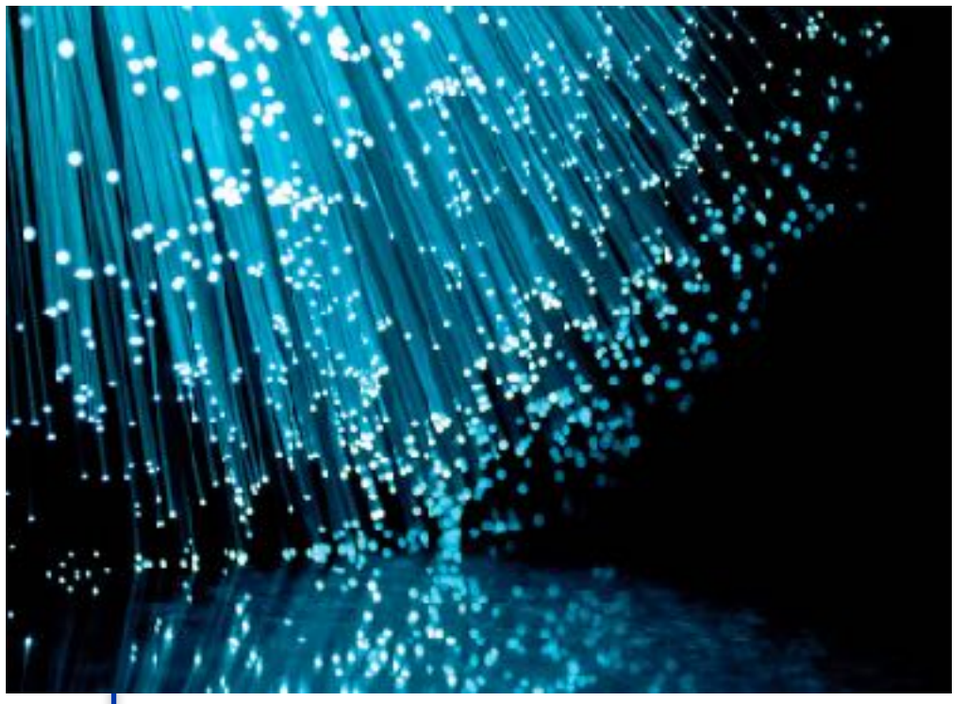
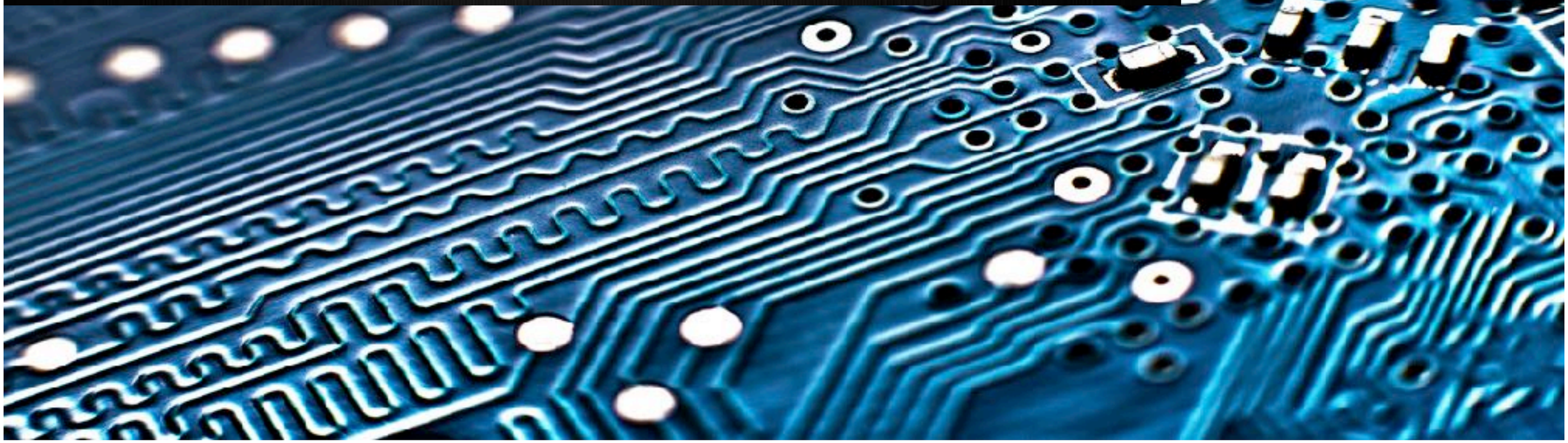


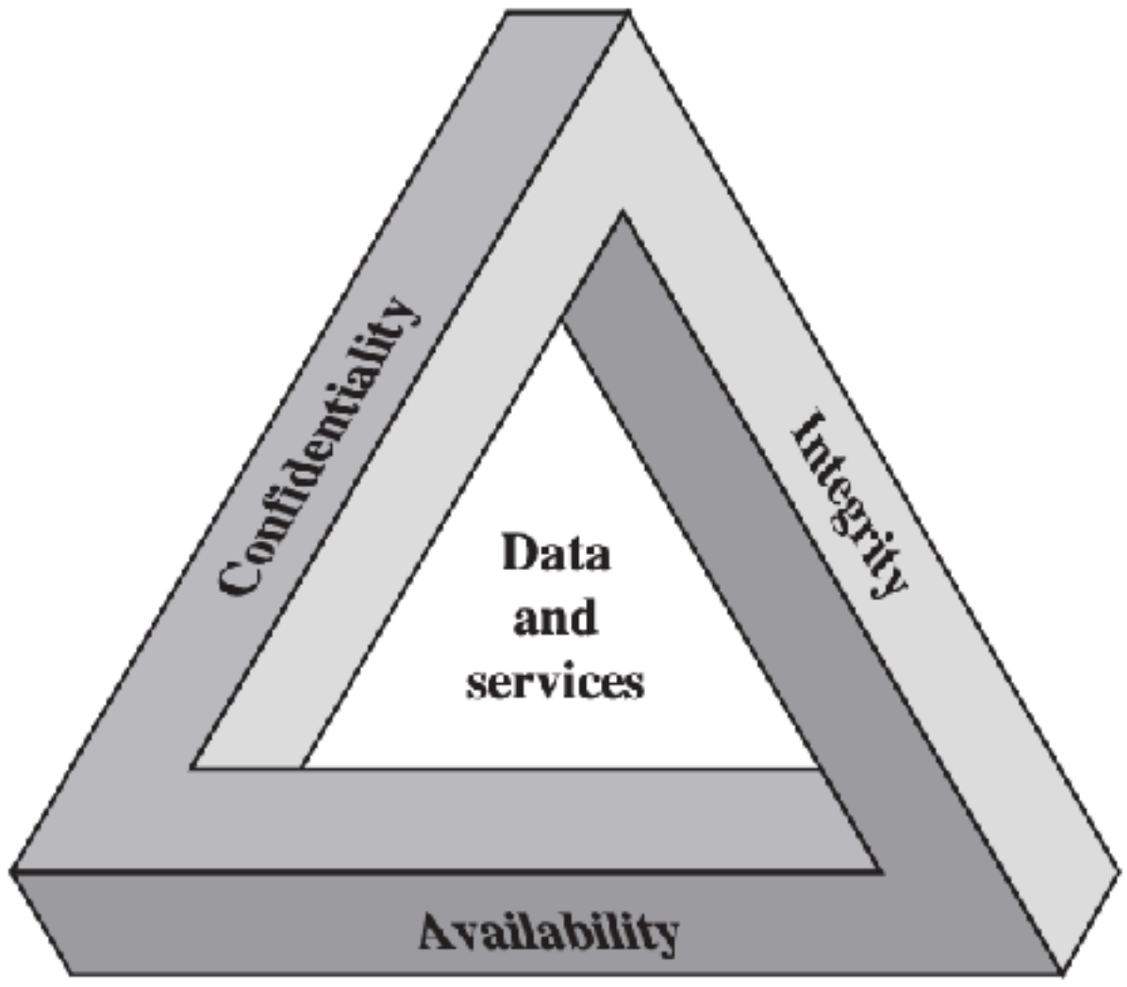
Cybersecurity Primer



Fundamentals

- Confidentiality: This term covers two related concepts:
    - Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
    - Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
- Integrity: This term covers two related concepts:
    - Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
    - System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- Availability: Assures that systems work promptly and service is not denied to authorized users.

CIA Triad


Confidentiality
Integrity
Data
and
services
Availability

Examples - Low

- Low: The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

- As defined in FIPS 199

Examples - Mod

- Moderate: The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

- As defined in FIPS 199

Examples - High

- High: The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious, life-threatening injuries.

- As defined in FIPS 199

Confidentiality

- Student grade information is an asset whose confidentiality is considered to be highly important by students. In the United States, the release of such information is regulated by the Family Educational Rights and Privacy Act (FERPA)

Integrity

- Several aspects of integrity are illustrated by the example of a hospital patient's allergy information stored in a database. The doctor should be able to trust that the information is correct and current. Now suppose that an employee (e.g., a nurse) who is authorized to view and update this information deliberately falsifies the data to cause harm to the hospital.

Availability

- The more critical a component or service, the higher is the level of availability required. Consider a system that provides authentication services for critical systems, applications, and devices. An interruption of service results in the inability for customers to access computing resources and for the staff to access the resources they need to perform critical tasks. The loss of the service translates into a large financial loss due to lost employee productivity and potential customer loss.

Exercise

- Provide 3 examples, in your organization, of Low/Mod/ High for each of the following:
  - Confidentiality concerns
  - Integrity concerns
  - Availability concerns

Challenge of Security

1. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, nonrepudiation, integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.

3. Because of point 2, the procedures used to provide particular services are often counterintuitive. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elab- orate security mechanisms make sense.

4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP (Transmission Control Protocol/Internet Protocol) should mechanisms be placed].

5. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the cre- ation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or net- work that introduces variable, unpredictable delays may render such time limits meaningless.

Challenge of Security (cont:)

- Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

- There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.

- Security requires regular, even constant, monitoring,and this is difficult in today's short-term, overloaded environment.

- Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.

- Many users (and even security administrators) view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

RFC 2828

- Threat
    - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
- Attack
    - An assault on system security that derives from an intelligent threat. That is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

OSI Security Architecture

For our purposes, the OSI security architecture provides a useful, if abstract, overview of many of the concepts that this book deals with. The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as

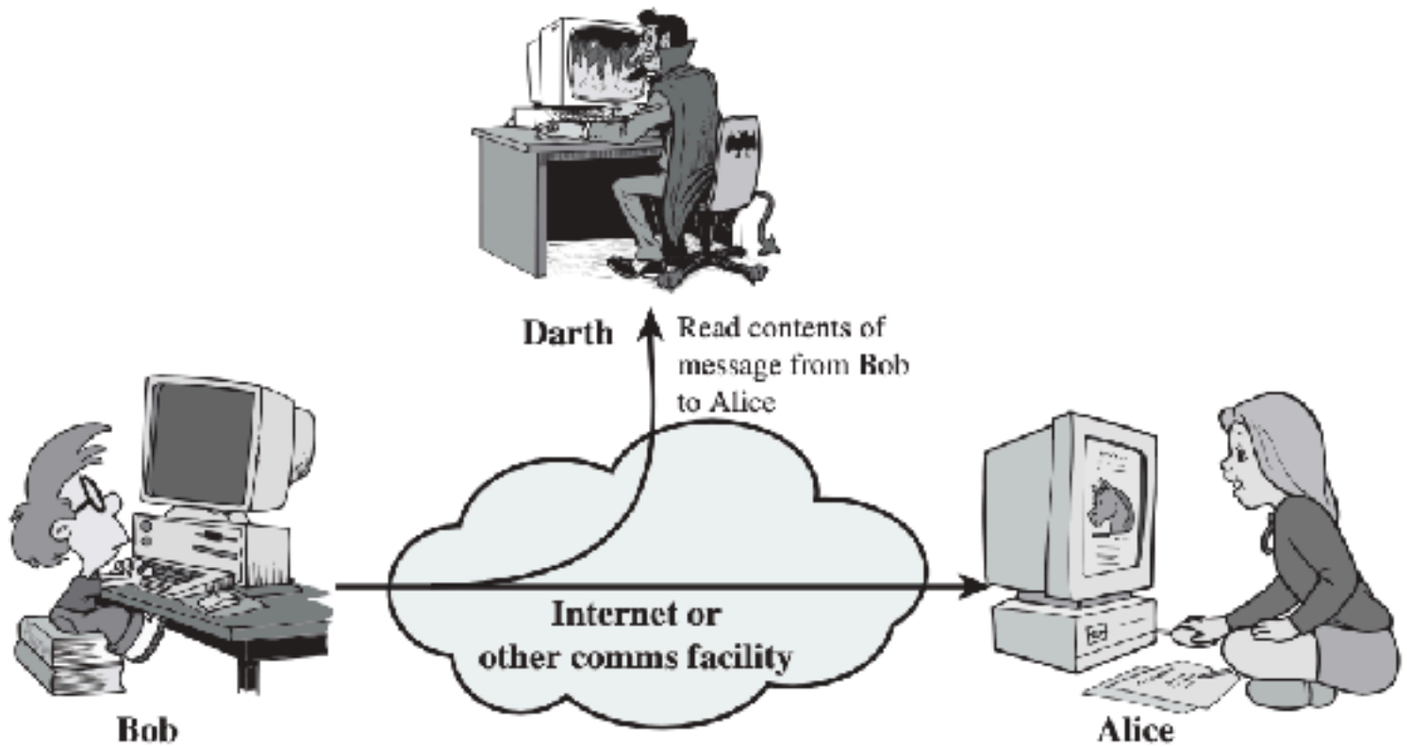
- Security attack: Any action that compromises the security of information owned by an organization.

- Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

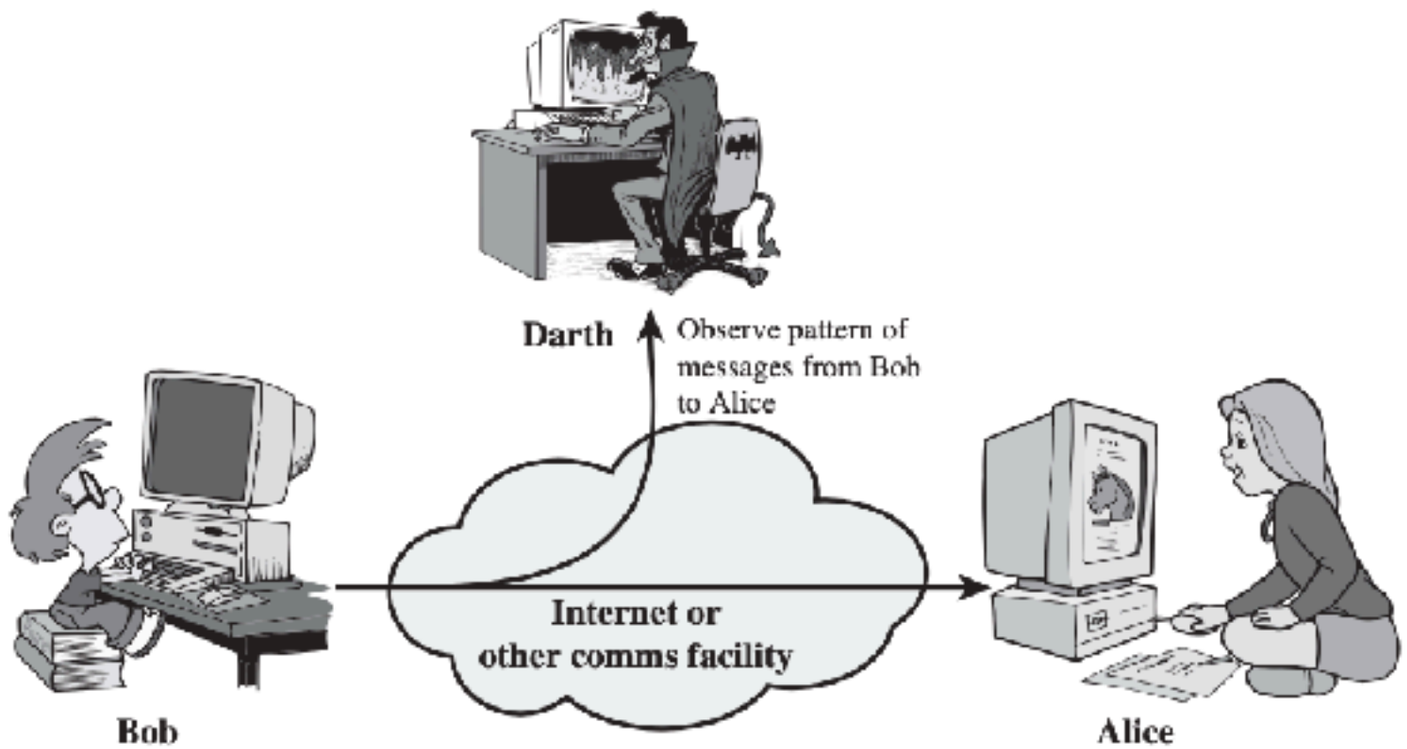
- Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Passive Attacks

- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

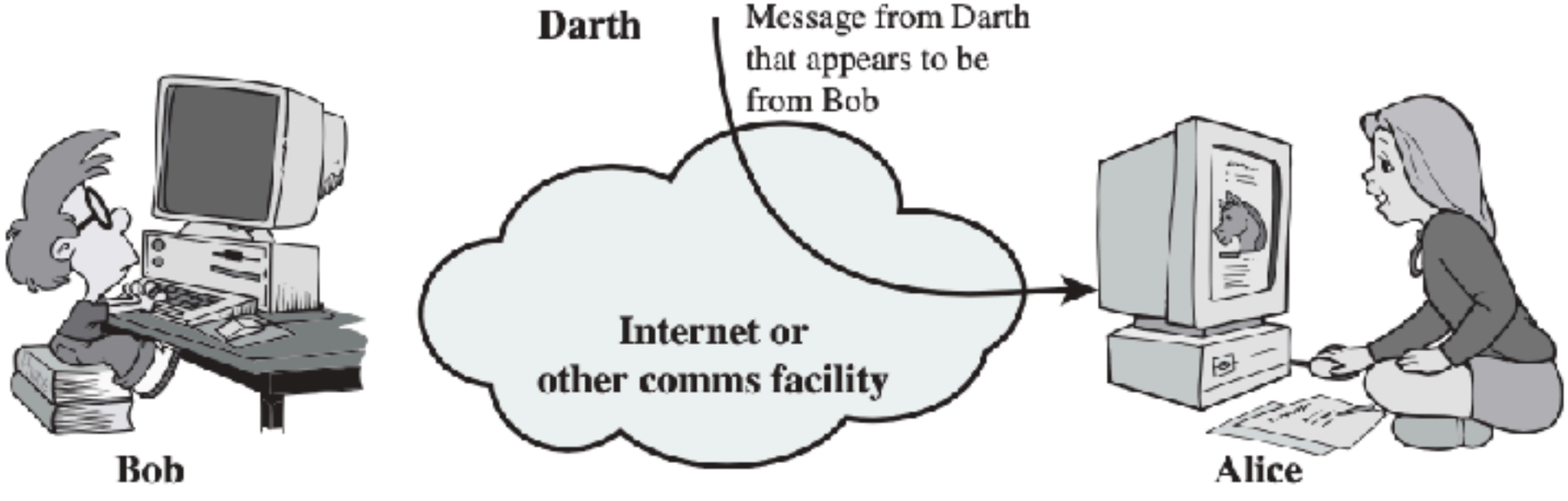


(a) Release of message contents

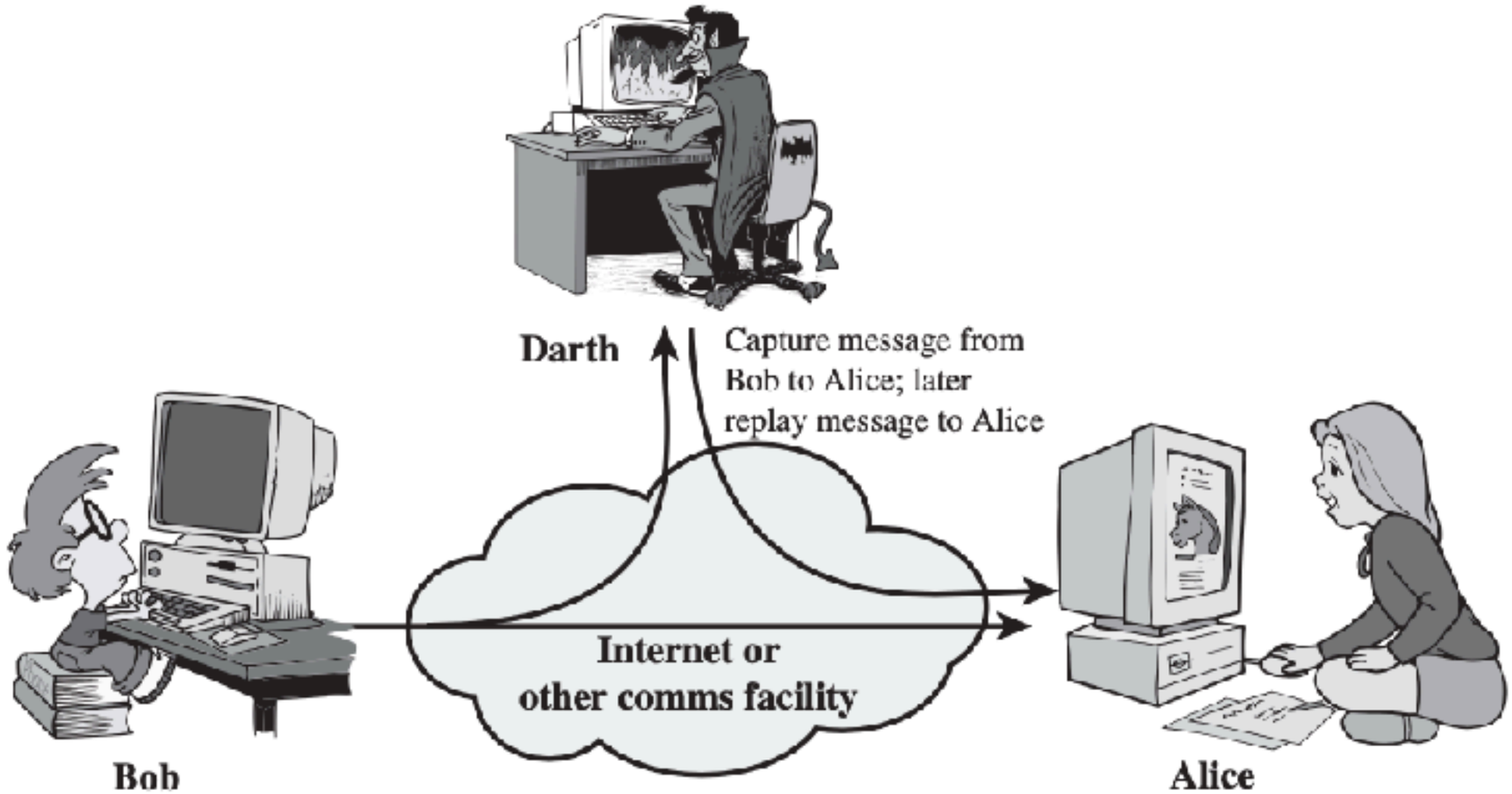


Active Attacks

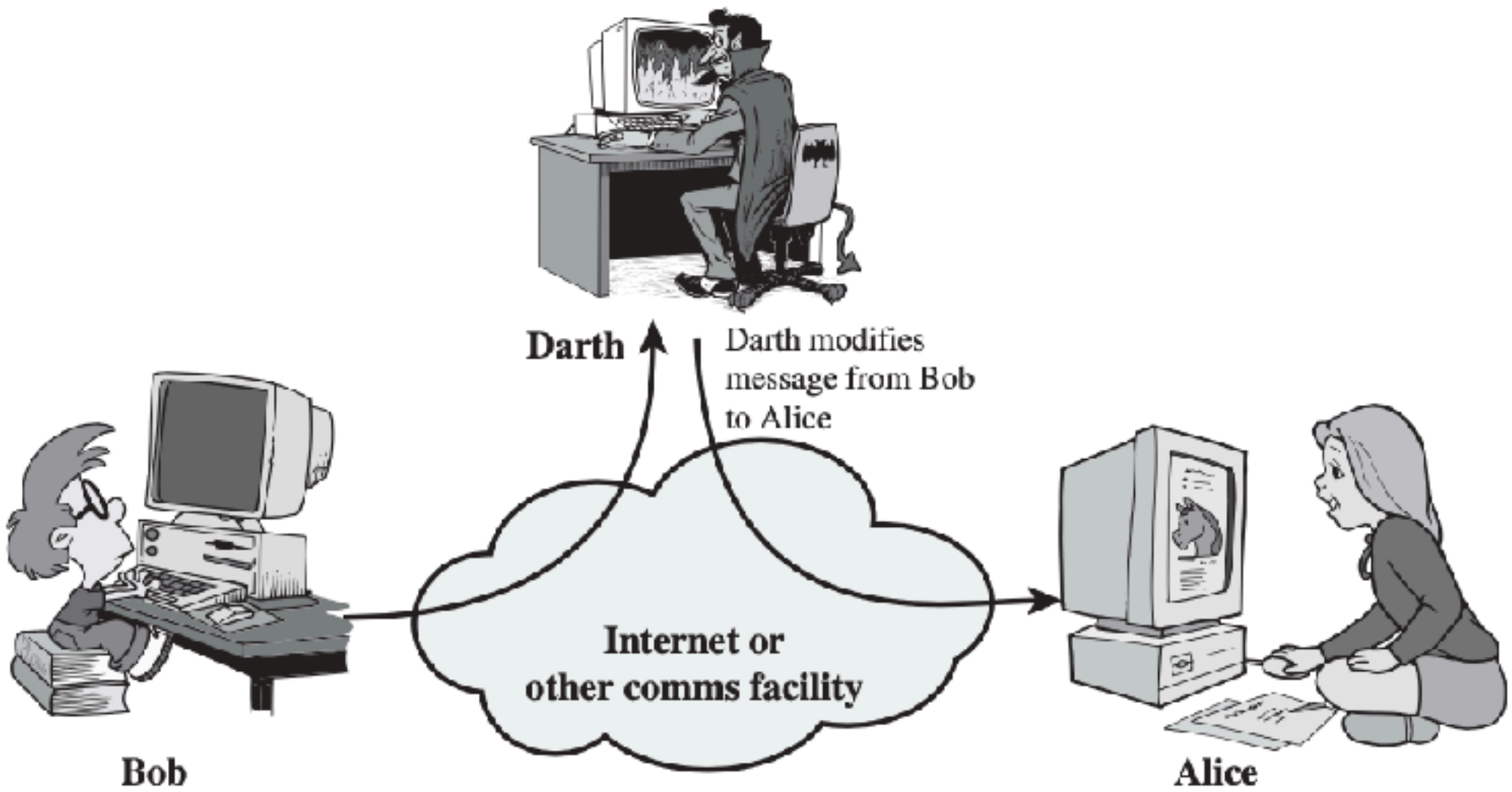
- Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service



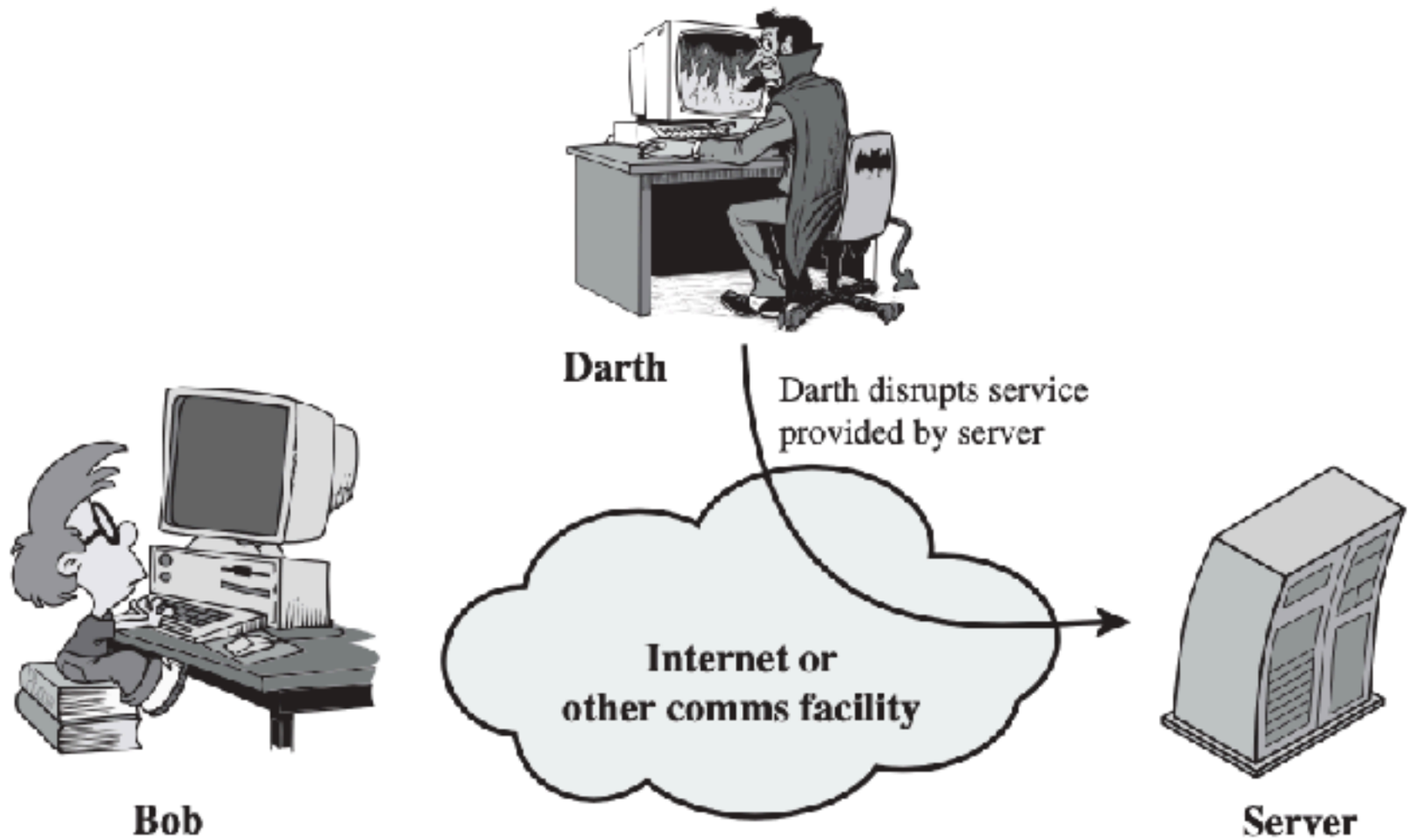
(a) Masquerade


Darth
Capture message from
Bob to Alice; later
replay message to Alice
Internet or
other comms facility
Bob
Alice

(b) Replay



(c) Modification of messages



(d) Denial of service

Exercise

- Using your creativity, provide 2 methods that you could employ to execute a passive and an active attack. Be specific.

X.800 Security Services

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block.

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

Security Mechanisms

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

Security Services related to Mechanisms

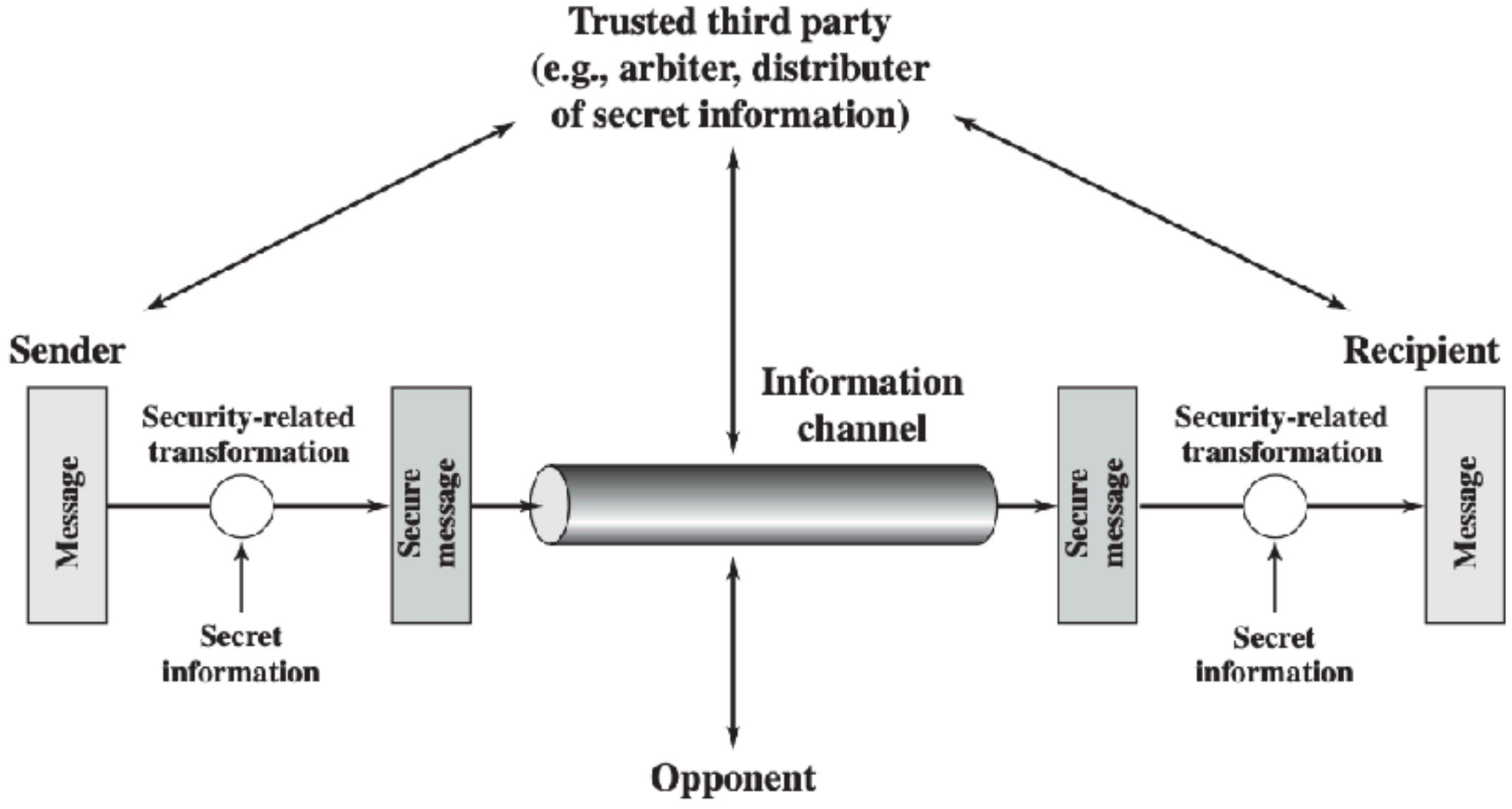
	Mechanism							
Service	**Encipherment**	**Digital Signature**	**Access Control**	**Data Integrity**	**Authentication Exchange**	**Traffic Padding**	**Routing Control**	**Notarization**
Peer Entity Authentication	Y	Y			Y			
Data-Origin Authentication	Y	Y						
Access Control			Y					
Confidentiality	Y						Y	
Traffic-Flow Confidentiality	Y					Y	Y	
Data Integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Model for Network Security

- A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

- Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception

Model for Network Security



Model for Security Services

- Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.

- Generate the secret information to be used with the algorithm.

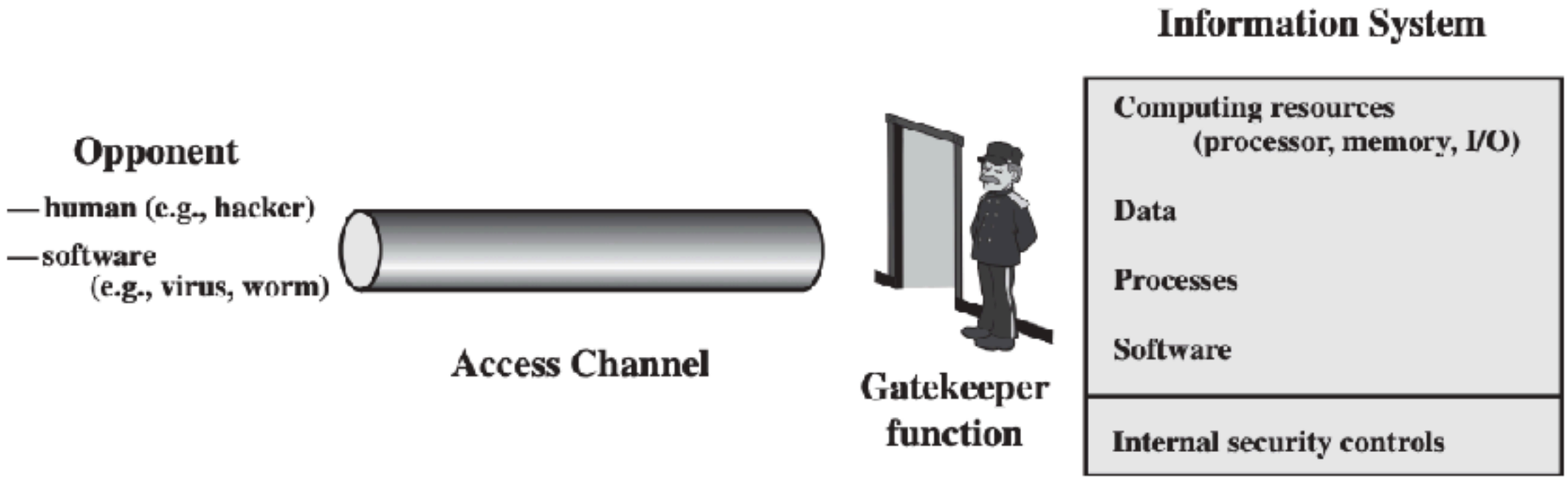
- Develop methods for the distribution and sharing of the secret information.

- Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Other Threats

- Information access threats: Intercept or modify data on behalf of users who should not have access to that data.
- Service threats: Exploit service flaws in computers to inhibit use by legitimate users.

Viruses/Worms



Exercise

- What is the difference between passive and active security threats?

- List and briefly define categories of passive and active security attacks.

- List and briefly define categories of security services.

- List and briefly define categories of security mechanisms.

Exercise

- Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system. In each case, indicate the degree of importance of the requirement.

Exercise

- For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.
    - An organization managing public information on its Web server.
    - A law-enforcement organization managing extremely sensitive investigative information.
    - A financial organization managing routine administrative information (not privacy-related information).
    - An information system used for large acquisitions in a contracting organization that contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.
    - A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

PUBLIC-KEY CRYPTOGRAPHY AND MESSAGE AUTHENTICATION

Introduction

- Encryption protects against passive attack (eavesdropping). A different requirement is to protect against active attack (falsification of data and transactions). Protection against such attacks is known as message authentication.

- A message, file, document, or other collection of data is said to be authentic

- when it is genuine and comes from its alleged source. Message authentication is a

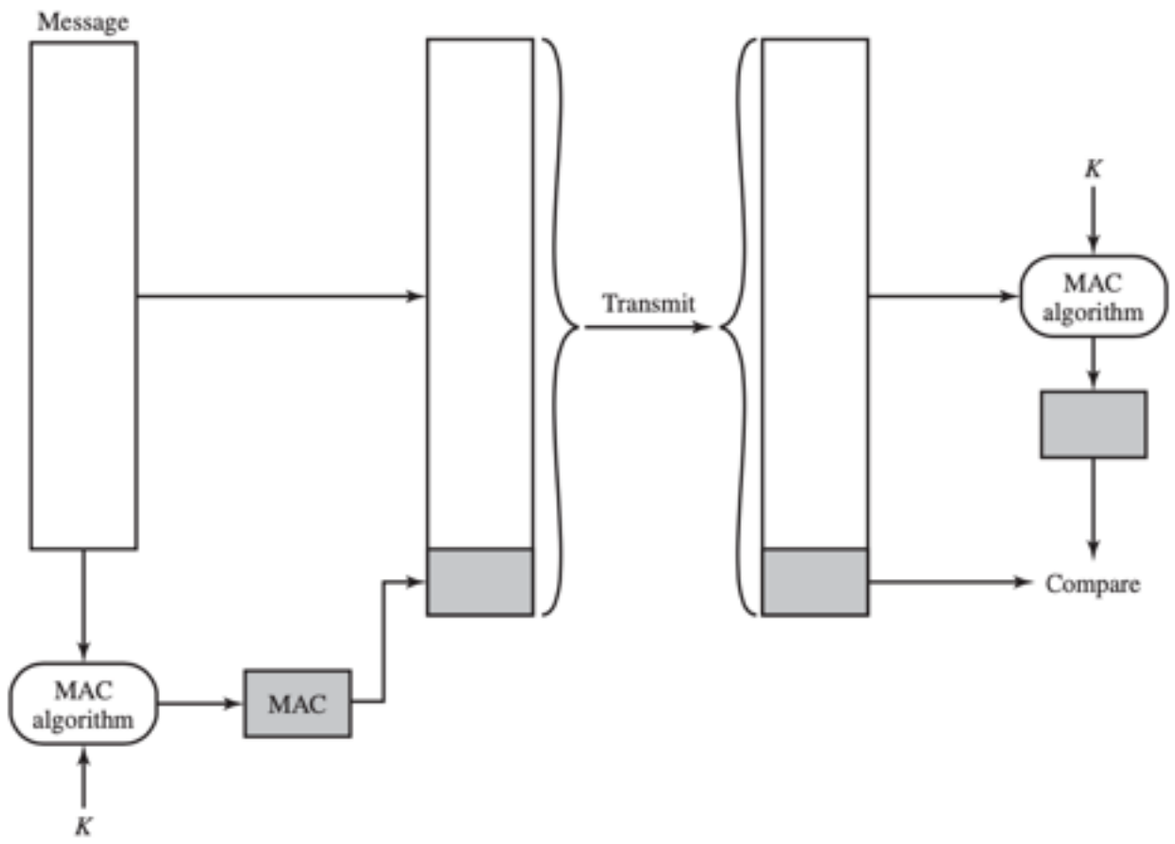
- procedure that allows communicating parties to verify that received messages are authentic

- The two important aspects are to verify that the contents oof the message have not been altered and that the source is authentic. We may also wish to verify a message's timeliness (it has not been artificially delayed and replayed) and sequence relative to other messages flowing between two parties. All of these concerns come under the category of data integrity

- Symmetric encryption alone is not a suitable tool for data authentication. To give one simple example, in the encryption, if an attacker reorders the blocks of ciphertext, then each block will still decrypt successfully. However, the reordering may alter the meaning of the overall data sequence. Although sequence numbers may be used at some level (e.g., each IP packet), it is typically not the case that a separate sequence number will be associated with each b-bit block of plaintext. Thus, block reordering is a threat.

Authentication Code

- One authentication technique involves the use of a secret key to generate a small block of data, known as a message authentication code (MAC), that is appended to the message. This technique assumes that two communicating parties, say A and B, share a common secret key K AB.



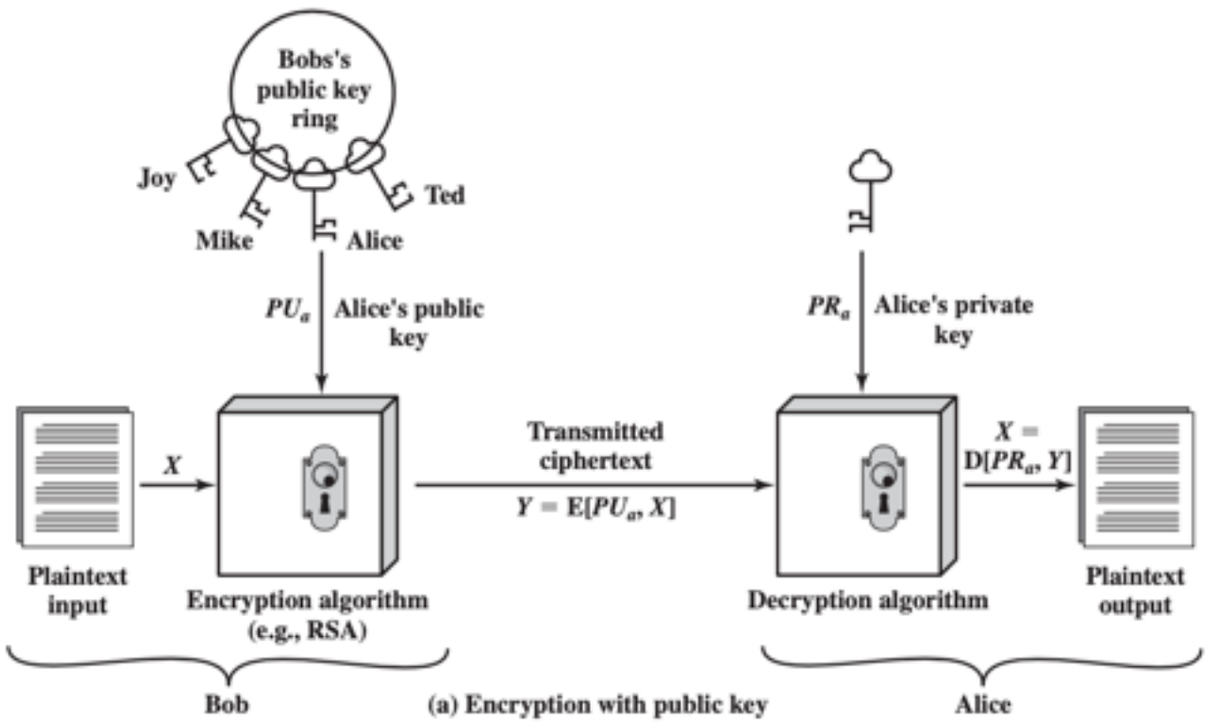
PUBLIC-KEY CRYPTOGRAPHY PRINCIPLES

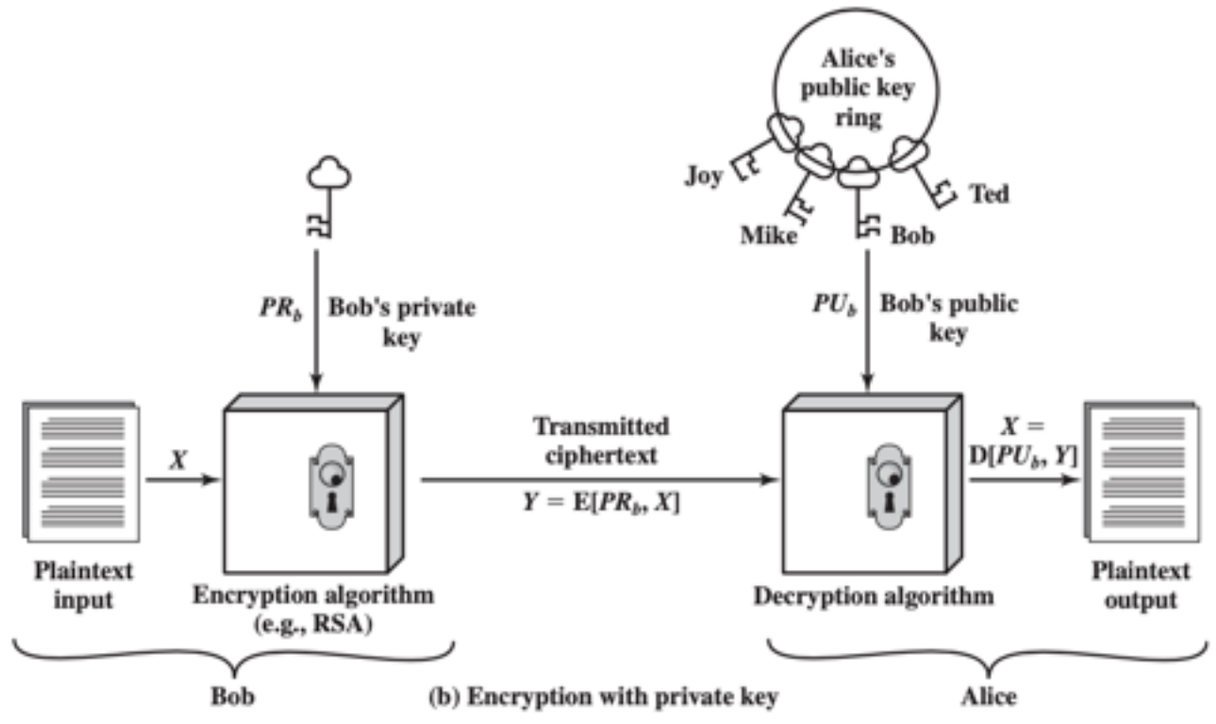
- Of equal importance to conventional encryption is public-key encryption, which finds use in message authentication and key distribution

- Public-key encryption, first publicly proposed by Diffie and Hellman in 1976 [DIFF76], is the first truly revolutionary advance in encryption in literally thousands of years. Public-key algorithms are based on mathematical functions rather than on simple operations on bit patterns, such as are used in symmetric encryption algo- rithms. More important, public-key cryptography is asymmetric, involving the use of two separate keys—in contrast to the symmetric conventional encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication

- A public-key encryption scheme has six ingredients .
    - Plaintext: This is the readable message or data that is fed into the algorithm as input.
    - Encryption algorithm: The encryption algorithm performs various transforma- tions on the plaintext.
    - Public and private key: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact trans- formations performed by the encryption algorithm depend on the public or private key that is provided as input.
    - Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.
    - Decryption algorithm: This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

Using Keys for Encryption





The essential steps are the following

- Each user generates a pair of keys to be used for the encryption and decryp- tion of messages.

- Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private. Each user maintains a collection of public keys obtained from others.

- If Bob wishes to send a private message to Alice, Bob encrypts the message using Alice’s public key.

- When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice’s pri- vate key.

Applications for Public-Key Cryptosystems

- Encryption/decryption: The sender encrypts a message with the recipient's public key

- Digital signature: The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.

- Key exchange: Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties

Exercise

- What are the principal ingredients of a public-key cryptosystem?
- List and briefly define three uses of a public-key cryptosystem.
- Name a network service that you know of that uses public/private key architecture.
- What type of system does azure blob storage use?

KEY DISTRIBUTION AND USER AUTHENTICATION

SYMMETRIC KEY DISTRIBUTION USING SYMMETRIC ENCRYPTION

- For symmetric encryption to work, the two parties to an exchange must share the same key, and that key must be protected from access by others. Furthermore, frequent key changes are usually desirable to limit the amount of data compromised if an attacker learns the key. Therefore, the strength of any cryptographic system rests with the key distribution technique, a term that refers to the means of delivering a key to two parties that wish to exchange data, without allowing others to see the key. Key distribution can be achieved in a number of ways. For two parties A and B, there are the following options:

- A key could be selected by A and physically delivered to B.

- A third party could select the key and physically deliver it to A and B.

- If A and B have previously and recently used a key, one party could transmit the new key to the other, using the old key to encrypt the new key.

- If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B.

KERBEROS

- Kerberos is a key distribution and user authentication service developed at MIT. The problem that Kerberos addresses is this: Assume an open distributed environ-ment in which users at workstations wish to access services on servers distributed throughout the network. We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. In this environ-ment, a workstation cannot be trusted to identify its users correctly to network services. In particular, the following three threats exist:

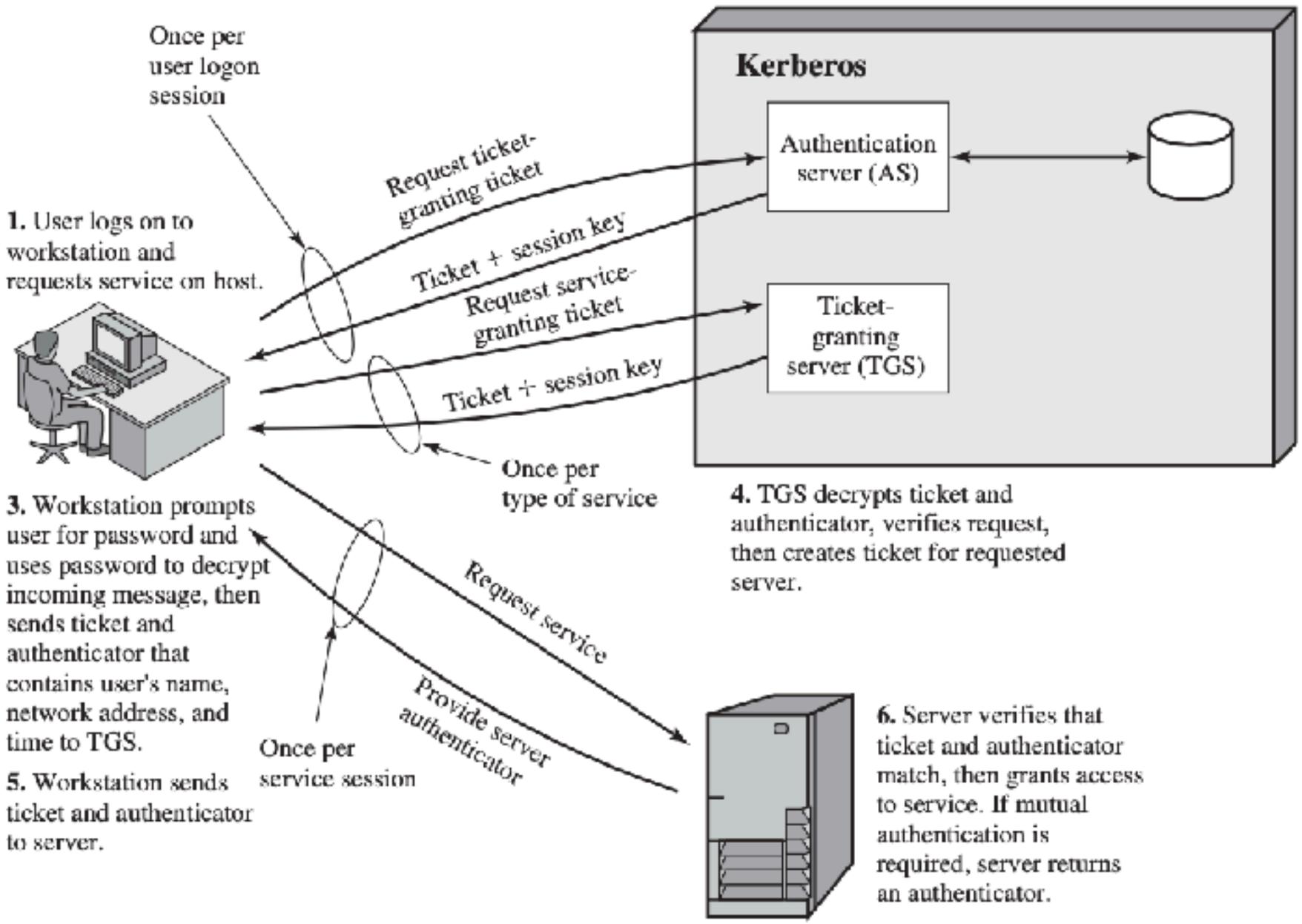
- A user may gain access to a particular workstation and pretend to be another user operating from that workstation.

- A user may alter the network address of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation.

- A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations

- In any of these cases, an unauthorized user may be able to gain access to services and data that he or she is not authorized to access. Rather than building elaborate authentication protocols at each server, Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. Kerberos relies exclusively on symmetric encryption, making no use of public-key encryption.

The Flow


2. AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.
Kerberos
Authentication server (AS)
Ticket-granting server (TGS)
Once per user logon session
1. User logs on to workstation and requests service on host.
Request ticket-granting ticket
Ticket + session key
Request service-granting ticket
Ticket + session key
Once per type of service
3. Workstation prompts user for password and uses password to decrypt incoming message, then sends ticket and authenticator that contains user's name, network address, and time to TGS.
4. TGS decrypts ticket and authenticator, verifies request, then creates ticket for requested server.
Request service
Provide server authenticator
Once per service session
5. Workstation sends ticket and authenticator to server.
6. Server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.

KEY DISTRIBUTION USING ASYMMETRIC ENCRYPTION

- One of the major roles of public-key encryption is to address the problem of key distribution. There are actually two distinct aspects to the use of public-key encryption in this regard.

- The distribution of public keys.

- The use of public-key encryption to distribute secret keys.

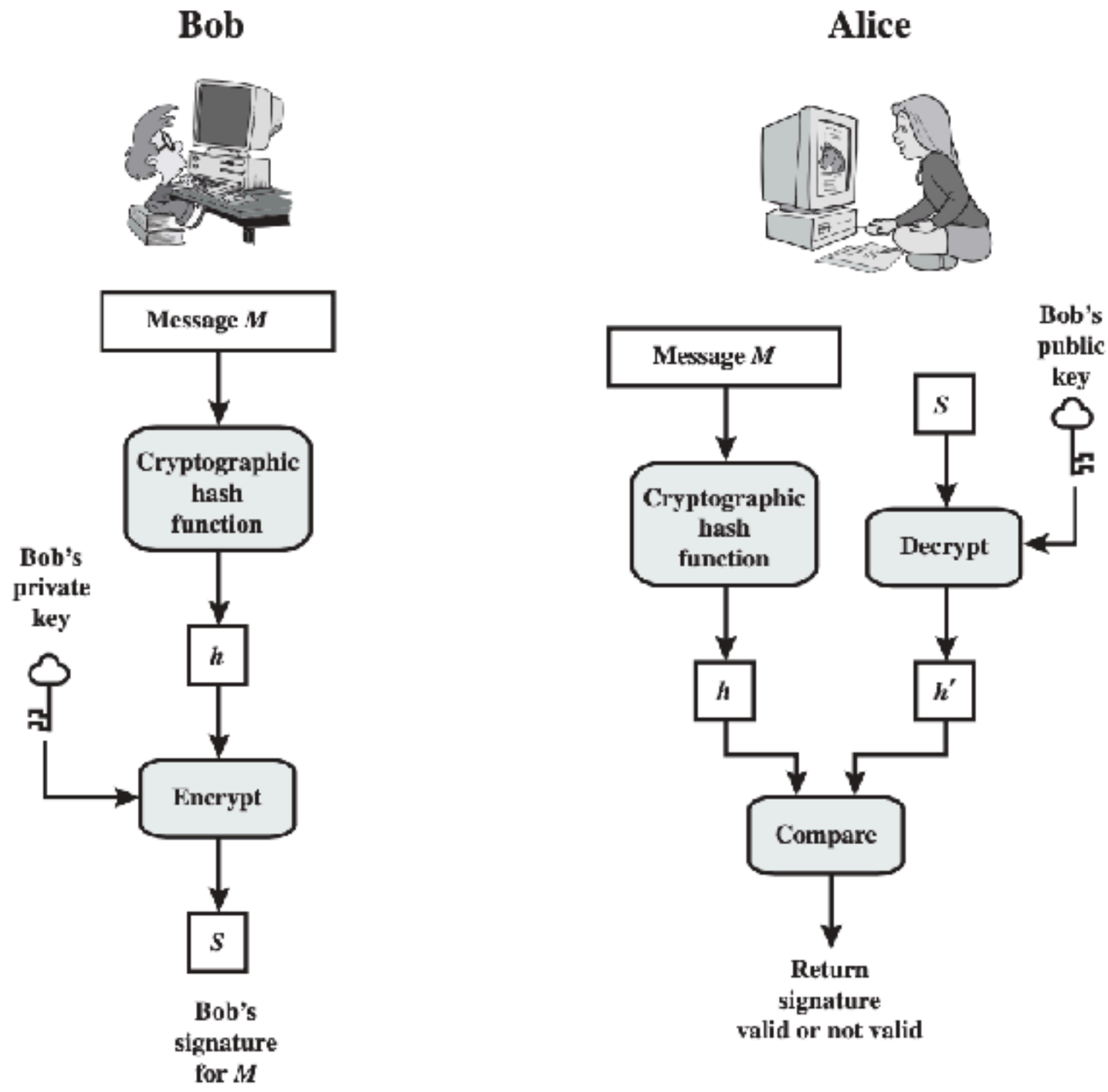
X.509 CERTIFICATES

- ITU-T recommendation X.509 is part of the X.500 series of recommendations that define a directory service. The directory is, in effect, a server or distributed set of servers that maintains a database of information about users. The information includes a mapping from user name to network address, as well as other attributes and information about the users.

- X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. The directory may serve as a repository of public-key certificates. Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority.

- The heart of the X.509 scheme is the public-key certificate associated with each user. These user certificates are assumed to be created by some trusted certification authority (CA) and placed in the directory by the CA or by the user.

X.509 Flow


Bob
Alice
Message M
Cryptographic hash function
h
Bob's private key
Encrypt
S
Bob's signature for M
Message M
Cryptographic hash function
h
S
Bob's public key
Decrypt
h'
Compare
Return signature valid or not valid

Key Components of identity Mgtmt

- Authentication: Confirmation that a user corresponds to the user name provided.
  Authorization: Granting access to specific services and/or resources based on the authentication.

- Accounting: A process for logging access and authorization.

- Provisioning: The enrollment of users in the system.

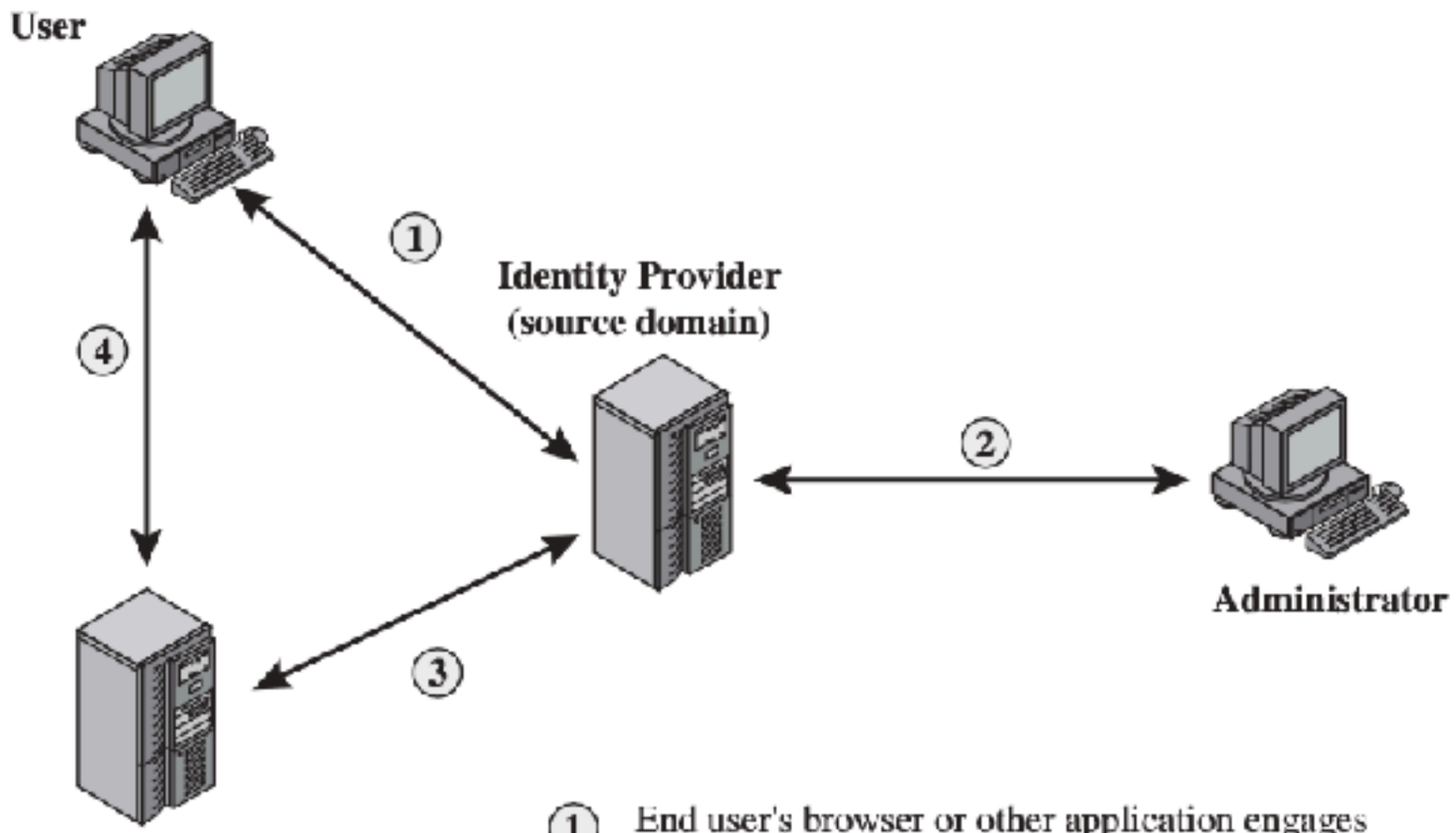
- Workflow automation: Movement of data in a business process.

- Delegated administration: The use of role-based access control to grant permissions.

- Password synchronization: Creating a process for single sign-on (SSO) or reduced sign-on (RSO). Single sign-on enables a user to access all network resources after a single authentication. RSO may involve multiple sign-ons but requires less user effort than if each resource and service maintained its own authentication facility.

- Self-service password reset: Enables the user to modify his or her password.

- Federation: A process where authentication and permission will be passed on from one system to another—usually across multiple enterprises, thereby reducing the number of authentications needed by the user.



(1) End user's browser or other application engages in an authentication dialogue with identity provider in the same domain. End user also provides attribute values associated with user's identity.

(2) Some attributes associated with an identity, such as allowable roles, may be provided by an administrator in the same domain.

(3) A service provider in a remote domain, which the user wishes to access, obtains identity information, authentication information, and associated attributes from the identity provider in the source domain.

(4) Service provider opens session with remote user and enforces access control restrictions based on user's identity and attributes.

Exercise

- List ways in which secret keys can be distributed to two communicating parties.

- Solve the following (continued on next page):

“We are under great pressure, Holmes.” Detective Lestrade looked nervous. “We have learned that copies of sensitive government documents are stored in computers of one foreign embassy here in London. Normally these documents exist in electronic form only on a selected few government computers that satisfy the most stringent security require- ments. However, sometimes they must be sent through the network connecting all gov- ernment computers. But all messages in this network are encrypted using a top secret encryption algorithm certified by our best crypto experts. Even the NSA and the KGB are unable to break it. And now these documents have appeared in hands of diplomats of a small, otherwise insignificant, country. And we have no idea how it could happen.”

“But you do have some suspicion who did it, do you?” asked Holmes.

“Yes, we did some routine investigation. There is a man who has legal access to one of the government computers and has frequent contacts with diplomats from the embassy. But the computer he has access to is not one of the trusted ones where these documents are normally stored. He is the suspect, but we have no idea how he could obtain copies of the documents. Even if he could obtain a copy of an encrypted docu- ment, he couldn’t decrypt it.”

“Hmm, please describe the communication protocol used on the network.” Holmes opened his eyes, thus proving that he had followed Lestrade’s talk with an attention that contrasted with his sleepy look.

“Well, the protocol is as follows. Each node N of the network has been assigned a unique secret key Kn. This key is used to secure communication between the node and a trusted server. That is, all the keys are stored also on the server. User A, wishing to send a secret message M to user B, initiates the following protocol:

Exercise cont:

1. A generates a random number R and sends to the server his name A, destination B, and E(Ka, R).

2. Server responds by sending E(Kb, R) to A.

3. A sends E(R, M) together with E(Kb, R) to B.

4. B knows Kb, thus decrypts E(Kb, R) to get R and will subsequently use R to decrypt E(R, M) to get M.

You see that a random key is generated every time a message has to be sent. I admit the man could intercept messages sent between the top secret trusted nodes, but I see no way he could decrypt them."

"Well, I think you have your man, Lestrade. The protocol isn't secure because the server doesn't authenticate users who send him a request.

Apparently designers of the protocol have believed that sending E(Kx, R) implicitly authenticates user X as the sender, as only X (and the server) knows Kx. But you know that E(Kx, R) can be intercepted and later replayed. Once you understand where the hole is, you will be able to obtain enough evidence by monitoring the man's use of the computer he has access to. Most likely he works as follows: After intercepting E(Ka, R) and E(R, M) (see steps 1 and 3 of the protocol), the man, let's denote him as Z, will continue by pretending to be A and...

Finish the sentence for Holmes.

TRANSPORT-LEVEL SECURITY

WEB SECURITY CONSIDERATIONS

- The World Wide Web is fundamentally a client/server application running over the Internet and TCP/IP intranets. As such, the security tools and approaches discussed so far in this book are relevant to the issue of Web security. But, as pointed out in [GARF02], the Web presents new challenges not generally appreciated in the con- text of computer and network security.

- The Internet is two-way. Unlike traditional publishing environments—even electronic publishing systems involving teletext, voice response, or fax-back— the Web is vulnerable to attacks on the Web servers over the Internet.

- The Web is increasingly serving as a highly visible outlet for corporate and product information and as the platform for business transactions. Reputations can be damaged and money can be lost if the Web servers are subverted.

- Although Web browsers are very easy to use, Web servers are relatively easy to configure and manage, and Web content is increasingly easy to develop, the underlying software is extraordinarily complex. This complex software may hide many potential security flaws. The short history of the Web is filled with examples of new and upgraded systems, properly installed, that are vulnerable to a variety of security attacks.

- A Web server can be exploited as a launching pad into the corporation's or agency's entire computer complex. Once the Web server is subverted, an attacker may be able to gain access to data and systems not part of the Web itself but connected to the server at the local site.

- Casual and untrained (in security matters) users are common clients for Web-based services. Such users are not necessarily aware of the security risks that exist and do not have the tools or knowledge to take effective countermeasures.

Threats

	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerability to all other threats	Cryptographic checksums
Confidentiality	• Eavesdropping on the net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web proxies
Denial of Service	• Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic techniques

- Another way to classify Web security threats is in terms of the location of the threat: Web server, Web browser, and network traffic between browser and server.

SECURE SOCKET LAYER AND TRANSPORT LAYER SECURITY

- Netscape originated SSL. Version 3 of the protocol was designed with public review and input from industry and was published as an Internet draft document. Subsequently, when a consensus was reached to submit the protocol for Internet standardization, the TLS working group was formed within IETF to develop a com- mon standard. This first published version of TLS can be viewed as essentially an SSLv3.1 and is very close to and backward compatible with SSLv3.

- Two important SSL concepts are the SSL session and the SSL connection, which are defined in the specification as follows.

SSL Key Components

- Connection: A connection is a transport (in the OSI layering model defini- tion) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session.

- Session: An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

SSL Record Protocol

- The SSL Record Protocol provides two services for SSL connections:

  - Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.

  - Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

HTTPS

- HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to imple- ment secure communication between a Web browser and a Web server. The HTTPS capability is built into all modern Web browsers. Its use depends on the Web server supporting HTTPS communication. For example, search engines do not support HTTPS.

- The principal difference seen by a user of a Web browser is that URL (uni- form resource locator) addresses begin with https:// rather than http://. A normal HTTP connection uses port 80. If HTTPS is specified, port 443 is used, which invokes SSL.

HTTPS Encryption

- When HTTPS is used, the following elements of the communication are encrypted:
    - URL of the requested document
    - Contents of the document
    - Contents of browser forms (filled in by browser user)
    - Cookies sent from browser to server and from server to browser
    - Contents of HTTP header

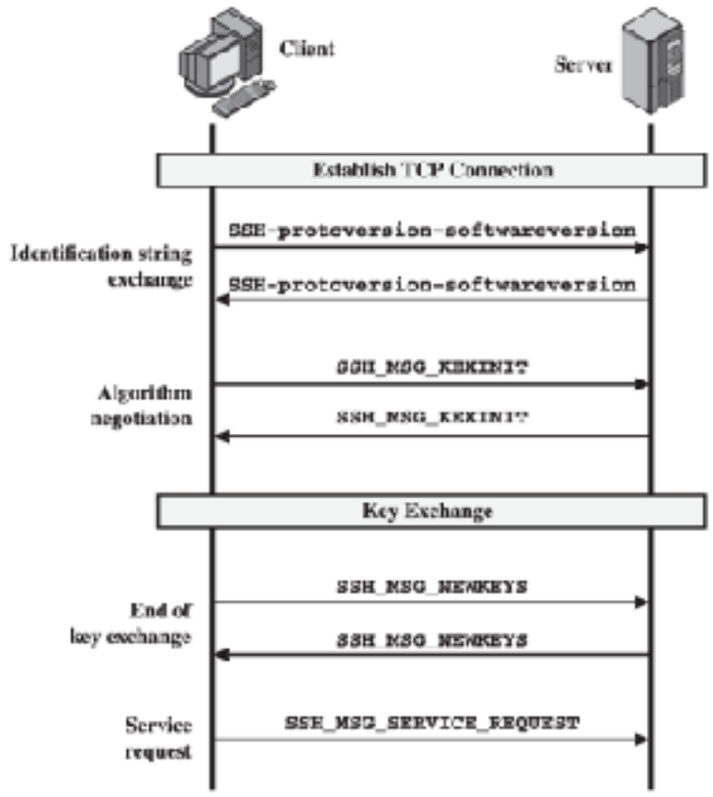
HTTPS is documented in RFC 2818, HTTP Over TLS. There is no fundamen- tal change in using HTTP over either SSL or TLS, and both implementations are referred to as HTTPS.

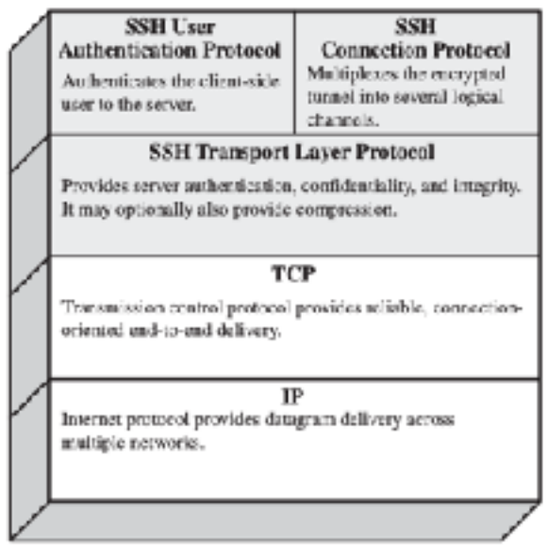
Connection Initiation

- For HTTPS, the agent acting as the HTTP client also acts as the TLS client. The client initiates a connection to the server on the appropriate port and then sends the TLS ClientHello to begin the TLS handshake. When the TLS handshake has finished, the client may then initiate the first HTTP request. All HTTP data is to be sent as TLS application data. Normal HTTP behavior, including retained connections, should be followed.

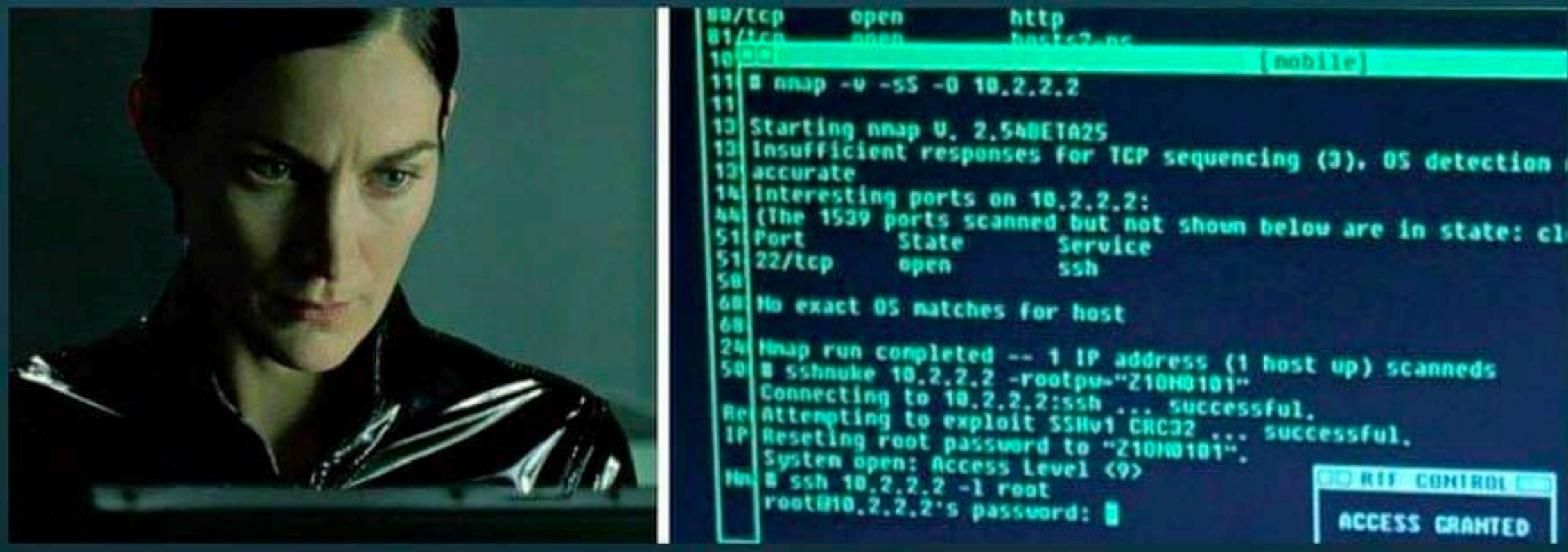
SECURE SHELL (SSH)

- Secure Shell (SSH) is a protocol for secure network communications designed to be relatively simple and inexpensive to implement. The initial version, SSH1 was focused on providing a secure remote logon facility to replace TELNET and other remote logon schemes that provided no security. SSH also provides a more general client/server capability and can be used for such network functions as file transfer and e-mail. A new version, SSH2, fixes a number of security flaws in the original scheme. SSH2 is documented as a proposed standard in IETF RFCs 4250 through 4256.





Reason why Matrix is one of the best geek movies of all time



While most of the movies show ridiculously animated scenes of hacking, Trinity in Matrix Reloaded actually does it in a proper way.

She uses nmap to find an open SSH server and then uses SSH1 CRC32 exploit, which was actually a real world exploit back in 2001.

Exercise

- Consider the following threats to Web security and describe how each is countered by a particular feature of SSL.

    - Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm.

    - Known Plaintext Dictionary Attack: Many messages will contain predictable plaintext, such as the HTTP GET command. An attacker constructs a dictionary containing every possible encryption of the known-plaintext message. When an encrypted message is intercepted, the attacker takes the portion containing the encrypted known plaintext and looks up the ciphertext in the dictionary. The ciphertext should match against an entry that was encrypted with the same secret key. If there are several matches, each of these can be tried against the full cipher- text to determine the right one. This attack is especially effective against small key sizes (e.g., 40-bit keys).

    - Replay Attack: Earlier SSL handshake messages are replayed.

    - Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client.

    - Password Sniffing: Passwords in HTTP or other application traffic are eaves-dropped.

    - IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data.

    - IP Hijacking: An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts.

    - SYN Flooding: An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacked TCP module typically leaves the “half-open connection” around for a few minutes. Repeated SYN messages can clog the TCP module.

IP Security

IPSec

- IP-level security encompasses three functional areas: authentication, confidentiality, and key management. The authentication mechanism assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header. In addition, this mechanism assures that the packet has not been altered in transit. The confidentiality facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties. The key management facility is concerned with the secure exchange of keys. Think VPN.

Application of IPsec

- IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include:

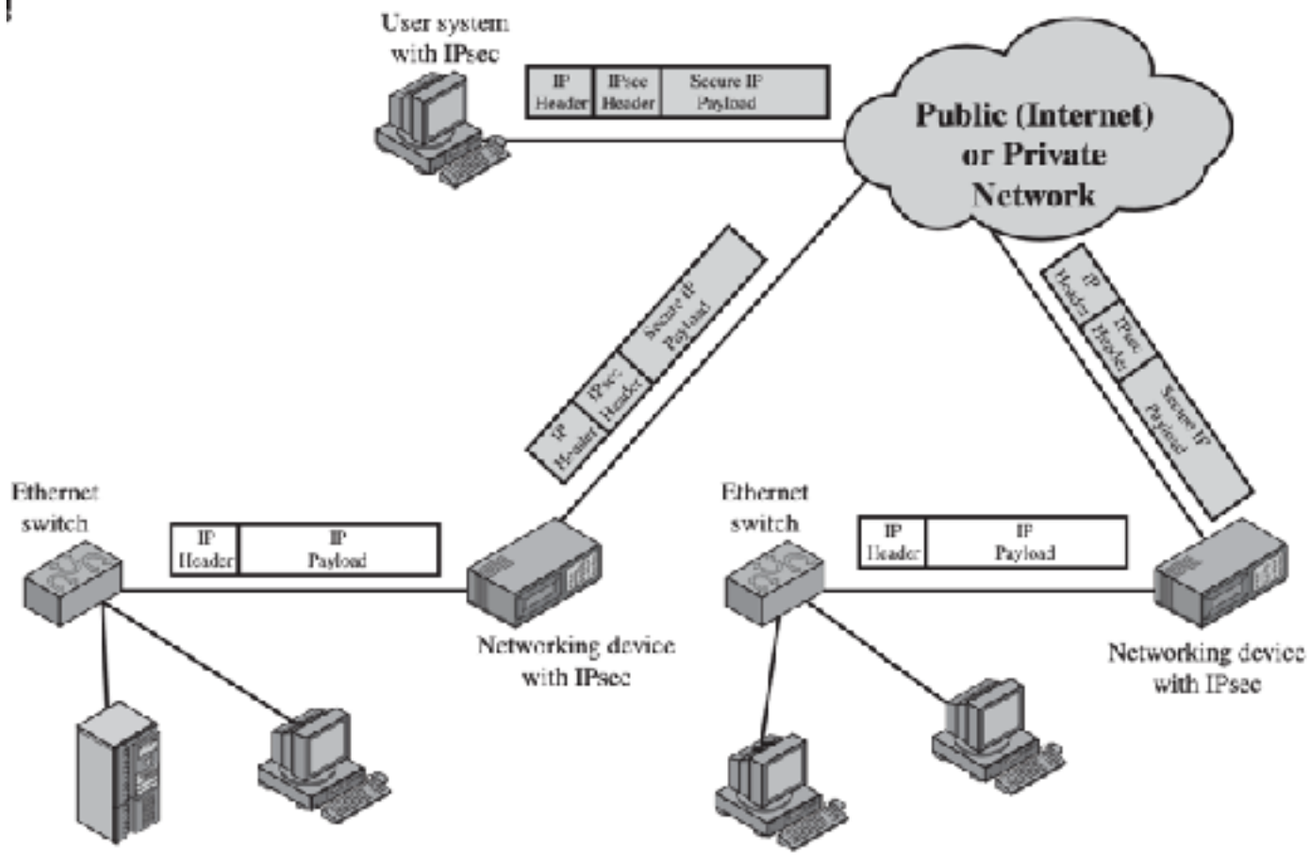
    - Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.

    - Secure remote access over the Internet: An end user whose system is equipped with IP security protocols can make a local call to an Internet Service Provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.

    - Establishing extranet and intranet connectivity with partners: IPsec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

    - Enhancing electronic commerce security: Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security. IPsec guarantees that all traffic designated by the network administrator is both encrypted and authenticated, adding an additional layer of security to whatever is provided at the application layer.

- The principal feature of IPsec that enables it to support these varied applications is that it can encrypt and/or authenticate all traffic at the IP level.



Benefits of IPsec

- When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.

- IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.

- IPsec is below the transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when IPsec is implemented in the firewall or router. Even if IPsec is implemented in end systems, upper-layer software, including applications, is not affected.

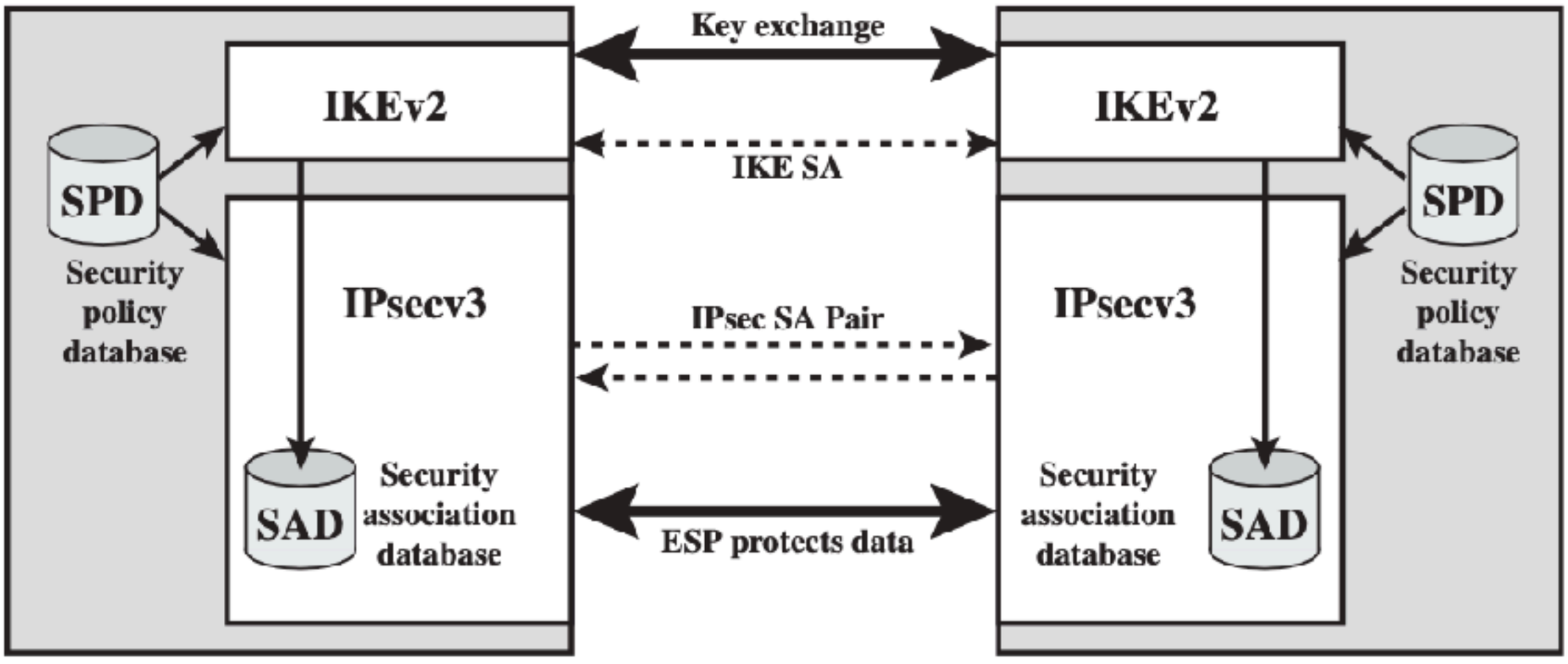
- IPsec can be transparent to end users.There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.

- IPsec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

IPsec Services

- IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. Two protocols are used to provide security: an authentication protocol designated by the header of the protocol, Authentication Header (AH); and a combined encryption/ authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP). RFC 4301 lists the following services:
• Access control
• Connectionless integrity
• Data origin authentication
• Rejection of replayed packets (a form of partial sequence integrity) • Confidentiality (encryption)
• Limited traffic flow confidentiality

IP SECURITY Architecture



Intruders

Introduction

- A significant security problem for networked systems is hostile, or at least unwanted, trespass by users or software. User trespass can take the form of unauthorized logon to a machine or, in the case of an authorized user, acquisition of privileges or performance of actions beyond those that have been authorized. Software trespass can take the form of a virus, worm, or Trojan horse.

Intruders

- One of the two most publicized threats to security is the intruder (the other is viruses), often referred to as a hacker or cracker. In an important early study of intrusion, Anderson [ANDE80] identified three classes of intruders:

    - Masquerader: An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account

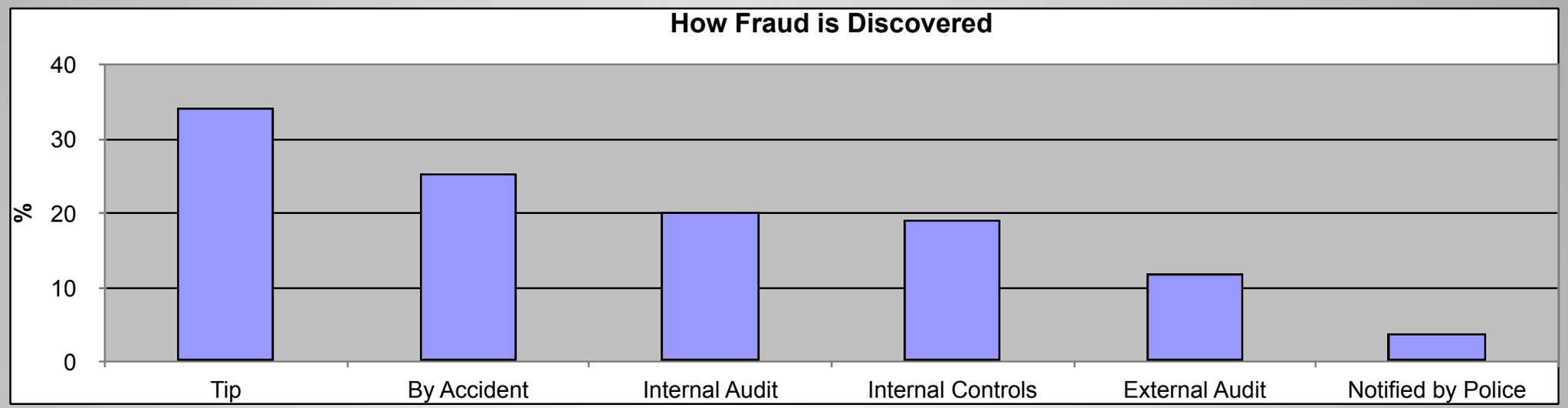
    - Misfeasor: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges

    - Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection

- The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider.

Note: In an IBM study, 60% of security incidents come from inside

Fraud Discovery



Tips are the most common way fraud is discovered.
Tips come from:

- Employee/Coworkers 64%,
- Anonymous 18%,
- Customer 11%,
- Vendor 7%

If you suspect possible fraud, report it anonymously to the USG ethics hot line at 877-516-3466.

Essentials of Corporate Fraud, T L Coenen, 2008, John Wiley & Sons

WHY HACKERS HACK

MOTIVES BEHIND CYBERATTACKS

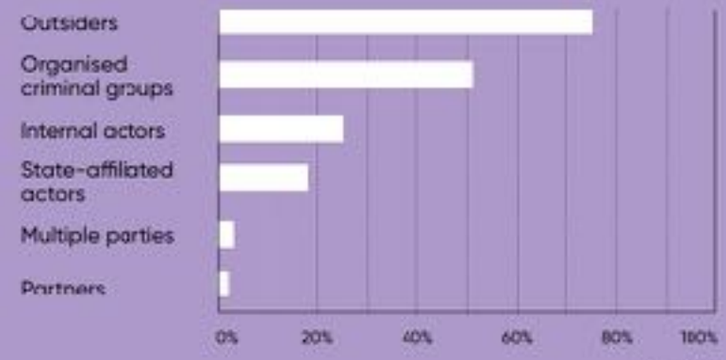
GLOBAL STUDY OF LARGE ORGANISATIONS THAT WERE VICTIMS TO A CYBERATTACK

41%	27%	26%	26%	24%	20%	11%
Ransom	Insider threat	Political	Competition	Cyberwar	Angry user	Motive unknown

Radware 2017

WHO'S BEHIND DATA BREACHES?

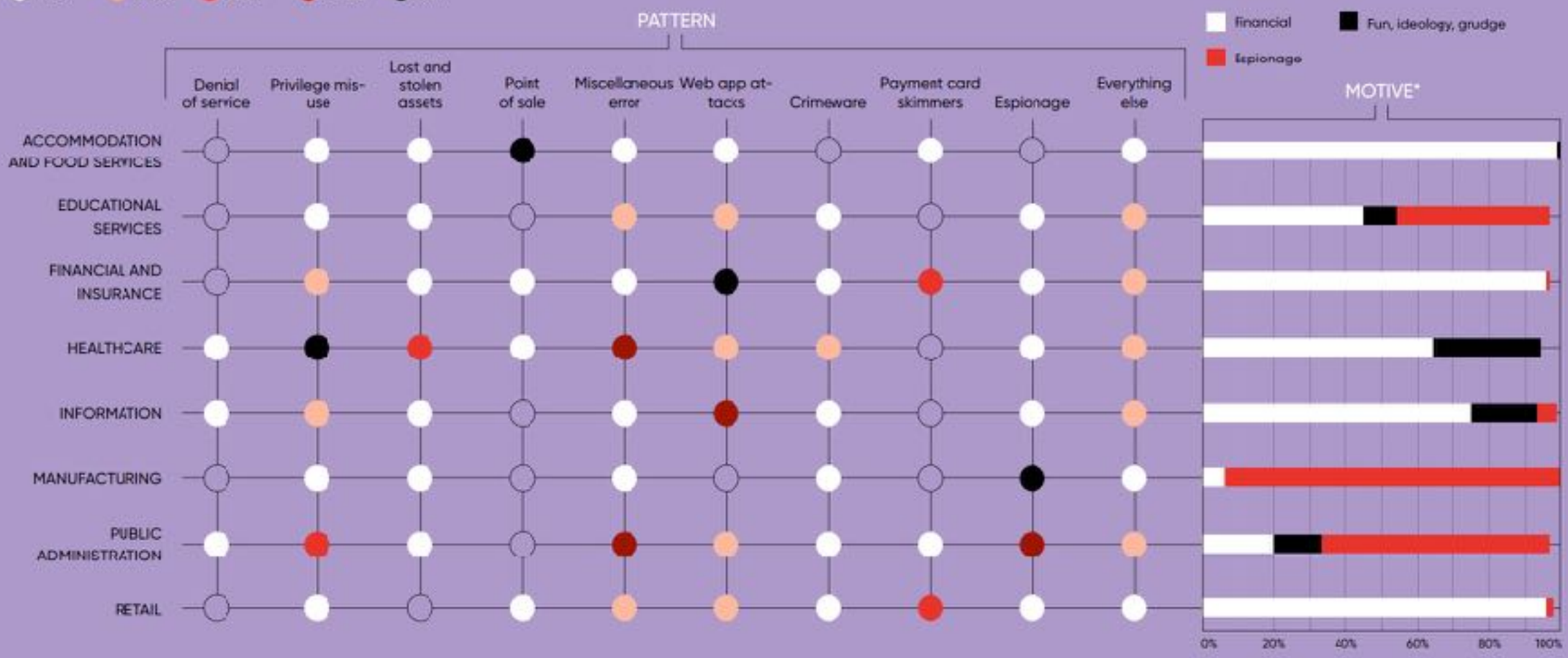
GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES



Verizon 2017

DATA BREACHES, BY PATTERN AND MOTIVE

GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES



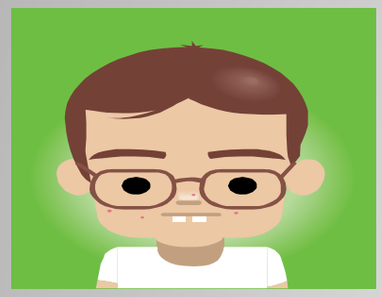
*Some motives were unknown so not included in this data

Verizon 2017

RACONTEUR

User Awareness

Cyber-Criminals



Cracker:
Computer-savvy programmer creates attack software

Posts to

System Administrators
Some scripts appear useful to manage networks…

Hacker Bulletin Board
SQL Injection
Buffer overflow
Password Crackers
Password Dictionaries

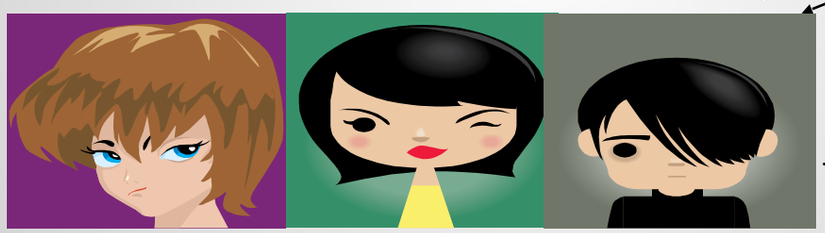
Successful attacks!
Crazyman broke into …
CoolCat penetrated…

Downloads

Reports

Posts to

Script Kiddies:
Unsophisticated computer users who know how to execute programs



Criminals: Create & sell bots
-> generate spam
Sell credit card numbers, etc…

Malware package earns $1K-2K
1 M Email addresses earn $8
10,000 PCs earn $1000

Intruder Pattern of Behavior

(a) Hacker

1. Select the target using IP lookup tools such as NSLookup, Dig, and others.
2. Map network for accessible services using tools such as NMAP.
3. Identify potentially vulnerable services (in this case, pcAnywhere).
4. Brute force (guess) pcAnywhere password.
5. Install remote administration tool called DameWare.
6. Wait for administrator to log on and capture his password.
7. Use that password to access remainder of network.

(b) Criminal Enterprise

1. Act quickly and precisely to make their activities harder to detect.
2. Exploit perimeter through vulnerable ports.
3. Use Trojan horses (hidden software) to leave back doors for reentry.
4. Use sniffers to capture passwords.
5. Do not stick around until noticed.
6. Make few or no mistakes.

(c) Internal Threat

1. Create network accounts for themselves and their friends.
2. Access accounts and applications they wouldn't normally use for their daily jobs.
3. E-mail former and prospective employers.
4. Conduct furtive instant-messaging chats.
5. Visit Web sites that cater to disgruntled employees, such as f'dcompany.com.
6. Perform large downloads and file copying.
7. Access the network during off hours.

Exercise

- Thinking of your home as an analogy, come up with 5 ideas for securing a cloud application.

- Bonus: What has been one of the number one security issues at Starbucks (in the cloud)?

Gaining Access

- Have to have credentials
- Try default passwords used with standard accounts that are shipped with the system. Many administrators do not bother to change these defaults.
- Exhaustively try all short passwords(those of one to three characters).
- Try words in the system's online dictionary or a list of likely passwords.Examples of the latter are readily available on hacker bulletin boards.
- Collect information about users, such as their full names, the names of their spouse and children, pictures in their office, and books in their office that are related to hobbies.
- Try users' phone numbers, Social Security numbers, and room numbers.
- Try all legitimate license plate numbers for this state.
- Use a Trojan horse to by pass restrictions on access.
- Tap the line between a remote user and the host system.

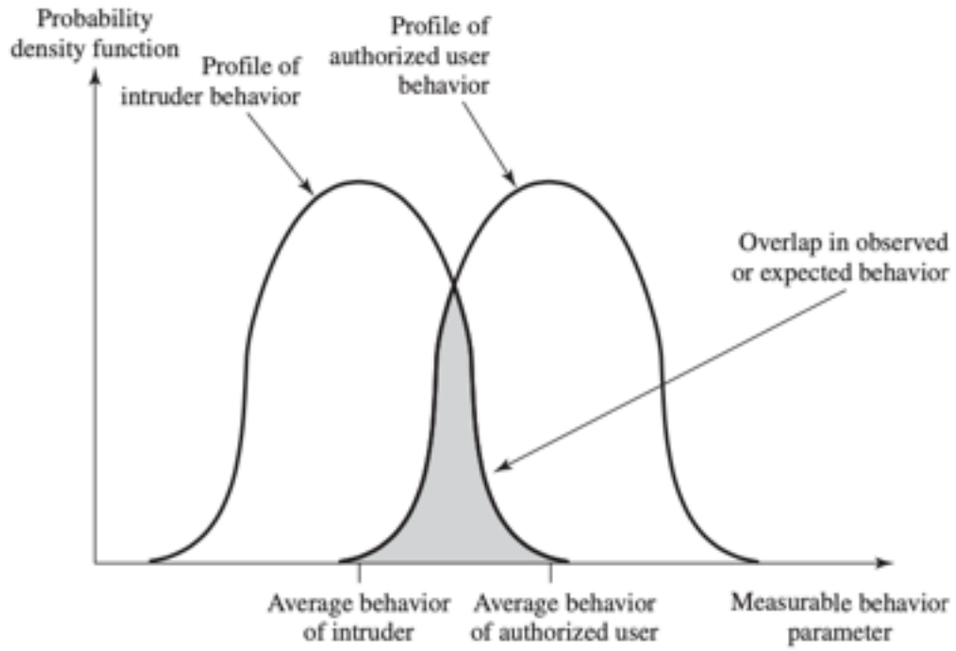
Counter-Measures: Detection

- If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. Even if the detection is not sufficiently timely to preempt the intruder, the sooner that the intrusion is detected, the less the amount of damage and the more quickly that recovery can be achieved.

- An effective intrusion detection system can serve as a deterrent, so acting to pre-vent intrusions.

- Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility

- Intrusion detection is based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified. Of course, we cannot expect that there will be a crisp, exact distinction between an attack by an intruder and the normal use of resources by an authorized user. Rather, we must expect that there will be some overlap.



Approaches to Intrusion Detection

- Statistical anomaly detection: Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.
    - Threshold detection: This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.
    - Profile based: A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.
- Rule-based detection: Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.
    - Anomaly detection: Rules are developed to detect deviation from previous usage patterns.
    - Penetration identification: An expert system approach that searches for suspicious behavior.

Exercise

- Pick one of the detection options and describe either the rules or anomalies in a system that you are familiar with, that could be used to detect intruders. Is there one type of attacker that your chosen approach is more likely to detect? What deficiencies are there in your approach? Are there any issues associated with a distributed system? What would be the sources of information your approach would use?

Password Management

- Do we really need to talk about this again? :-)
    - Have a policy for password change intervals as well as length/type
- Password/Secret storage
    - What are the storage options for system passwords/ secrets

How secure is your password?

- One demonstration of the effectiveness of guessing is reported in [KLEI90]. From a variety of sources, the author collected UNIX password files, containing nearly 14,000 encrypted passwords. The result, which the author rightly characterizes as frightening, is shown in the table. In all, nearly one-fourth of the passwords were guessed. The following strategy was used:

    1. Try the user's name, initials, account name, and other relevant personal information. In all, 130 different permutations for each user were tried.

    2. Try words from various dictionaries. The author compiled a dictionary of over 60,000 words, including the online dictionary on the system itself, and various other lists as shown

    3. Try various permutations on the words from step 2. This included making the first letter uppercase or a control character, making the entire word uppercase, reversing the word, changing the letter "o" to the digit "zero," and so on. These permutations added another 1 million words to the list.

    4. Try various capitalization permutations on the words from step 2 that were not considered in step 3. This added almost 2 million additional words to the list.

Results

- Thus, the test involved in the neighborhood of 3 million words. Using the fastest Thinking Machines implementation listed earlier, the time to encrypt all these words for all possible salt values is under an hour. Keep in mind that such a thorough search could produce a success rate of about 25%, whereas even a single hit may be enough to gain a wide range of privileges on a system.

Type of Password	Search Size	Number of Matches	Percentage of Passwords Matched	Cost/Benefit Ratio[a]
User/account name	130	368	2.7%	2.830
Character sequences	866	22	0.2%	0.025
Numbers	427	9	0.1%	0.021
Chinese	392	56	0.4%	0.143
Place names	628	82	0.6%	0.131
Common names	2239	548	4.0%	0.245
Female names	4280	161	1.2%	0.038
Male names	2866	140	1.0%	0.049
Uncommon names	4955	130	0.9%	0.026
Myths & legends	1246	66	0.5%	0.053
Shakespearean	473	11	0.1%	0.023
Sports terms	238	32	0.2%	0.134
Science fiction	691	59	0.4%	0.085
Movies and actors	99	12	0.1%	0.121
Cartoons	92	9	0.1%	0.098
Famous people	290	55	0.4%	0.190
Phrases and patterns	933	253	1.8%	0.271
Surnames	33	9	0.1%	0.273
Biology	58	1	0.0%	0.017
System dictionary	19683	1027	7.4%	0.052
Machine names	9018	132	1.0%	0.015
Mnemonics	14	2	0.0%	0.143
King James bible	7525	83	0.6%	0.011
Miscellaneous words	3212	54	0.4%	0.017
Yiddish words	55	0	0.0%	0.000
Asteroids	2407	19	0.1%	0.007
TOTAL	62727	3340	24.2%	0.053

Password Cracking

Dictionary Attack and Brute Force

Pattern	Calculation	Result	Time to Guess (2.6×10^{18} tries/month)
Personal Info: interests, relatives		20	Manual 5 minutes
Social Engineering		1	Manual 2 minutes
American Dictionary		80,000	< 1 second
4 chars: lower case alpha	26^4	5×10^5	
8 chars: lower case alpha	26^8	2×10^{11}	
8 chars: alpha	52^8	5×10^{13}	
8 chars: alphanumeric	62^8	2×10^{14}	3.4 min.
8 chars alphanumeric +10	72^8	7×10^{14}	12 min.
8 chars: all keyboard	95^8	7×10^{15}	2 hours
12 chars: alphanumeric	62^{12}	3×10^{21}	96 years
12 chars: alphanumeric + 10	72^{12}	2×10^{22}	500 years
12 chars: all keyboard	95^{12}	5×10^{23}	
16 chars: alphanumeric	62^{16}	5×10^{28}	

Credentials-The Real issue

- Privilege escalation
- It’s not the account that is cracked often that matters. Is the downstream accounts that are now accessible.

Exercise

- Think about what you have access to in your organization. Assuming that your account was cracked, look 3 steps downstream and identify systems that the hacker would now have access to and in turn what those systems would give her access to.

Malicious Software

Introduction

- Perhaps the most sophisticated types of threats to computer systems are presented by programs that exploit vulnerabilities in computing systems. Such threats are referred to as malicious software, or malware. In this context, we are concerned with threats to application programs as well as utility programs, such as editors and compilers, and kernel-level programs

The Business

- Several companies specialize in finding and selling exploits
  - ReVuln, Vupen, Netragard, Exodus Intelligence
  - The average flaw sells for $35-160K
  - $100K+ annual subscription fees
- Nation-state buyers
  - "Israel, Britain, Russia, India and Brazil are some of the biggest spenders. North Korea is in the market, as are some Middle Eastern intelligence services. Countries in the Asian Pacific, including Malaysia and Singapore, are buying, too" -- NY Times (Jul 2013)

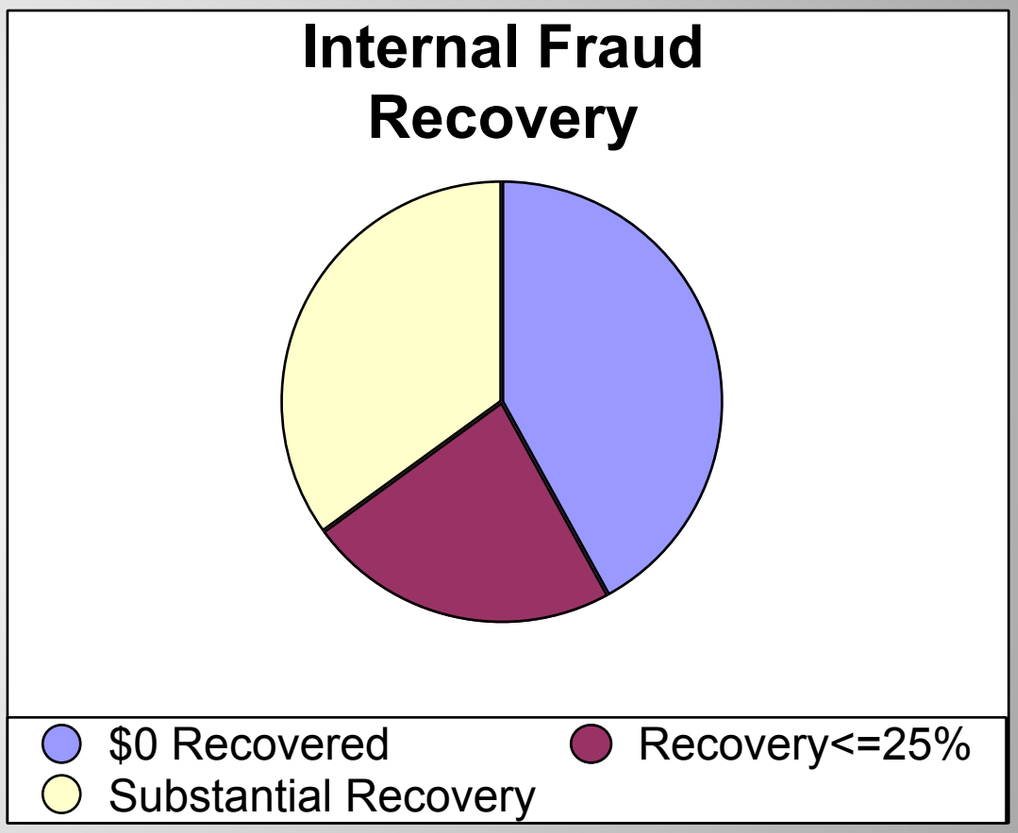
The Market

- Single credit card number: $4-15
- Single card with magnetic track data: $12-30
- "Fullz": $25-40
  - Full name, address, phone, email addresses (with passwords), date of birth, SSN, bank account and routing numbers, online banking credentials, credit cards with magnetic track data and PINs
- Online credentials for a bank account with $70-150K balance: under $300

- Prices dropped since 2011, indicating supply glut

Fraud

- Organizations lose 5-6% of revenue annually due to internal fraud = $652 Billion in U.S. (2006)
- Average scheme lasts 18 months, costs $159,000
- 25% costs exceed $1M
- Smaller companies suffer greater average dollar losses than large companies



Essentials of Corporate Fraud, T L Coenen, 2008, John Wiley & Sons

Terminology

Name	Description
Virus	Malware that, when executed, tries to replicate itself into other executable code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network.
Logic bomb	A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met; the program then triggers an unauthorized act.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
Backdoor (trapdoor)	Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality.
Mobile code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Downloaders	Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Kit (virus generator)	Set of tools for generating new viruses automatically.
Spammer programs	Used to send large volumes of unwanted e-mail.
Flooders	Used to attack networked computer systems with a large volume of traffic to carry out a denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.
Spyware	Software that collects information from a computer and transmits it to another system.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.

Exercise: The King Virus's

- Stuxnet

- Watch: https://www.zdnet.com/article/infographic-how-stuxnet-supervirus-works/

Three Parts to a Virus

- Infection mechanism: The means by which a virus spreads, enabling it to replicate. The mechanism is also referred to as the infection vector.

- Trigger: The event or condition that determines when the payload is activated or delivered.

- Payload: What the virus does, besides spreading. The payload may involve damage or may involve benign but noticeable activity.

Phases of a Virus

- Dormant phase: The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.

- Propagation phase: The virus places a copy of itself into other programs or into certain system areas on the disk. The copy may not be identical to the propa- gating version; viruses often morph to evade detection. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.

- Triggering phase: The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.

- Execution phase: The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

Exercise

- List 3 ways to stop/detect a virus at each of the phases.

Virus Classifications-Target

- Boot sector infector: Infects a master boot record or boot record and spreads
  when a system is booted from the disk containing the virus.

- File infector: Infects files that the operating system or shell consider to be executable.

- Macro virus: Infects files with macro code that is interpreted by an application.

Virus Classifications- Strategy

- Encrypted virus: A typical approach is as follows. A portion of the virus creates a random encryption key and encrypts the remainder of the virus. The key is stored with the virus. When an infected program is invoked, the virus uses the stored random key to decrypt the virus. When the virus replicates, a different random key is selected. Because the bulk of the virus is encrypted with a different key for each instance, there is no constant bit pattern to observe

- Stealth virus: A form of virus explicitly designed to hide itself from detection by antivirus software. Thus, the entire virus, not just a payload is hidden.

- Polymorphic virus: A virus that mutates with every infection, making detection by the “signature” of the virus impossible.

- Metamorphic virus: As with a polymorphic virus, a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses may change their behavior as well as their appearance.

Exercise

- NIST has an incident reporting system. Look at https://nvd.nist.gov/

- Find 3 incidents of 3 different virus types

- Find 3 incidents of software bugs that created security issues

Social Engineering

Social engineering manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.

Email:
ABC Bank has noticed a problem with your account…

Phone Call:
This is John, the System Administrator. What is your password?

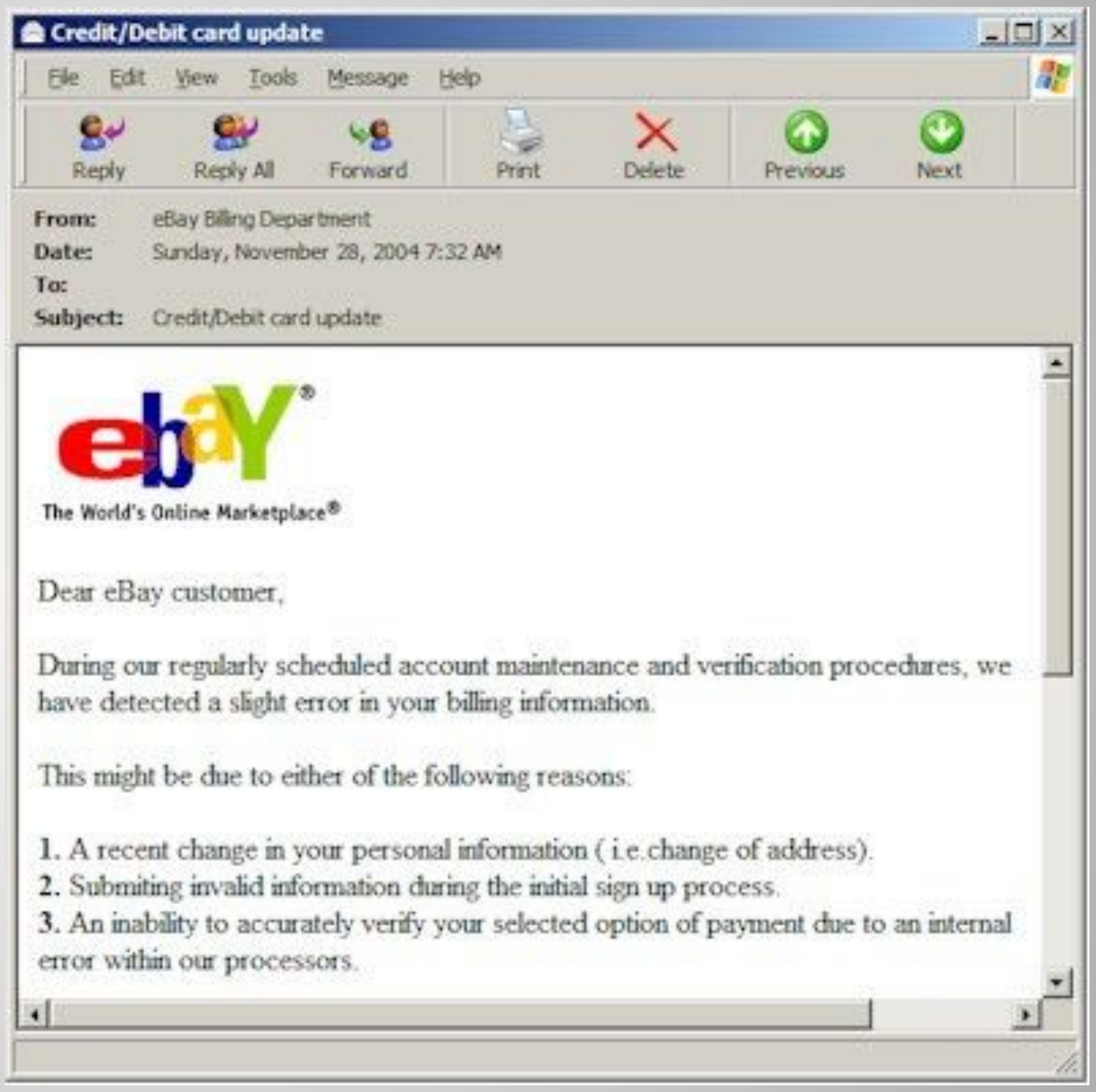
In Person:
What ethnicity are you? Your mother's maiden name?

I have come to repair your machine…

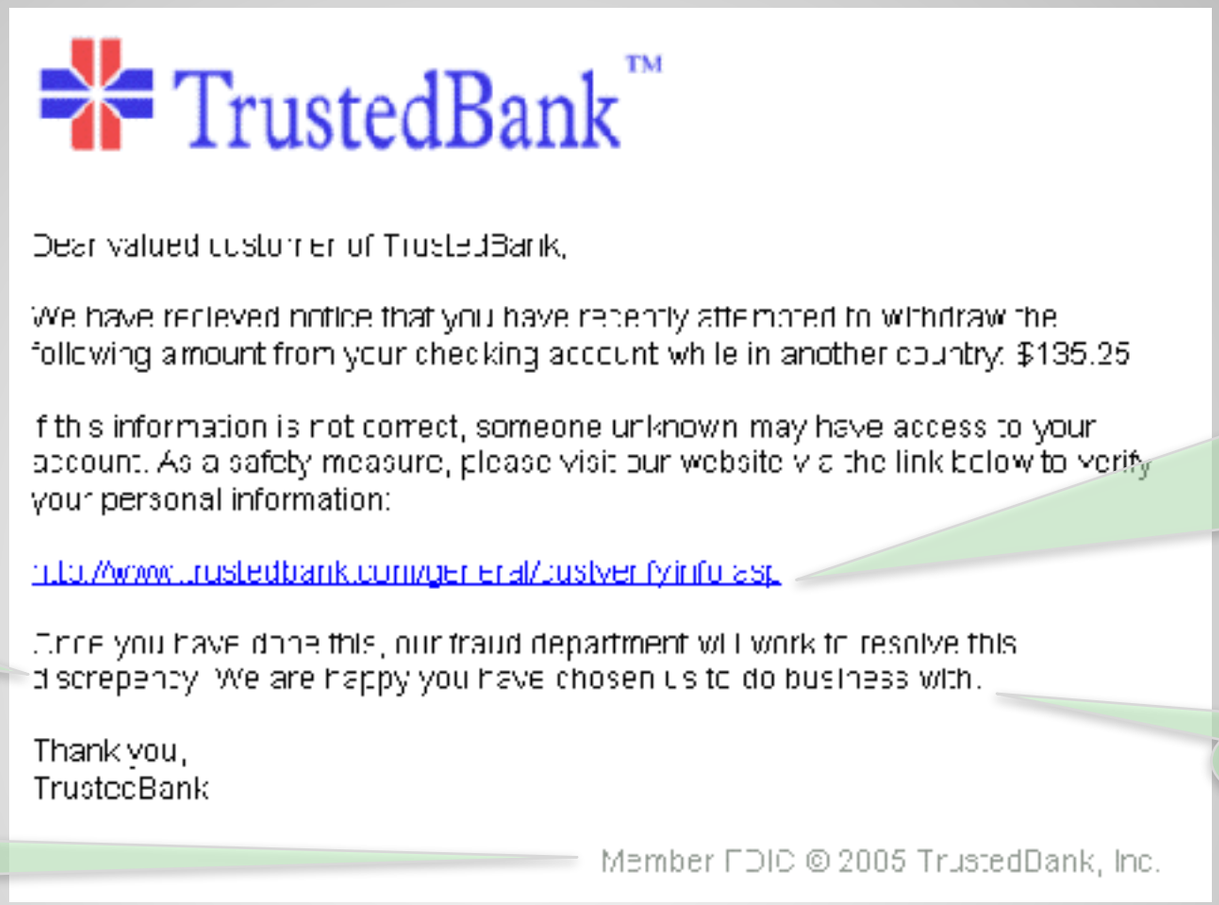
and have some lovely software patches!

Phishing: Counterfeit Email

Phishing: A seemingly trustworthy entity asks for sensitive information such as SSN, credit card numbers, login IDs or passwords via e-mail.



Pharming: Counterfeit Web Pages



Misspelled

Wiping over, but not clicking the link may reveal a different address.

With whom?

Copyright date is old

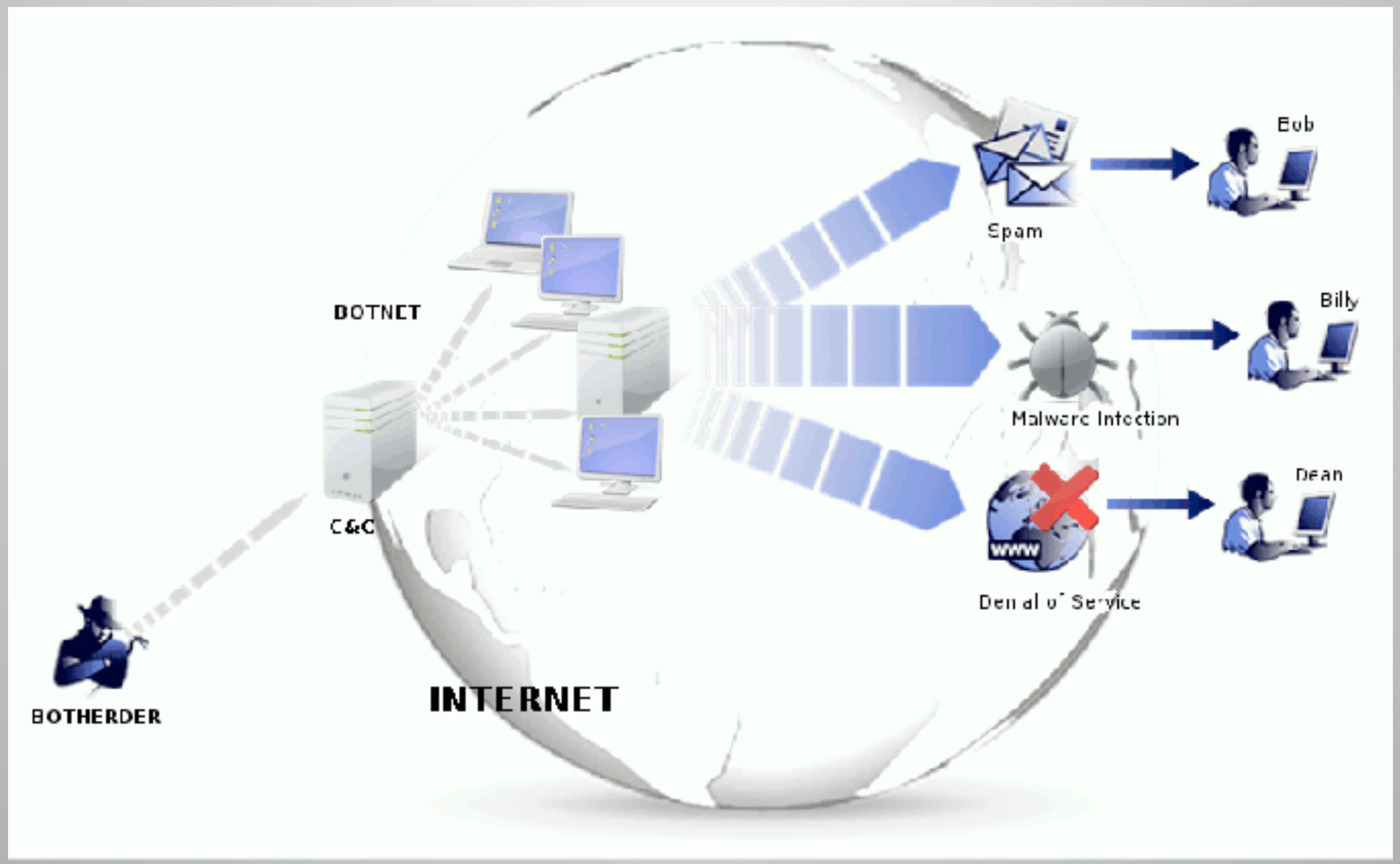
The link provided in the e-mail leads to a counterfeit webpage which collects important information and submits it to the owner.

The counterfeit web page looks like the real thing

Extracts account information

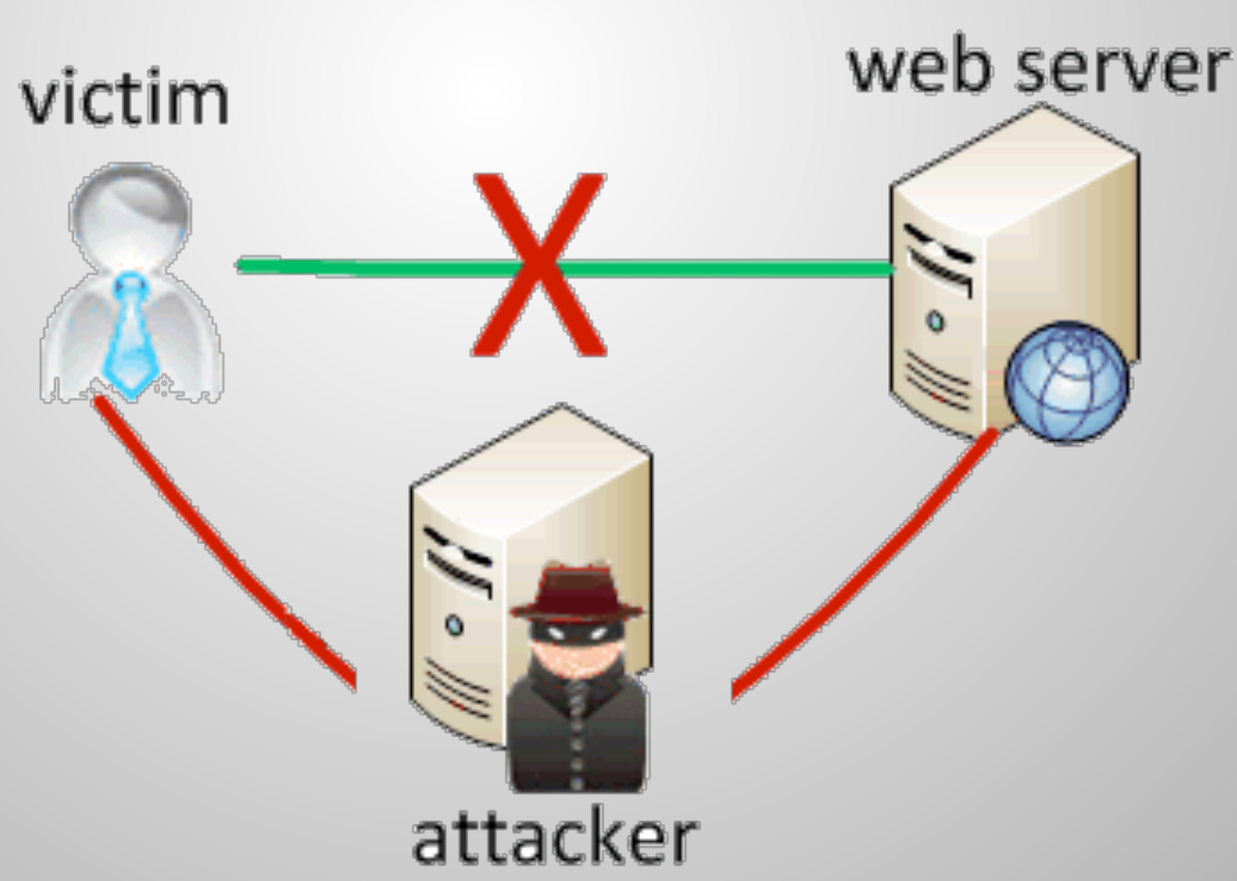
Botnet

- A botnet is a number of compromised computers used to create and send spam or viruses or flood a network with messages as a denial of service attack.
- The compromised computers are called zombies.



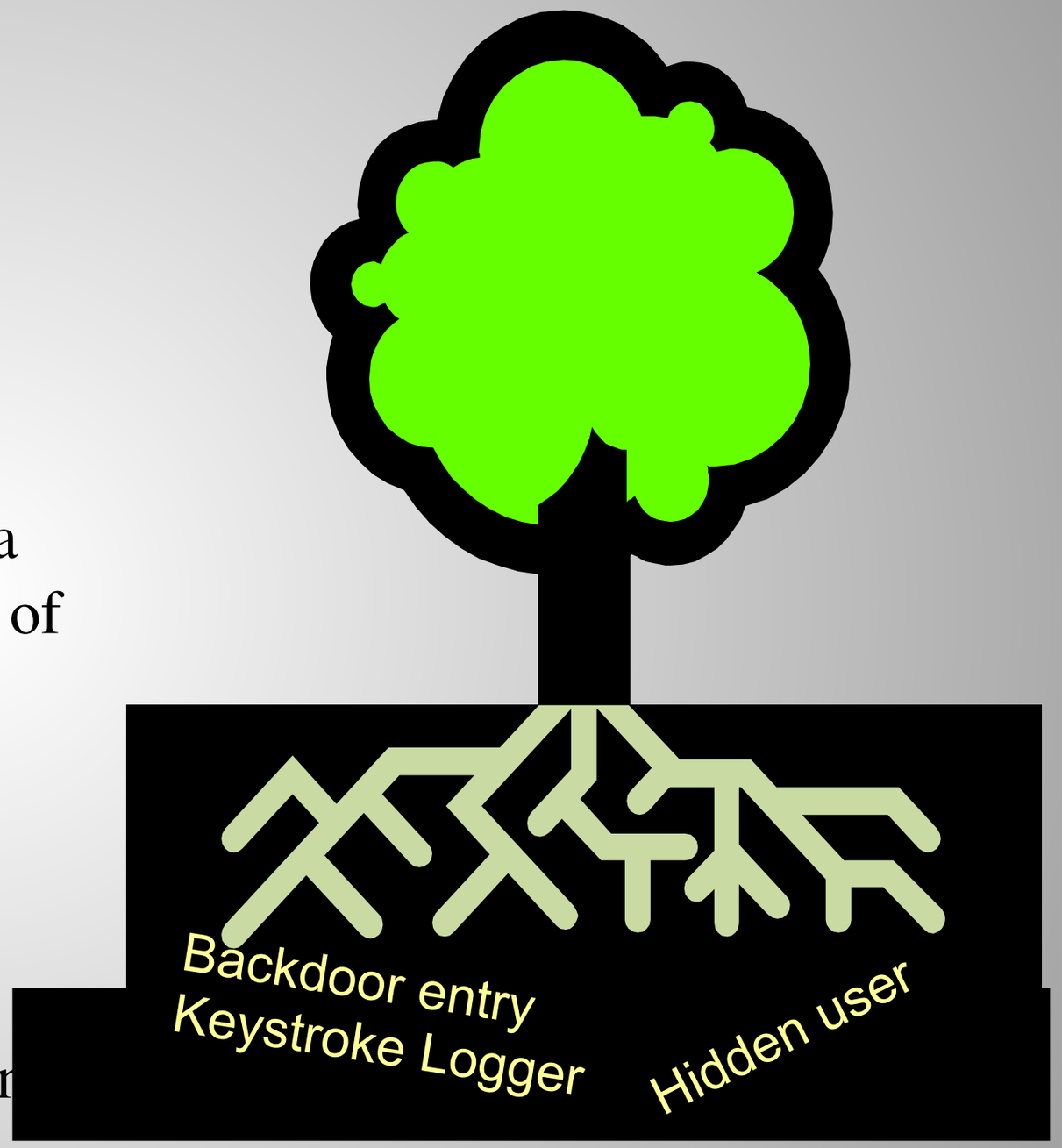
Man In The Middle Attack

An attacker pretends to be your final destination on the network. When a person tries to connect to a specific destination, an attacker can mislead him to a different service and pretend to be that network access point or server.



Rootkit

- Upon penetrating a computer, a hacker may install a collection of programs, called a rootkit.
- May enable:
  - Easy access for the hacker (and others)into the enterprise
  - Keystroke logger
- Eliminates evidence of break-in
- Modifies the operating system.



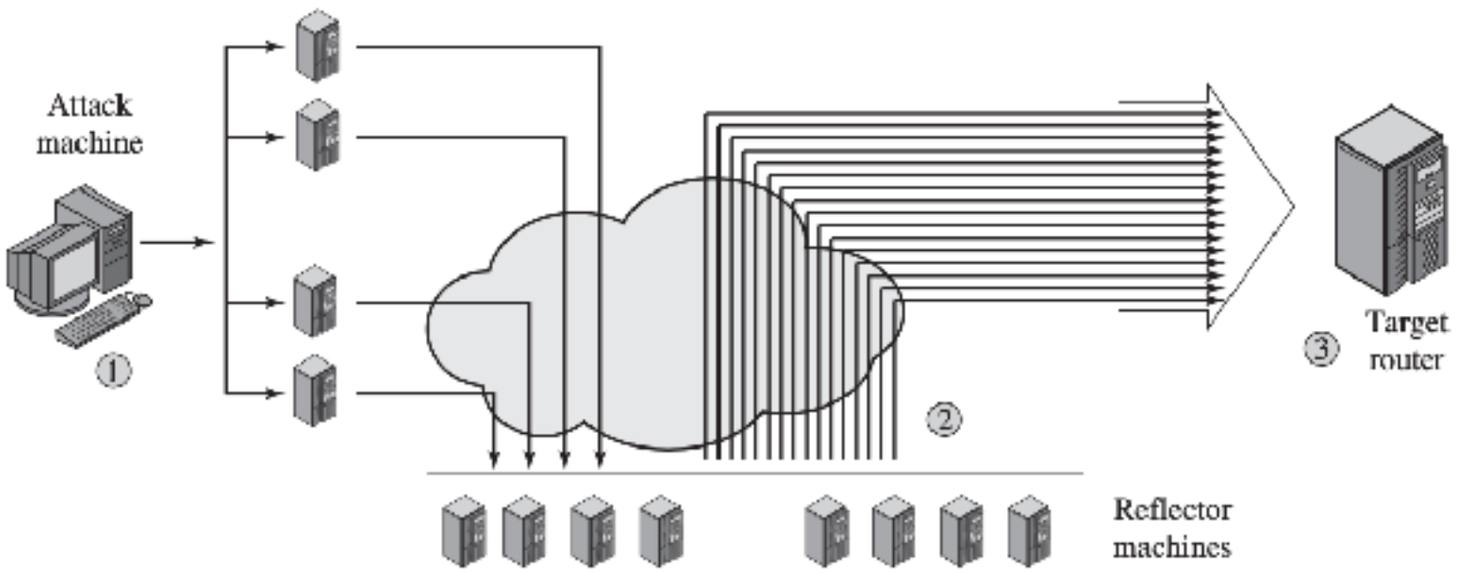
DOS/DDOS

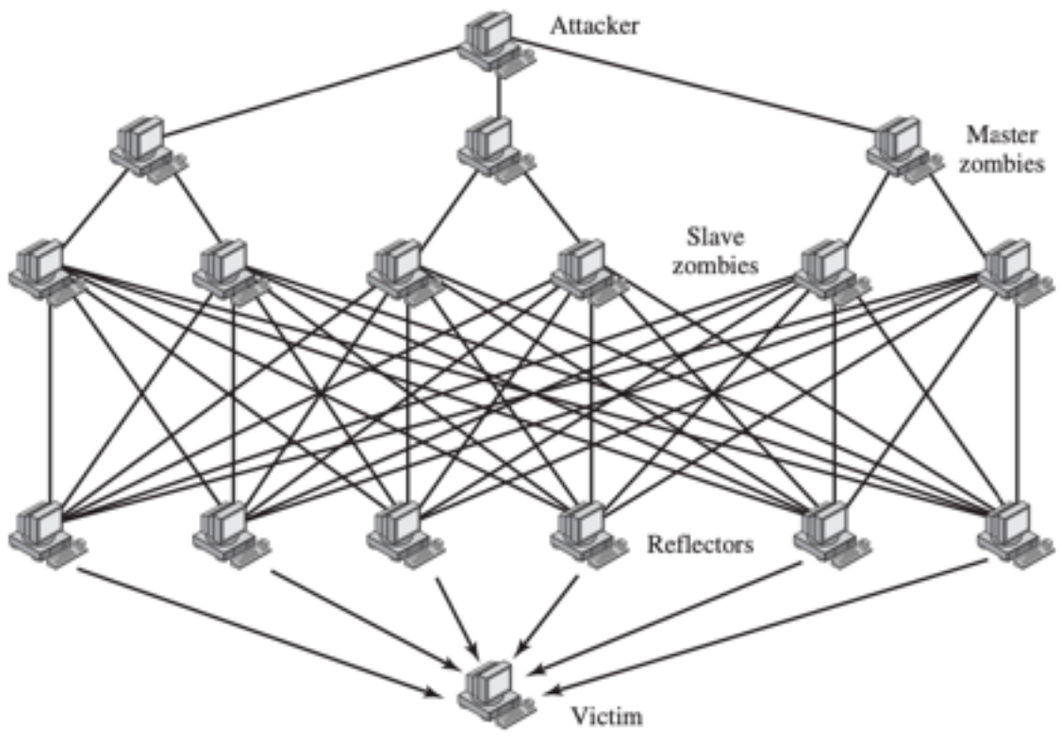
- A denial of service (DoS) attack is an attempt to prevent legitimate users of a service from using that service. When this attack comes from a single host or net- work node, then it is simply referred to as a DoS attack. A more serious threat is posed by a DDoS attack. In a DDoS attack, an attacker is able to recruit a number of hosts throughout the Internet to simultaneously or in a coordinated fashion launch an attack upon the target

DDOS Description

- A DDoS attack attempts to consume the target's resources so that it cannot provide service. One way to classify DDoS attacks is in terms of the type of resource that is consumed. Broadly speaking, the resource consumed is either an internal host resource on the target system or data transmission capacity in the local network to which the target is attacked.

Example of a DDOS Attack





The Marketplace

- Option 1: bug bounty programs
  - Google: up to $3133.7 in 2010, now up to $20K per bug
  - Facebook: up to $20K per bug
  - Microsoft: up to $150K per bug
  - Pwn2Own competition: $10-15K
- Option 2: vulnerability brokers
  - ZDI, iDefense: $2-25K
- Option 3: gray and black markets
  - Up to $100-250K reported (hard to verify)
  - A zero-day against iOS sold for $500K (allegedly)

Closing Thoughts

Correctness vs Secure

- System correctness:
- system satisfies specification
  - For reasonable input, get reasonable output
- System security:
- system properties preserved in face of attack
  - For unreasonable input, output not completely disastrous
- Main difference: active interference from adversary
- Modular design may increase vulnerability …
  - Abstraction is difficult to achieve in security: what if the adversary operates below your level of abstraction?
- … but also increase security (small TCB)

The Bad News

- Security often not a primary consideration
  - Performance and usability take precedence
- Feature-rich systems may be poorly understood
- Implementations are buggy
  - Buffer overflows are the "vulnerability of the decade"
  - Cross-site scripting and other Web attacks
- Networks are more open and accessible than ever
  - Increased exposure, easier to cover tracks
- Many attacks are not even technical in nature
  - Phishing, social engineering, etc.