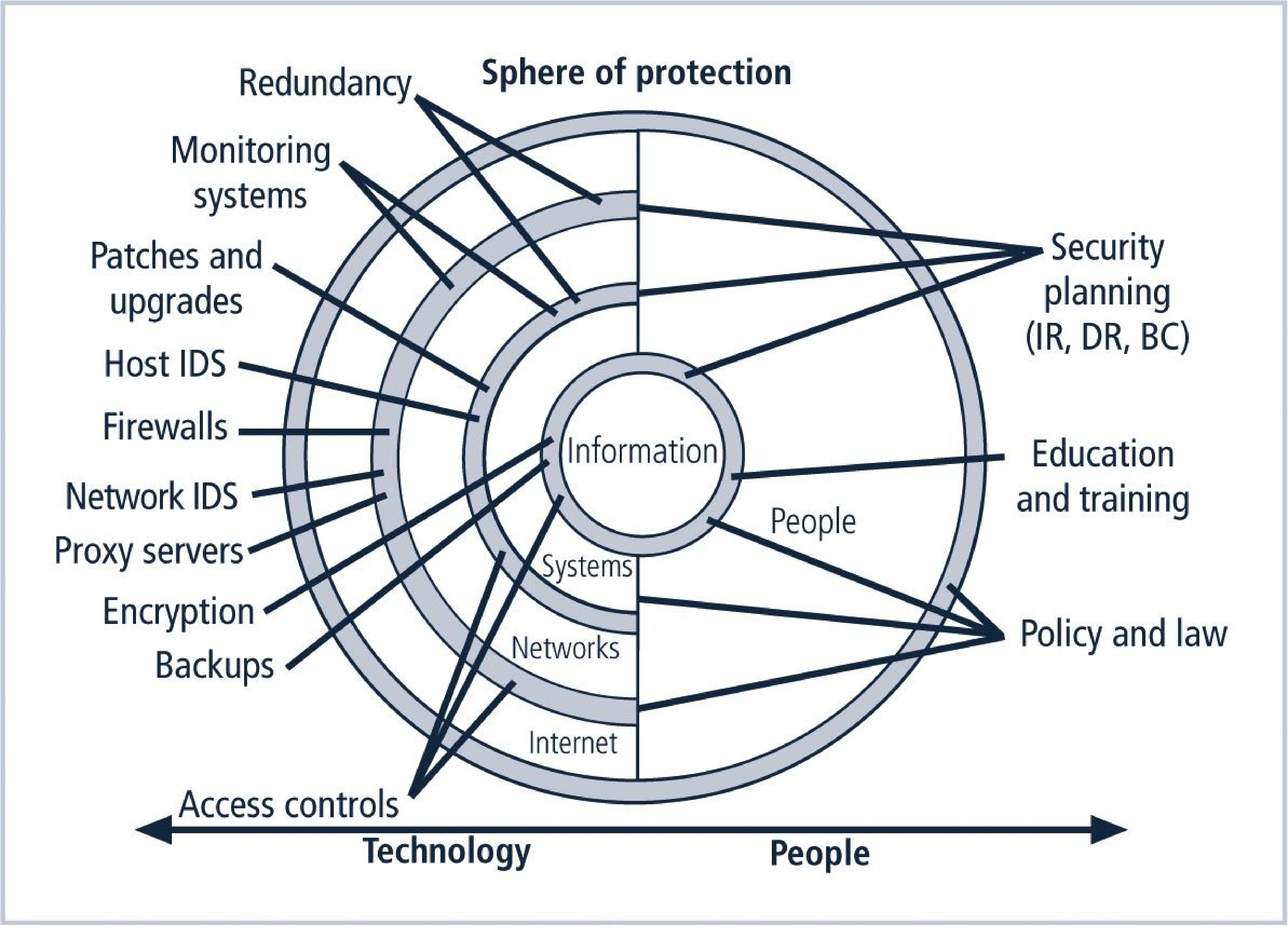


FIGURE 9-1 Sphere of Security

Access control encompasses two processes:

1. Confirming identity of entity
accessing a logical or physical area
(**authentication**)

2. Determining which actions
that entity can perform
in that physical or logical area
(**authorization**)

A successful access control approach
—whether intended to control
physical access or logical access—
always consists of both
authentication & authorization

Authentication mechanism types:

✓ Something you know
✓ Something you have
✓ Something you are
✓ Something you produce

Strong authentication
uses at least 2 different
authentication mechanism types

Something you know

Verifies user’s identity by means of
a password, passphrase, or other unique code

Password: a private word
or combination of characters
that only the user should know

Passphrase: a plain-language phrase,
typically longer than a password,
from which a virtual password is derived

Pick a good password.

“John the Ripper”
(http://www.openwall.com/john/)
will make mincemeat of poor passwords.

The guidelines:

1. Don’t use easy passwords
2. Mix of 3 of these 4: A a 1 #
3. At least 8 characters
4. Easy to remember & hard to guess

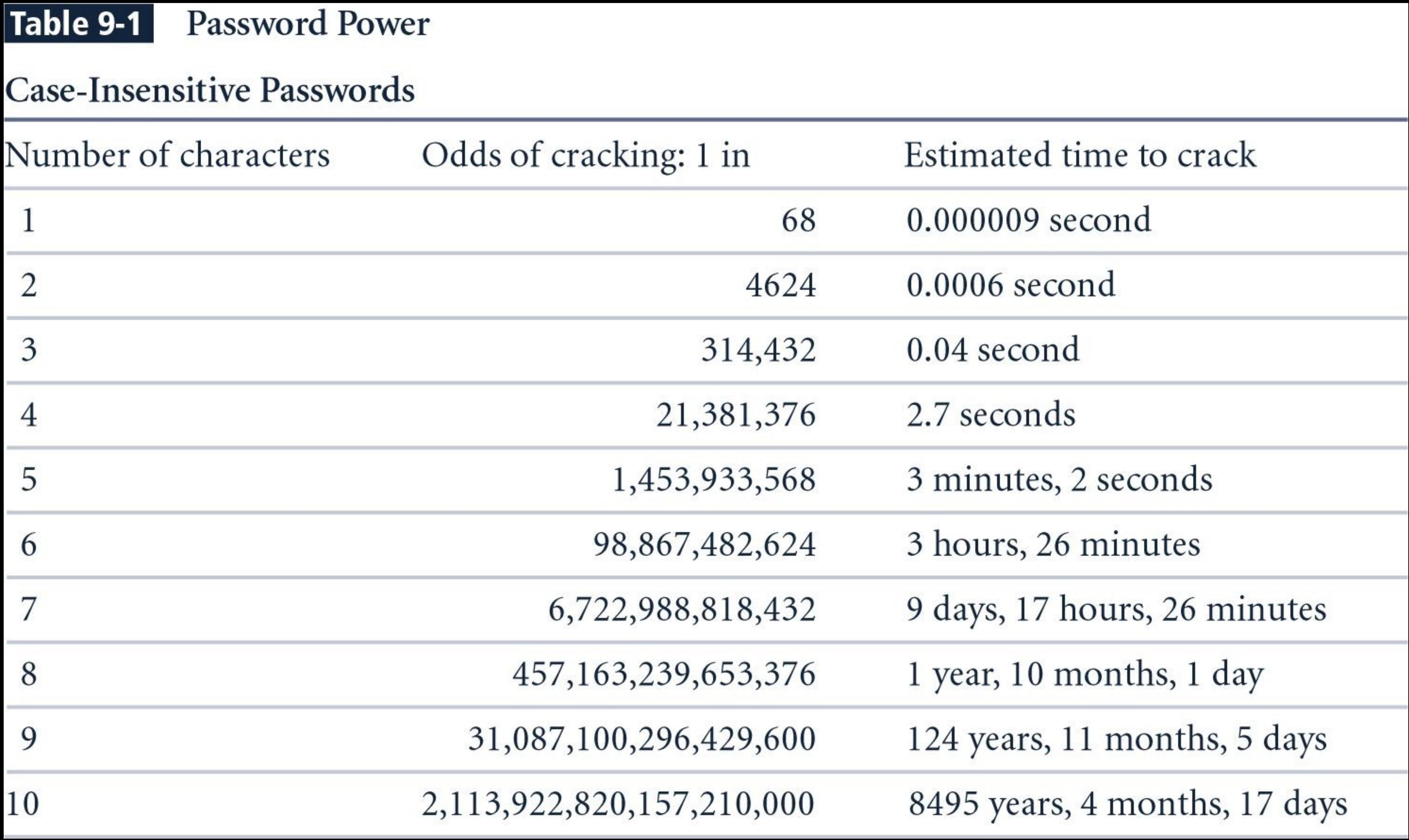


Table 9-1 Password Power

Case-Insensitive Passwords

Number of characters	Odds of cracking: 1 in	Estimated time to crack
1	68	0.000009 second
2	4624	0.0006 second
3	314,432	0.04 second
4	21,381,376	2.7 seconds
5	1,453,933,568	3 minutes, 2 seconds
6	98,867,482,624	3 hours, 26 minutes
7	6,722,988,818,432	9 days, 17 hours, 26 minutes
8	457,163,239,653,376	1 year, 10 months, 1 day
9	31,087,100,296,429,600	124 years, 11 months, 5 days
10	2,113,922,820,157,210,000	8495 years, 4 months, 17 days

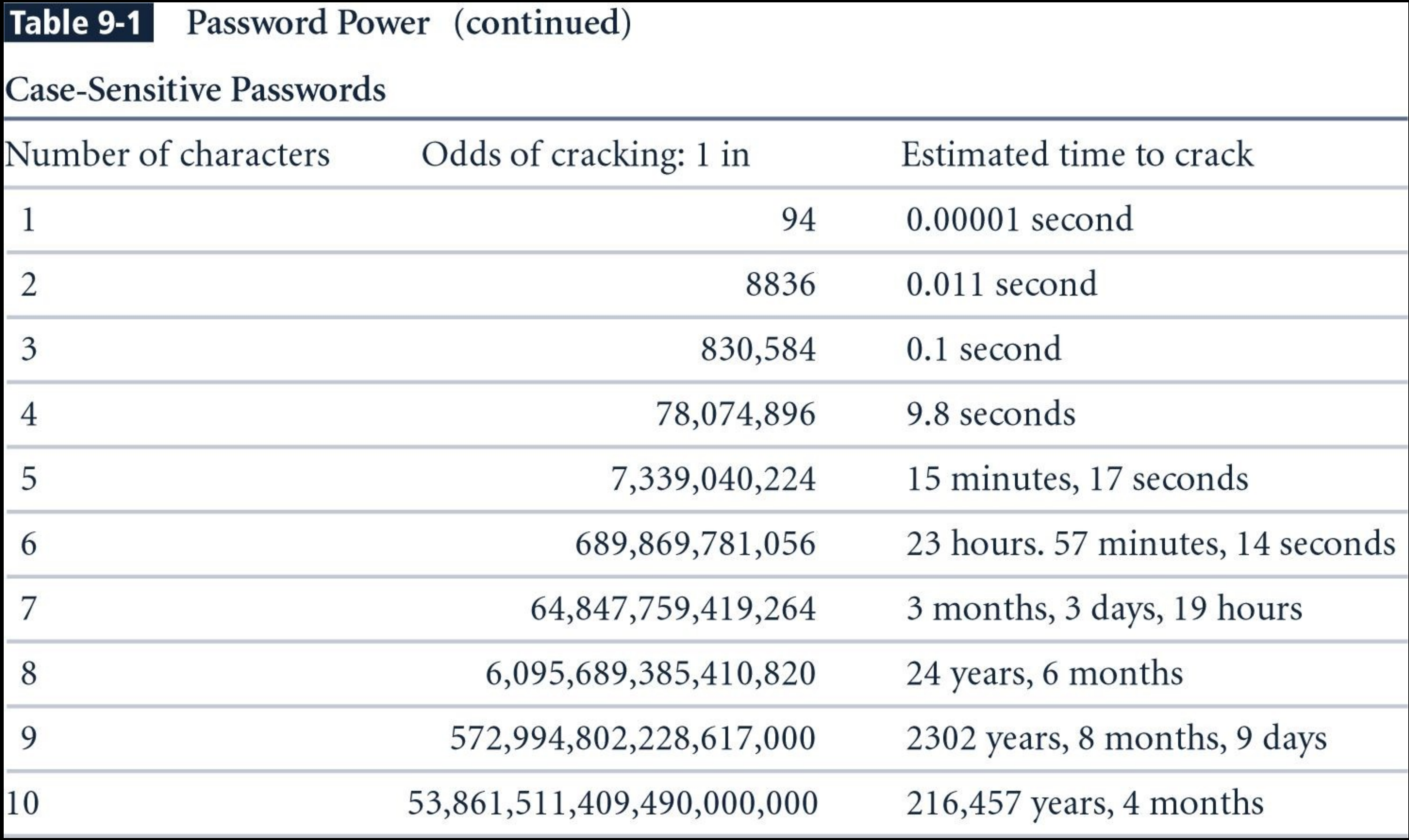


Table 9-1 Password Power (continued)

Case-Sensitive Passwords

Number of characters	Odds of cracking: 1 in	Estimated time to crack
1	94	0.00001 second
2	8836	0.011 second
3	830,584	0.1 second
4	78,074,896	9.8 seconds
5	7,339,040,224	15 minutes, 17 seconds
6	689,869,781,056	23 hours. 57 minutes, 14 seconds
7	64,847,759,419,264	3 months, 3 days, 19 hours
8	6,095,689,385,410,820	24 years, 6 months
9	572,994,802,228,617,000	2302 years, 8 months, 9 days
10	53,861,511,409,490,000,000	216,457 years, 4 months

Here’s a good method
for picking a good password:

“There’s a lady who’s sure
all that glitters is gold”

`Talwsatgig`

⇩

`Ta1w5atg1g`

⇩

`Ta1w5atg1g!`

“I'm gonna fight 'em off,
A seven nation army
couldn't hold me back”

⇩

`1gfe0,A7nachm6`

“Somewhere over the rainbow,
way up high”

⇩

`S0tr,wuh`

“Shut up Just shut up Shut up”

⇩

`SuJsuSu`

Something you have

Uses something (a card, key, or token) that user or system possesses

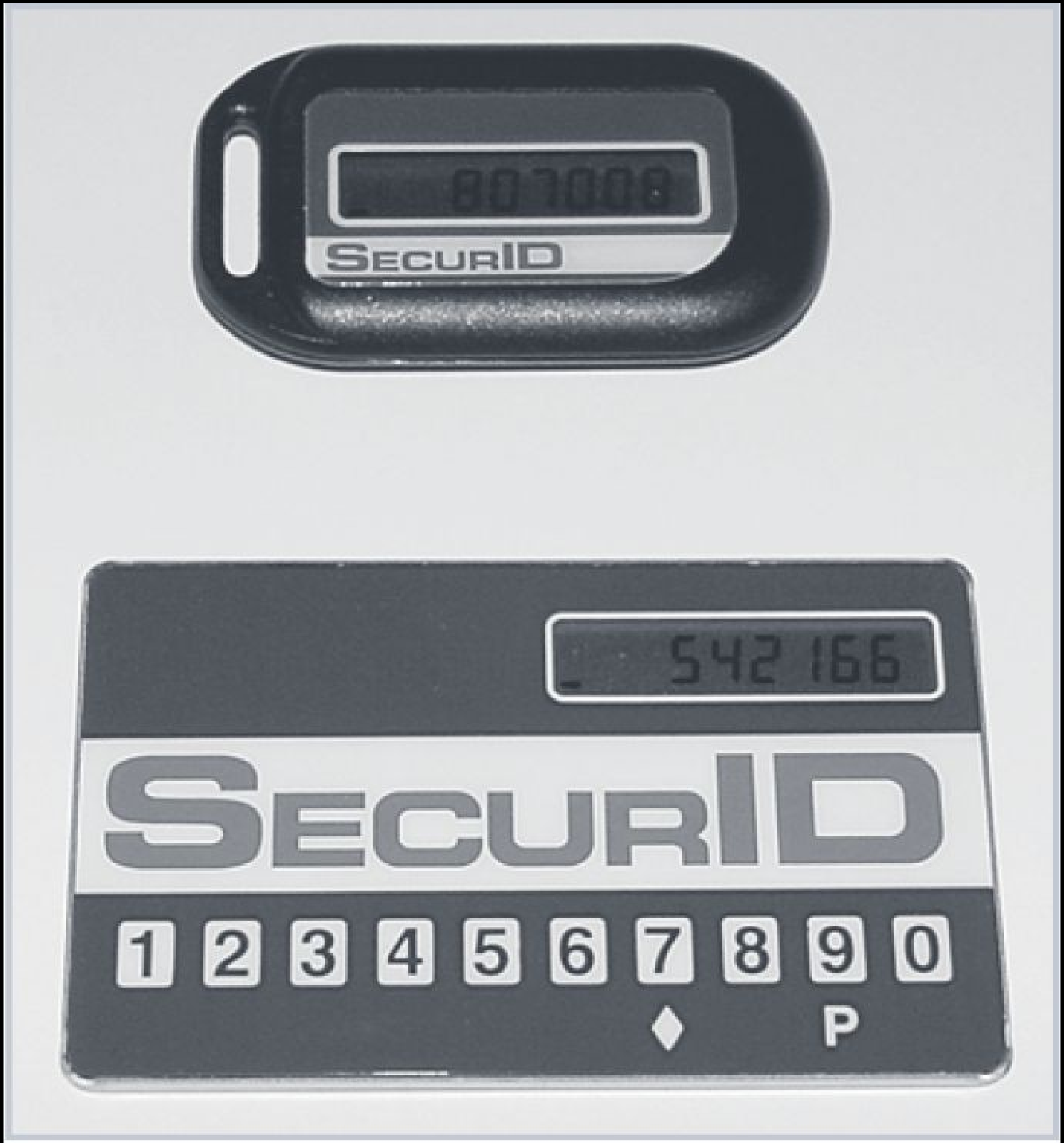
Examples:

✓ A dumb card (such as an ATM cards) with magnetic stripes

✓ A smart card containing a processor

✓ A cryptographic token, a processor in a card that has a display

Either synchronous or asynchronous



Source: RSA Security

FIGURE 9-3 Access Control Tokens

Something you are

Takes advantage
of something inherent in the user
that is evaluated using biometrics

Most of the technologies
that scan human characteristics
convert these images
to obtain some form of minutiae:
unique points of reference
that are digitized
& stored in an encrypted format

Something you do

Uses something
the user performs or produces

Includes technology related
to signature & voice recognition,
for example

Authorization for each authenticated user

✓ System performs authentication process to verify specific entity

✓ Grants access to resources for only that entity

Authorization for members of a group

✓ System matches authenticated entities to a list of group memberships

✓ Grants access to resources based on group’s access rights

Authorization across multiple systems

✓ Central authentication & authorization system verifies entity identity

✓ Grants a set of credentials to verified entity

Evaluating biometrics

False reject rate:
Percentage of authorized users
who are denied access (Type I Error)

False accept rate:
Percentage of unauthorized users
who are allowed access (Type II Error)

Crossover error rate:
Point at which
the number of false rejections
equals the false acceptances

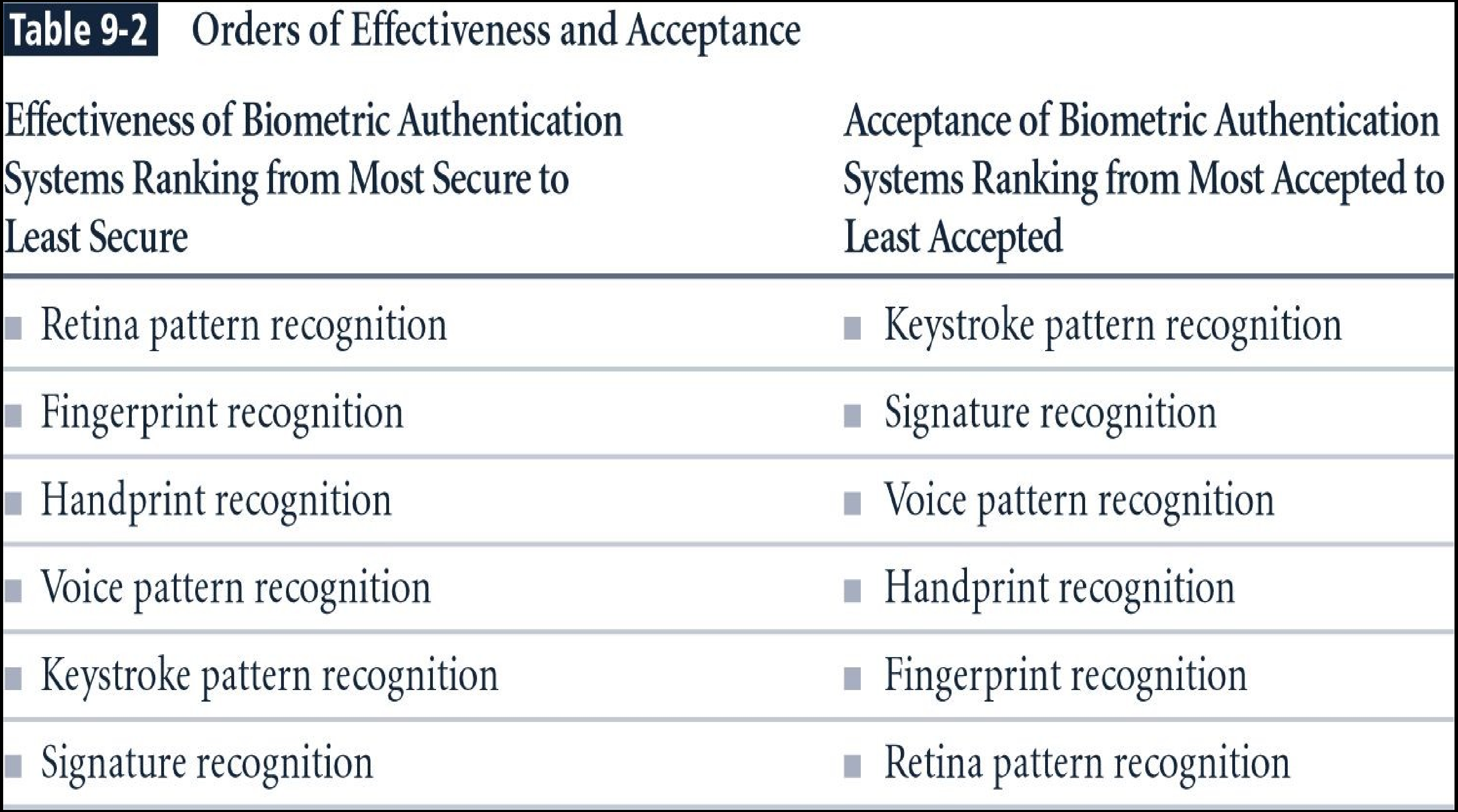


Table 9-2 Orders of Effectiveness and Acceptance

Effectiveness of Biometric Authentication Systems Ranking from Most Secure to Least Secure	Acceptance of Biometric Authentication Systems Ranking from Most Accepted to Least Accepted
Retina pattern recognition	Keystroke pattern recognition
Fingerprint recognition	Signature recognition
Handprint recognition	Voice pattern recognition
Voice pattern recognition	Handprint recognition
Keystroke pattern recognition	Fingerprint recognition
Signature recognition	Retina pattern recognition

To appropriately manage access controls,
an organization must have
a formal access control policy in place

Determines how access rights
are granted to entities & groups

Must include provisions
for periodically reviewing all access rights,
granting access rights to new employees,
changing access rights
when job roles change,
& revoking access rights as appropriate

In InfoSec, a **firewall**
is any device that prevents
a specific type of information
from moving between two networks

Often from the outside
(the untrusted network; e.g., the Internet),
& the inside (the trusted network)

Firewall may be
a separate computer system,
a service running
on an existing router or server,
or a separate network
containing a number of supporting devices

1st generation of firewalls
(packet filtering firewalls)
are simple networking devices
that filter packets by examining
every incoming & outgoing packet header

Can selectively filter packets
based on values in the packet header,
accepting or rejecting packets as needed

Can be configured to filter based on
IP address, type of packet, port request,
&/or other elements present in the packet

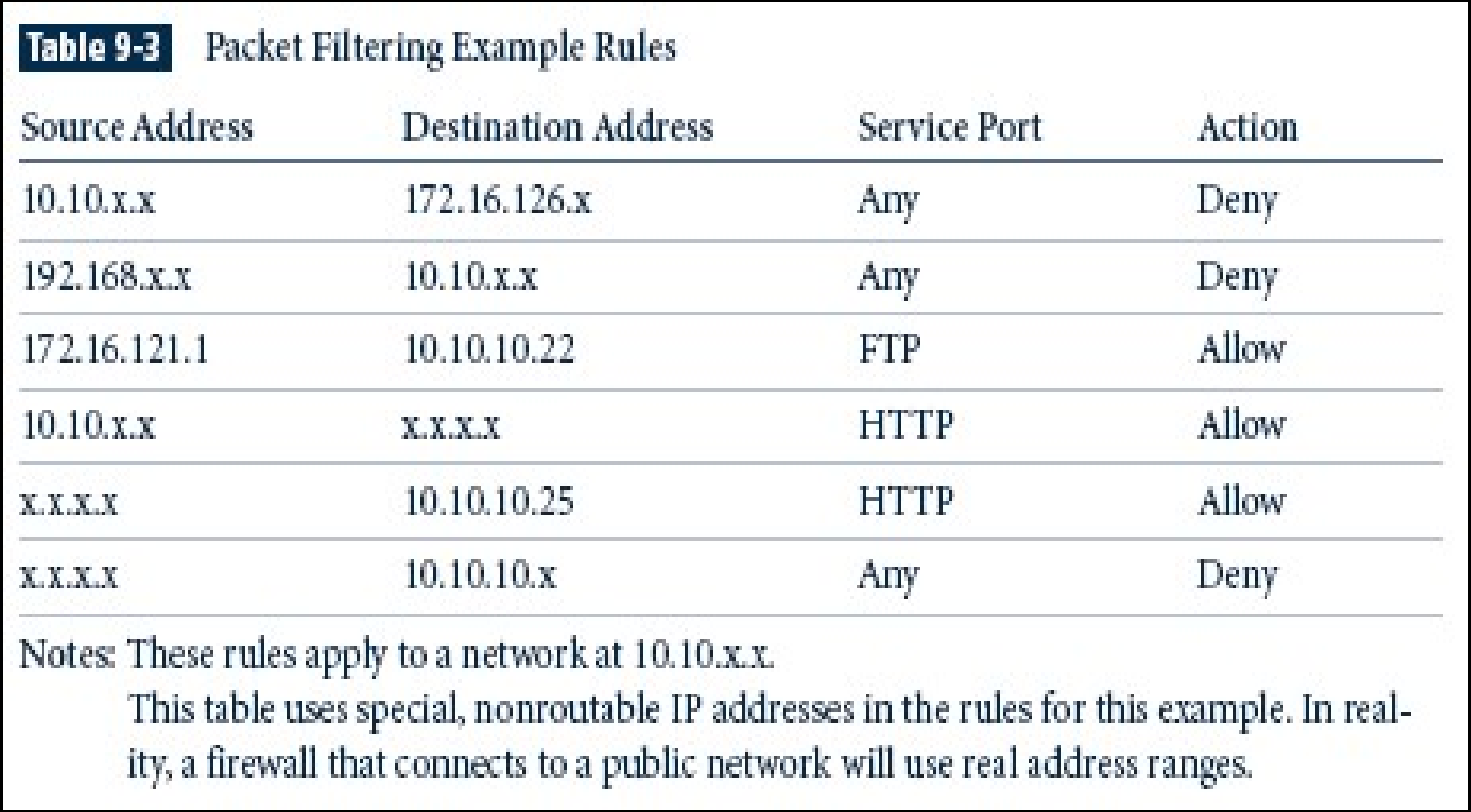


Table 9-3 Packet Filtering Example Rules

Source Address	Destination Address	Service Port	Action
10.10.x.x	172.16.126.x	Any	Deny
192.168.x.x	10.10.x.x	Any	Deny
172.16.121.1	10.10.10.22	FTP	Allow
10.10.x.x	x.x.x.x	HTTP	Allow
x.x.x.x	10.10.10.25	HTTP	Allow
x.x.x.x	10.10.10.x	Any	Deny

Notes: These rules apply to a network at 10.10.x.x.

This table uses special, nonroutable IP addresses in the rules for this example. In reality, a firewall that connects to a public network will use real address ranges.

2nd generation of firewalls,
known as application-level firewalls,
often consists of dedicated computers
kept separate from the 1st filtering router
(edge router)

Commonly used in conjunction
with a 2nd or internal filtering router,
or proxy server

Proxy server, rather than the Web server,
is exposed to outside world
from within a network segment
called the demilitarized zone (DMZ),
an intermediate area between
a trusted network & an untrusted network

Application-level firewalls are implemented
for specific protocols

3rd generation of firewalls,
stateful inspection firewalls,
keep track
of each network connection established
between internal & external systems
using a state table

State tables track the state & context
of each packet exchanged
by recording which station sent which
packet & when

A stateful inspection firewall
can restrict incoming packets
by allowing access only to packets
that constitute responses to requests
from internal hosts

If the stateful inspection firewall
receives an incoming packet
that it cannot match in its state table,
then it uses ACL rights
to determine
whether to allow the packet to pass

4th generation firewall,
or dynamic packet filtering firewall,
allows only a particular packet
with a specific
source, destination, & port address
to pass through the firewall

Does so by understanding
how the protocol functions,
& by opening & closing
pathways in the firewall

Dynamic packet filters
are an intermediate form,
between traditional static packet filters
& application proxies

Each of the firewall generations
can be implemented
in a number of architectural configurations

4 architectural implementations
of firewalls
are especially common:

✓ Packet filtering routers
✓ Screened-host firewalls
✓ Dual-homed host firewalls
✓ Screened-subnet firewalls

Most organizations
with an Internet connection
use some form of router
between their internal networks
& the external service provider

Many of these routers
can be configured to block packets
that the organization doesn’t allow
into the network

Such an architecture lacks auditing
& strong authentication

Complexity of the access control lists
used to filter the packets
can grow to the point
of degrading network performance

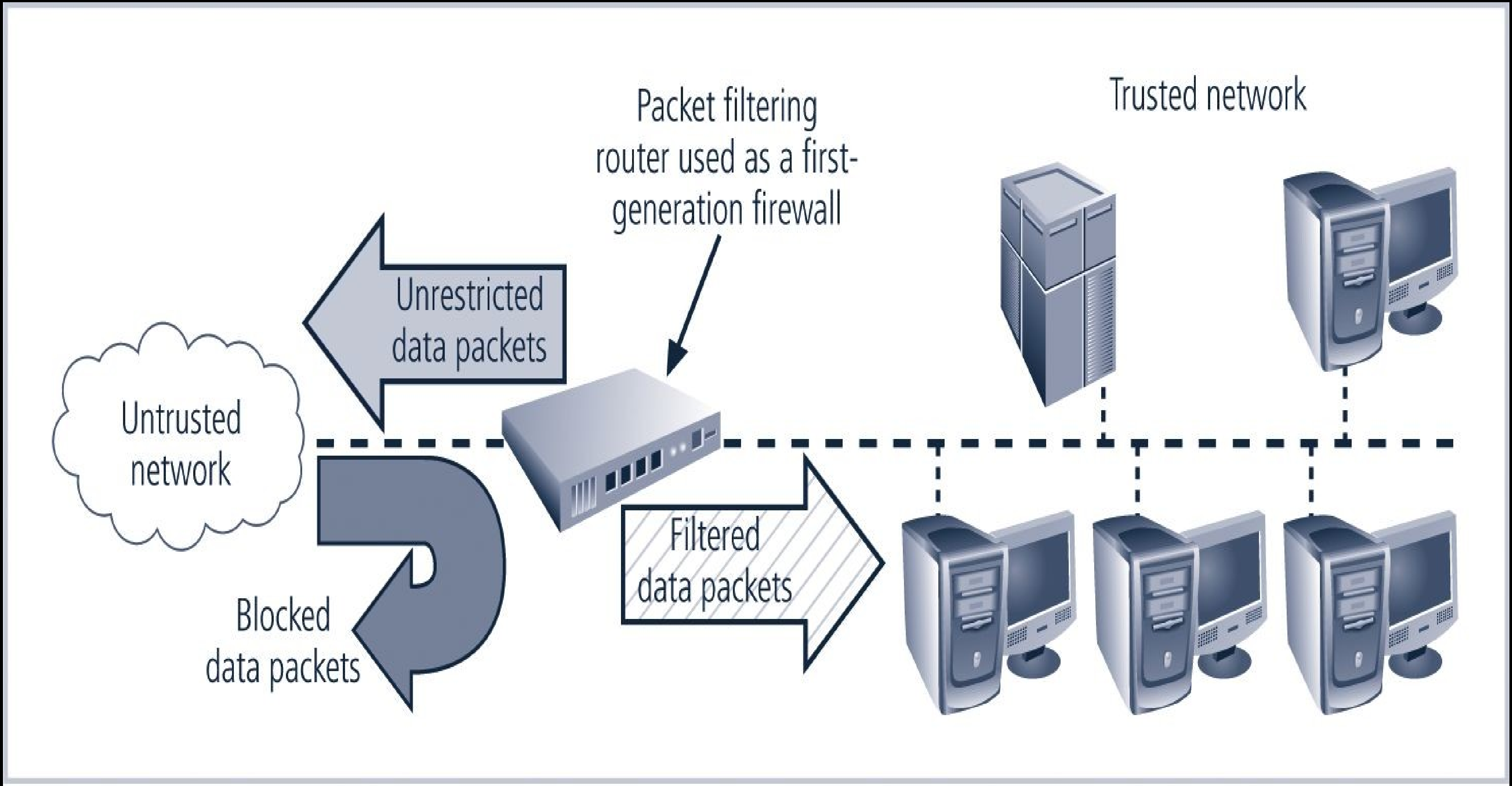

Packet filtering router used as a first-generation firewall
Trusted network
Unrestricted data packets
Untrusted network
Filtered data packets
Blocked data packets

FIGURE 9-5 Packet Filtering Firewall

Screened-host firewall systems
combine packet filtering router
with a separate, dedicated firewall
such as an application proxy server

This approach allows the router
to screen packets to minimize network traffic
& load on the internal proxy

Application proxy examines
an application layer protocol, such as HTTP,
& performs the proxy services

This separate host,
which is often referred to as a bastion host,
represents a single, rich target
for external attacks,
& should be very thoroughly secured

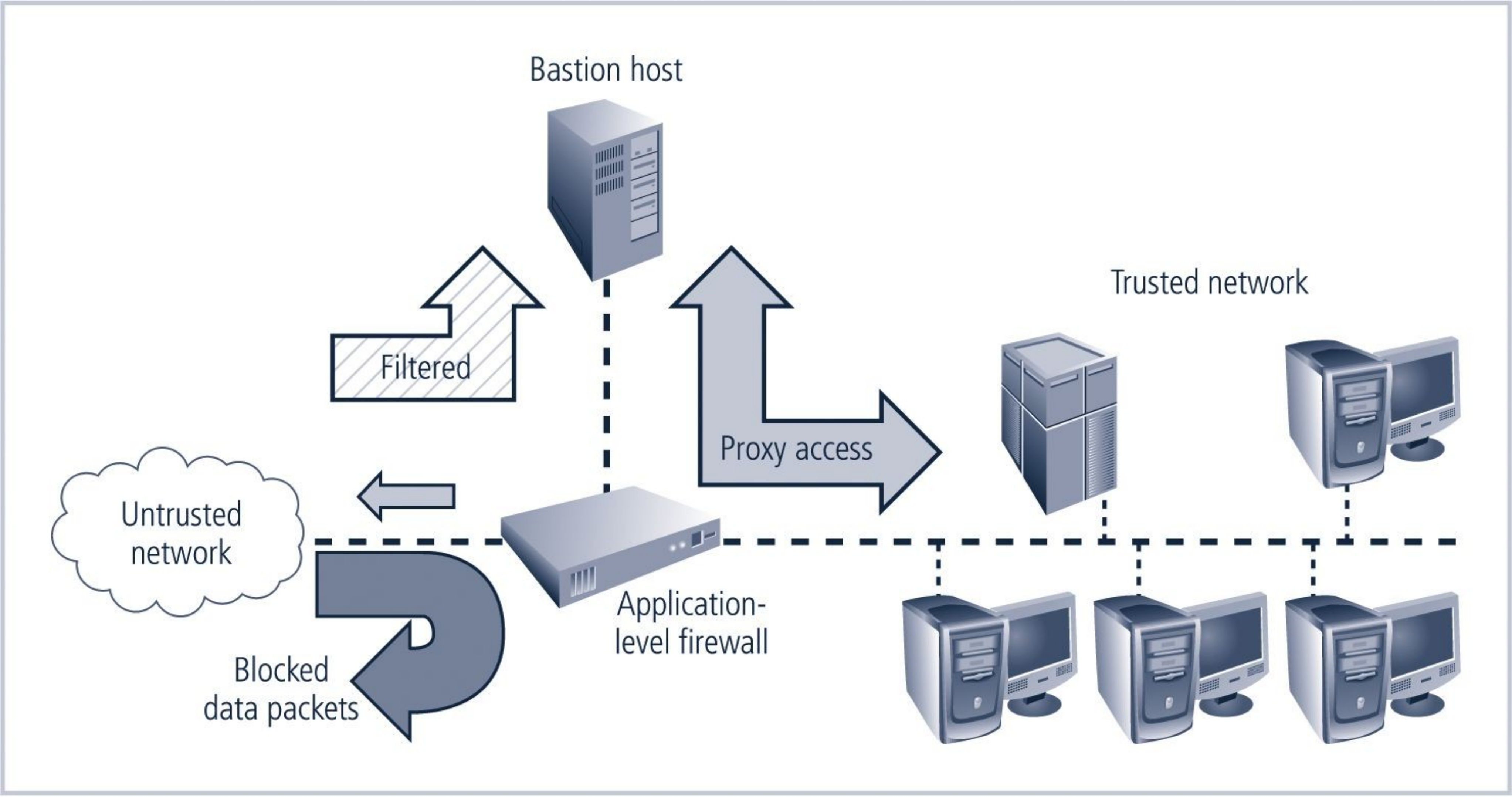


FIGURE 9-6 Screened-Host Firewall

With dual-homed host firewalls,
the bastion host contains
2 network interfaces:

1. One connected to external network
2. One connected to internal network,
requiring all traffic to travel
through the firewall to move
between internal & external networks

Network–address translation (NAT)
is often implemented with this architecture

Converts external IP addresses
to special ranges of internal IP addresses

These special, non-routable addresses consist of 3 different ranges:

10.x.x.x
> 16.5 million usable addresses

192.168.x.x
> 65,500 addresses

172.16.0.x – 172.16.15.x
> 4000 usable addresses

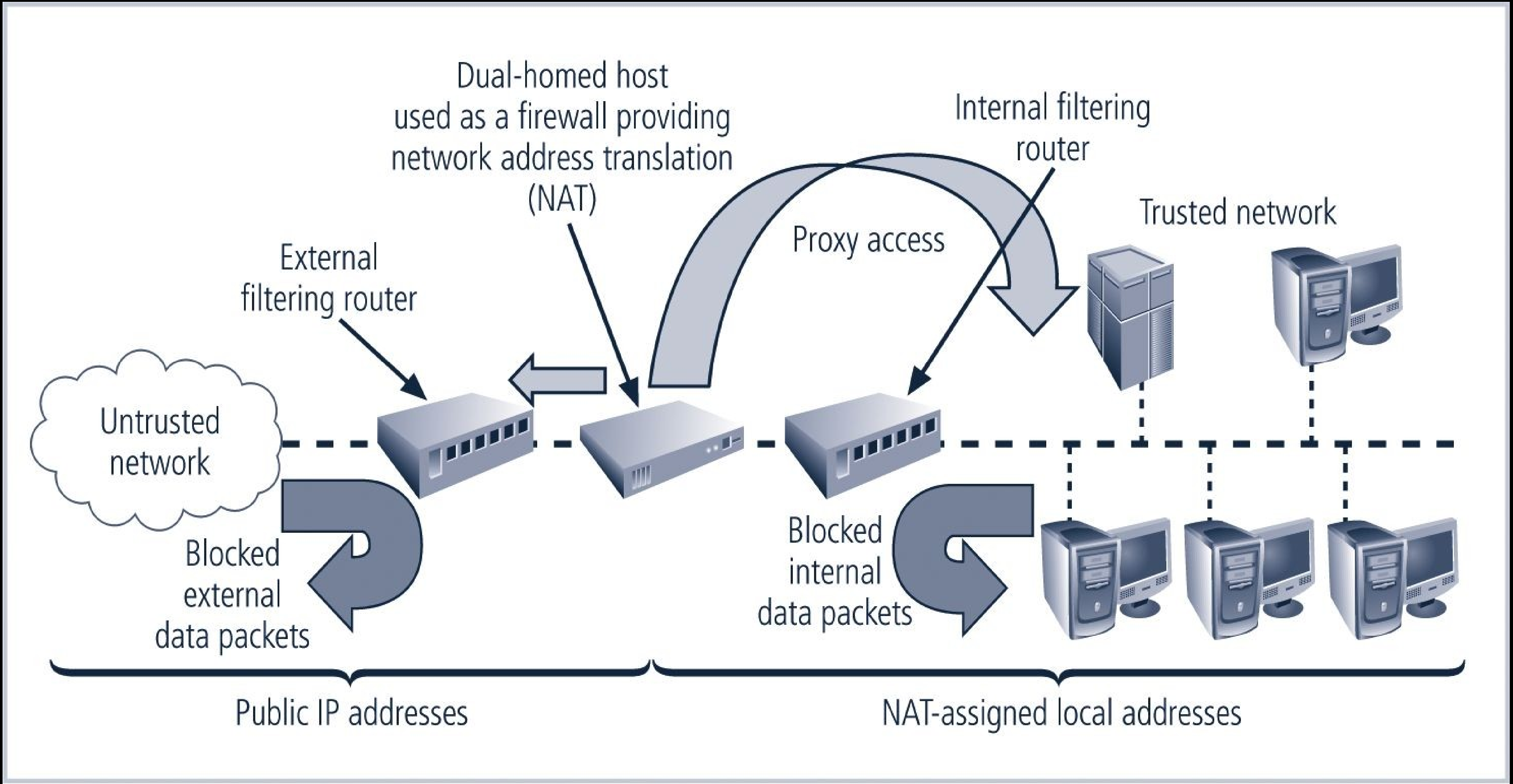


FIGURE 9-7 Dual-Homed Host Firewall

Screened-subnet firewall
consists of 1 or more
internal bastion hosts
located behind a packet filtering router,
with each host
protecting the trusted network

First general model uses
2 filtering routers,
with 1 or more
dual-homed bastion hosts between them

Second general model shows connections
are routed as follows:

Connections from the outside
or untrusted network
are routed through
an external filtering router

Connections from the outside
or untrusted network
are routed into—& then out of—
a routing firewall
to the DMZ

Connections into
the trusted internal network
are allowed only from
the DMZ bastion host servers

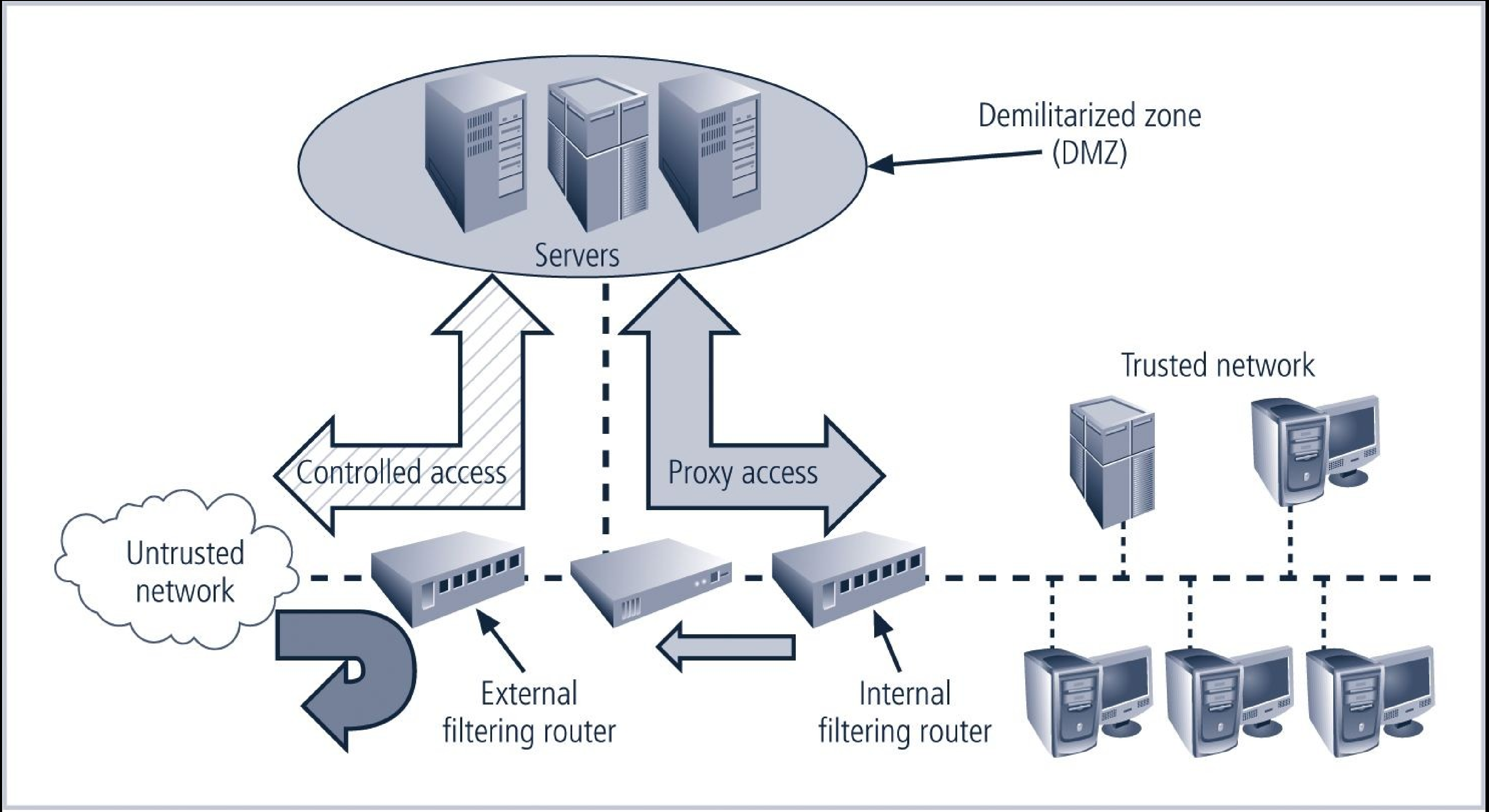


FIGURE 9-8 Screened-Subnet (DMZ)

When evaluating a firewall,
ask the following questions:

What type of firewall technology
offers the right balance
between protection & cost
for the needs of the organization?

What features are included in the base price?
What features are available at extra cost?
Are all cost factors known?

How easy is it to set up & configure the firewall?
How accessible are the staff technicians
who can competently configure the firewall?

Can the candidate firewall adapt
to the growing network in the target organization?

Any firewall device
—whether a packet filtering router, bastion host,
or other firewall implementation—
must have its own configuration
that regulates its actions

A policy regarding the use of a firewall
should be articulated
before it is made operable

In practice, configuring firewall rule sets
can be something of a nightmare

Each firewall rule must be carefully crafted,
placed into the list in the proper sequence,
debugged, & tested

Proper sequence ensures
that the most resource-intensive actions
are performed after
the most restrictive ones,
thereby reducing the number of packets
that undergo intense scrutiny

Remember this about firewalls:

Deal strictly with defined patterns
of measured observation

Are prone to programming errors,
flaws in rule sets,
& other inherent vulnerabilities

Are designed to function
within limits of hardware capacity

Can only respond to patterns of events
that happen in an expected
& reasonably simultaneous sequence

Firewall Best Practices

All traffic from trusted network is allowed out

Firewall device is never accessible
directly from public network

Simple Mail Transport Protocol (SMTP) data
is allowed to pass through the firewall,
but should be routed to a SMTP gateway

Deny Internet Control Message Protocol (ICMP)

No telnet or FTP into the network:
SSH & SFTP only

When Web services are offered outside the firewall,
HTTP traffic should be handled
by some form of proxy access or DMZ

Dial-Up Protection

Attacker who suspects
that an organization has dial-up lines
can use a device called a **war-dialer**
to locate connection points

Network connectivity
using dial-up connections
is usually much simpler & less sophisticated
than Internet connections

For the most part,
simple user name & password schemes
are the only means of authentication

RADIUS & TACACS:

Systems that authenticate credentials
of users trying to access
an organization’s network via dial-up

Typical dial-up systems
place authentication of users
on system connected to modems

Remote Authentication Dial-In User Service
(RADIUS)
centralizes management of user authentication

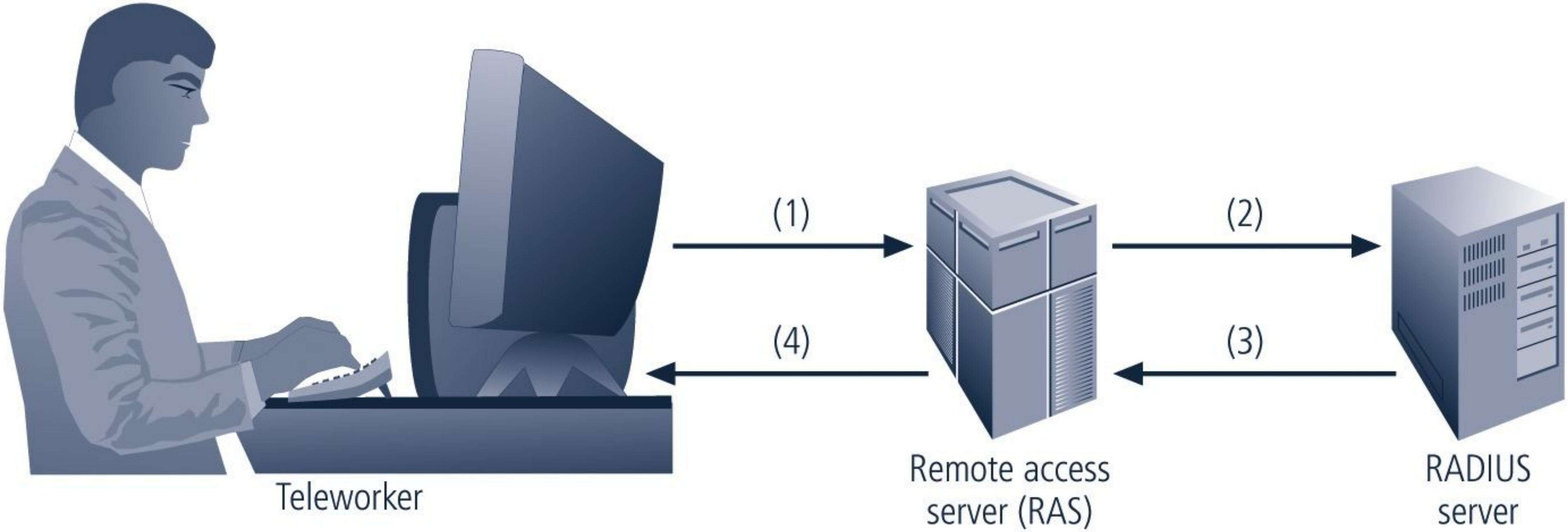
Places responsibility for authenticating each user
in the central RADIUS server

more … →

When a remote access server (RAS)
receives a request
for a network connection
from a dial-up client ...

it passes the request
along with the user’s credentials
to the RADIUS server,
& RADIUS then validates the credentials

Terminal Access Controller
Access Control System
(TACACS)
works similarly, but is
based on a client/server configuration



1. Remote worker dials RAS and submits username and password.
2. RAS passes user name and password to RADIUS server.
3. RADIUS server approves or rejects request and provides access authorization.
4. RAS provides access to authorized remote worker.

FIGURE 9-9 RADIUS Configuration

Organizations that continue
to offer dial-up remote access
must deal with a number of thorny issues:

✓ Determine how many
dial-up connections the organization has

✓ Control access
to authorized modem numbers

✓ Use call-back whenever possible

✓ Use token-based authentication
if at all possible

InfoSec intrusion detection systems (IDSs)
work like burglar alarms

Administrators can choose alarm level

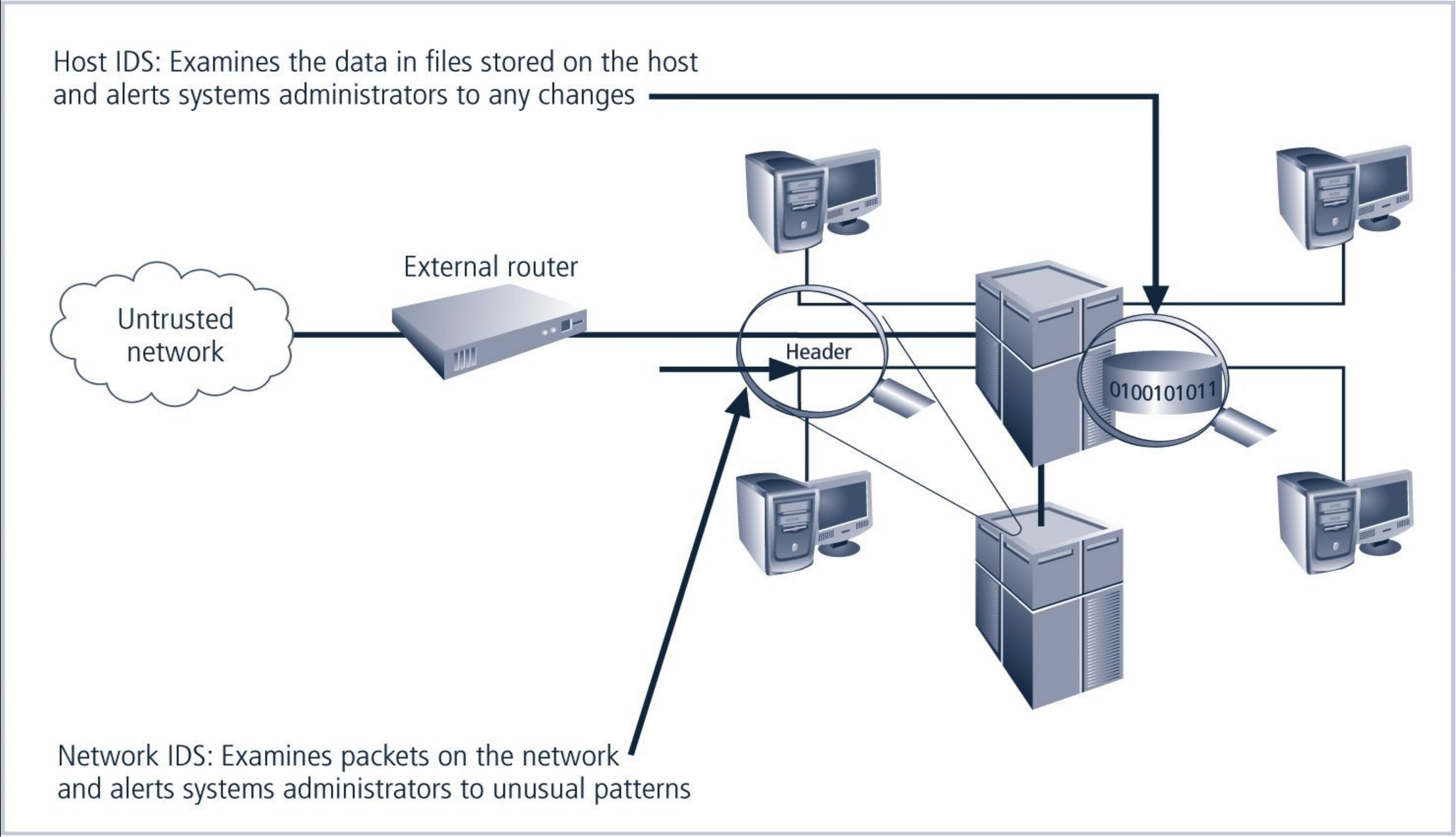
Many can be configured
to notify administrators
via e-mail & numerical or text paging

Like firewall systems,
require complex configurations

Either network based
to protect network information assets,
or host based
to protect server or host information assets

Use one of two detection methods:

✓ Signature based
✓ Statistical anomaly based



Host IDS: Examines the data in files stored on the host and alerts systems administrators to any changes

Network IDS: Examines packets on the network and alerts systems administrators to unusual patterns

FIGURE 9-10 Intrusion Detection Systems

Host-based IDS works
by configuring & classifying
various categories of systems & data files

In many cases,
IDSs provide only a few general levels
of alert notification

Unless the IDS is very precisely configured,
benign actions can generate
a large volume of false alarms

Host-based IDSs can monitor
multiple computers simultaneously

Network-based IDSs monitor network traffic
&, when a predefined condition occurs,
notify appropriate administrator

Looks for patterns of network traffic

Must match known & unknown attack strategies
against their knowledge base
to determine whether an attack has occurred

Yield many more false-positive readings
than do host-based IDSs,
because they attempt to read
network activity pattern
to determine what is normal & what is not

Signature-based IDS or knowledge-based IDS
examines data traffic
for something that matches signatures
which comprise preconfigured, predetermined
attack patterns

Problem is that
signatures must be continually updated,
as new attack strategies emerge

Weakness is time frame over which attacks occur

If attackers are slow & methodical,
they may slip undetected through the IDS,
as their actions may not match a signature
that includes factors
based on duration of the events

Statistical anomaly-based IDS (stat IDS)
or behavior-based IDS

First collects data from normal traffic
& establishes a baseline,
then periodically samples network activity,
based on statistical methods

Compares samples to baseline

When activity falls outside baseline parameters
(known as the clipping level),
IDS notifies the administrator

Advantage is that system
is able to detect new types of attacks
because it looks for abnormal activity of any type

IDSs must be configured
using technical knowledge
& adequate business & security knowledge
to differentiate between
routine circumstances
& low, moderate, or severe threats

Properly configured IDS
can translate a security alert
into different types of notification

Poorly configured IDS may yield only noise

Most IDSs monitor systems by means of agents,
software that resides on a system
& reports back to a management server

Consolidated enterprise manager
is a valuable tool in managing an IDS

Software that allows security pro
to collect data
from multiple host- & network-based IDSs
& look for patterns
across systems & subnetworks

Collects responses from all IDSs
used to identify
cross-system probes & intrusions

Scanning & analysis tools
can find vulnerabilities in systems,
holes in security components,
& other unsecured aspects of the network

Conscientious administrators
will frequently browse their own networks
for new vulnerabilities,
recent conquests,
& favorite assault techniques

Nothing wrong with using tools
used by attackers
to examine own defenses
& search out areas of vulnerability

Scanning tools collect the information
that an attacker needs to succeed

Footprinting

Organized research of the Internet addresses
owned or controlled by a target organization

Fingerprinting

Entails the systematic examination
of all of the organization's network addresses

Yields a detailed network analysis
that reveals useful information
about the targets of the planned attack

Port:
network channel or connection point
in a data communications system

Port scanning utilities (or **port scanners**)
can identify (or fingerprint)
active computers on a network
& active ports & services
on those computers,
the functions & roles
fulfilled by the machines,
& other useful information

Well-known ports: 0 – 1023

Registered ports: 1024 – 49151

Dynamic & private ports: 49152 - 65535

Open ports can be used:

✓ to send commands to a computer

✓ to gain access to a server

✓ to exert control over a networking device

… & thus must be secured

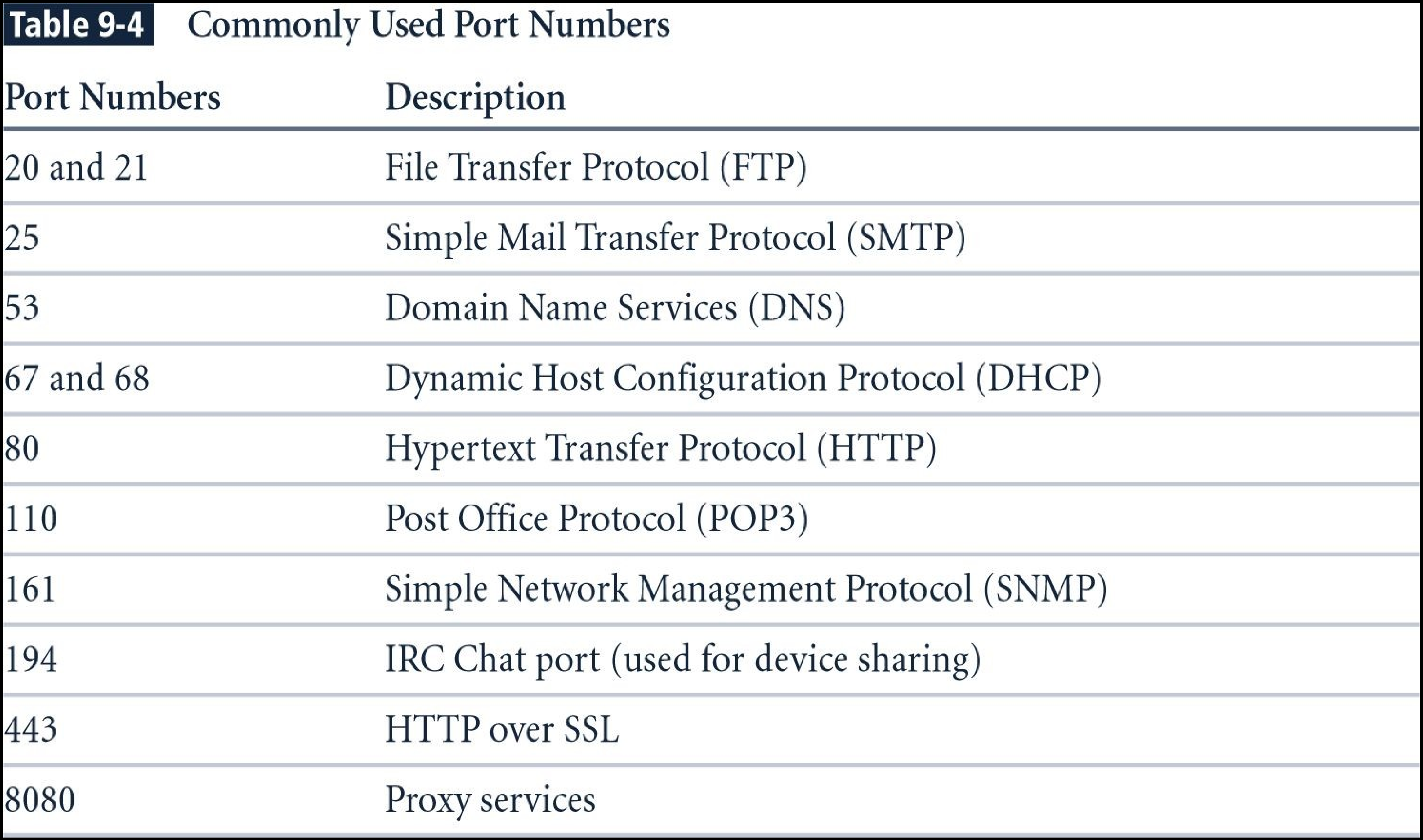


Table 9-4 Commonly Used Port Numbers

Port Numbers	Description
20 and 21	File Transfer Protocol (FTP)
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name Services (DNS)
67 and 68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol (POP3)
161	Simple Network Management Protocol (SNMP)
194	IRC Chat port (used for device sharing)
443	HTTP over SSL
8080	Proxy services

Vulnerability scanners

✓ Variants of port scanners

✓ Capable of scanning networks for very detailed information

✓ Identify exposed user names & groups

✓ Show open network shares

✓ Expose configuration problems & other server vulnerabilities

Packet sniffer

✓ Network tool
that collects & analyzes packets
on a network

✓ Can be used to eavesdrop
on network traffic

✓ Must be connected directly
to a local network
from an internal location

To use a packet sniffer legally,
you must:

✓ Be on a network
that the organization owns,
not leases

✓ Be under the direct authorization
of the network’s owners

✓ Have the knowledge & consent of users

✓ Have a justifiable business reason

Content filter

✓ Effectively protects organization’s systems
from misuse
& unintentional denial-of-service conditions

✓ Software program
or a hardware/software appliance
that allows administrators
to restrict content that comes into a network

✓ Most common application
is restriction of access to Web sites
with non–business-related material, like porn

✓ Another application is restriction of spam e-mail

✓ Ensure that employees
are using network resources appropriately

Trap & Trace

Trap function

✓ Describes software designed
to entice individuals
illegally perusing internal areas of a network

Trace function

✓ Process by which the organization
attempts to determine the identity
of someone discovered in unauthorized areas
of the network or systems

✓ If identified individual
is outside the security perimeter,
then policy will guide the process of escalation
to law enforcement or civil authorities

Vitally important that security manager
be able to see
organization’s systems & networks
from viewpoint of potential attackers

Should develop a program
using in-house resources, contractors,
or an outsourced service provider
to periodically scan
his or her own systems & networks
for vulnerabilities
with the same tools the hacker might use

Drawbacks
to using scanners & analysis tools,
content filters, & trap & trace tools:

✓ Do not have human-level capabilities

✓ Most function by pattern recognition,
so only handle known issues

✓ Most are computer-based,
so prone to their own
errors, flaws, & vulnerabilities

more ... →

✓ Designed, configured, & operated by humans,
so subject to human errors

✓ Some governments, agencies,
institutions, & universities
have established policies or laws
that protect the individual user’s
right to access content

✓ Tool usage & configuration
must comply with explicitly articulated policy,
so policy must provide for valid exceptions

Encryption

Process of converting original message
into a form that cannot be understood
by unauthorized individuals

Cryptography

From Greek words κρψπτοσ, meaning “hidden,”
& γραφειν, meaning “to write”

Describes processes involved
in encoding & decoding messages
so that others cannot understand them

Cryptanalysis

From αναλψειν, meaning “to break up”

Process of deciphering original message
(or **plaintext**)
from encrypted message
(or **ciphertext**)
without knowing algorithms & keys
used to perform the encryption

Some cryptography defintions

Algorithm: Mathematical formula or method used to convert unencrypted message into encrypted message

Cipher: Transformation of individual components (characters, bytes, or bits) of unencrypted message into encrypted components

Ciphertext or **cryptogram**: Unintelligible encrypted or encoded message resulting from encryption

more ... →

Cryptosystem: Set of transformations necessary to convert unencrypted message into encrypted message

Plaintext: Original unencrypted message that is encrypted
& results from successful decryption

Decipher: To decrypt or convert ciphertext to plaintext

Encipher: To encrypt or convert plaintext to ciphertext

more ... →

Key: Information used
in conjunction with algorithm
to create ciphertext from plaintext

Can be a series of bits
used in mathematical algorithm,
or knowledge of how to manipulate plaintext

Keyspace: Entire range of values
that can possibly be used
to construct an individual key

more … →

Steganography: Process of hiding messages, usually within graphic images

Work factor: Amount of effort (usually expressed in hours)

Common Ciphers

Most commonly used algorithms include 3 functions:

1. substitution
2. transposition
3. XOR

more ... →

Substitution cipher

- ✓ You substitute one value for another
- ✓ Monoalphabetic substitution uses only 1 alphabet
- ✓ Polyalphabetic substitution use 2 or more alphabets

more … →

Transposition cipher
(or permutation cipher)

Simply rearranges the values
within a block
to create the ciphertext

This can be done at the bit level
or at the byte (character) level

more ... →

In the XOR cipher conversion,
the bit stream is subjected
to a Boolean XOR function
against some other data stream,
typically a key stream

more ... →

XOR works as follows:

‘0’ XOR’ed with ‘0’ results in a ‘0’. $(0 \otimes 0 = 0)$
‘0’ XOR’ed with ‘1’ results in a ‘1’. $(0 \otimes 1 = 1)$
‘1’ XOR’ed with ‘0’ results in a ‘1’. $(1 \otimes 0 = 1)$
‘1’ XOR’ed with ‘1’ results in a ‘0’. $(1 \otimes 1 = 0)$

Simply put, if the 2 values
are the same, you get “0”

If not, you get “1”

Process is reversible:
if you XOR the ciphertext
with the key stream,
you get the plaintext

Vernam Cipher

- ✓ Also known as the one-time pad

- ✓ Developed at AT&T

- ✓ Uses set of characters used for encryption operations only one time & then discarded

- ✓ Values from this one-time pad are added to the block of text

- ✓ Resulting sum is converted to text

Another method,
used in the occasional spy movie,
is the use of text in a book
as the algorithm to decrypt a message

The key relies on two components:

✓ Knowing which book to use

✓ List of codes
representing the page number,
line number,
& word number of the plaintext word

Private key encryption, or symmetric encryption

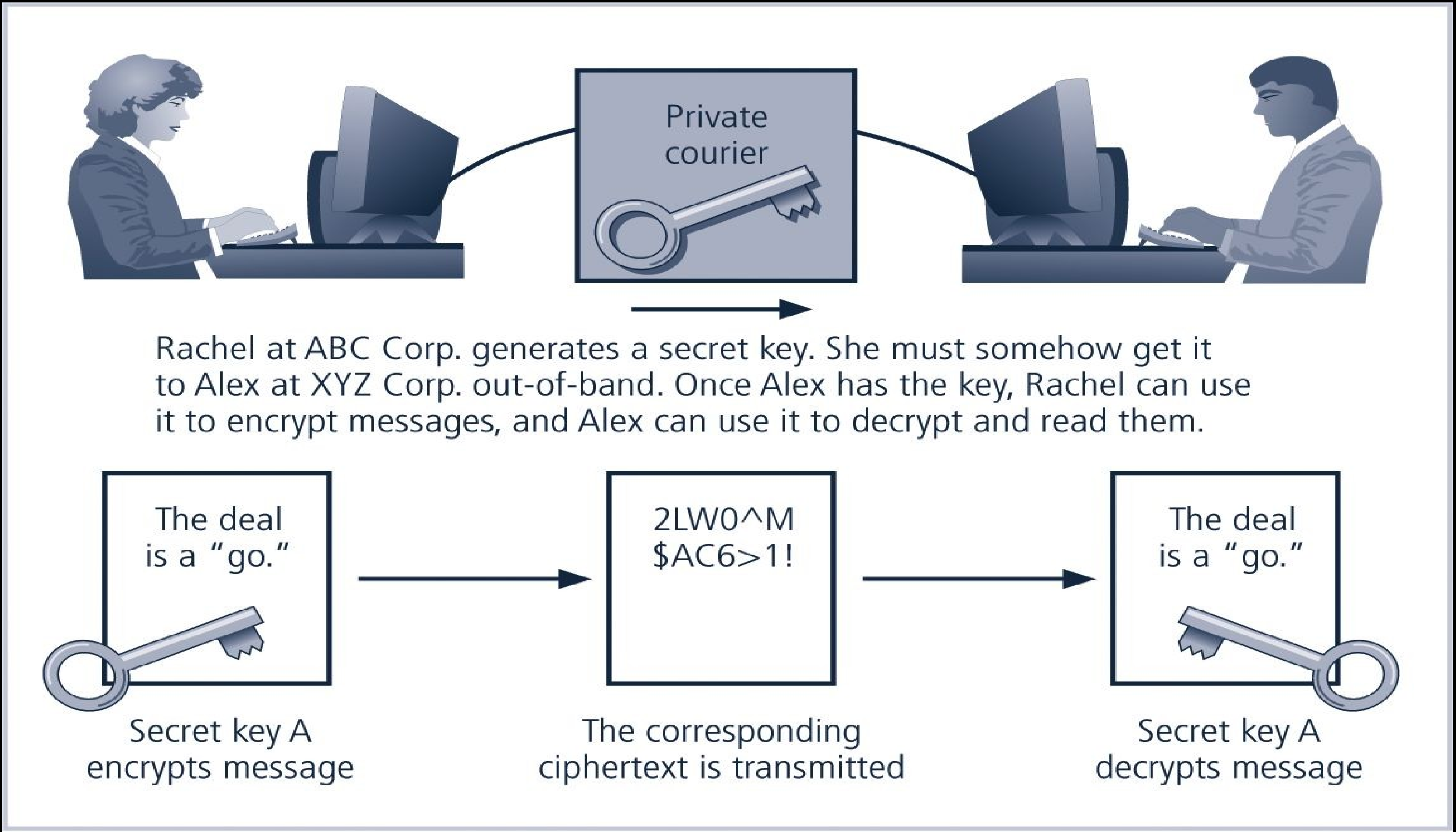
✓ Same key—a secret key—is used to encrypt & decrypt the message

✓ Usually extremely efficient

✓ Require easily accomplished processing to encrypt or decrypt the message

✓ One challenge is getting a copy of the key to the receiver

✓ Must be conducted out-of-band to avoid interception



Rachel at ABC Corp. generates a secret key. She must somehow get it to Alex at XYZ Corp. out-of-band. Once Alex has the key, Rachel can use it to encrypt messages, and Alex can use it to decrypt and read them.

FIGURE 9-11 Symmetric Encryption

Data Encryption Standard (DES)

✓ Developed in 1977 by IBM

✓ Based on Data Encryption Algorithm (DEA)
which uses a 64-bit block size & a 56-bit key

✓ Federally approved standard
for nonclassified data

✓ Cracked in 1997,
when developers of a new algorithm
– Rivest-Shamir-Aldeman –
offered a $10,000 reward
for the 1st person or team to crack the algorithm

✓ 14,000 users collaborated over the Internet
to finally break the encryption

Triple DES (3DES)

✓ Developed as an improvement to DES

✓ Uses as many as three keys in succession

Advanced Encryption Standard (AES)

✓ Successor to 3DES

✓ Based on the Rinjndael Block Cipher which features a variable block length & a key length of either 128, 192, or 256 bits

✓ In 1998, it took a special computer designed by the Electronic Frontier Foundation more than 56 hours to crack DES

✓ It would take the same computer approximately 4,698,864 quintillion years to crack AES

Asymmetric, or public key, encryption

✓ Uses two different, but related, keys

✓ Either key can be used
to encrypt or decrypt message

✓ However, if Key A is used to encrypt message,
then only Key B can decrypt it

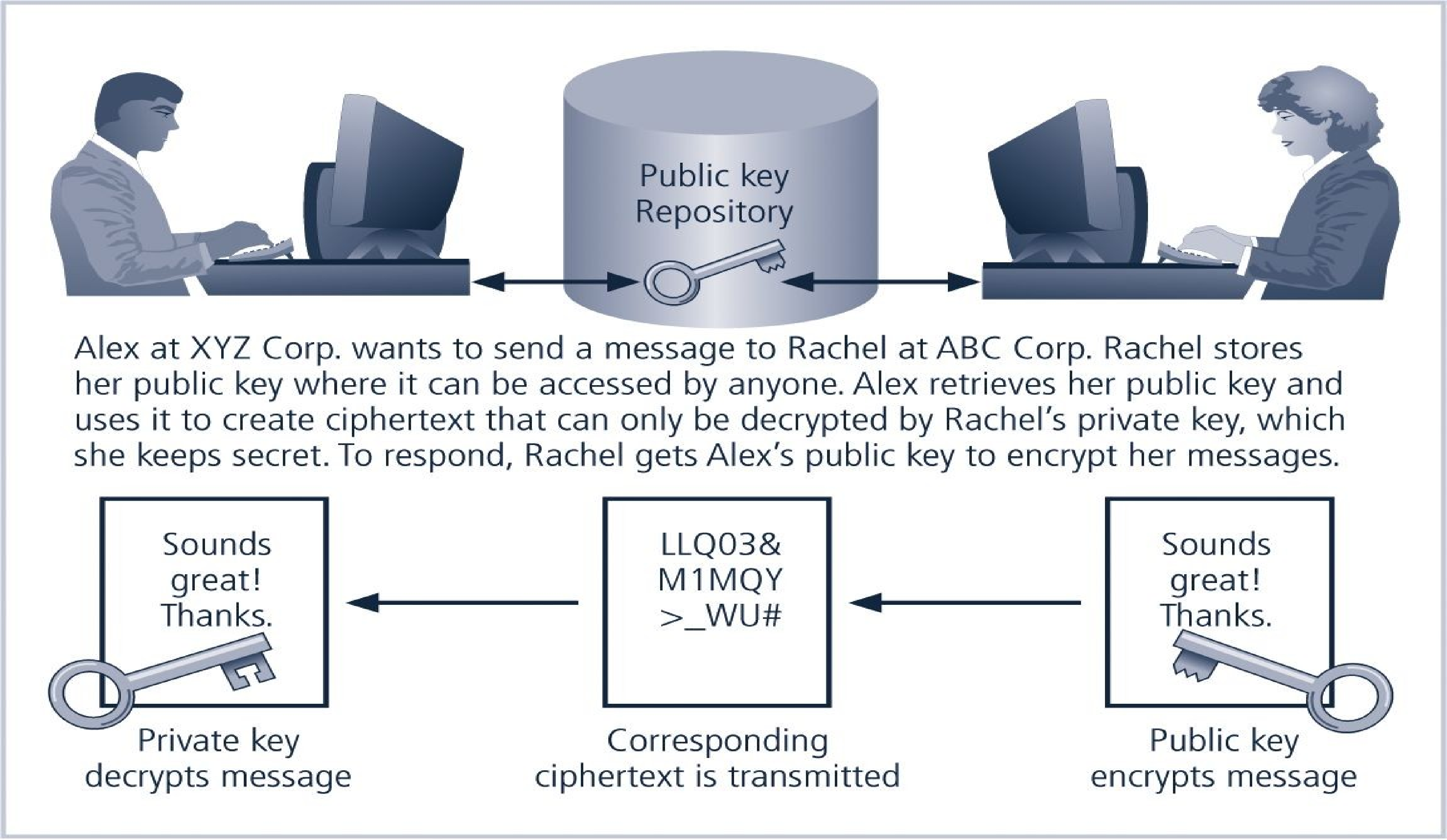
✓ Conversely, if Key B is used
to encrypt a message,
then only Key A can decrypt it

more … →

✓ Most valuable when
one of the keys is private
& the other is public

✓ Problem is that it requires 4 keys
to hold a single conversation between 2 parties

✓ Number of keys grows geometrically
as parties are added



Alex at XYZ Corp. wants to send a message to Rachel at ABC Corp. Rachel stores her public key where it can be accessed by anyone. Alex retrieves her public key and uses it to create ciphertext that can only be decrypted by Rachel's private key, which she keeps secret. To respond, Rachel gets Alex's public key to encrypt her messages.

Sounds great! Thanks.
LLQ03&
M1MQY
>_WU#
Sounds great! Thanks.
Private key decrypts message
Corresponding ciphertext is transmitted
Public key encrypts message

FIGURE 9-12 Public Key Encryption

Digital signatures

Encrypted messages independently verified
by a central facility (registry) as authentic

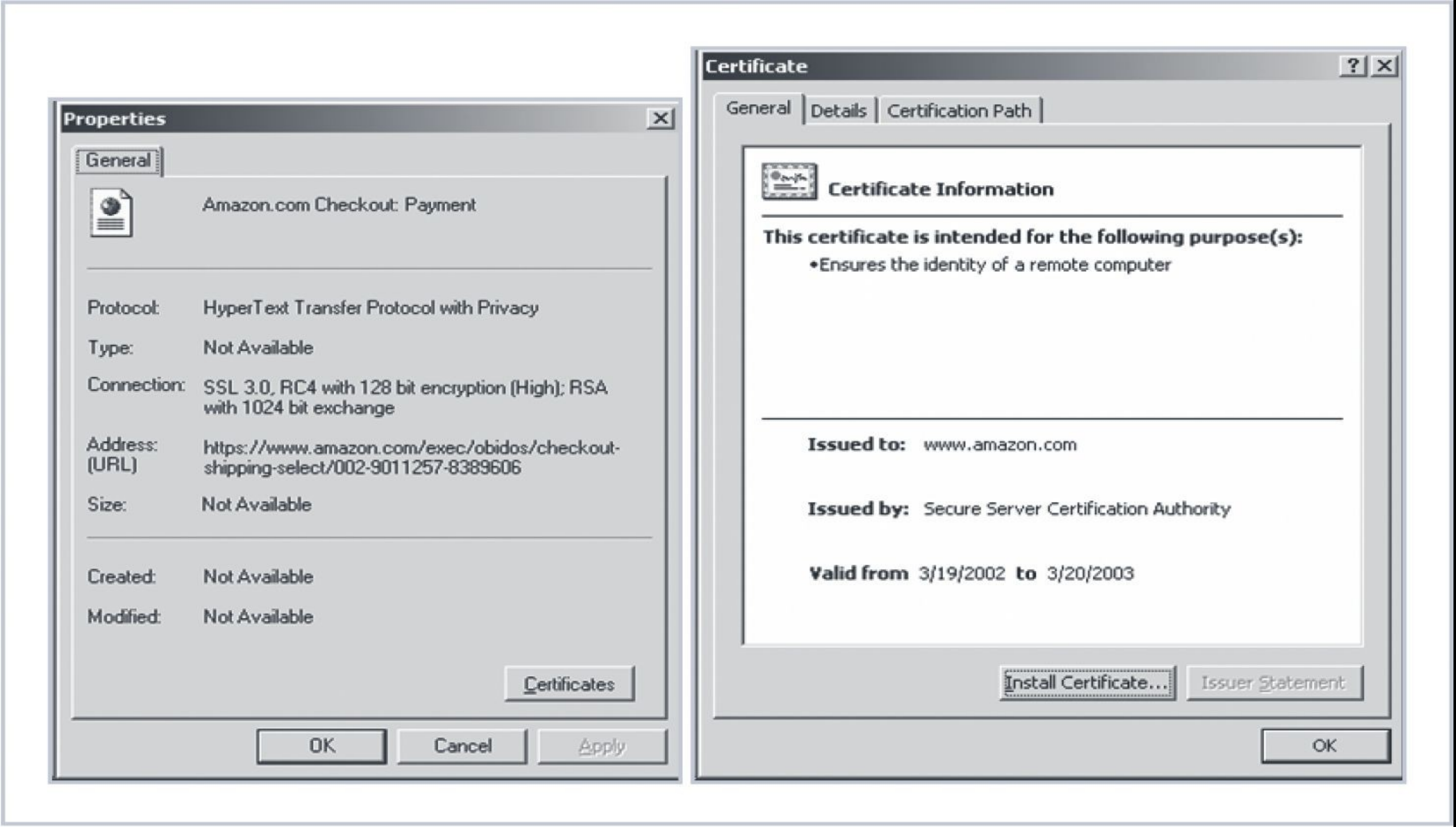
Digital certificate

Electronic document attached to a file
certifying that the file
is from the organization it claims to be from
& has not been modified
from the original format

Certificate authority (CA)

✓ Agency that manages
the issuance of certificates

✓ Serves as the electronic notary public
to verify certificate origin & integrity



Amazon.com Checkout: Payment

Protocol: HyperText Transfer Protocol with Privacy

Type: Not Available

Connection: SSL 3.0, RC4 with 128 bit encryption (High); RSA with 1024 bit exchange

Address: (URL) https://www.amazon.com/exec/obidos/checkout-shipping-select/002-9011257-8389606

Size: Not Available

Created: Not Available

Modified: Not Available

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: www.amazon.com

Issued by: Secure Server Certification Authority

Valid from 3/19/2002 **to** 3/20/2003

FIGURE 9-13 Digital Signature

Public key infrastructure (PKI)

✓ Entire set
of hardware, software, & cryptosystems
necessary to implement public key encryption

✓ Based on public key cryptosystems

✓ Include digital certificates
& certificate authorities

more … →

Can increase capabilities
of an organization
in protecting information assets
by providing the following services:

Authentication: Digital certificates
permit individuals, organizations, & web servers
to authenticate identity of each party
in an Internet transaction

Integrity: Digital certificate demonstrates
that content signed by certificate
has not been altered in transit

more ... →

Confidentiality: PKI keeps information confidential
by ensuring it is not intercepted
during transmission over the Internet

Authorization: Digital certificates
can replace user IDs & passwords,
enhance security, & reduce some of the overhead
required for authorization processes
& controlling access privileges
for specific transactions

Nonrepudiation: Digital certificates
can validate actions, making it less likely
that customers or partners can later repudiate
a digitally signed transaction,
such as an online purchase

Hybrid Crypto Systems

Pure asymmetric key encryption

✓ Not widely used
except in the area of certificates

✓ Typically employed
in conjunction with symmetric key encryption,
creating a hybrid system

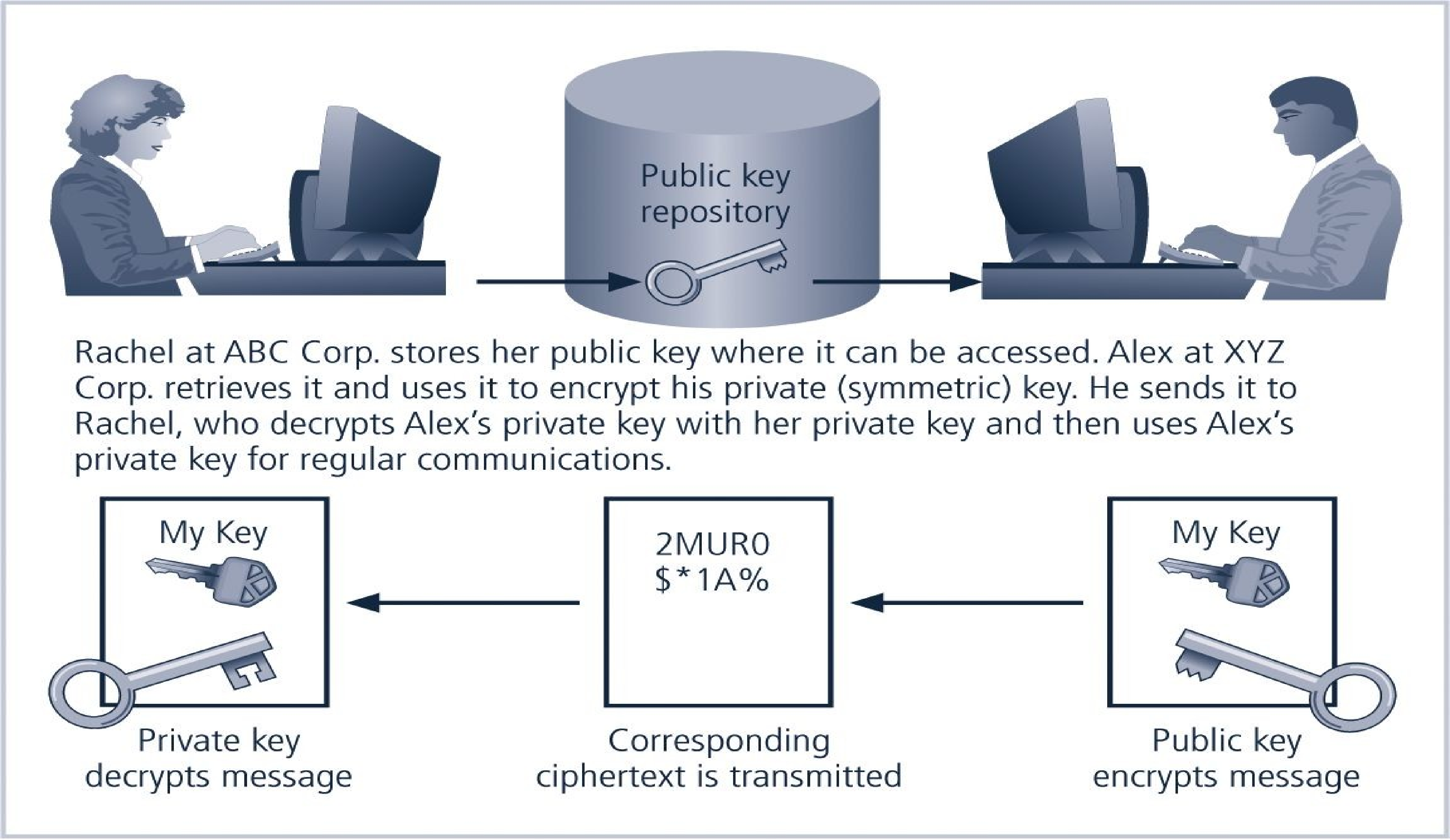
more ... →

Hybrid process in current use is based on the Diffie-Hellman key exchange method

✓ Provides a way to exchange private keys
using public key encryption
without exposure to any third parties

✓ Asymmetric encryption is used
to exchange symmetric keys
so that two organizations can conduct
quick, efficient, secure communications
based on symmetric encryption

✓ Diffie-Hellman provided foundation
for subsequent developments
in public key encryption



Rachel at ABC Corp. stores her public key where it can be accessed. Alex at XYZ Corp. retrieves it and uses it to encrypt his private (symmetric) key. He sends it to Rachel, who decrypts Alex's private key with her private key and then uses Alex's private key for regular communications.

FIGURE 9-14 Hybrid Encryption

Cryptographic controls can be used to support several aspects of business:

✓ Confidentiality & integrity of e-mail
& its attachments

✓ Authentication, confidentiality, integrity,
& nonrepudiation
of e-commerce transactions

✓ Authentication & confidentiality
of remote access through VPN connections

✓ A higher standard of authentication
when used to supplement
access control systems

E-mail Security

Secure
Multipurpose Internet Mail Extensions
(S/MIME)

Builds on
Multipurpose Internet Mail Extensions (MIME)
encoding format
by adding encryption & authentication
via digital signatures
based on public key cryptosystems

more ... →

Privacy Enhanced Mail (PEM)

Proposed by
Internet Engineering Task Force (IETF)
as a standard that will function
with public key cryptosystems

Uses 3DES symmetric key encryption
& RSA
for key exchanges
& digital signatures

more … →

Pretty Good Privacy (PGP)

Uses IDEA Cipher,
a 128-bit symmetric key block encryption algorithm
with 64-bit blocks for message encoding

Uses RSA for symmetric key exchange
& to support digital signatures

Securing the Internet

IP Security (IPSec)

Primary & dominant
cryptographic authentication & encryption product
of IETF’s IP Protocol Security Working Group

Has 2 components:

✓ IP Security protocol which specifies information
to be added to an IP packet
& indicates how to encrypt packet data

✓ Internet Key Exchange which uses
asymmetric key exchange
& negotiates the security associations

more ... →

IPSec works in 2 modes of operation

1. Transport mode

Only IP data is encrypted,
not IP headers themselves,
which allows intermediate nodes
to read source & destination addresses

2. Tunnel mode

Entire IP packet is encrypted
& inserted as the payload
in another IP packet

Securing the Web

Secure Electronic Transactions (SET)

Encrypts credit card transfers
with DES for encryption
& RSA for key exchange

Secure Sockets Layer (SSL)

Uses number of algorithms,
but mainly relies on RSA for key transfer
& on IDEA, DES, or 3DES
for encrypted symmetric key-based data transfer

more … →

Secure Hypertext Transfer Protocol (SHTTP)

Encrypted version of HTTP

Provides secure e-commerce transactions
as well as encrypted Web pages
for secure data transfer over the Web,
using a number of different algorithms

Secure Shell (SSH)

Provides security
for remote access connections
over public networks
by using tunneling
& authentication services
between a client & a server

Used to secure replacement tools for
terminal emulation,
remote management,
& file transfer applications

Kerberos system
knows private keys
& can authenticate
one network node (client or server)
to another

Kerberos also generates
temporary session keys
—that is, private keys
given to the 2 parties in a conversation

Managing Cryptographic Controls

✓ Don’t lose your keys

✓ Know who you are communicating with

✓ It may be illegal to use
a specific encryption technique
when communicating to some nations

✓ Every cryptosystem has weaknesses

✓ Give access
only to those with a business need

more … →

When placing trust into a certificate authority,
ask “Who watches the watchers?”

There is no security in obscurity

Security protocols
& the cryptosystems they use
are installed & configured by humans,
& thus they are only as good as their installers

As with all other InfoSec program components,
make sure that
your organization’s use of cryptography
is based on well-constructed policy
& supported with sound management procedures

Summary

Introduction

Access Controls

Firewalls

Dial-Up Protection

Intrusion Detection Systems

Scanning & Analysis Tools

Cryptography

Thank you!

Scott Granneman