Introduction to Management Information Systems

Network Security

Telecommunications and Networks

Learning objectives

identify the need and technology behind network security

Network Security

principles :

- encryption = cryptography

CIA

- confidentiality
- integrity
- authentication

in practice:

- firewalls and intrusion detection systems
- security in application, transport, network, link layers

What is network security?

Confidentiality: only sender, intended receiver should "understand" message contents

- sender encrypts / receiver decrypts message

Integrity:

- sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Authentication:

- sender, receiver want to confirm identity of each other

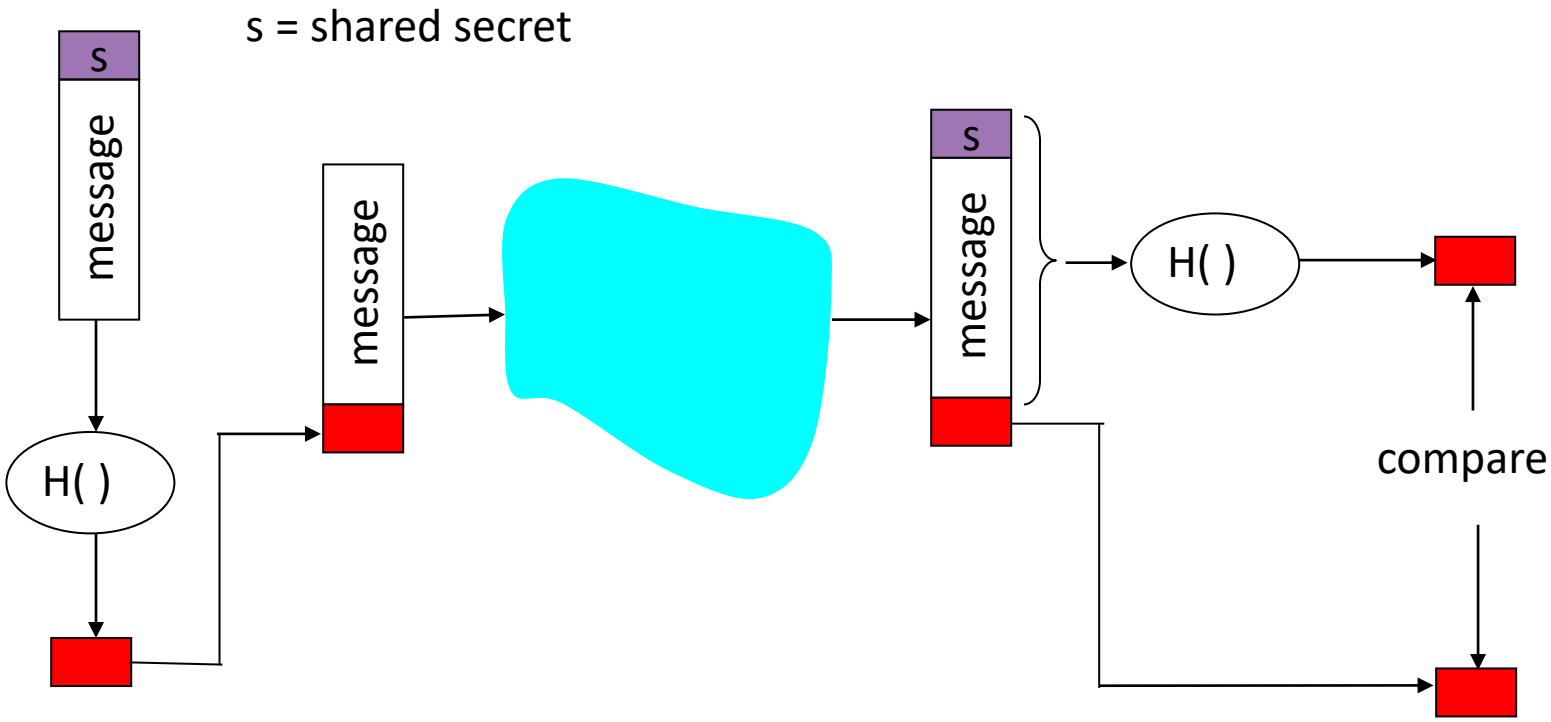
Non-repudiation:

- Proof of sender such as signature, if denied

Access and availability:

- services must be accessible and available to users

Message Authentication Code (MAC)



- ***Authenticates sender***
- ***Verifies message integrity***
- No encryption !
- Shared secret is called the authentication key
- Notation: $MD_m = H(s||m)$; send $m||MD_m$

encryption

substitution cipher: substituting one thing for another

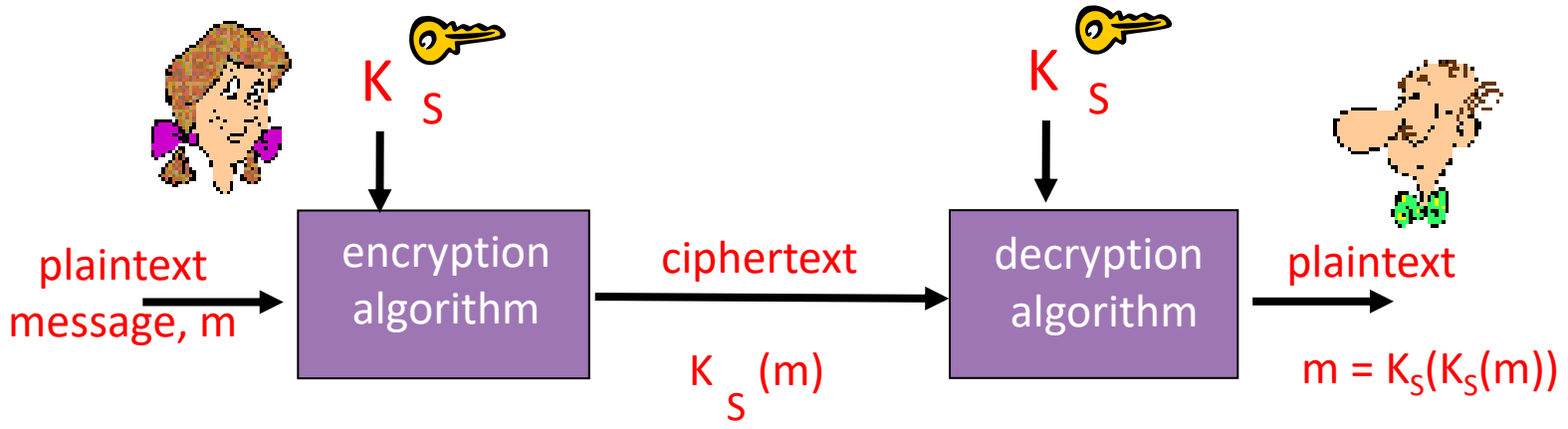
- monoalphabetic cipher: substitute one letter for another

```
plaintext:   abcdefghijklmnopqrstuvwxyz
                ↓                    ↓
ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

e.g.:

```
Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc
```

Symmetric key cryptography

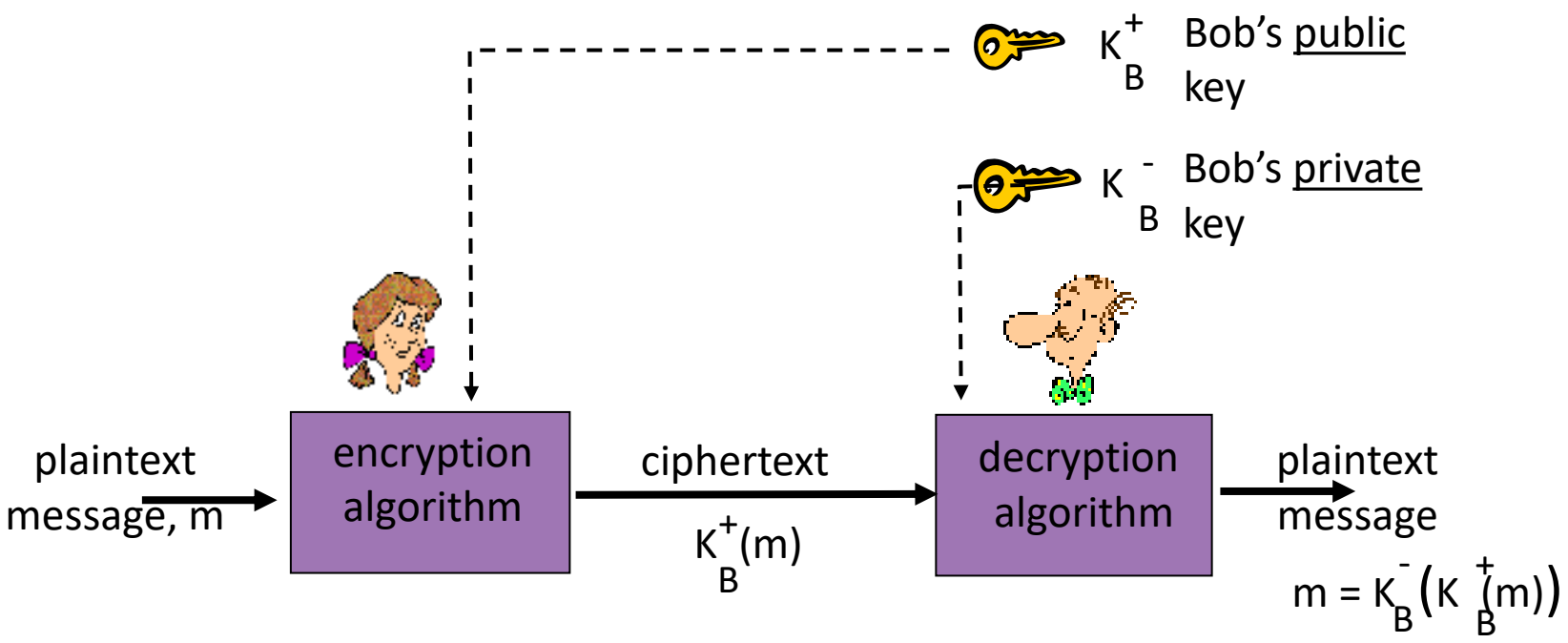


symmetric key crypto: Bob and Alice share same (symmetric) key: K

- e.g. key is knowing pattern substitution cipher

Q: how do Bob and Alice agree on key value?

Public key cryptography



Public key encryption algorithms

Requirements:

1. need $K_B^+(\ )$ and $K_B^-(\ )$ such that

$$K_B^-(K_B^+(m)) = m$$

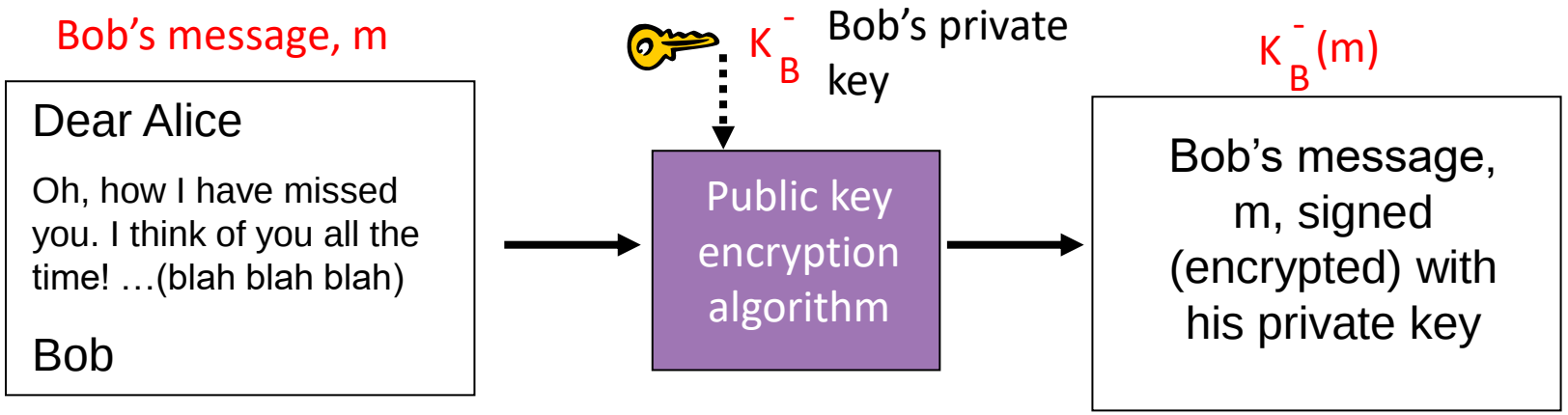
2. given public key K_B^+, it should be impossible to compute private key K_B^-

Example:

RSA: Rivest, Shamir, Adelson algorithm

Digital Signatures

Bob signs message *m* by encrypting with his private key K_B, creating "signed" message, $K_B(m)$



Decrypted using his public key

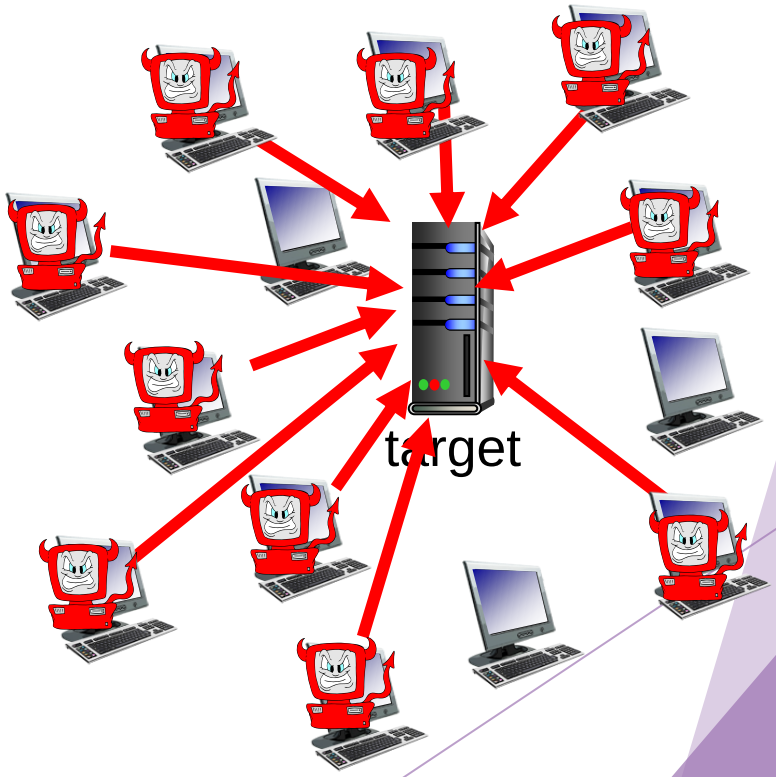
Denial of Service (DoS)

attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

1. select target

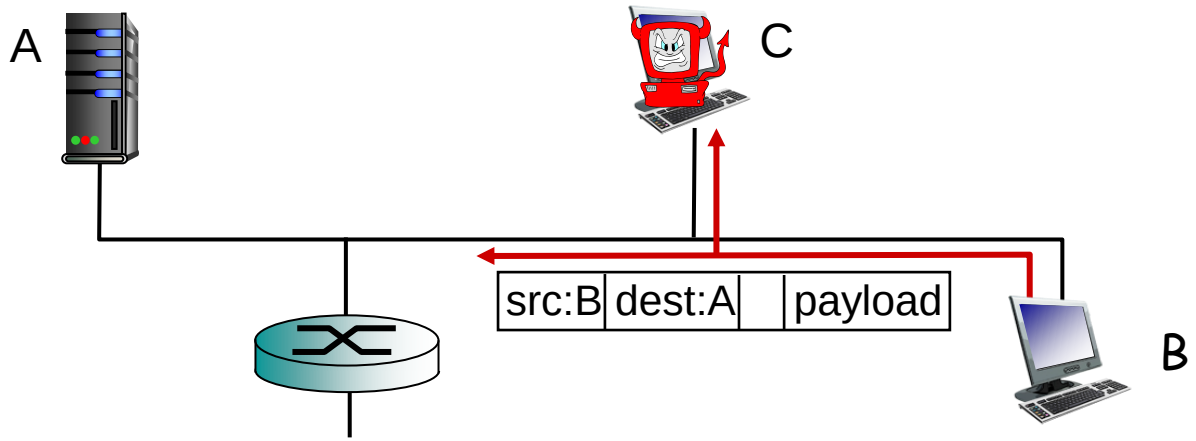
2. break into hosts around the network (see botnet)

3. send packets to target from compromised hosts



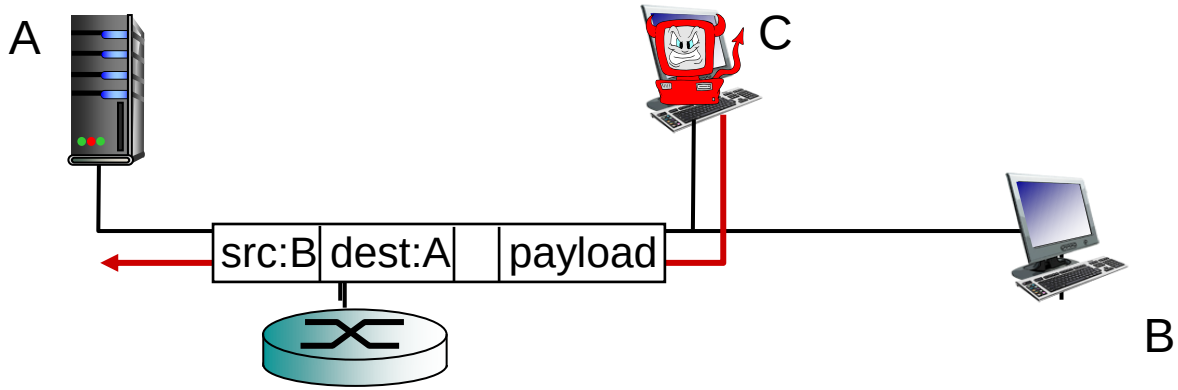
packet sniffing

- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



IP spoofing

send packet with false source address



Network Connection Authentication

Goal: Bob wants Alice to "prove" her identity to him

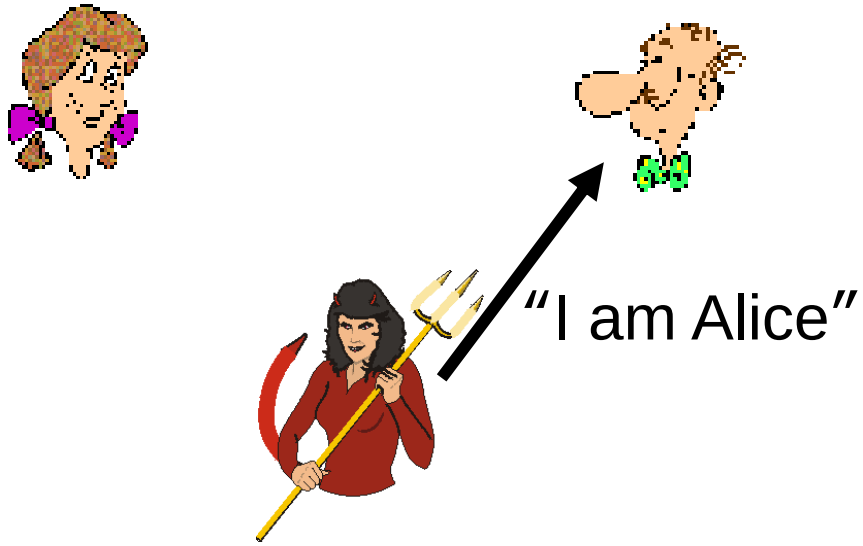
Protocol ap1.0: Alice says "I am Alice"

Failure scenario??

Authentication

Goal: Bob wants Alice to "prove" her identity to him

Protocol ap1.0: Alice says "I am Alice"



in a network,
Bob can not "see" Alice,
so Trudy simply declares herself to be Alice

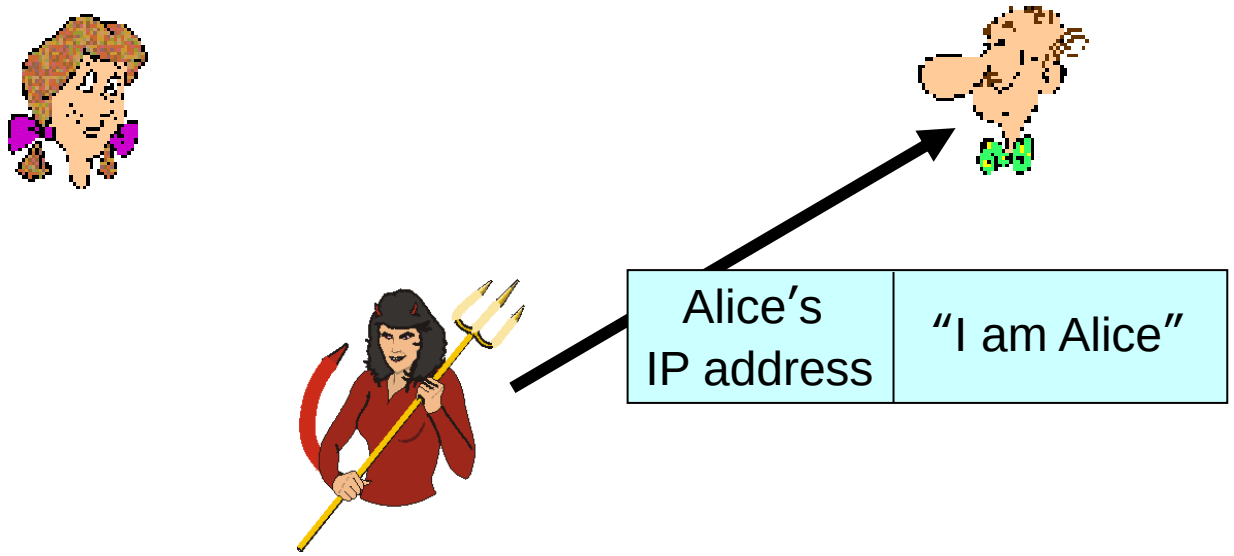
Authentication: another try

Protocol ap2.0: Alice says "I am Alice" in an IP packet containing her source IP address

Failure scenario??

Authentication: another try

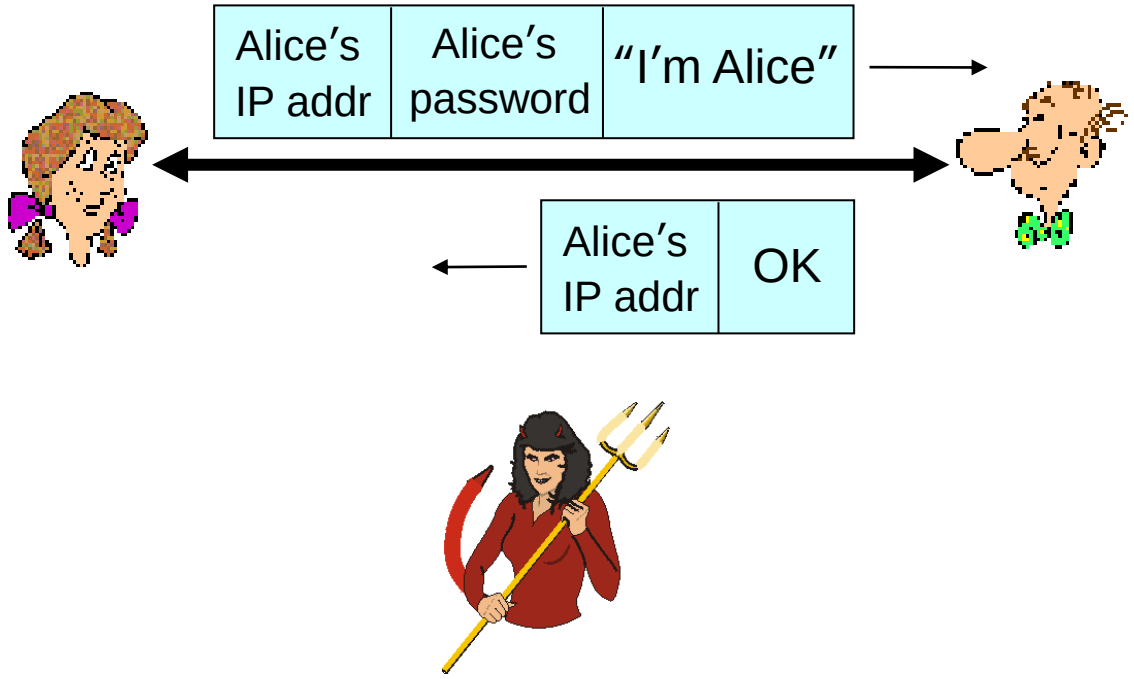
Protocol ap2.0: Alice says "I am Alice" in an IP packet containing her source IP address



Trudy can create a packet "spoofing" Alice's address

Authentication: another try

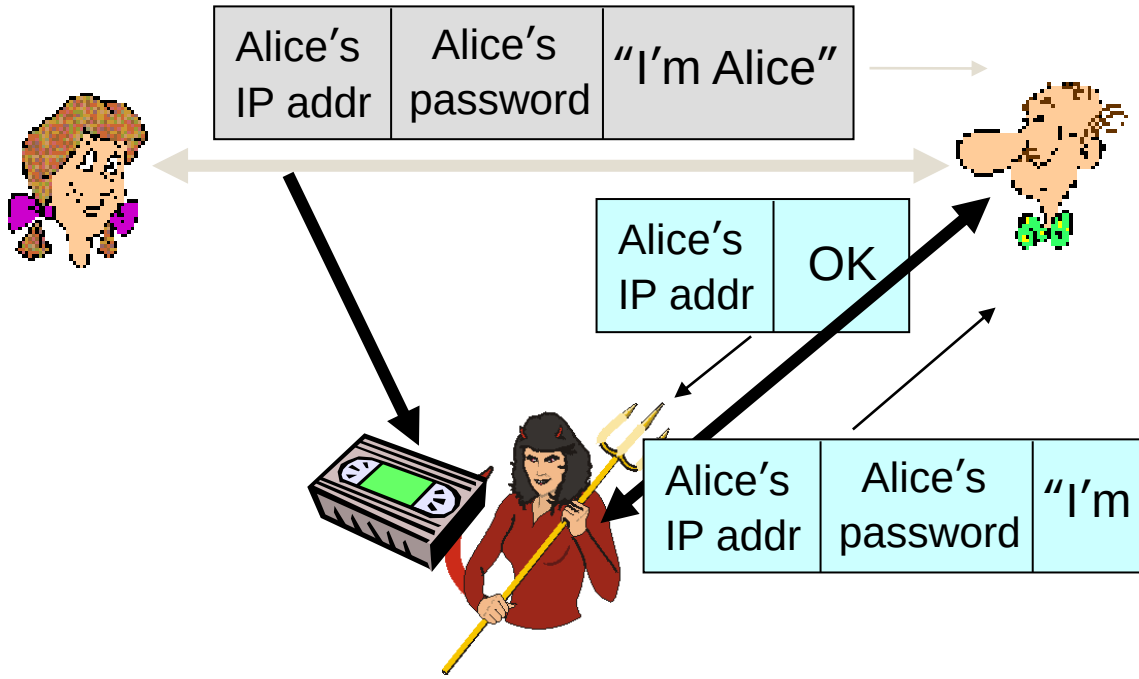
Protocol ap3.0: Alice says "I am Alice" and sends her secret password to "prove" it.



Failure scenario??

Authentication: another try

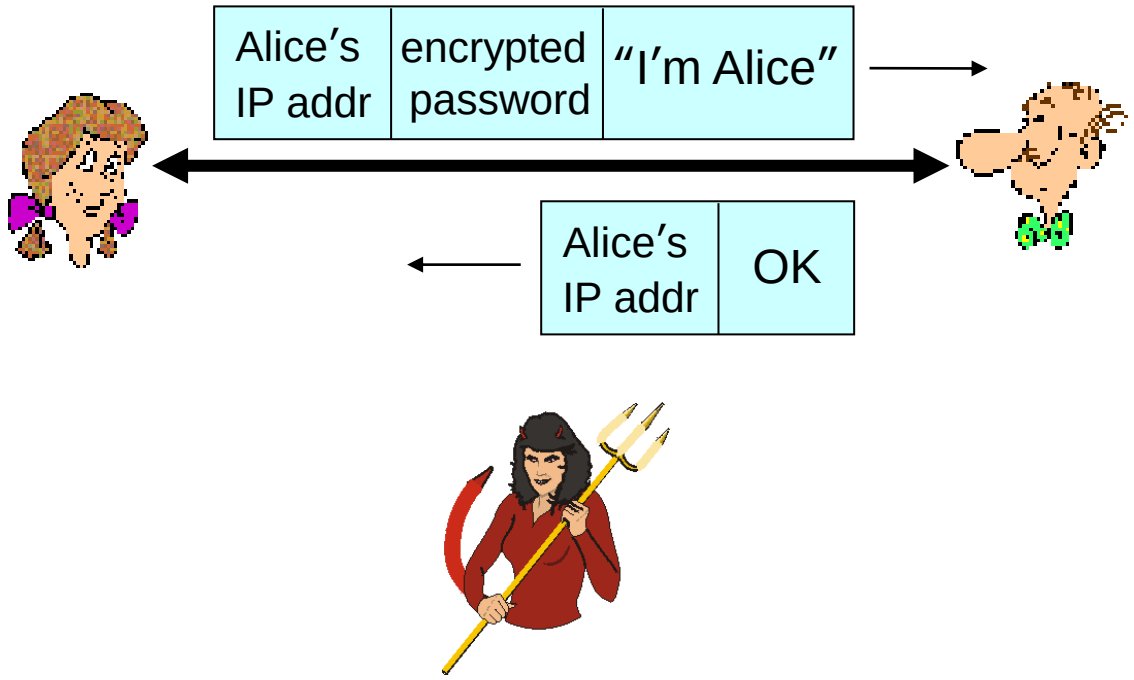
Protocol ap3.0: Alice says "I am Alice" and sends her secret password to "prove" it.



playback attack: Trudy records Alice's packet and later plays it back to Bob

Authentication: yet another try

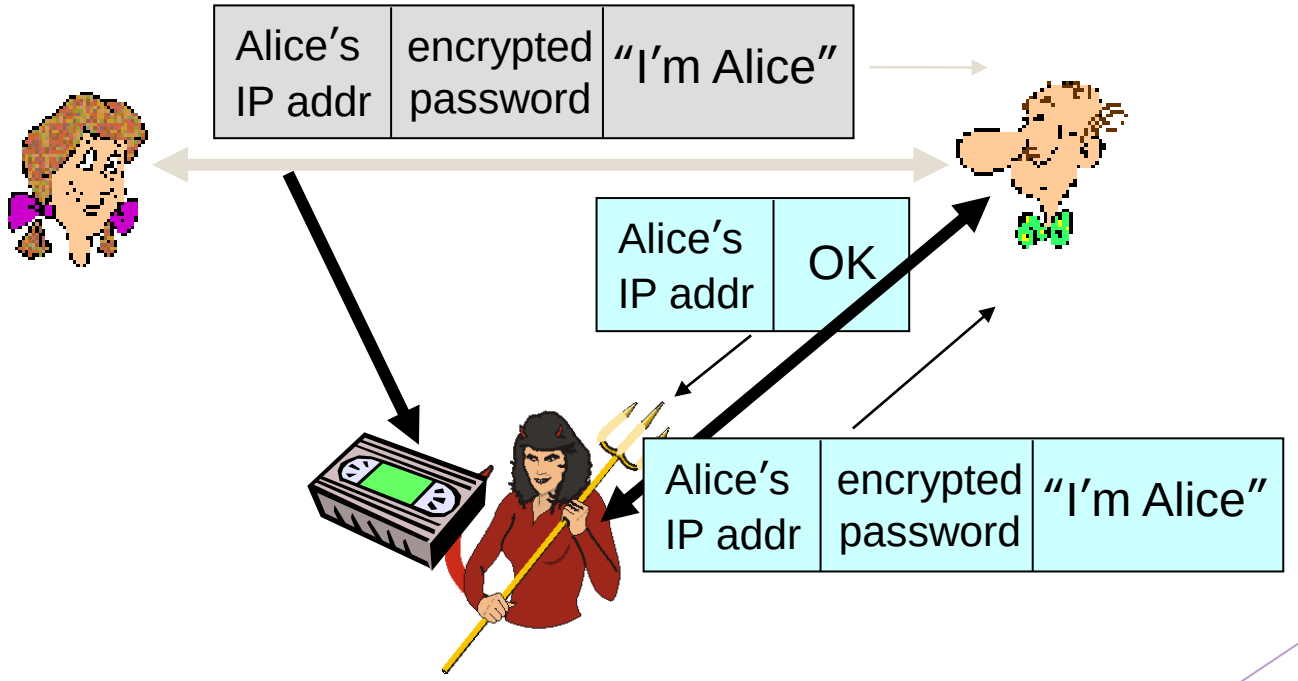
Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.



Failure scenario??

Authentication: yet another try

Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.



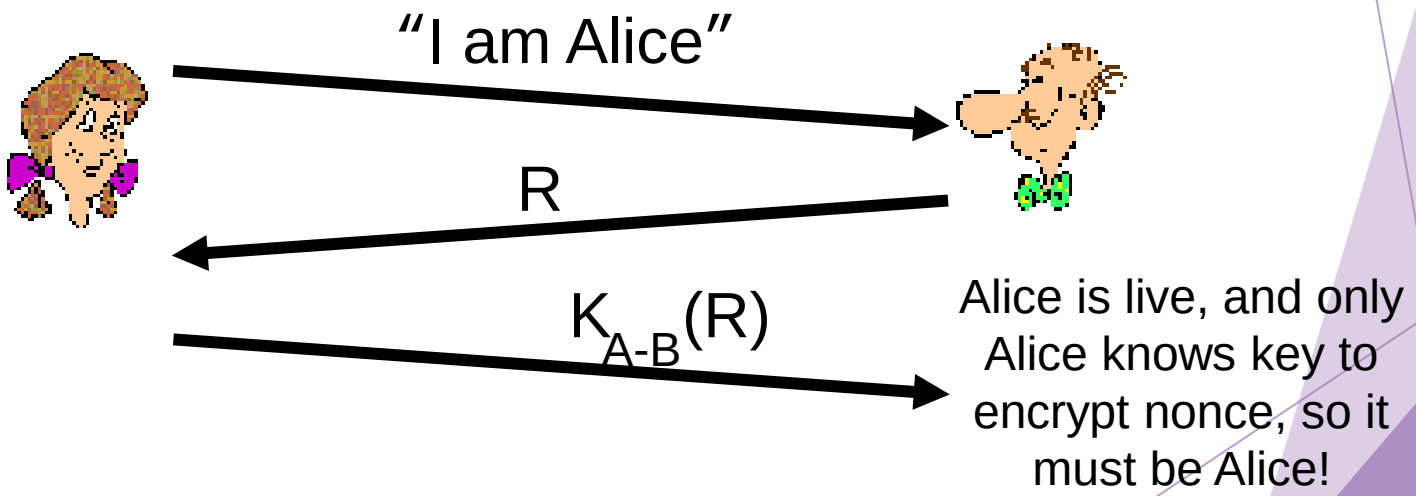
record and playback *still* works!

Authentication: yet another try

Goal: avoid playback attack

nonce: number (R) used only *once-in-a-lifetime*

ap4.0: to prove Alice "live", Bob sends Alice *nonce*, R. Alice must return R, encrypted with shared secret key



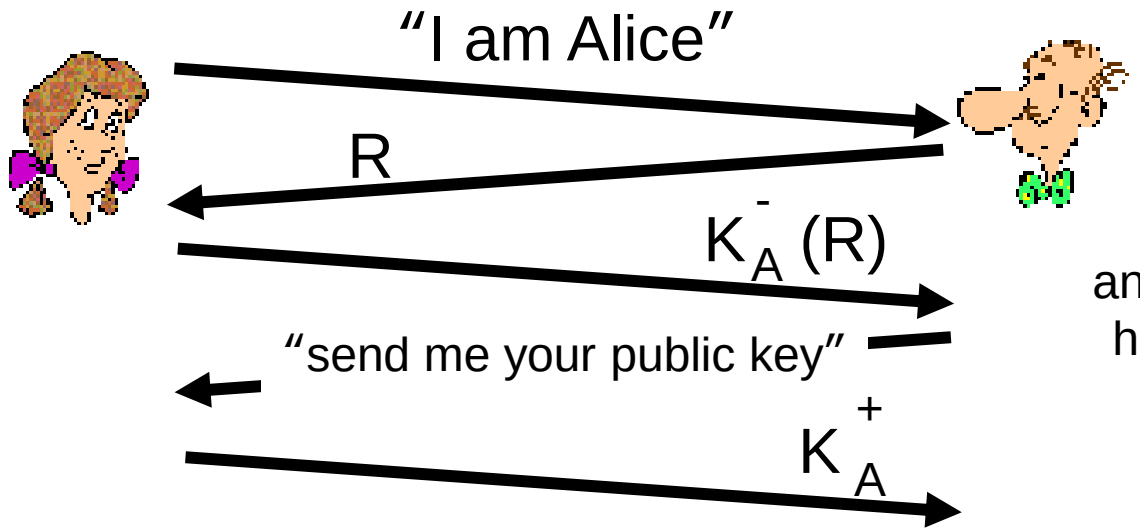
Failures, drawbacks?

Authentication: ap5.0

ap4.0 requires shared symmetric key

- can we authenticate using public key techniques?

ap5.0: use nonce, public key cryptography



Bob computes

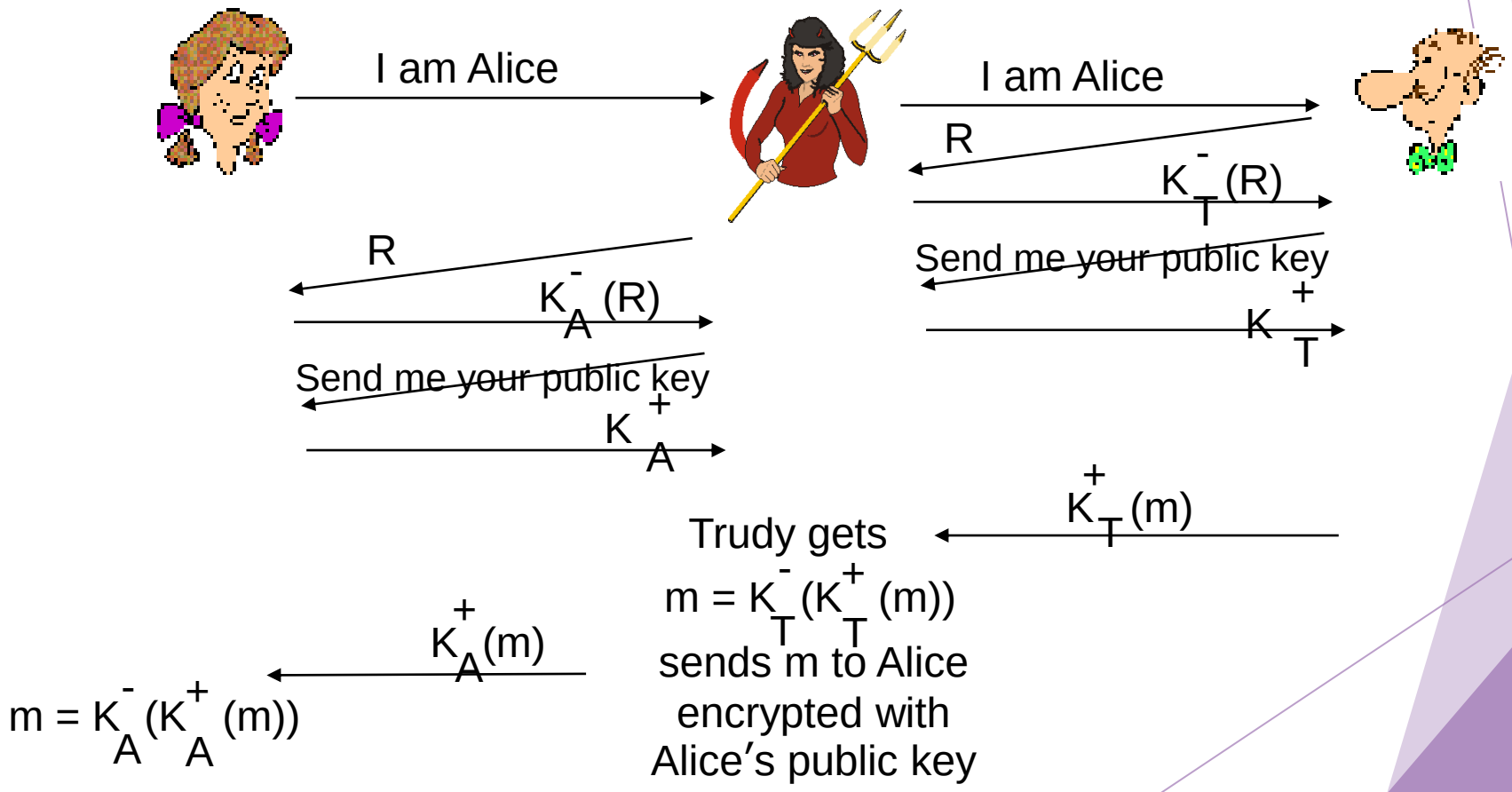
$K_A^+(K_A^-(R)) = R$

and knows only Alice could have the private key, that encrypted R such that

$K_A^+(K_A^-(R)) = R$

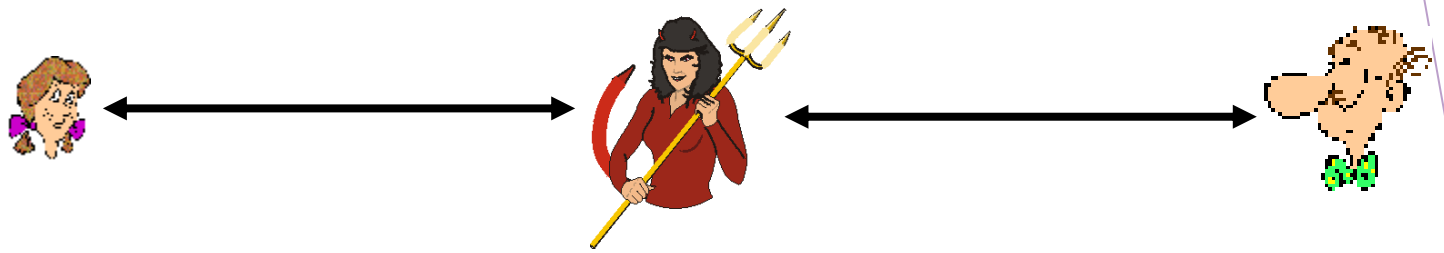
ap5.0: security hole

man (or woman) in the middle attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)



ap5.0: security hole

man (or woman) in the middle attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)



difficult to detect:

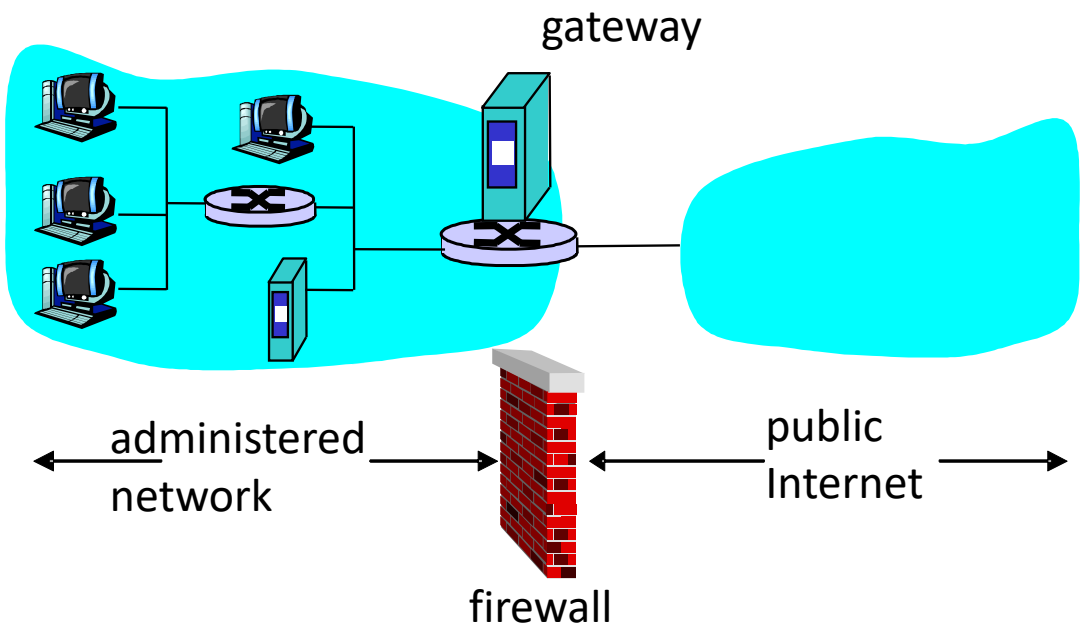
- Bob receives everything that Alice sends, and vice versa. (e.g., so Bob, Alice can meet one week later and recall conversation!)
- problem is that Trudy receives all messages as well!

Personal Authentication

- What the user *knows*
  - Userid and password
  - Userid and PIN
- What the user *has*
  - Smart card
  - Token
- What the user *is*
  - Biometrics (fingerprint, handwriting, voice, etc.)

Firewalls

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others



Firewalls:

Three types of firewalls:

1. stateless (traditional) packet filters
2. stateful filters
3. application gateways

Access Control Lists

Firewall rules are implemented in routers with access control lists

- A table of rules, applied top to bottom to incoming packets:
- action, condition pairs

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Limitations of firewalls and gateways

- if multiple app's. need special treatment, each has own app. Gateway
- IP spoofing - router can't know if data "really" comes from claimed source
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser
- Web server & web cache act as app gateways
- filters often use all or nothing policy for UDP.
- tradeoff: degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks.

Intrusion systems

packet filtering:

- operates on TCP/IP headers only
- no correlation check among sessions

IDS: intrusion detection system

- A devise that generates alerts when there are suspicious packets

IPS: intrusion prevention system

- A devise that filters out suspicious packets

Intrusion detection systems (IDS)

1. Signature-based systems
   - Uses a database of signatures
2. Anomaly-based systems
   - Compares packets to a traffic profile

- deep packet inspection:
  - look at packet contents
  - check character strings in packet against database of known viruses
- examine correlation among multiple packets
  - port scanning, network mapping, DoS attack

Intrusion detection systems

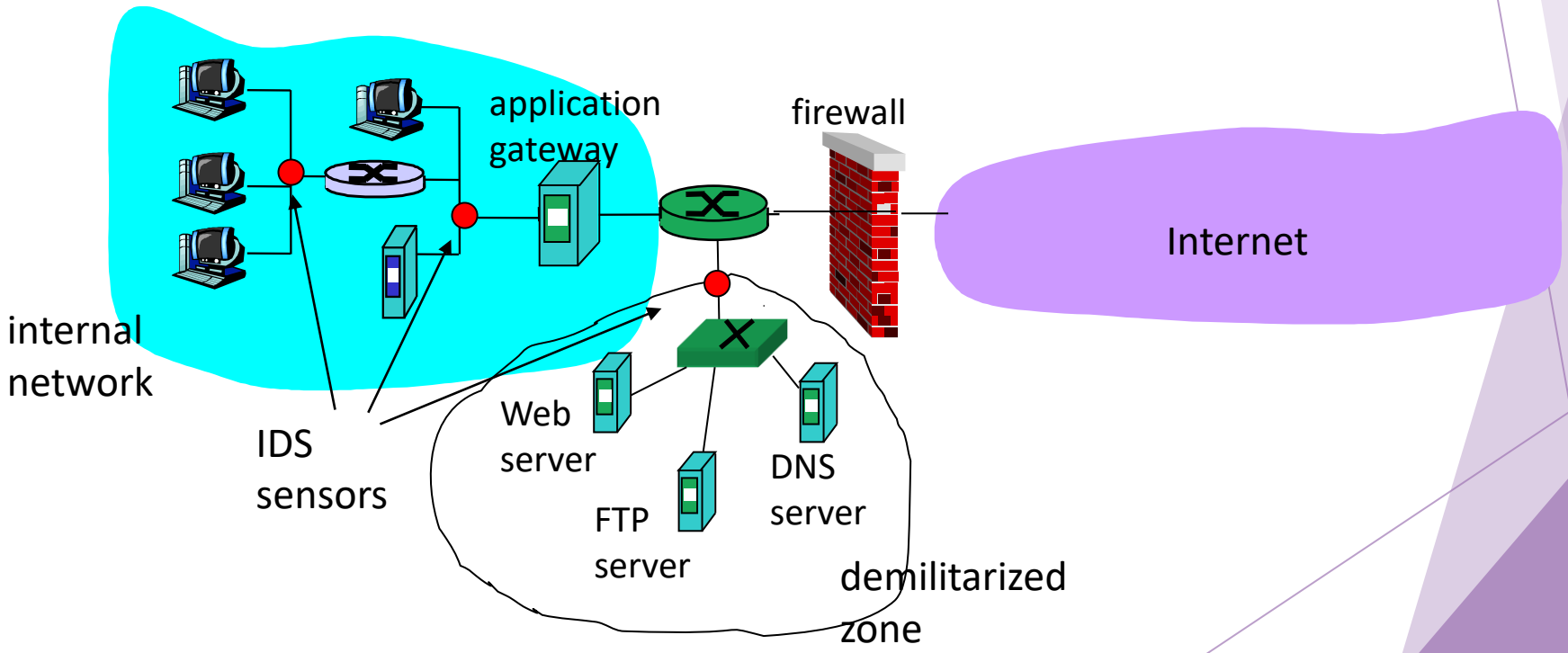
IDS: intrusion detection system

- deep packet inspection: look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
- examine correlation among multiple packets
  - port scanning
  - network mapping
  - DoS attack

1. Signature-based systems
   - Uses a database of signatures
2. Anomaly-based systems
   - Compares packets to a traffic profile

Intrusion detection systems

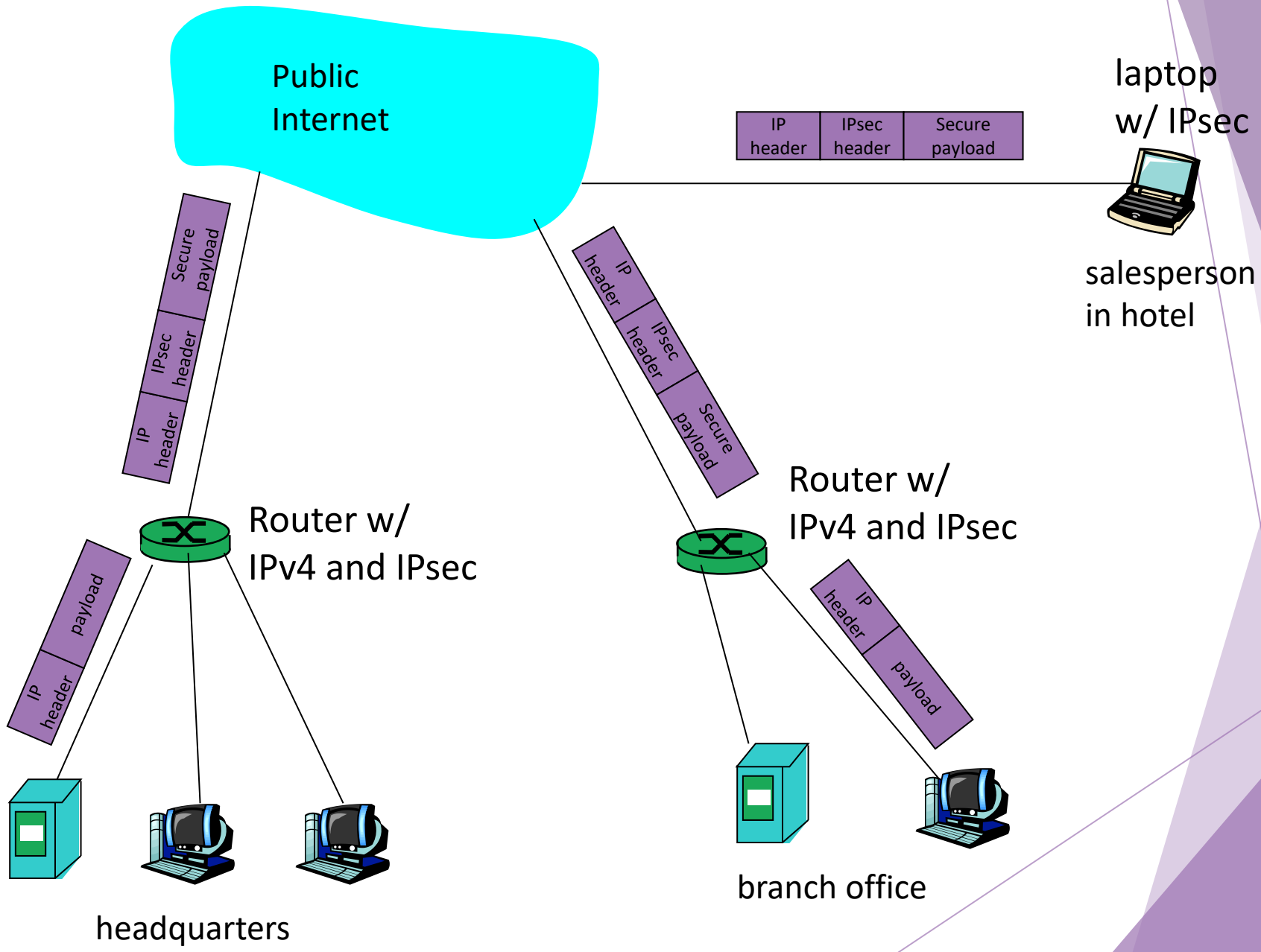
- multiple IDSs: different types of checking at different locations



Virtual Private Networks (VPNs)

- Institutions often want private networks for security.
  - Costly! Separate routers, links, DNS infrastructure.
- With a VPN, institution's inter-office traffic is sent over public Internet instead.
  - But inter-office traffic is encrypted before entering public Internet

Virtual Private Network (VPN)



Thank you!

any questions?