Lecture: Network Security

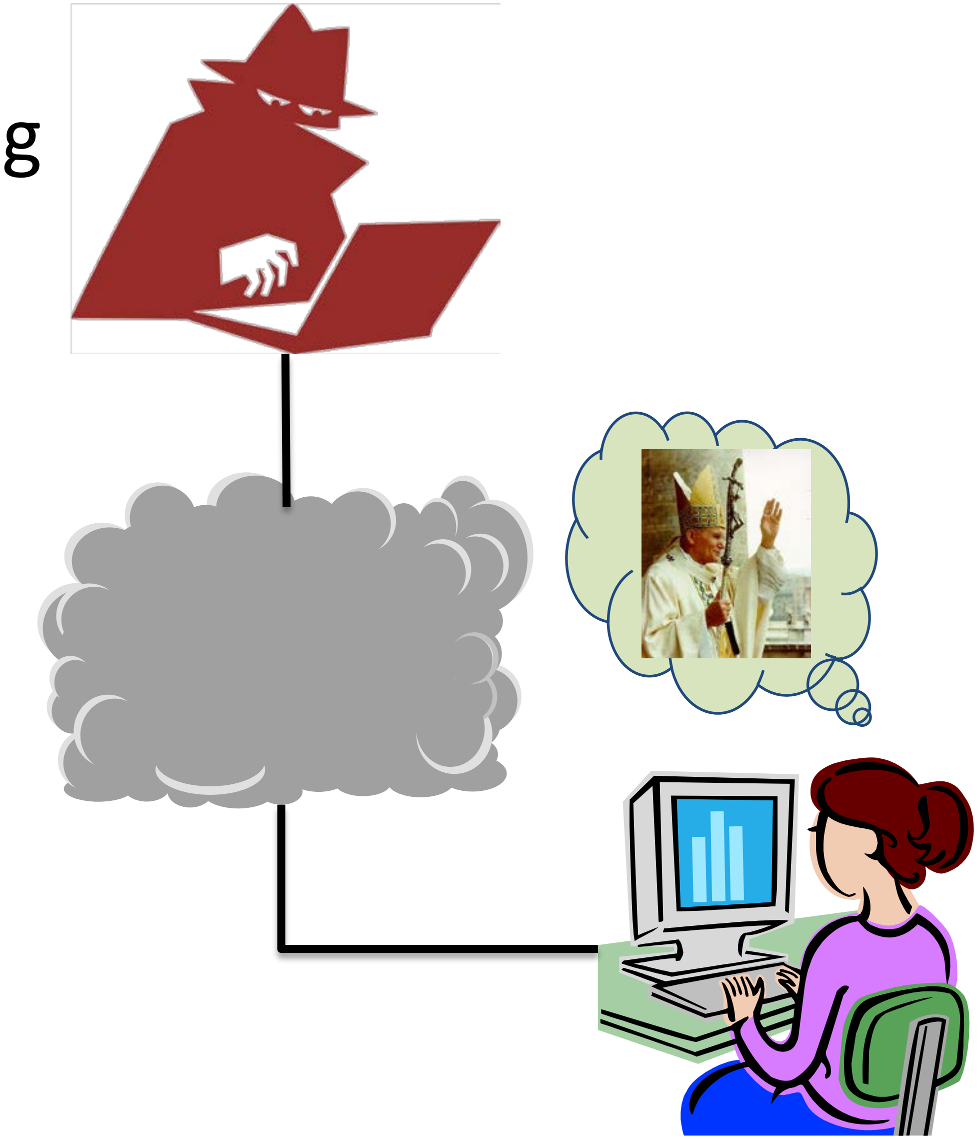
Magnus Almgren (Erland Jonsson)

Department of Computer Science and Engineering

Chalmers University of Technology

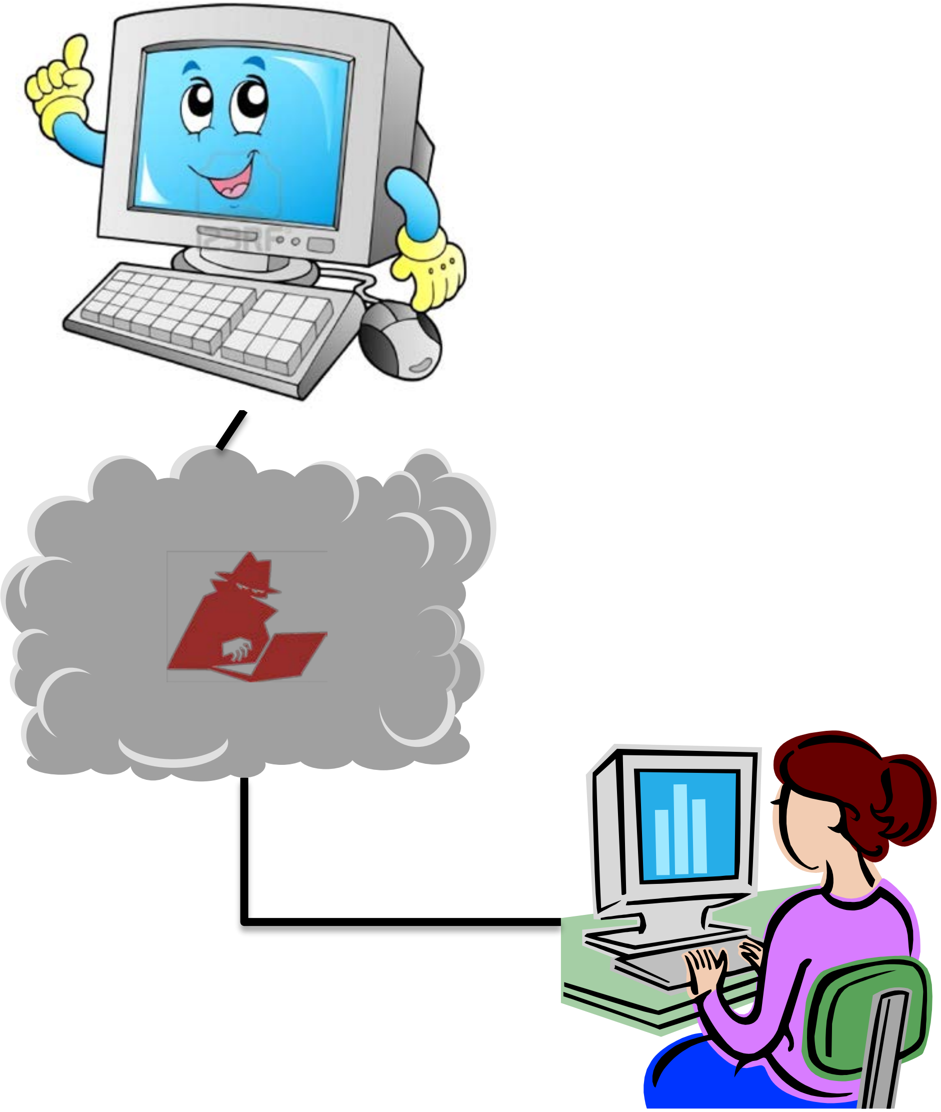
Overview: Authentication

- When communicating the other party's identity must be verified
  - Authentication
    - Spoofing
    - Kerberos



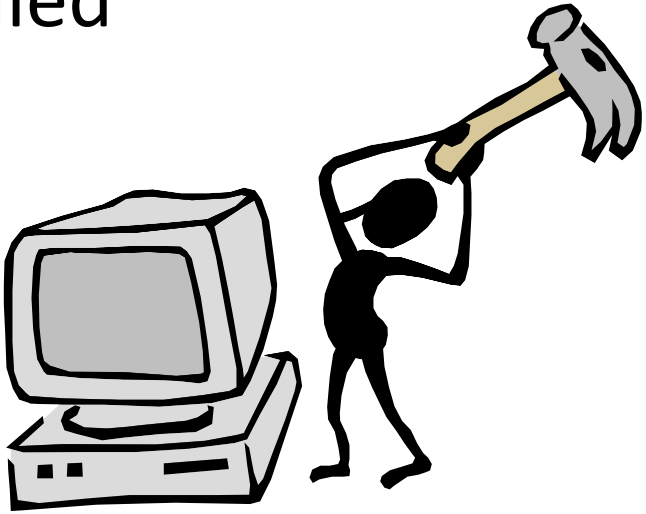
Overview: Man in the Middle

- Security aspects for your data are the “usual” ones:
  - **Confidentiality**
  - **Integrity**
  - Availability
- How do you know that the information has not been **modified and/or intercepted?**



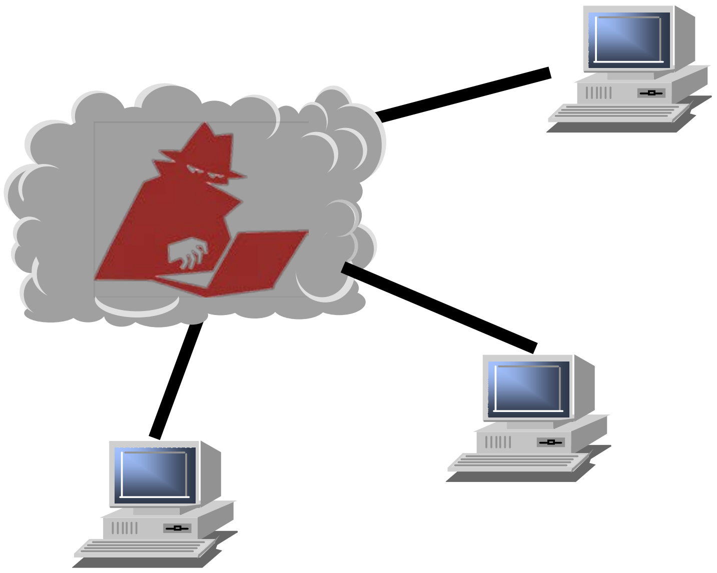
Overivew: Availability

- Security aspects for your data are the "usual" ones:
  - Confidentiality
  - Integrity
  - **Availability**
- Attack against availability is called **"denial of service" attack**
- Extremely difficult to protected against



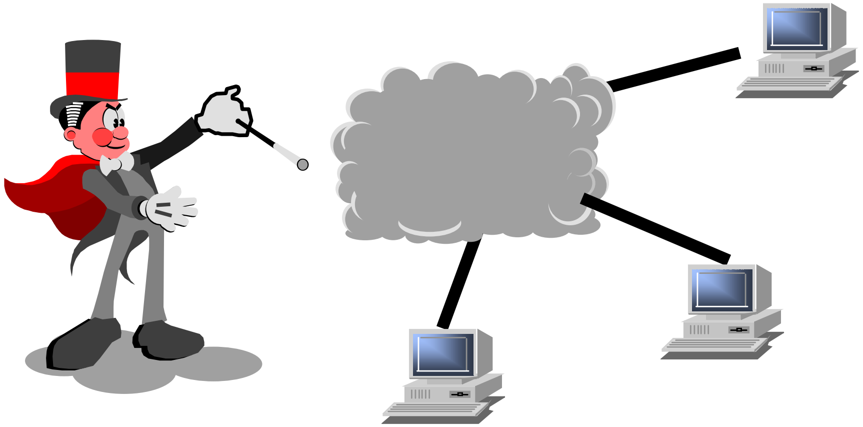
Network insecurity

- **Insecure Medium**
  - It is almost impossible to secure the network itself, i.e. the communication links
  - You must always assume that attackers are able to bug and modify all traffic
- Unknown communication path
  - Several routes between two nodes
  - Lack of control of the network
- Unknown perimeter boundary
  - Several points of attacks
    ➔ **Firewalls!**
- Anonymity?
  - TOR
  - Protecting the accessed information



Finding vulnerabilites

- Port Scanning:
  is a general information-gathering activity. It is a way to find open ports in hosts that can be used for attacks.
  Variant: Stealth Scanning



Spoofing

Spoofing means pretending to be the real owner of an address, which is incorrect.
It may also mean falsely providing a service instead of the real service provider.

- There are several types of spoofing:
  - **IP address** spoofing
  - **ARP** (Address Resolution Protocol) spoofing
  - **Web** spoofing
  - **DNS** (Domain Name Service or System) spoofing

ARP is used in LANs to map the host's IP address to the physical (MAC) address.
DNS translates alphabetic host addresses to IP addresses (is really a network).

IP Spoofing

- **IP address spoofing** exploits the trust relationship between two hosts, the trusted host and the victim host:
  - Send an attack packet to the victim host with a **false source address** (i.e. that of the trusted host)
  - The **victim's replies** would still go to the trusted host. Thus, the attacker does not see them.
  - **Disable the trusted host** in some way (DOS attack?), so that it does not interfere with the communication.
  - Find out the **sequence numbers** somehow, otherwise the spoofed packets will not be accepted by the victim.

Web spoofing

- **Web spoofing** fools the victim to think that he is visiting a legitimate site, whereas he is really visiting the attacker's site.
  - Can be achieved by providing a false link by compromising a common web page.
  - Can also be achieved by providing a false web address, that may be confused with the real one.
    E.g. www.bank.com or www.bank.nu instead of www.bank.se
  - This may cause all communication to pass through the attacker's server.

DNS Spoofing

- **DNS spoofing** means directing users to a false server. This can be accomplished in several ways:
  - By making a fake mapping between hostname and IP address at the victim's web server.
  - By IP spoofing, so that the IP address request goes to a false DNS server.
  - Attacking the real DNS server and changing entries in its cache memory (DNS Poisoning).

ARP Spoofing

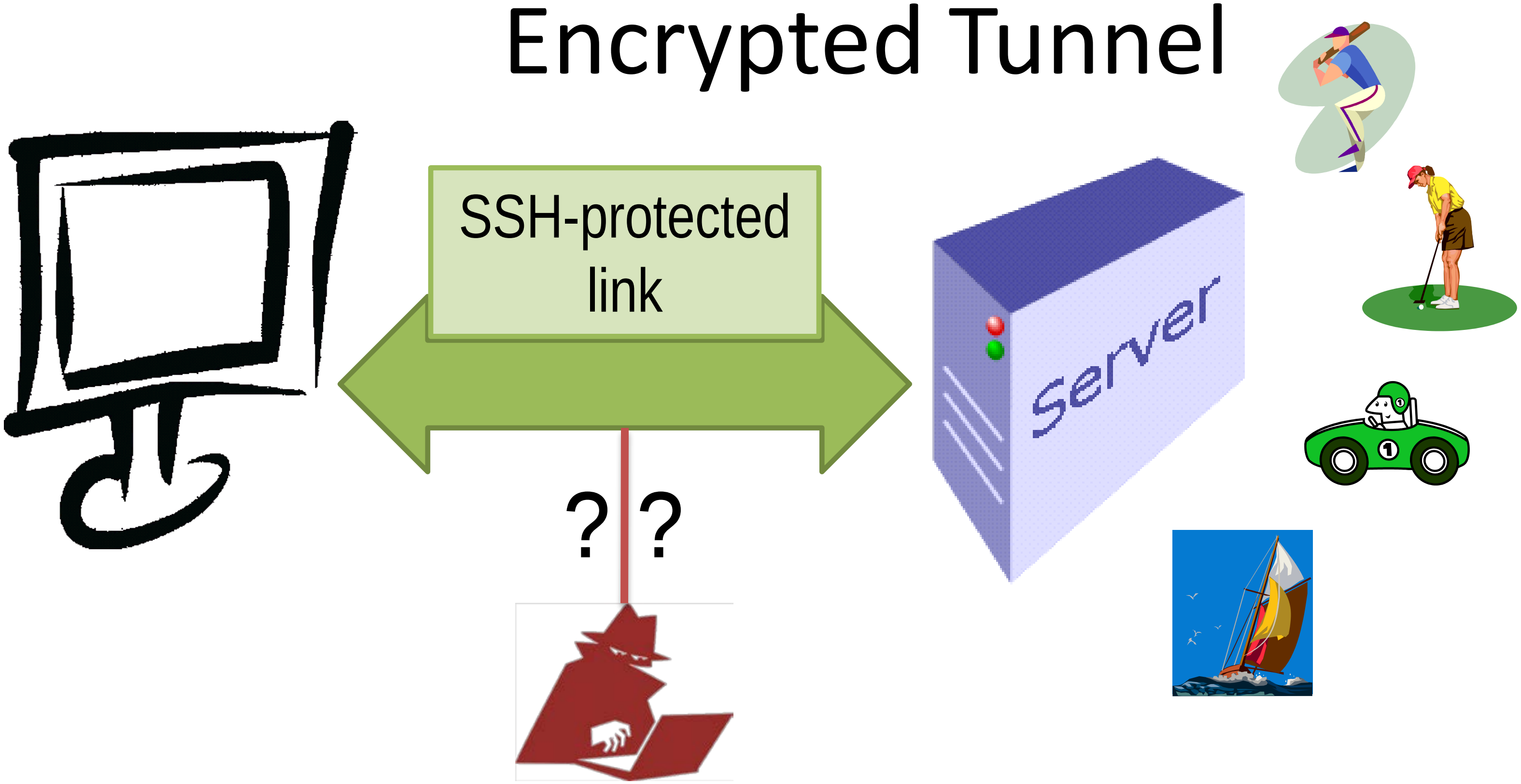
- **ARP spoofing** (or poisoning) means sending faked ARP replies to a LAN.
  - – The ARP request packet is broadcast to the network segment. Anyone can answer.
  - – Giving a wrong answer will confuse network devices, e.g. routers.
  - – This may result in that the communication will be directed to an incorrect host.
  - – It may also result in that the correct host is unreachable, a DOS attack.

Man-in-the-middle attack

- A **man-in-the-middle attack** is an attack in which the attacker (logically) places himself *between* the two hosts that are communicating. Both hosts think that they are communicating with one another, but both of them are in fact communicating with the attacker's server.
- Can be accomplished in many ways:
  - Using web spoofing
  - By ARP poisoning (available tool: Hunt)
  - By ICMP redirection of packages
  - By DNS poisoning
- The attacker can also passively monitor the communication between the parties, e.g. to collect sensitive information (a passive attack).

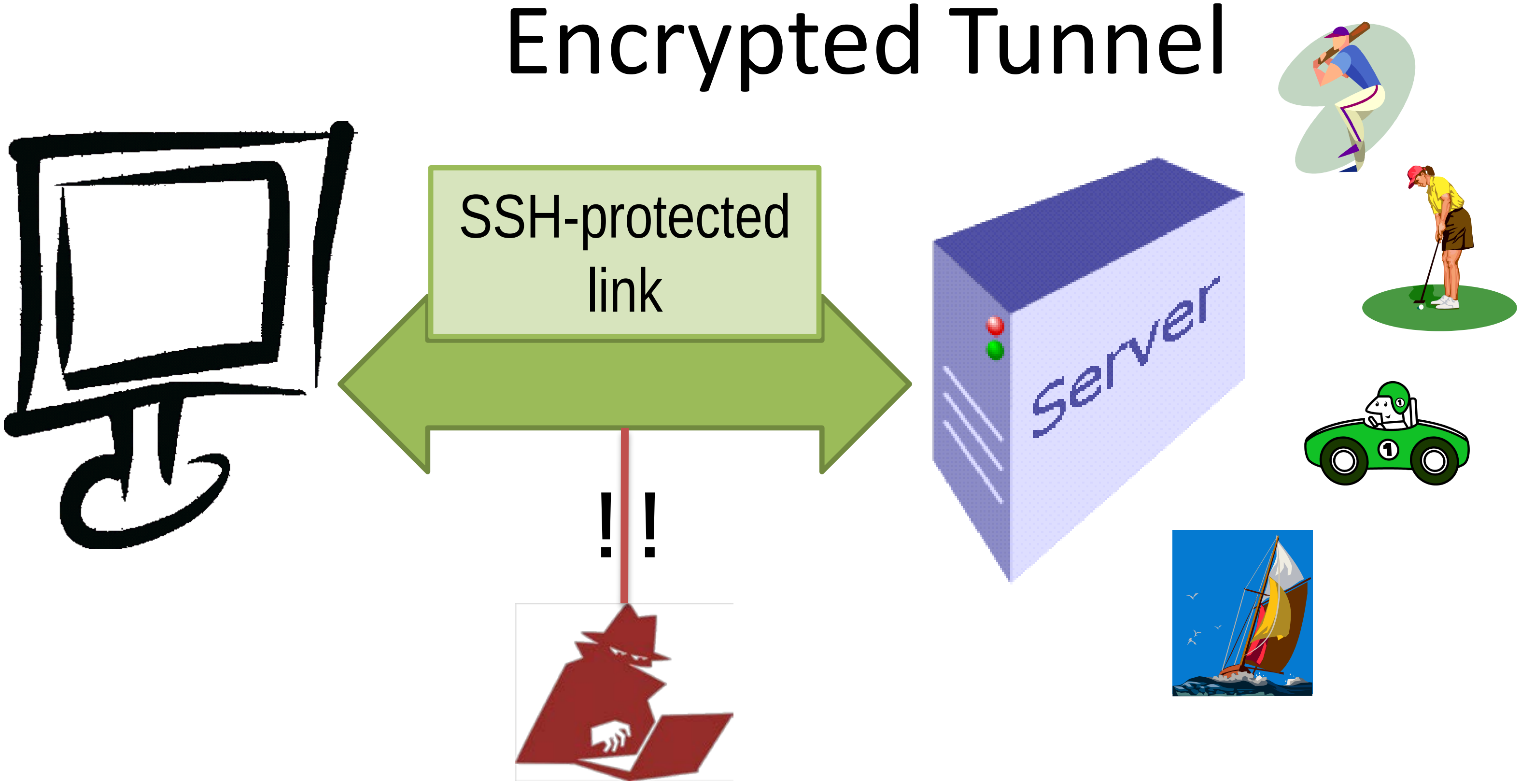
Internet Control Message Protocol

Protection Mechanism: Encrypted Tunnel



- Attacker’s goal is to identify the webpage requested.
- Possible?

Protection Mechanism: Encrypted Tunnel



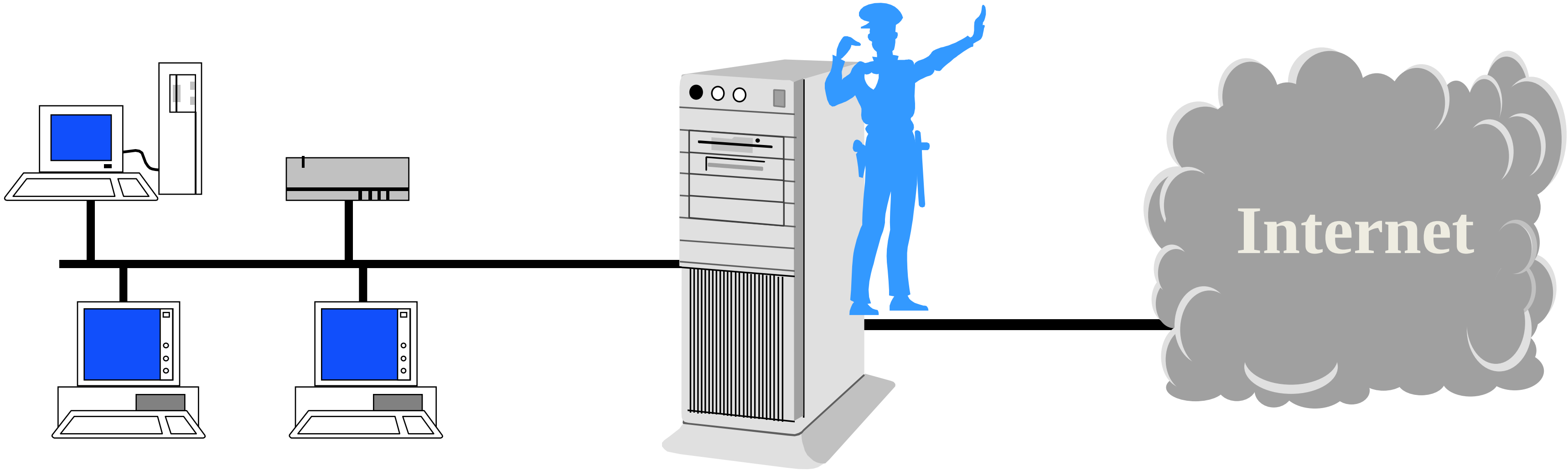
- Yes, with 68% accuracy. Packet length, packet direction, packet timing ➔ traffic analysis attacks

[SoK]: Peek-a-Boo, I Still See you: Why Efficient Traffic Analysis Countermeasures Fail
Kevin P. Dyer (Portland State University), Scott E. Coull (RedJack, LLC), Thomas Ristenpart (University of Wisconsin-Madison), and Thomas Shrimpton (Portland State University)

FIREWALLS

Firewalls

- A firewall is an access control device between two networks.
- A firewall monitors all traffic (in both directions) and filters away (denies) unwanted traffic
- Thus it protects against attacks from outside



Firewalls

- The firewall determines which inside services may be accessed from outside and which outsiders that are allowed to access to those inside services.
- It determines which outside services may be accessed by insiders.

Firewall Capabilities and Limits

- capabilities:
  - defines a single choke point
  - provides a location for monitoring security events
  - convenient platform for some Internet functions such as NAT[1], usage monitoring, IPSEC VPN[2]s
- limitations:
  - cannot protect against attacks bypassing firewall
  - may not protect fully against internal threats
  - improperly secure wireless LAN
  - laptop, PDA, portable storage device infected outside then used inside

[1] Network Address Translation [2] Virtual Private Network

Firewalls – basic functionality

A firewall implements an organization's security policy with respect to Internet

- The ***stance*** of a firewall describes the fundamental security philosophy of the organisation
  - The ***default deny (discard)*** stance: everything is denied unless specifically permitted
  - The ***default permit (forward)*** stance: everything is permitted unless specifically denied

Firewalls techniques

Basic principles:

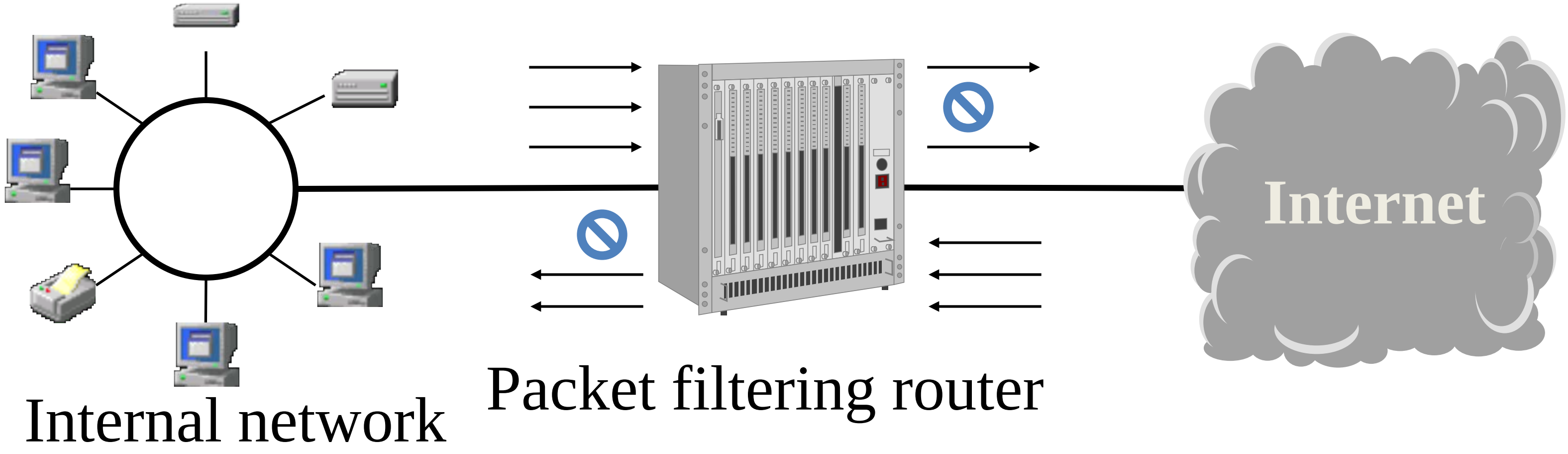
- Packet filter
- Application-level gateway (proxy)
- Circuit-level gateway
- Stateful inspection (dynamic filtering)

Architectures:

- Packet filtering router
- Single-homed host
- Dual-homed host
- Demilitarized Zone (DMZ)

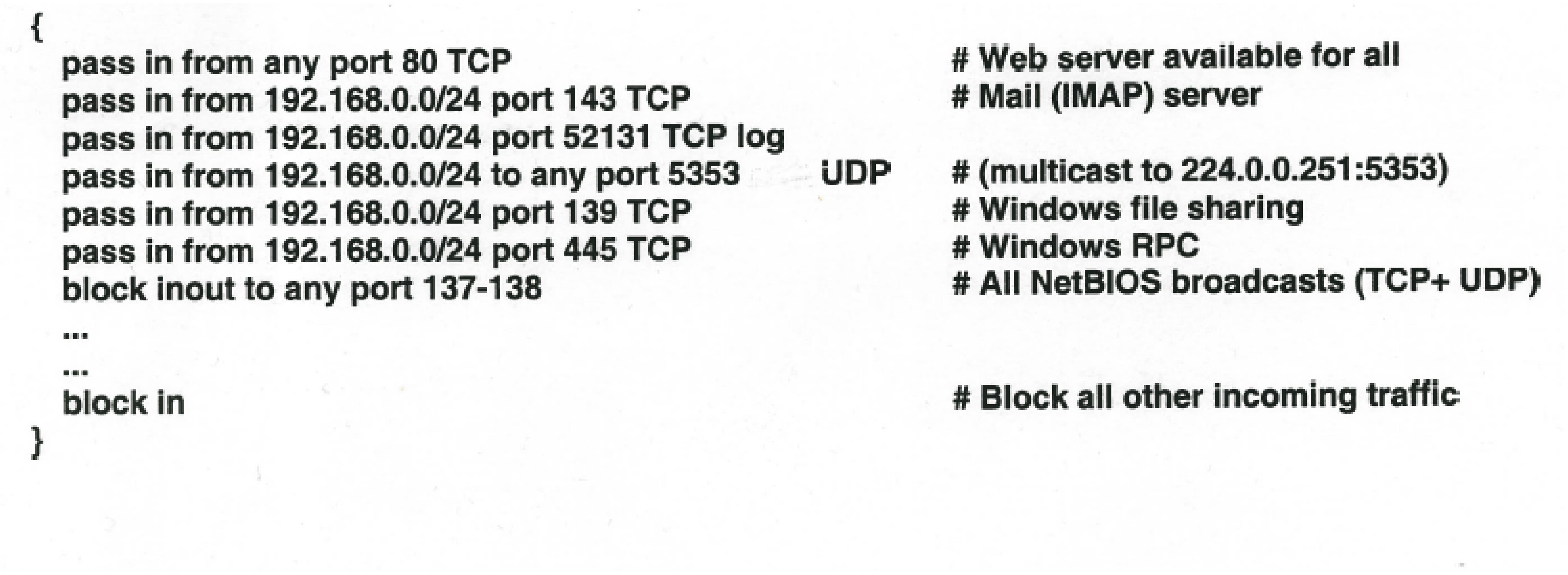
Firewalls, basic principles (and architecture):

Packet filter



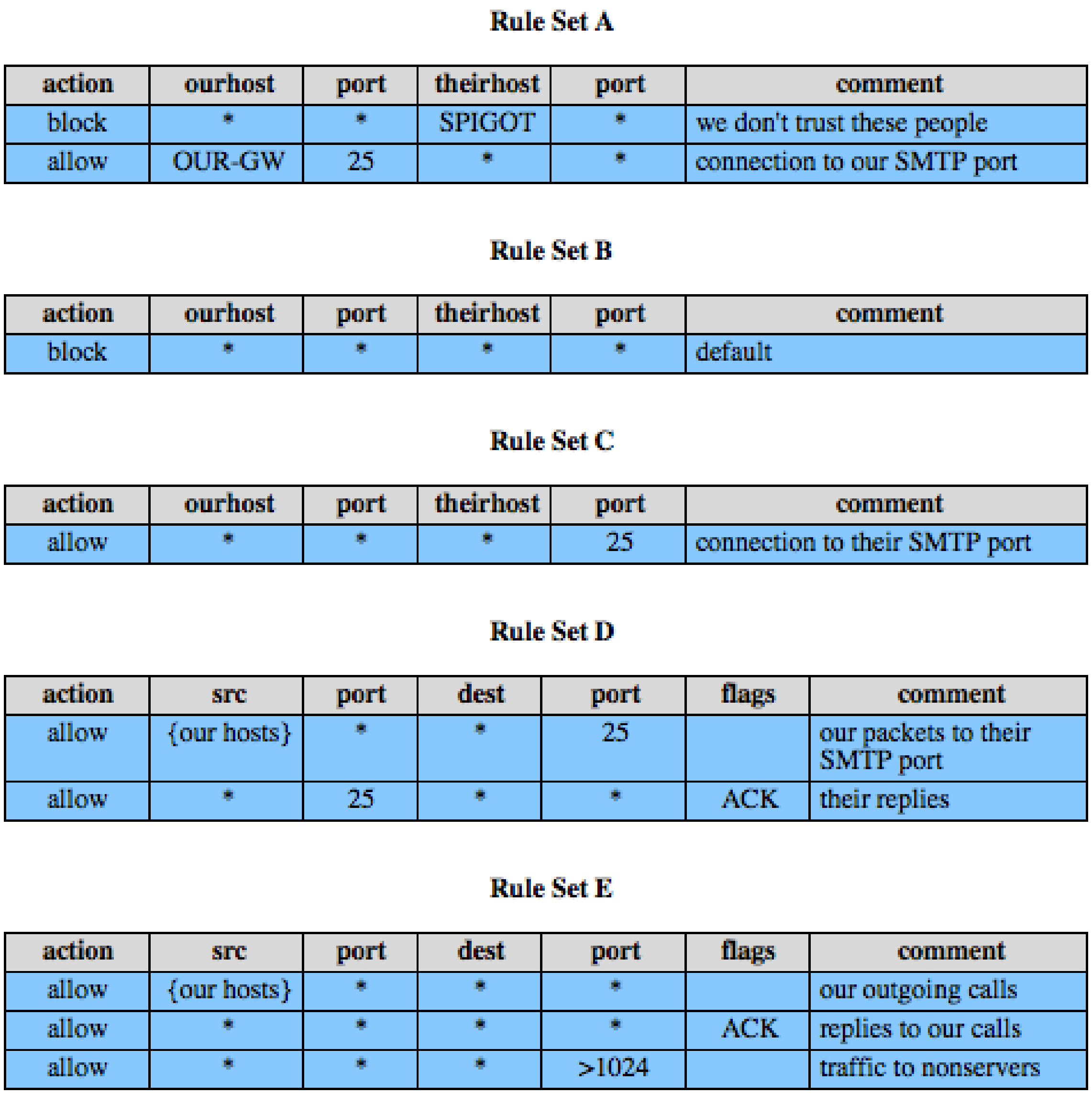
- Allows or denies a packet based on address, direction, port and protocol
- Does not understand the contents of the packet
- Advanced variation: dynamic filtering/stateful inspection

Firewall Rules – practical example



```
{
   pass in from any port 80 TCP                                   # Web server available for all
   pass in from 192.168.0.0/24 port 143 TCP                       # Mail (IMAP) server
   pass in from 192.168.0.0/24 port 52131 TCP log
   pass in from 192.168.0.0/24 to any port 5353         UDP       # (multicast to 224.0.0.251:5353)
   pass in from 192.168.0.0/24 port 139 TCP                       # Windows file sharing
   pass in from 192.168.0.0/24 port 445 TCP                       # Windows RPC
   block inout to any port 137-138                                # All NetBIOS broadcasts (TCP+ UDP)
   ...
   ...
   block in                                                       # Block all other incoming traffic
}
```

Packet Filter Rules



Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

Rule Set D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Rule Set E

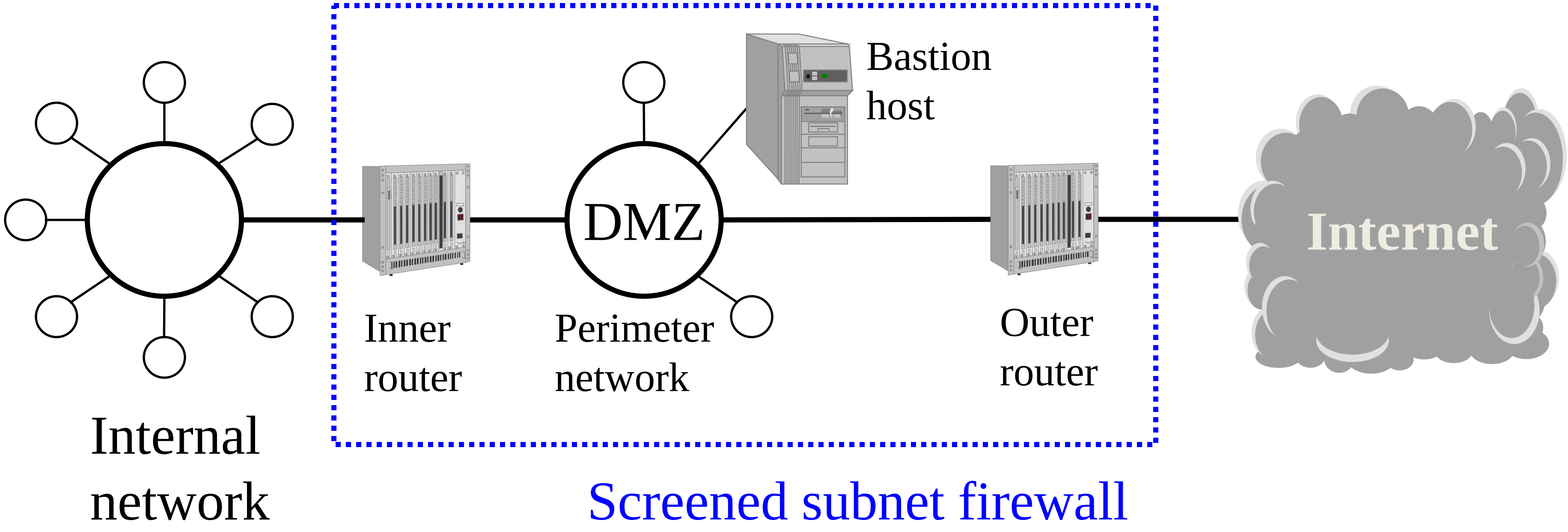
action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Host-Based Firewalls

- A software module used to secure an individual host
- available in (or as an add-on for) many O/S
- often located in servers
- advantages:
  - taylored filter rules for specific host needs
  - protection from both internal/external attacks
  - additional layer of protection to stand-alone firewall

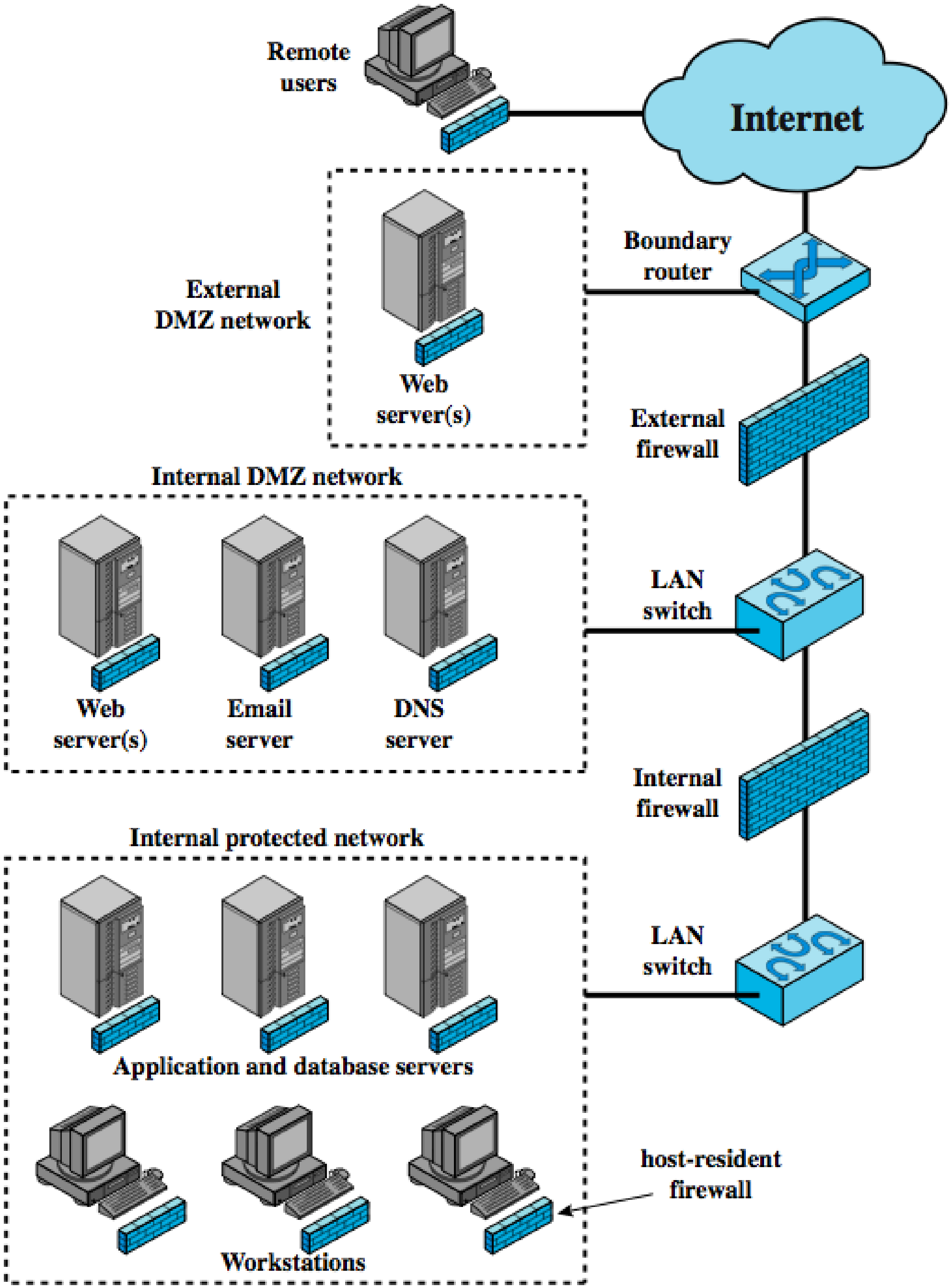
Firewalls, architectures:

Demilitarized Zone (DMZ)



- Web- and mail-servers etc are placed in DMZ
- Provides in-depth defence

Distributed Firewalls



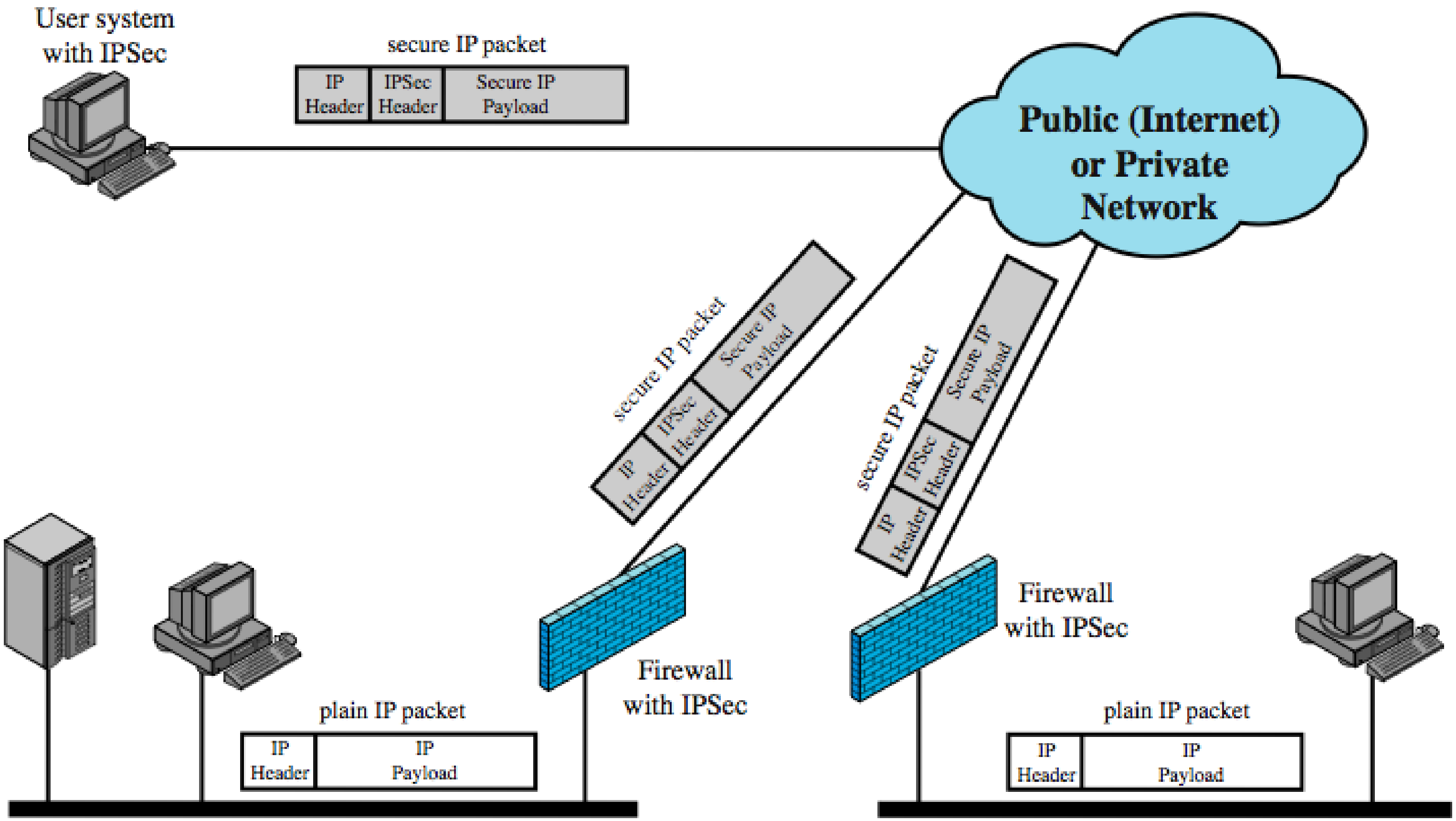
Firewalls – functional limitations

- Protects only those connections that passes the firewall - is the firewall really the *only* connection to Internet?
- Does not protect against insiders
- Does not protect againts viruses
- Does not protect against data-driven attacks
- Open for availability attacks
- Errors, weaknesses and deficient installations may impair functionality

Firewalls - problems

- Must be installed and adapted, which could be difficult
- Installation details may be important
- Must be maintained
- Difficult to test
- Affects the performance of the Internet connection?
- May be seen as a hindrance by the users

Virtual Private Networks



Kerberos

Kerberos Basics

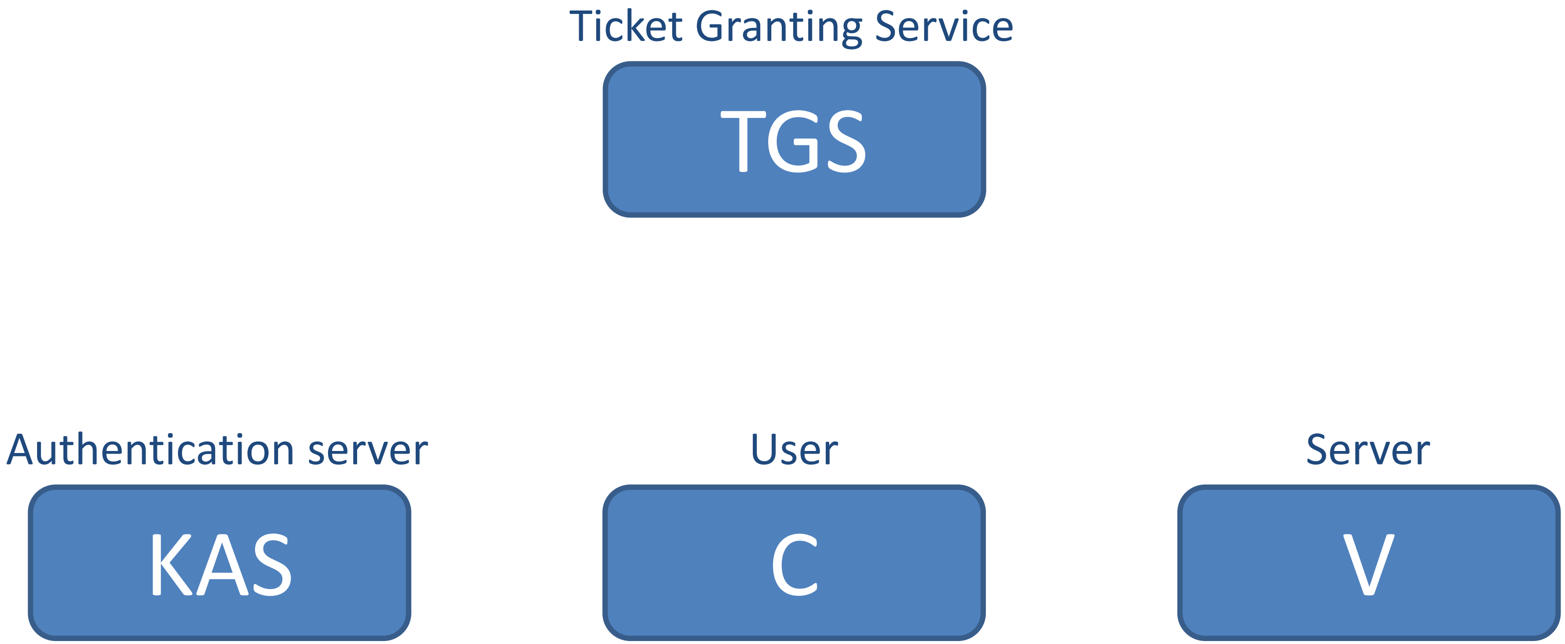
- Kerberos is an **authentication** system (client ←→ server)
- The original requirements were:
  - **Secure** (wrt eavesdropping – not the weakest link)
  - **Reliable** (service should be available when needed)
  - **Transparent** (to the user)
  - **Scalable**
- The system is based on a secure Kerberos installation, where the account name and password are stored.
- Other nodes in the network may be insecure
- Password stored in Kerberos (not locally)
- Passwords are never sent over the network
- The authentication gives a basis for **authorizations**

Authentication separated from authorizations

Kerberos Concepts

- **Ticket:** a token used by the user, so that his identity can be securely transferred to the server. It contains the necessary information needed for the user and server to be able to communicate (e.g. crypto keys). One ticket for each service is generated, often valid for hours.
- **Authenticator**: a one-time token showing that the user has the permission to use a service (one ticket per session, short lifetime ~5 min, to prove user's identity)
- **Session key**: a temporary key for the communication between the user and the service
- **Life time**: the lifetime of a ticket
- **Time stamp:** the time when the ticket was created
- **Nonce:** a random number, to prevent replay attacks

The Kerberos authentication protocol



Ticket Granting Service

TGS

Authentication server

KAS

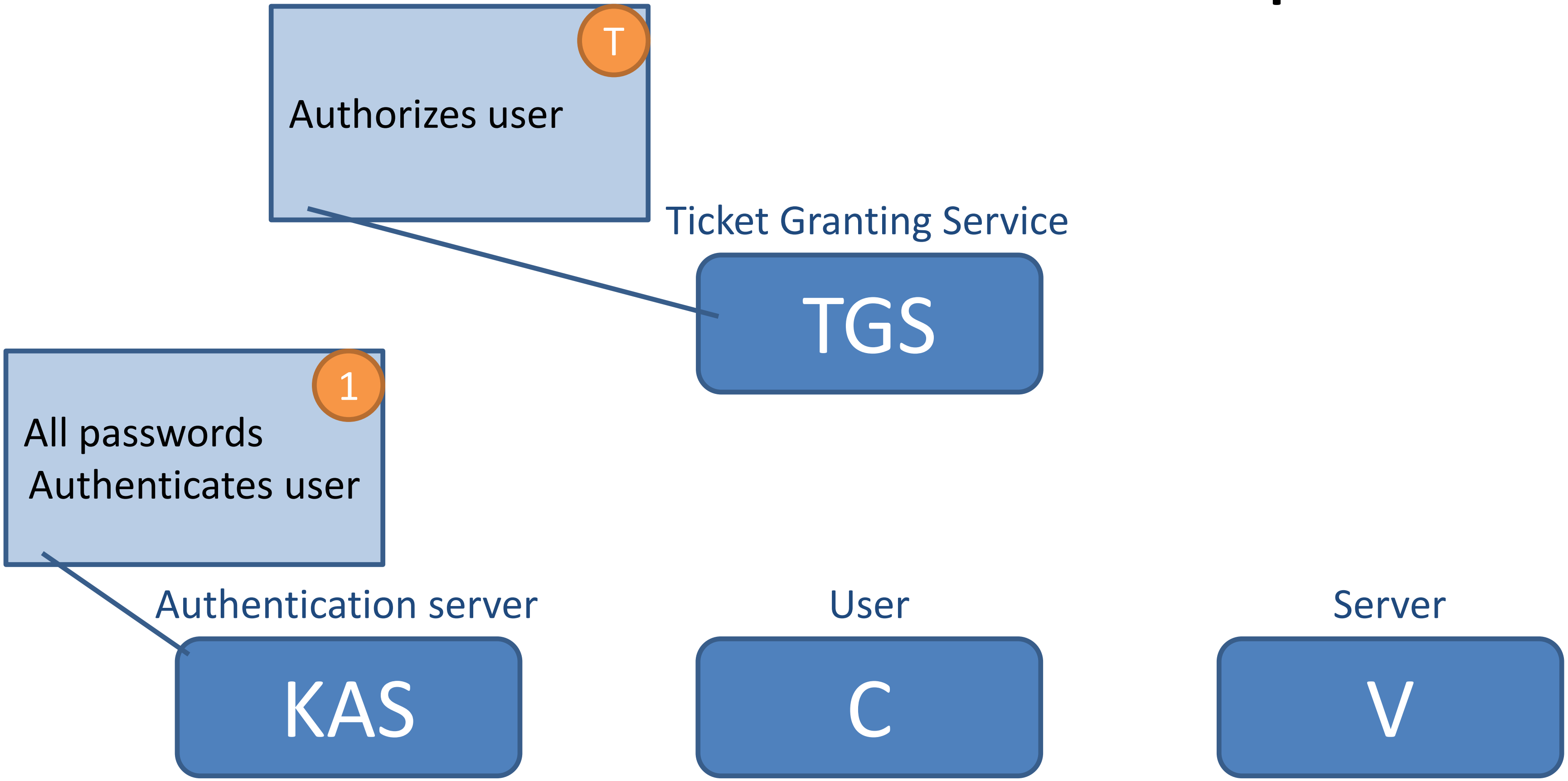
User

C

Server

V

The Kerberos authentication protocol



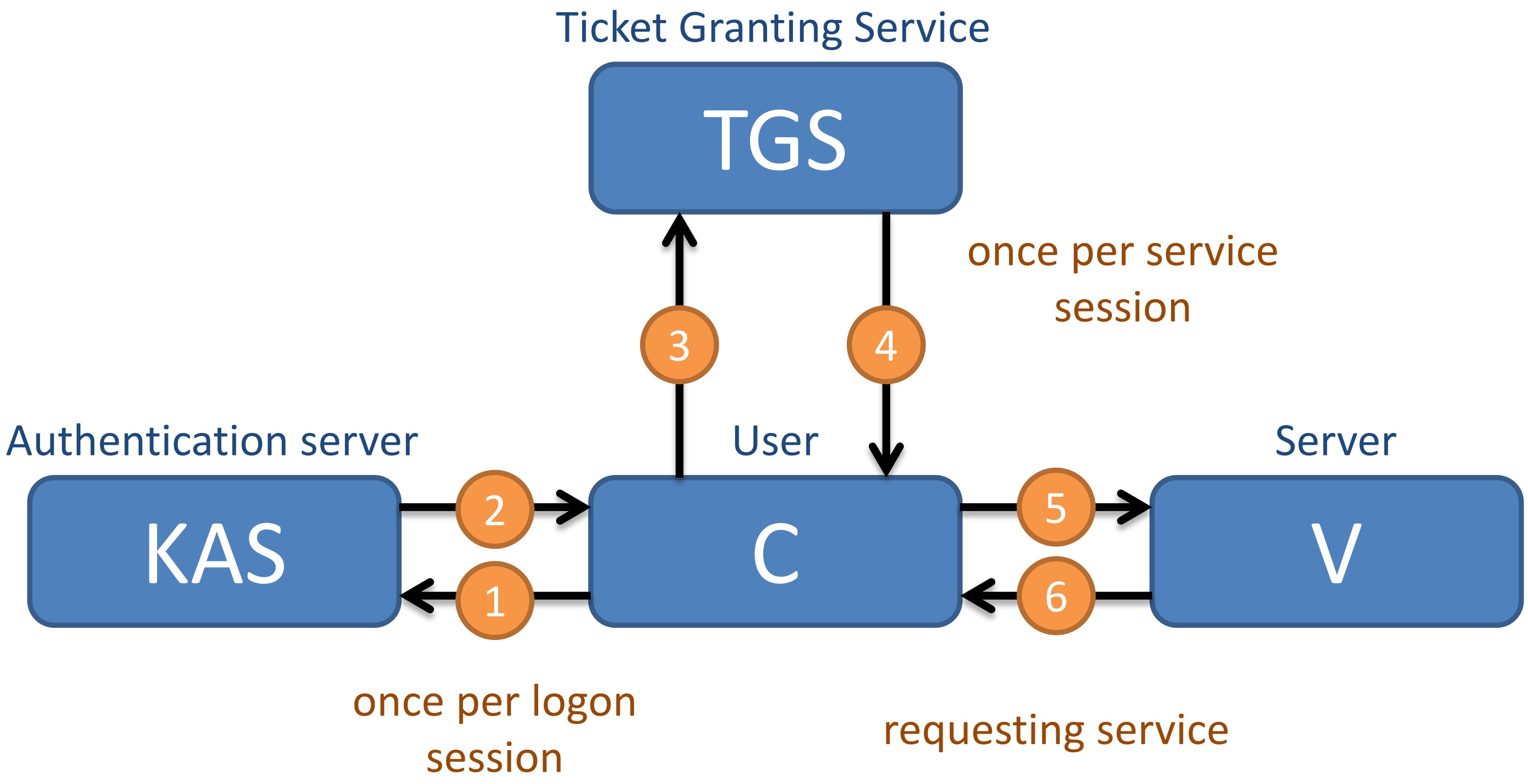
T

Authorizes user

1

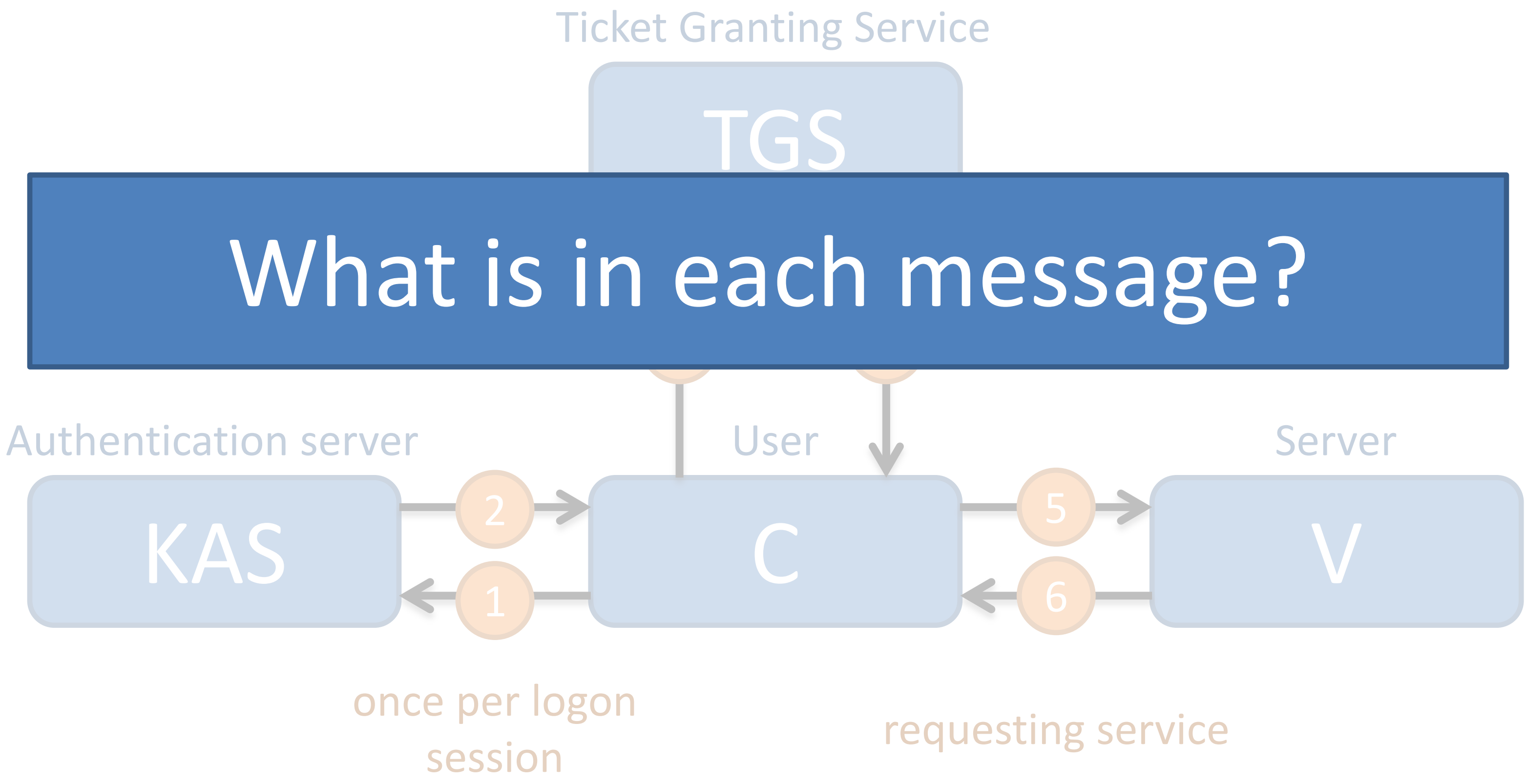
All passwords
Authenticates user

The Kerberos authentication protocol

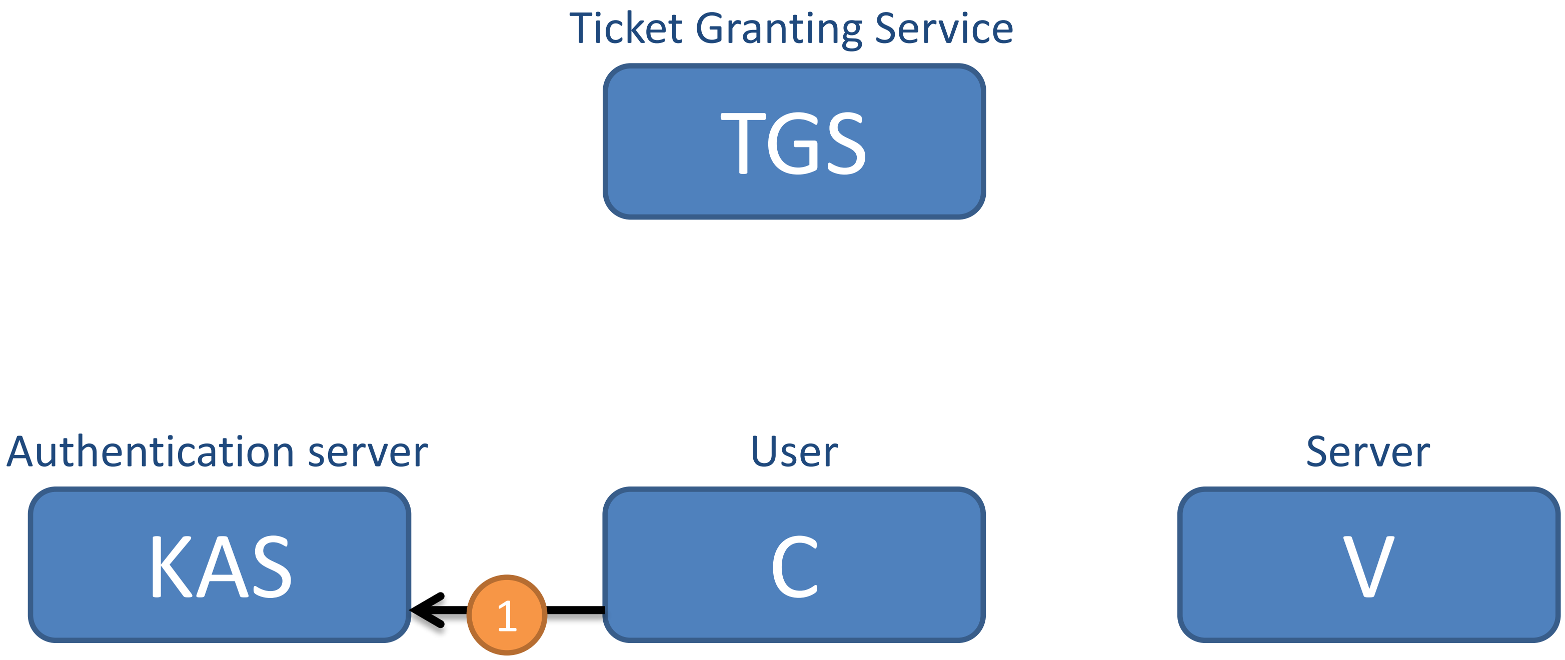


The Kerberos authentication protocol

What is in each message?



The Kerberos authentication protocol

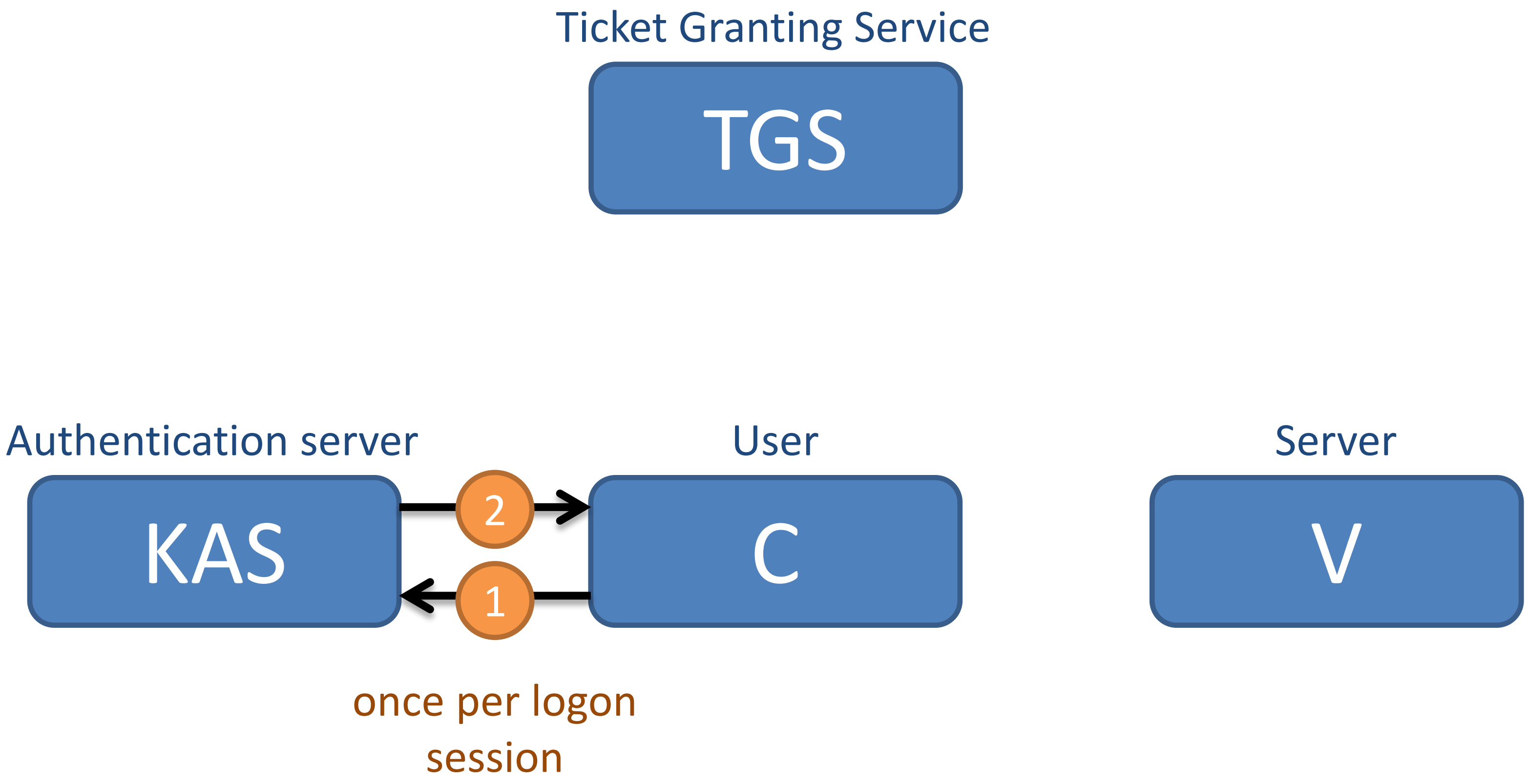


once per logon session

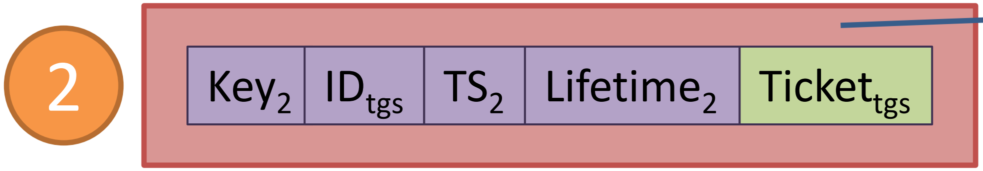
1 $ID_c \quad || \quad ID_{tgs} \quad || \quad TS_1$

NOT encrypted!

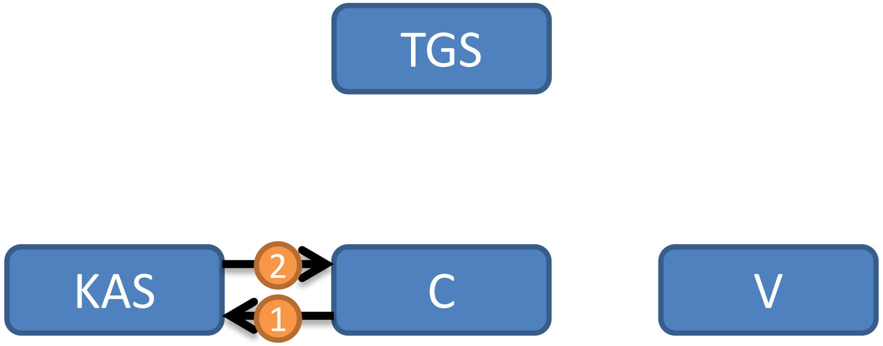
The Kerberos authentication protocol



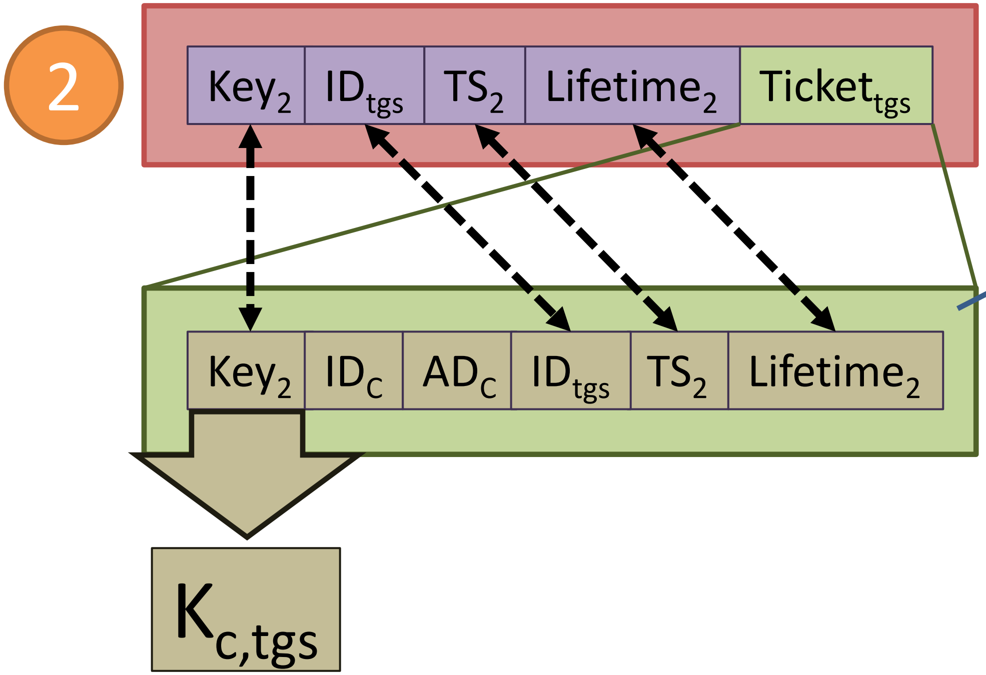
The Kerberos authentication protocol



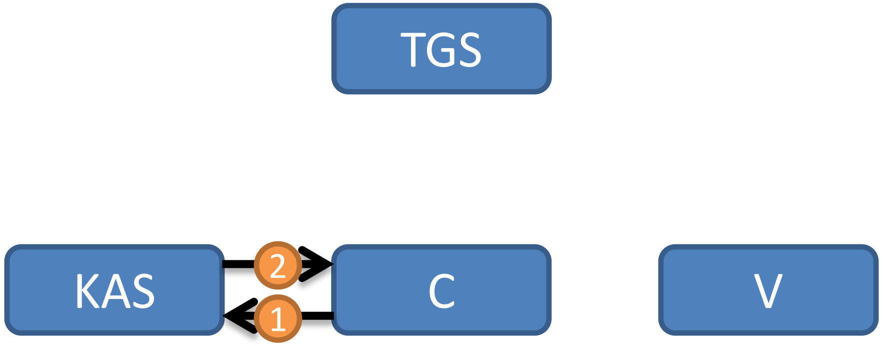
Encrypted with a key ***derived*** from the user's password. Only user with correct password can decrypt.



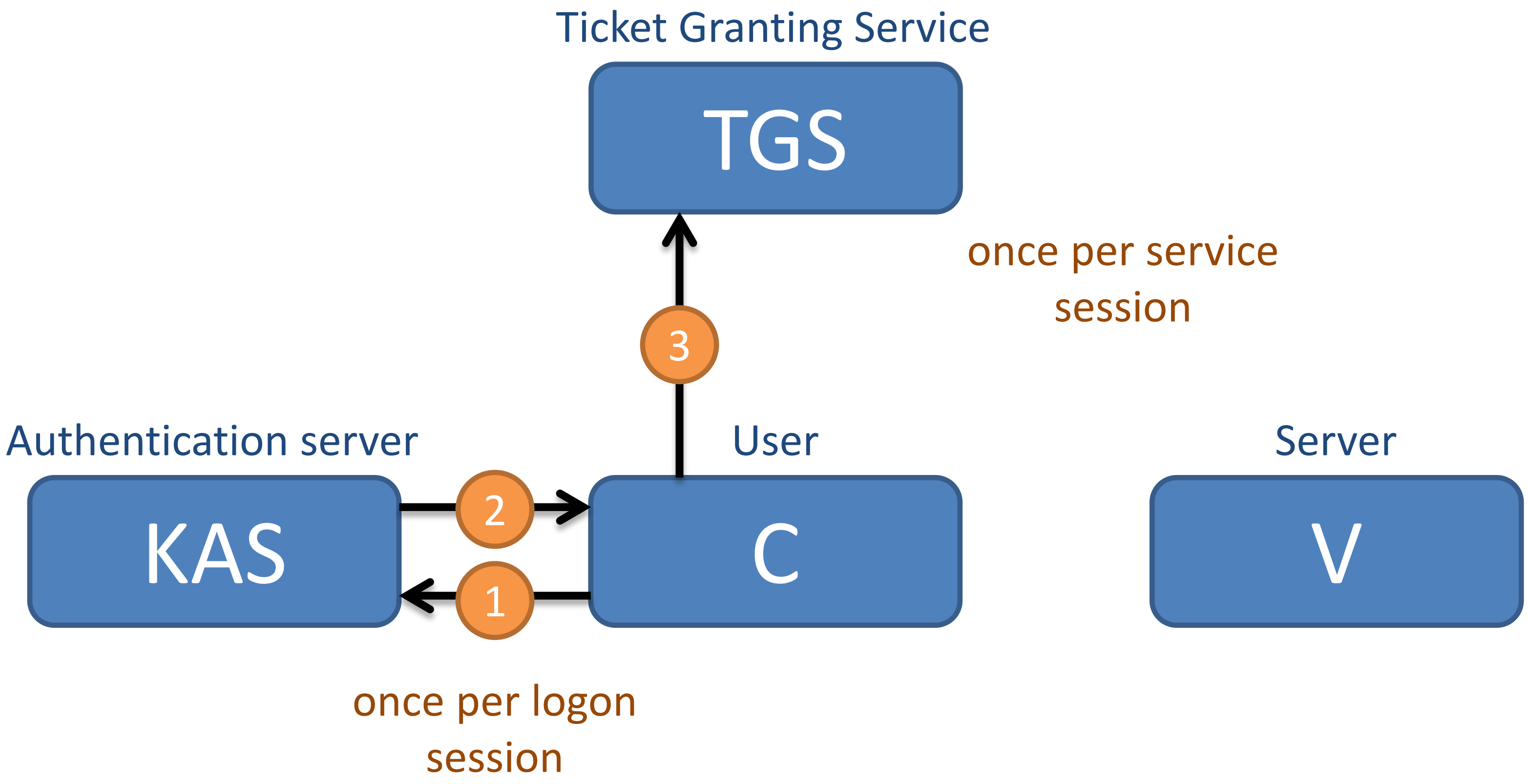
The Kerberos authentication protocol



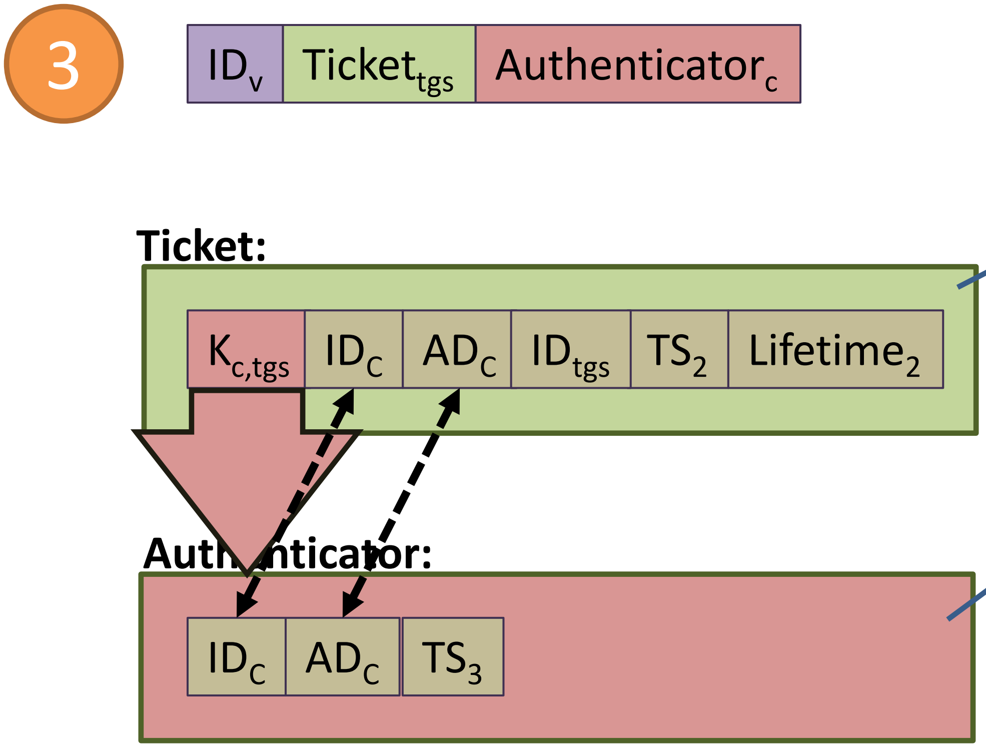
Encrypted with a key ***shared*** between KAS and TGS. User cannot change.



The Kerberos authentication protocol



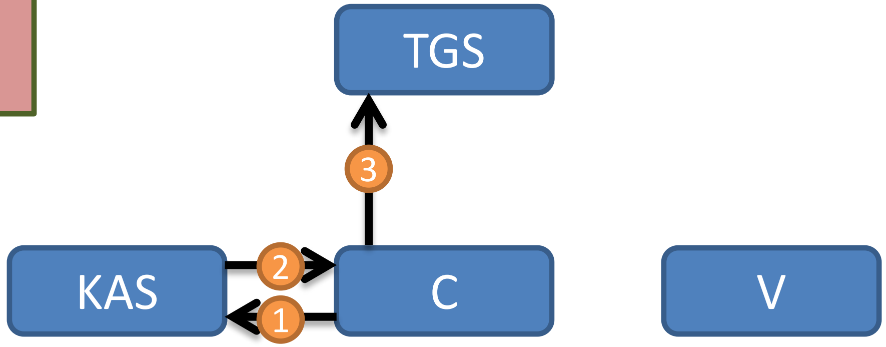
The Kerberos authentication protocol



Encrypted with a key ***shared*** between KAS and TGS. User cannot change.

Encrypted with session key ***shared*** between client and TGS – found in ticket.

Authenticator assures TGS that sender of ticket is indeed the tickets owner. Only the client can create the authenticator as it is encrypted with $K_{c,tgs}$.
Used only once and with short lifetime.


TGS
3
KAS
2
1
C
V