

COSC 301

Network Management

Lecture 18: Network Security

Zhiyi Huang

Computer Science, University of Otago

Security of Networks

- Security is something that is not necessary in a trusted world!



FIGURE 10-2 Number of incidents reported to CERT (Computer Emergency Response Team). SOURCE: CERT Statistics, www.cert.org/stats/cert_stats.html.

Cyber Crime Statics and Trends (1)



<http://www.go-gulf.com/blog/cyber-crime/>

Cyber Crime Statics and Trends (2)

By 2017, the global Cyber Security market is expected to skyrocket to \$120.1 billion from \$63.7 billion in 2011.

Common Types of Cyber Attacks

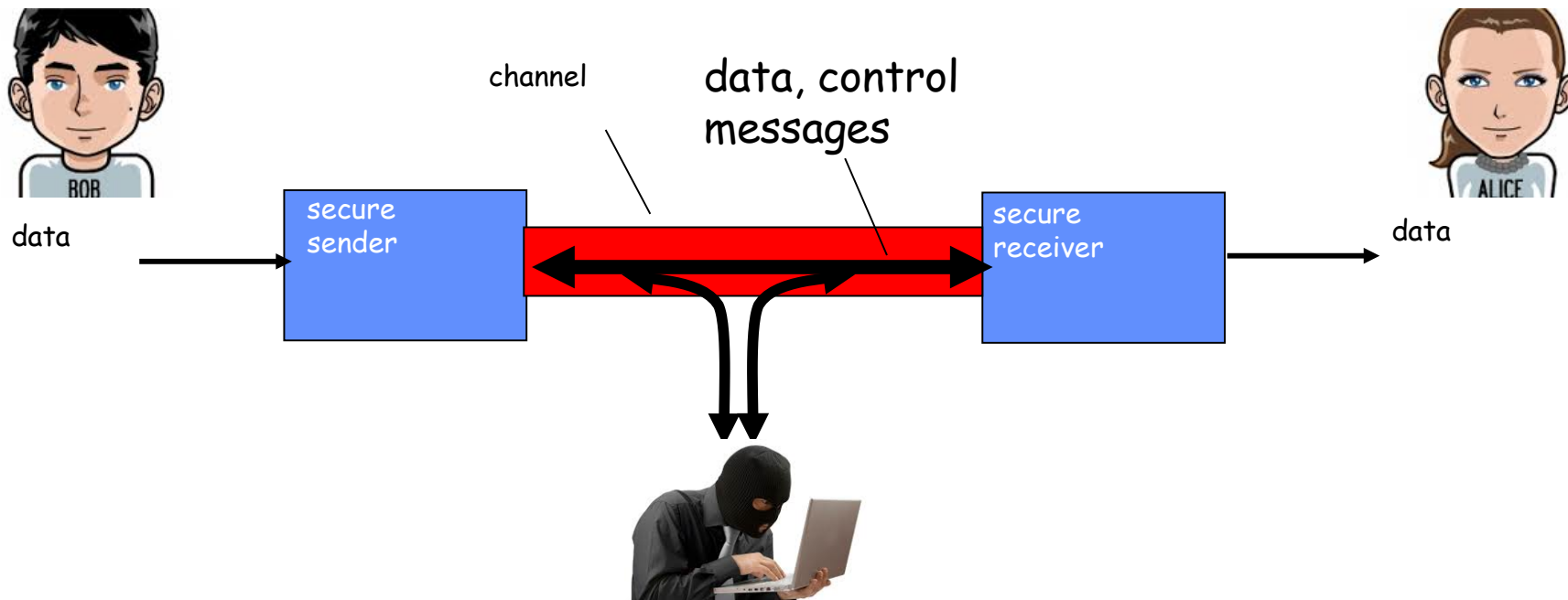
Attack types	%
Viruses, malware, worms, trojans	50%
Criminal insider	30%
Theft of data-bearing devices	28%
SQL injection	28%
Phishing	22%
Web-based attacks	17%
Social engineering	17%
others	11%

What is network security (1)

- Secures the network, as well as protecting and overseeing operations being done.
 - **Confidentiality**: only sender, intended receiver should “understand” message contents
 - **Authentication**: sender, receiver want to confirm identity of each other
 - **Message Integrity**: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection
 - **Access and Availability**: which service or device should be accessible to which user

Confidentiality

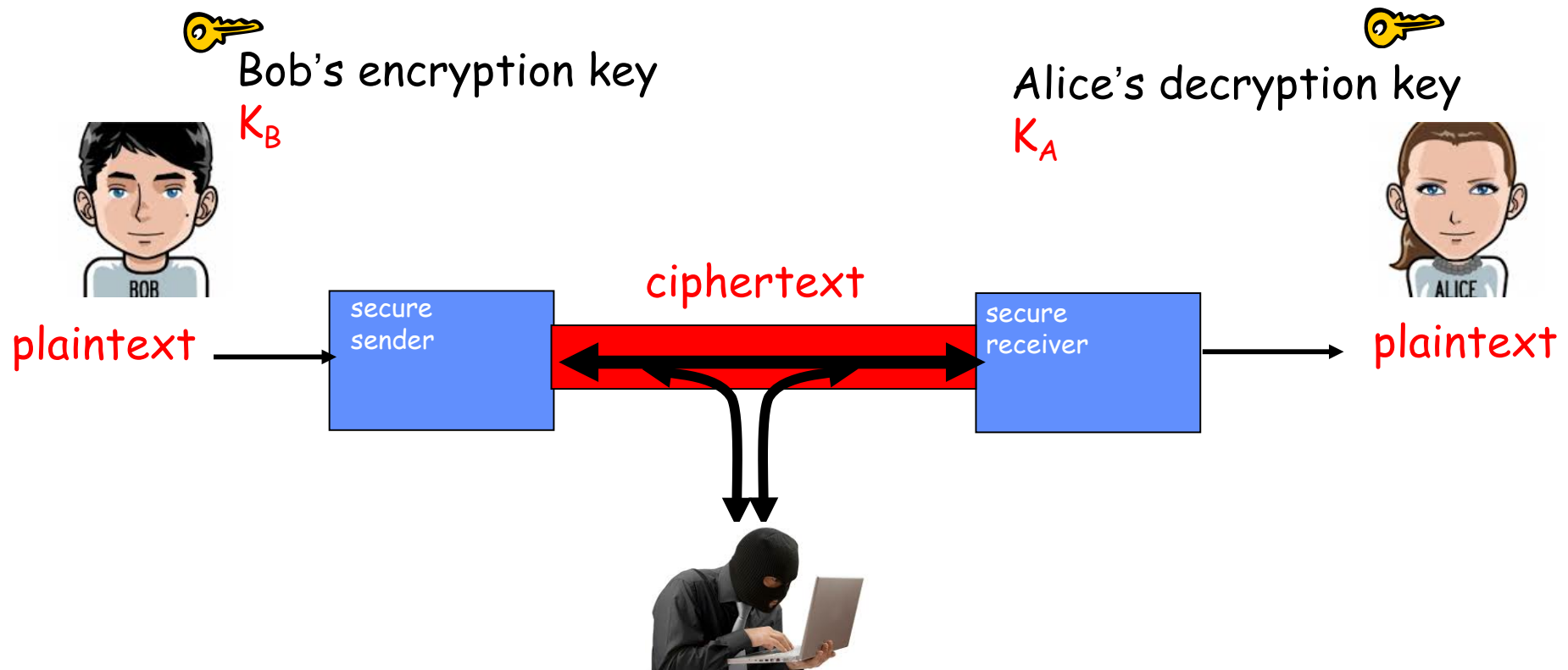
- Friends and enemies: Alice, Bob, and Trudy
 - Bob, Alice (lovers) want to communicate “securely”
 - Trudy (intruder) may intercept, delete, and add messages



What can a Trudy do?

- A lot
 - *eavesdrop*: intercept messages
 - actively *insert* messages into connection
 - *impersonation*: can fake (spoof) source address in packet (or any field in packet)
 - *hijacking*: “take over” ongoing connection by removing sender or receiver, inserting himself in place
 - *denial of service*: prevent service from being used by others (e.g., by overloading resources)
 - ...

Principle of Cryptography

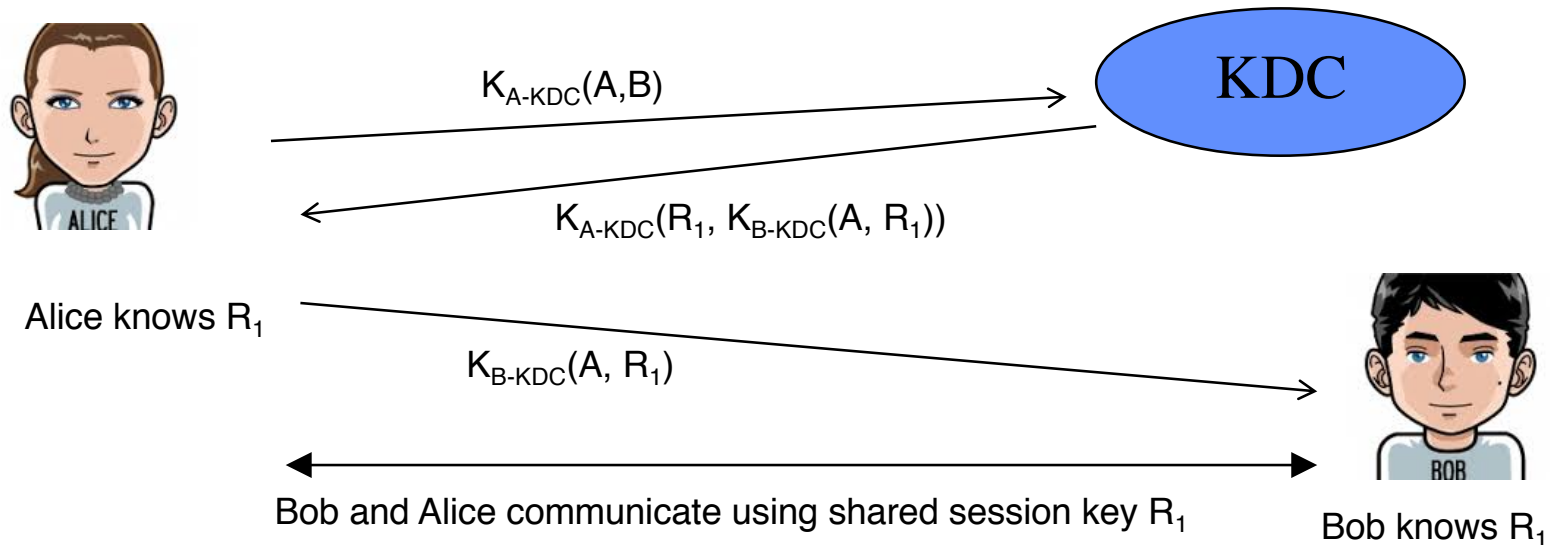


symmetric key crypto: identical sender and receiver keys

public-key crypto: encryption key *public*, decryption key *private*

Key Distribution

- Key Distribution Centre (KDC)
 - Everyone has his/her individual key manually installed at KDC (a server) when he/she registers



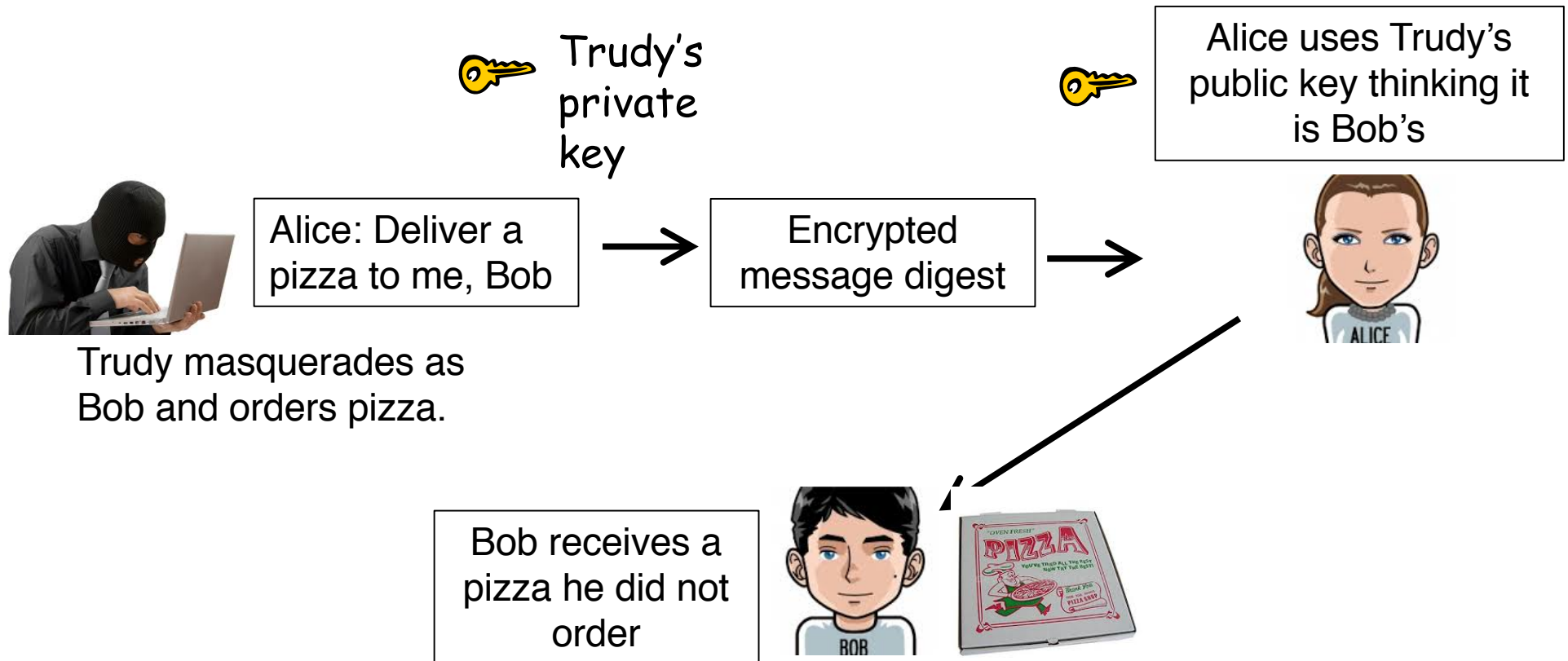
Setting up a one-time session key using a key distribution center

Key Distribution

- Using K_{A-KDC} to encrypt her communication with the KDC, Alice sends a message to the KDC saying she (A) wants to communicate with Bob(B). The message is denoted as $K_{A-KDC}(A,B)$
- The KDC, knowing K_{A-KDC} , decrypts $K_{A-KDC}(A,B)$. The KDC then generates a random number, R1. This is the shared key value that Alice and Bob will use to perform symmetric encryption when they communicate with each other. R1 is the one-time session key. In addition KDC will send Alice a pair of values A and R1 encrypted by the KDC using Bob's key K_{B-KDC}
- When Alice receives the message from the KDC, extracts R1 from the message and save it, then forwards $K_{B-KDC}(A, R1)$ to Bob
- Bob decrypts the message and knows the shared key with Alice. He takes care to authenticate Alice using R1 before proceeding further

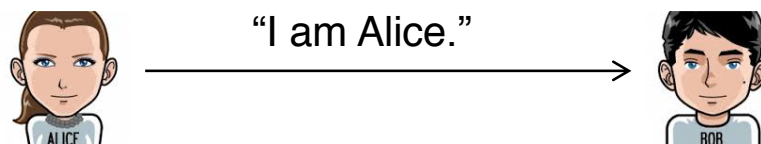
Public Key Certification

- Masquerading using public key cryptography



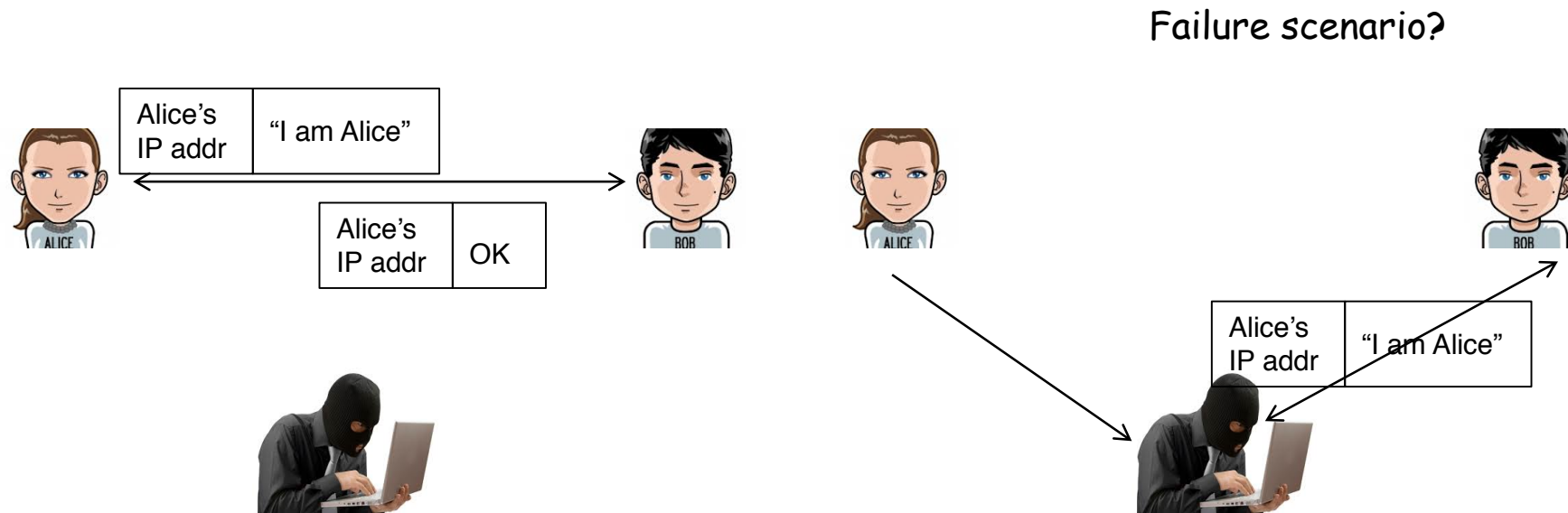
Authentication Protocols (1)

- Scenario
 - Alice, the sender, wants to communicate with Bob, the receiver
 - Bob wants Alice to “prove” her identity to him
 - Trudy tries to pretend to be Alice
- AP1.0
 - Alice sends a message to Bob saying she is Alice



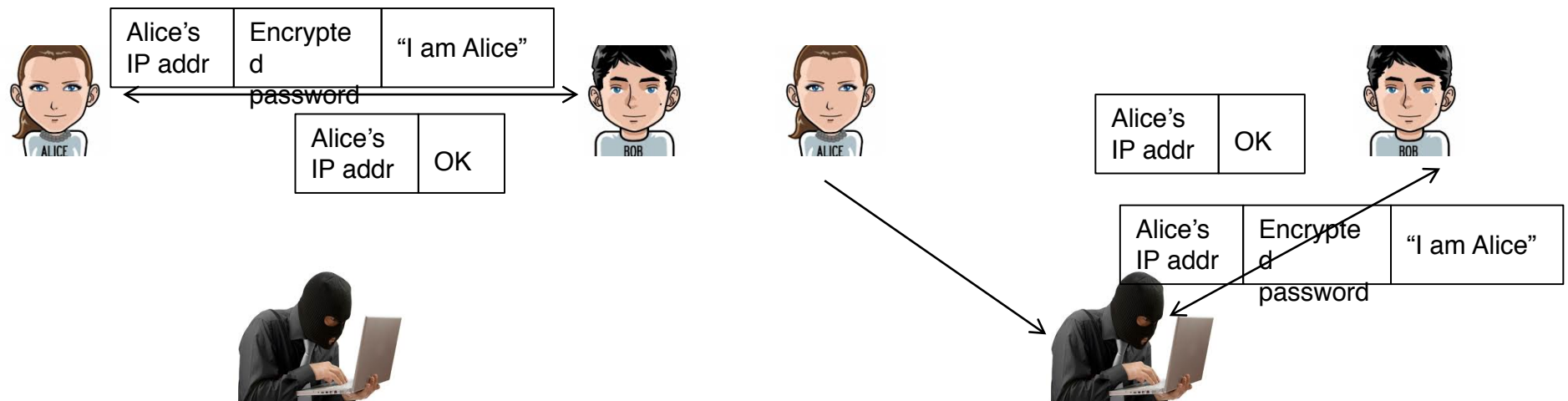
Authentication Protocols (2)

- AP2.0
 - Use the source IP address to authenticate
 - Fails if IP spoofing is used



Authentication Protocols (2)

- AP3.0
 - Use secret password
 - Password can be eavesdropped
 - Encrypted password can be played back

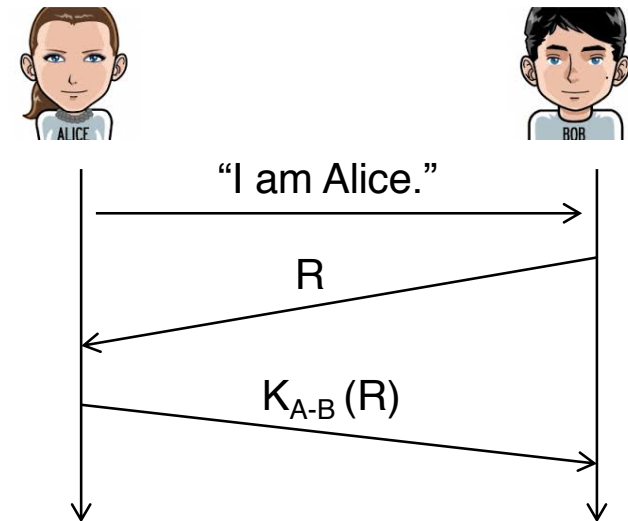


Playback attack

Authentication Protocols (3)

- AP4.0

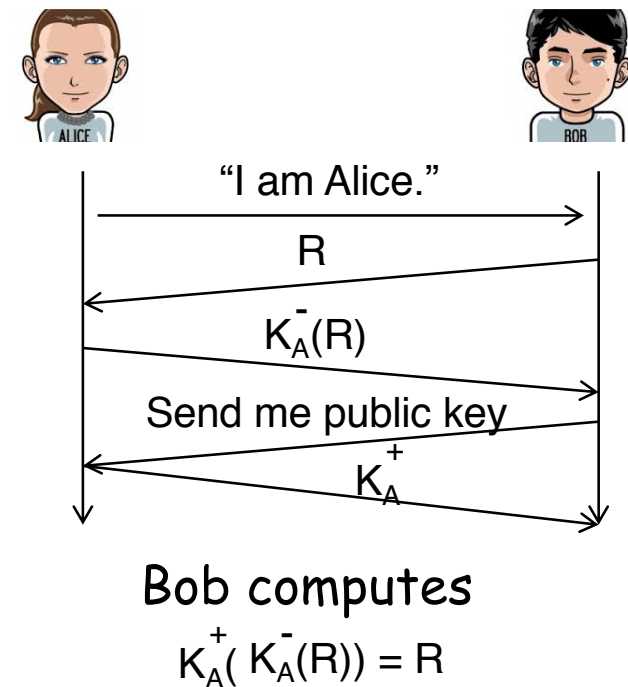
- Use a number, called a nonce, that will be used only once in a lifetime
- The protocol has the following procedures
 - Alice sends “I am Alice”, to Bob
 - Bob sends a nonce, R , to Alice
 - Alice encrypts the nonce using Alice and Bob’s symmetric secret key, K_{A-B} , and sends it back to Bob
 - Bob decrypts the received message. If the decrypted nonce equals the nonce he sent Alice, then Alice is authenticated.
- Key distribution can be a logistic problem.



Authentication Protocols (3)

- AP5.0

- Use the public key encryption in AP4.0
- The protocol has the following procedures
 - Alice sends “I am Alice”, to Bob
 - Bob sends a nonce, R , to Alice
 - Alice encrypts the nonce using Alice’s private key A and sends the encrypted nonce back to Bob
 - Bob decrypts the received message using Alice public key. If the decrypted nonce equals the nonce he sent Alice, then Alice is authenticated.



- The retrieval of the public key could be a security hole

Access & Availability (1)

- Securing physical access to the network
 - Physical security to servers
 - Physical security to networking devices
- A common guideline

**If there is physical access to the equipment,
there is no security!**

Access & Availability (2)

- Securing access to data
 - *Authentication and authorization*: who is permitted to access which network resources
 - *Encryption/decryption*: data unusable to anyone except the authorized users
 - *Virtual private networks (VPNs)*: allow authorized remote access to a private network via the public Internet
 - *Firewalls*: protect a computer from unauthorized access and attacks
 - *Virus and worm protection*: secure data from software designed to destroy data or slow down the computer
 - *Spyware protection*: securing from downloading and running programs that gather personal information
 - *Wireless security*

Security Policy

- Security policy
 - A formal statement of the rules by which people who are given access to an organisation's technology and information assets must abide
 - RFC 2196: Site Security Handbook. It is a guide to developing security policies for sites that are connected to the Internet
- Purposes of security policies
 - Policy is the first layer of protection for your resources and information
 - To inform users, staff and managers of their obligations for protecting technology and information assets
 - Should specify the mechanism through which these requirements can be met

Security Policy

- Policies have to be written explicitly
 - Implied policies do not help
- Who should be involved in writing of a policy?
 - Site security manager
 - IT technical staff
 - User representatives
 - Security incident response team
 - Responsible management
 - Legal counsel

Security Policy

- Aspects of a security policy
 - From outside the organisation
 - From inside the organisation
 - Against the interruption of services
 - From user error
 - User convenience
 - What resources are we trying to protect?
 - Whom are we trying to protect the resources from?
 - What will happen if the system is compromised?
 - How much work will we need to put into protecting the system? What risk is acceptable?
 - Protect from loss: backup should be stored at a different physical location to the original.

Security Policy

- Criteria for a good policy
 - Viable implementation through system administration procedures,
 - Acceptable by the users
 - Can be forced with security tools and sanctions
 - Clearly defines the areas of responsibility for the users, administrators and management
- Otago IT policies
 - <http://www.otago.ac.nz/its/policies/otago018522.html>