Security of Information System

Security in Networks and Distributed Systems

Nandika Kasun

Department of Communication and Media Technologies
University of Colombo School of Computing
University of Colombo
Sri Lanka

UCSC

kasun@cmb.ac.lk

Objectives:

Security in networks and distributed systems:

- Describe the authentication mechanisms and protocols in open network environment
- Design security polices and network protection systems to prevent unauthorized access in open network environment
- Identify the security requirement of the Internet
- Describe the existing security solutions and protocols
- Design new solutions to address the security problems in open network environment

UCSC
kasun@cmb.ac.lk

Security in Networks and Distributed Systems

5.1 Network Security

- Network Security Issues such as Impersonation, Message Confidentiality, Message Integrity, Code Integrity, Denial of Service
- IP Security (IPSec) protocol and Virtual Private Networks (VPN)
- Securing wireless (IEEE 802.11) networks
- PKI based Authentication and Kerberos Authentication
- Biometrics Authentication Mechanisms
- Access Control Mechanisms
- Firewalls

IP Security Overview

- Benefits of IPSec
  - Transparent to applications (below transport layer (TCP, UDP)
  - Provide security for individual users
- IPSec can assure that:
  - A router or neighbor advertisement comes from an authorized router
  - A redirect message comes from the router to which the initial packet was sent
  - A routing update is not forged

What can IPSEC do for us?

- **Authentication**
- **Integrity**
- **Access control**
- **Confidentiality**
- **Replay protection (Partial)**

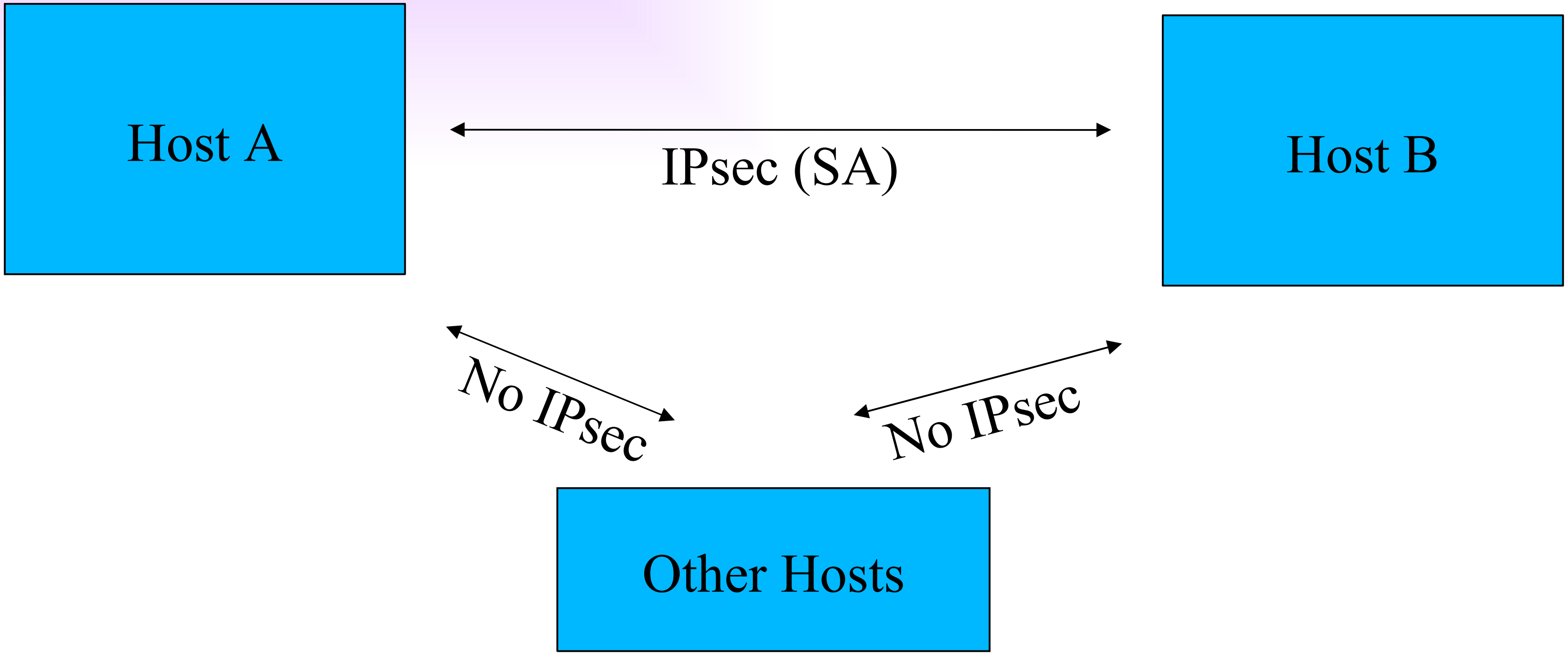
kasun@cmb.ac.lk

Types of communications

- Host To Host
- Host To Security Gateway
- Security Gateway To Security Gateway
  - Security Gateway = Firewall
  - Also refer to as Network (i.e. Network To Network)

How does IPSEC work?

- **Host To Host**



Host A

IPsec (SA)

Host B

No IPsec

No IPsec

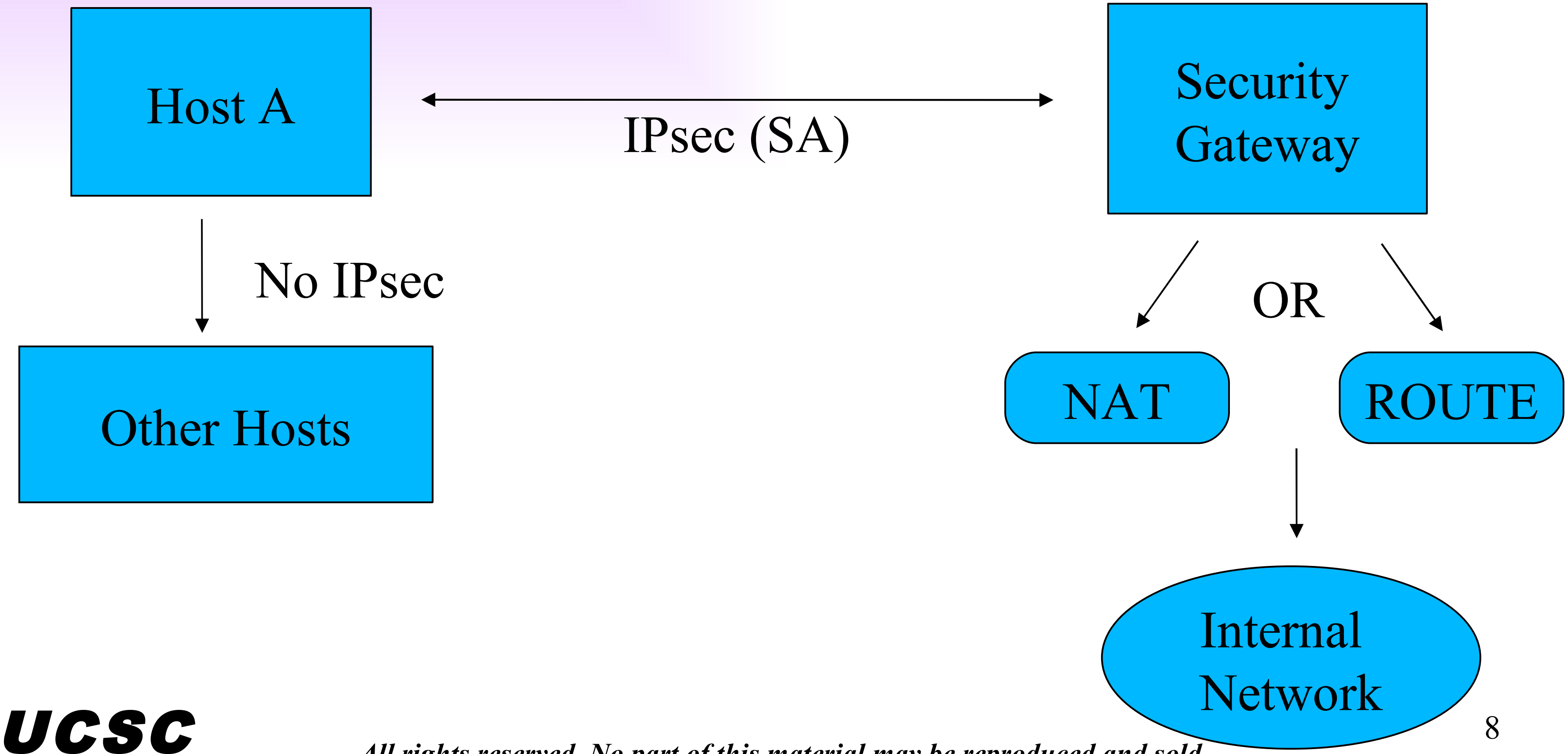
Other Hosts

UCSC

kasun@cmb.ac.lk

All rights reserved. No part of this material may be reproduced and sold.

Host To Security Gateway



Host A

IPsec (SA)

Security Gateway

No IPsec

Other Hosts

OR

NAT

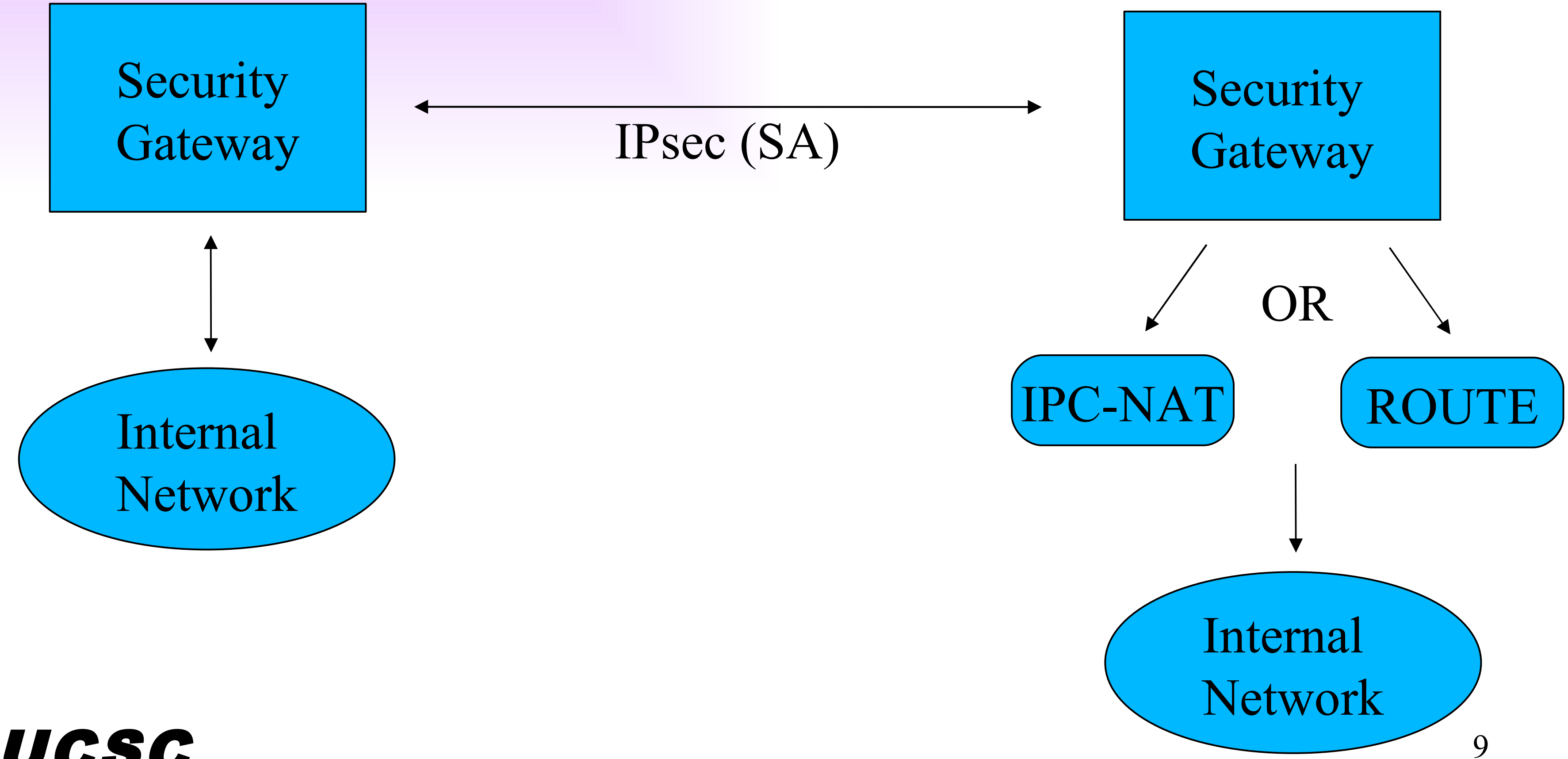
ROUTE

Internal Network

UCSC

kasun@cmb.ac.lk

Security Gateway to Security Gateway



Security Gateway

IPsec (SA)

Security Gateway

Internal Network

OR

IPC-NAT

ROUTE

Internal Network

Security Associations (SA)

- A one way relationsship between a sender and a receiver.
- Identified by three parameters:
  - Security Parameter Index (SPI)
  - IP Destination address
  - Security Protocol Identifier

- **Stored in the SPD (Security Policy Database)**

UCSC

kasun@cmb.ac.lk

Security Policy Database (SPD)

Each entry defines a subset of IP traffic and points to an SA for that traffic: defined using IP and upper layer protocol field values called *selectors*.

Outbound traffic processing includes:

- Compare the values of the selector fields against SPD to find an SPD entry
- Determine the SA for this packet and associated SPI
- Do the required IPSec processing (AH or ESP)

kasun@cmb.ac.lk

Types of IPSEC Connections

- **Transport Mode**
  - Does not encrypt the entire packet
  - Uses original IP Header
  - Faster
- **Tunnel Mode**
  - Encrypts entire packet including IP Header (ESP)
  - Creates a new IP header
  - Slower

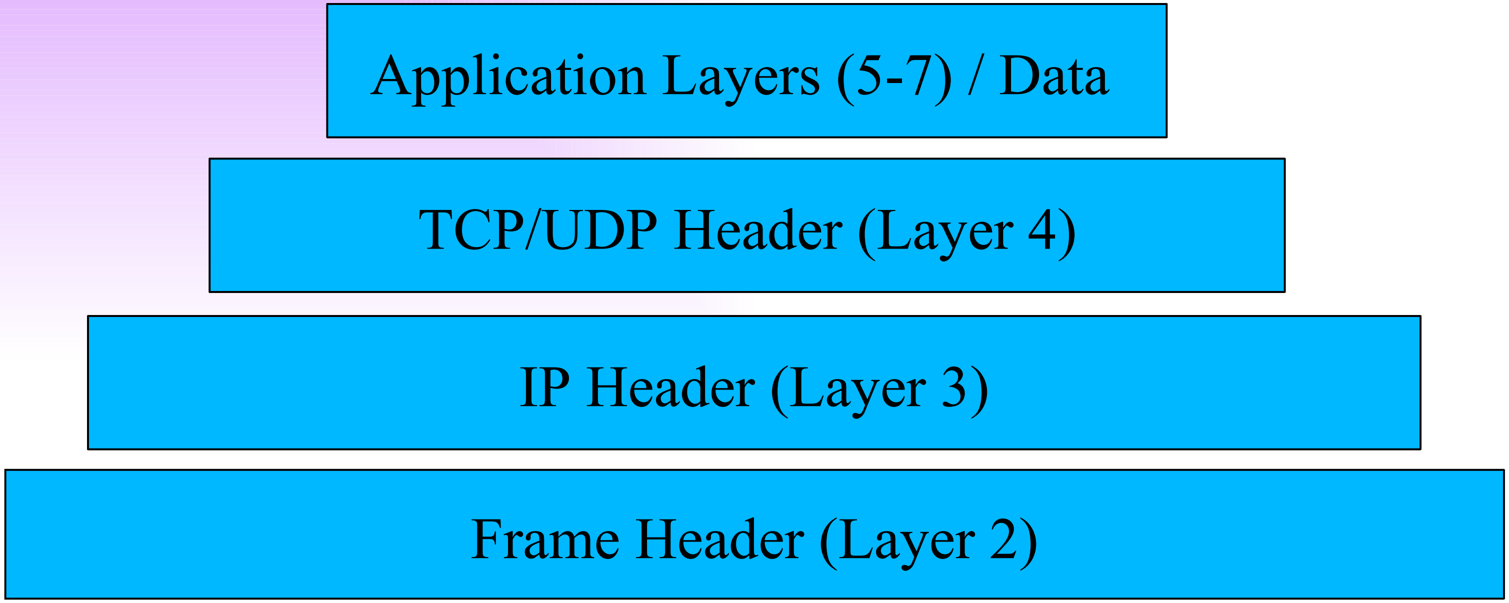
kasun@cmb.ac.lk

Security Associations (SA)

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers	Authenticates entire inner IP packet plus selected portions of outer IP header
ESP	Encrypts IP payload and any IPv6 extension header	Encrypts inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extension header. Authenticates IP payload but no IP header	Encrypts inner IP packet. Authenticates inner IP packet.

kasun@cmb.ac.lk

Normal TCP/IP Packet

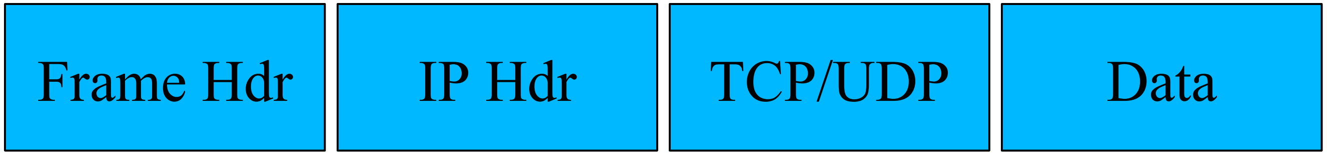

Application Layers (5-7) / Data

TCP/UDP Header (Layer 4)

IP Header (Layer 3)

Frame Header (Layer 2)

OR


Frame Hdr

IP Hdr

TCP/UDP

Data

kasun@cmb.ac.lk

AH (Authentication Header)

- **IP Protocol 51**
- **Provides authentication of packets**
- **Does not encrypt the payload**

Transport Mode

IP Hdr	AH	TCP/UDP	Data

Tunnel Mode

New IP Hdr	AH	Org. IP Hdr	TCP/UDP	Data

kasun@cmb.ac.lk

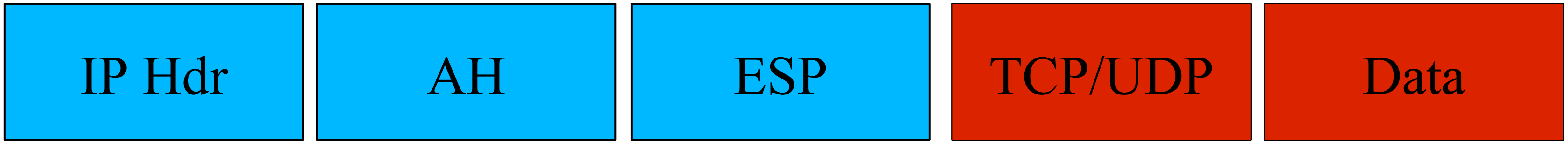
Transport vs Tunnel Mode ESP

- Transport mode is used to encrypt & optionally authenticate IP data
- data protected but header left in clear
- can do traffic analysis but is efficient
- good for ESP host to host traffic
- Tunnel mode encrypts entire IP packet
- add new header for next hop
- good for VPNs, gateway to gateway security

ESP (Encapsulating Security Payload)

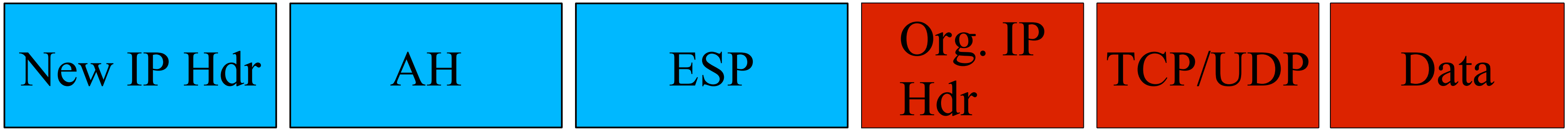
- **IP Protocol 50**
- **Encrypts the Payload**
- **Provides Encryption and Authentication**

Transport Mode



IP Hdr | AH | ESP | TCP/UDP | Data

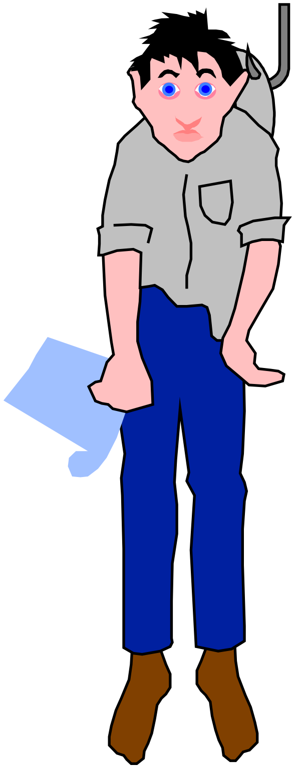
Tunnel Mode



New IP Hdr | AH | ESP | Org. IP Hdr | TCP/UDP | Data

IPSec Pitfalls

- Too complicated, many different ways to configure
- Can be configured insecurely
- Client security is an issue

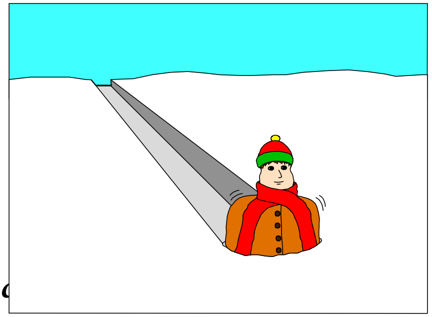


kasun@cmb.ac.lk

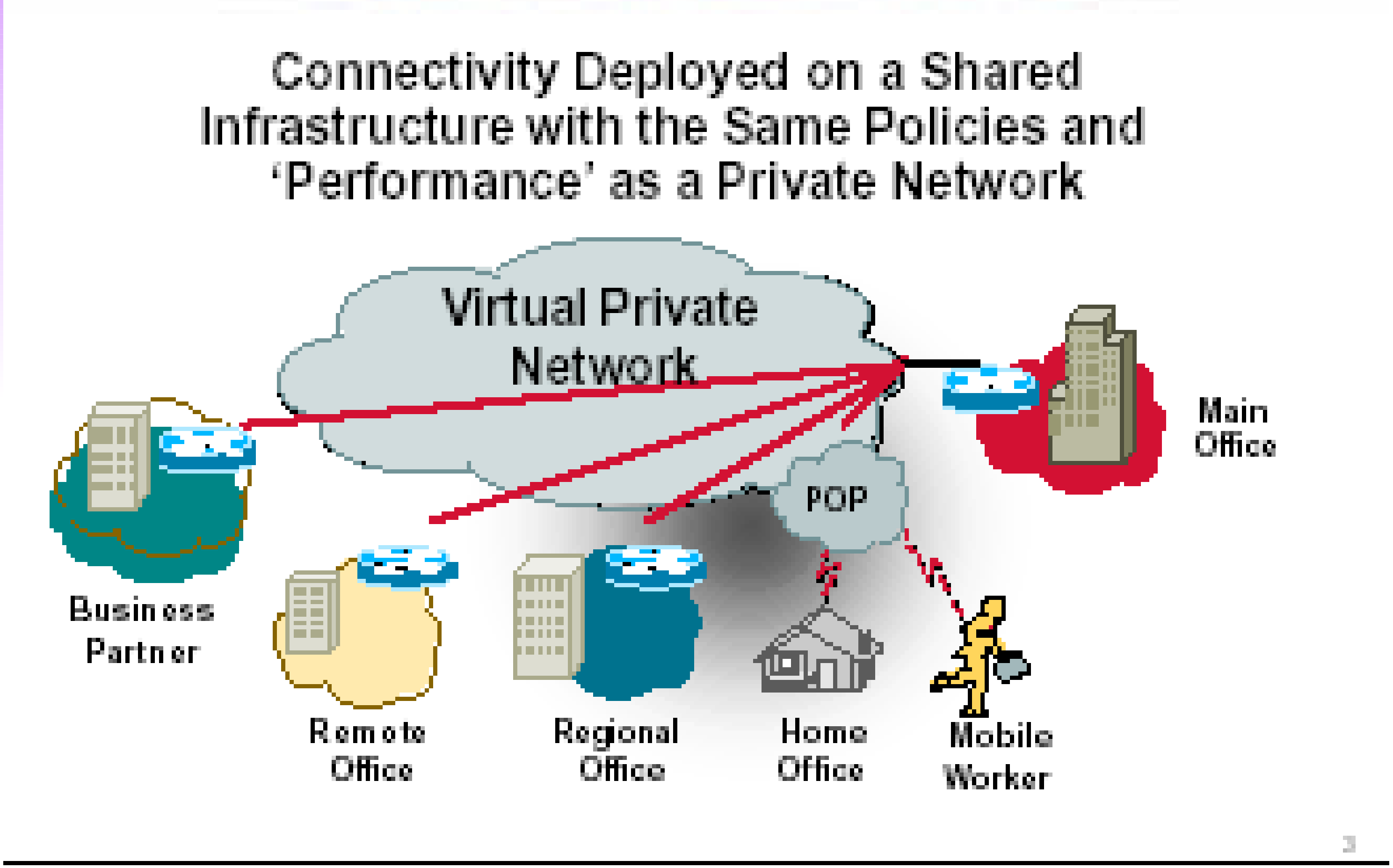
VPN (Virtual Private Network)

A Virtual Private Network Carries Private Traffic Over a Public Network

- Secure communications between two hosts or networks
- IPsec is one of the more popular VPN technology's



What is VPN ?

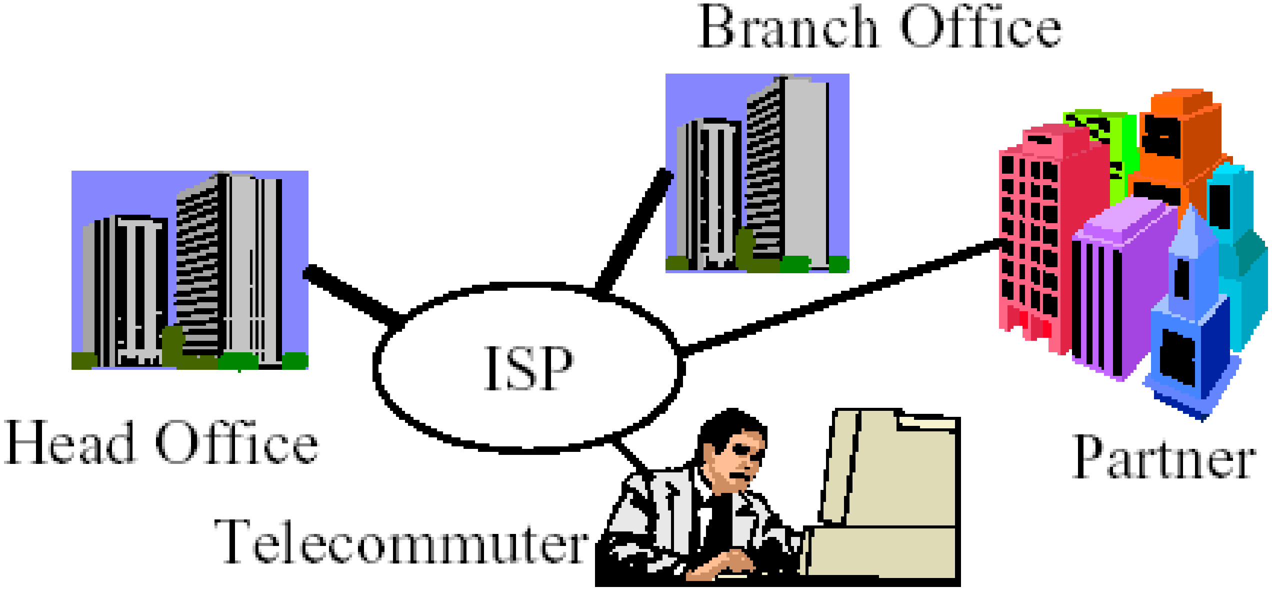


Connectivity Deployed on a Shared Infrastructure with the Same Policies and ‘Performance’ as a Private Network

kasun@cmb.ac.lk

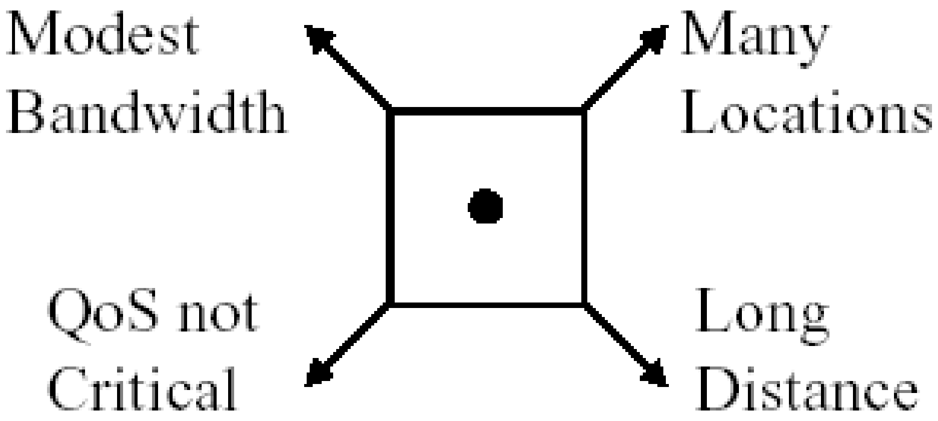
Types of VPN

- WAN VPN: Branch offices
- Access VPN: Roaming Users
- Extranet VPNs: Suppliers and Customers



kasun@cmb.ac.lk

When to VPN ?



Modest Bandwidth

Many Locations

QoS not Critical

Long Distance

- More Locations, Longer Distances, Less Bandwidth/site, QoS less critical
  ⇒ VPN more justifiable
- Fewer Locations, Shorter Distances, More Bandwidth/site, QoS more critical
  ⇒ VPN less justifiable

kasun@cmb.ac.lk

VPN Security Issues

- Authentication methods supported
- Encryption methods supported
- Key Management
- Data stream filtering for viruses, JAVA, active X
- Supported certificate authorities
- Encryption Layer: Datalink, network, session, application. Higher Layer . More granular
- Granularity of Security: Departmental level, Application level, Role-based

Security Risk of Wireless

- **Bypassing the firewalls**
- **Short message service spamming**
- **Malicious downloadable code or content**
- **Weak Encryption key or non-existent**
- **Turning on wireless encryption does not mean data is protected end-to-end**
- **Wired portion of the traffic may travel in the clear**

kasun@cmb.ac.lk

Security Problems

- Unauthorized or “rogue” access points on trusted networks
- Access to network by unauthorized clients (theft of service, "war driving")
- Interception and monitoring of wireless traffic
  - range can be hundreds of feet
  - packet analyser software freely available
- Jamming is easy, unlicensed frequency

Security Problems (cont'd)

- Client-to-client attacks (in ad hoc mode)
- Denial or degradation of service
  - flood with bogus packets, association/authentication requests, …
- Misconfiguration possibilities
  - no encryption used
  - weak (guessable) password used to generate key
  - weak protection of encryption key on client machine
  - weak protection of management interface for access point

(In)Security in 802.11b

- Authentication is the process of proving identity
  - open: just supply correct SSID
  - shared key: relies on WEP
- **WEP**: Wired Equivalent Privacy

WEP

- Without WEP, no confidentiality, integrity, or authentication of user data
- The cipher used in WEP is RC4, keylength from 40 up to 128 bits
- Key is shared by all clients and the base station
  - compromising one node compromises network
- Manual key distribution among clients makes changing the key difficult

WEP Encryption Weakness

- Initialization Vector (IV) used during encryption is only 24 bits long
- Key to cracking: find packets with duplicate public IVs
  - repetition of IV guaranteed on busy networks due to small IV space
- Tools: WEPCrack, AirSnort
  - 15 minutes to 24 hours to collect enough packets

UCSC

kasun@cmb.ac.lk

Recommendations: General

- Get informed about risks!
- Regular security audits and penetration assessments
- Require "strong" passwords, limit number of login attempts
- Disable ad hoc mode

  invites access by unauthorized nodes to your computer

UCSC

kasun@cmb.ac.lk

Recommendations:WLAN Security

- WEP (fair)
  - enable wireless frame encryption
  - use longest key
  - change the WEP key regularly (manually)
- 802.1X and WPA (user authentication + dynamic keys) (better)
  - use as soon as practical and stable
  - set rekeying to occur every few hours
- 802.11i (best)
  - upgrade / use when available and supported

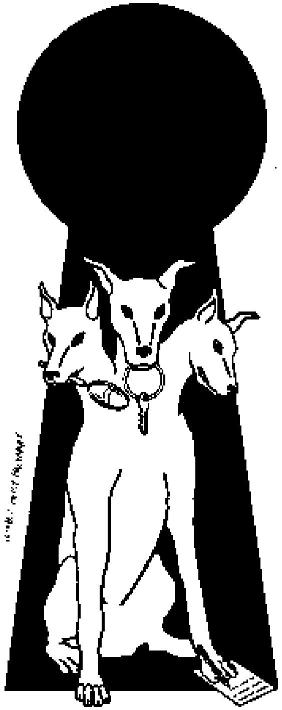
kasun@cmb.ac.lk

What is Kerberos?

- **The 3-headed dog who guards the entrance to Hades**
- **Network Authentication Protocol**

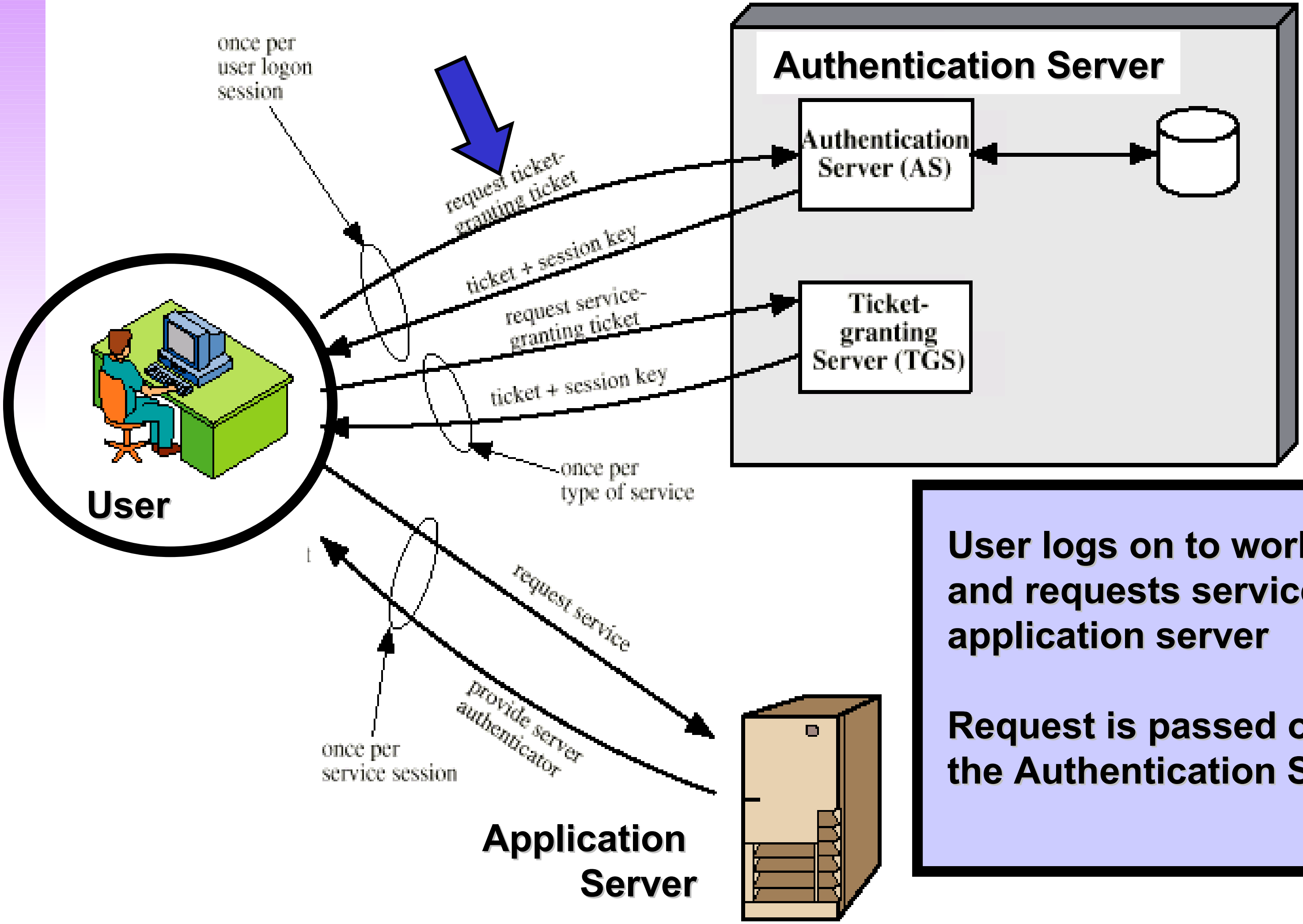
- **Used in:**
  - **Client/Server**
  - **Peer-to-Peer**

- Developed by the Massachusetts Institute of Technology (MIT) ‘s Project Athena
- Current Release – Version 5
- Adoption by Microsoft Windows 2000



kasun@cmb.ac.lk

Kerberos – Message 1

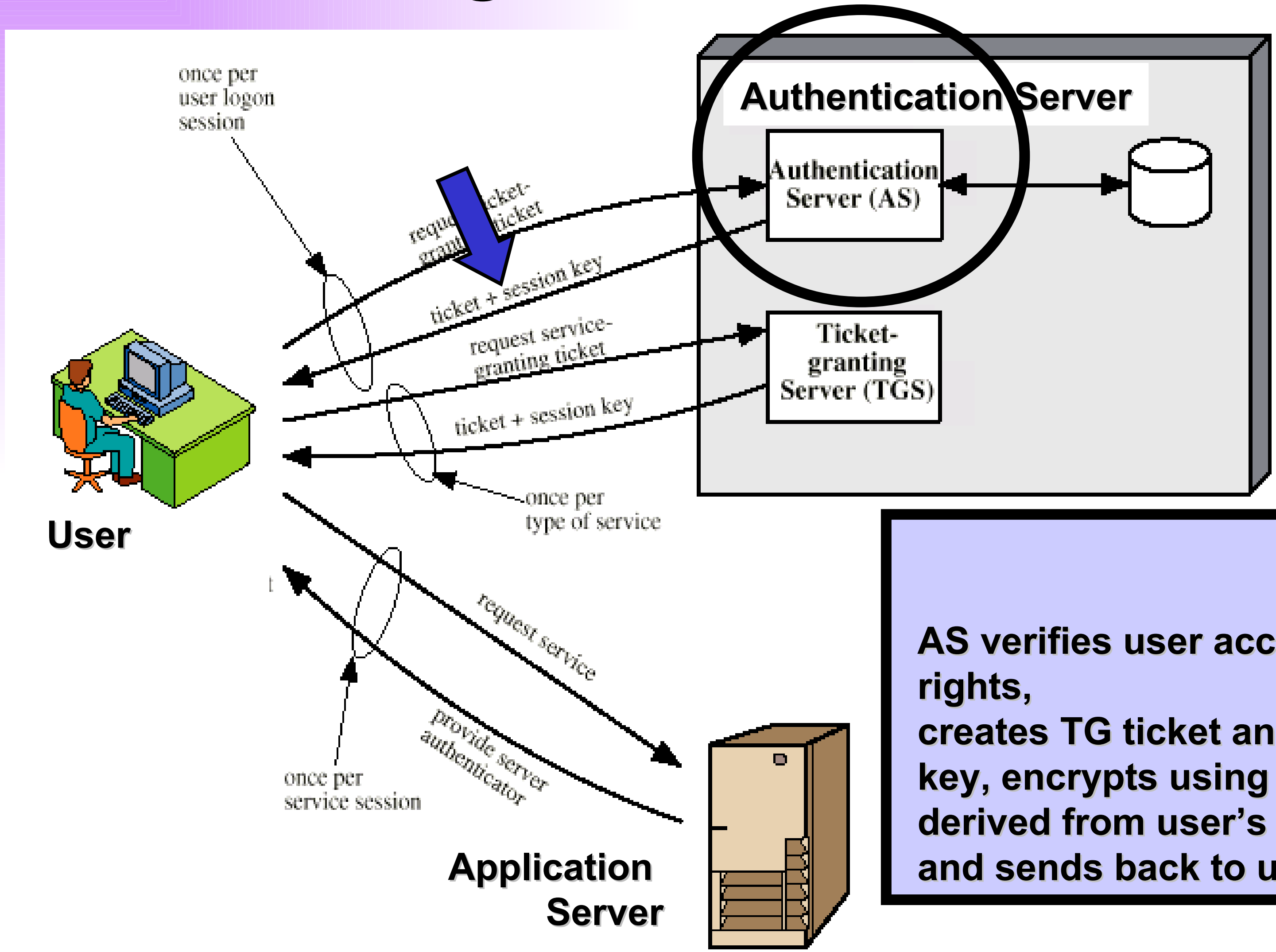


User logs on to workstation and requests service on application server

Request is passed over to the Authentication Server

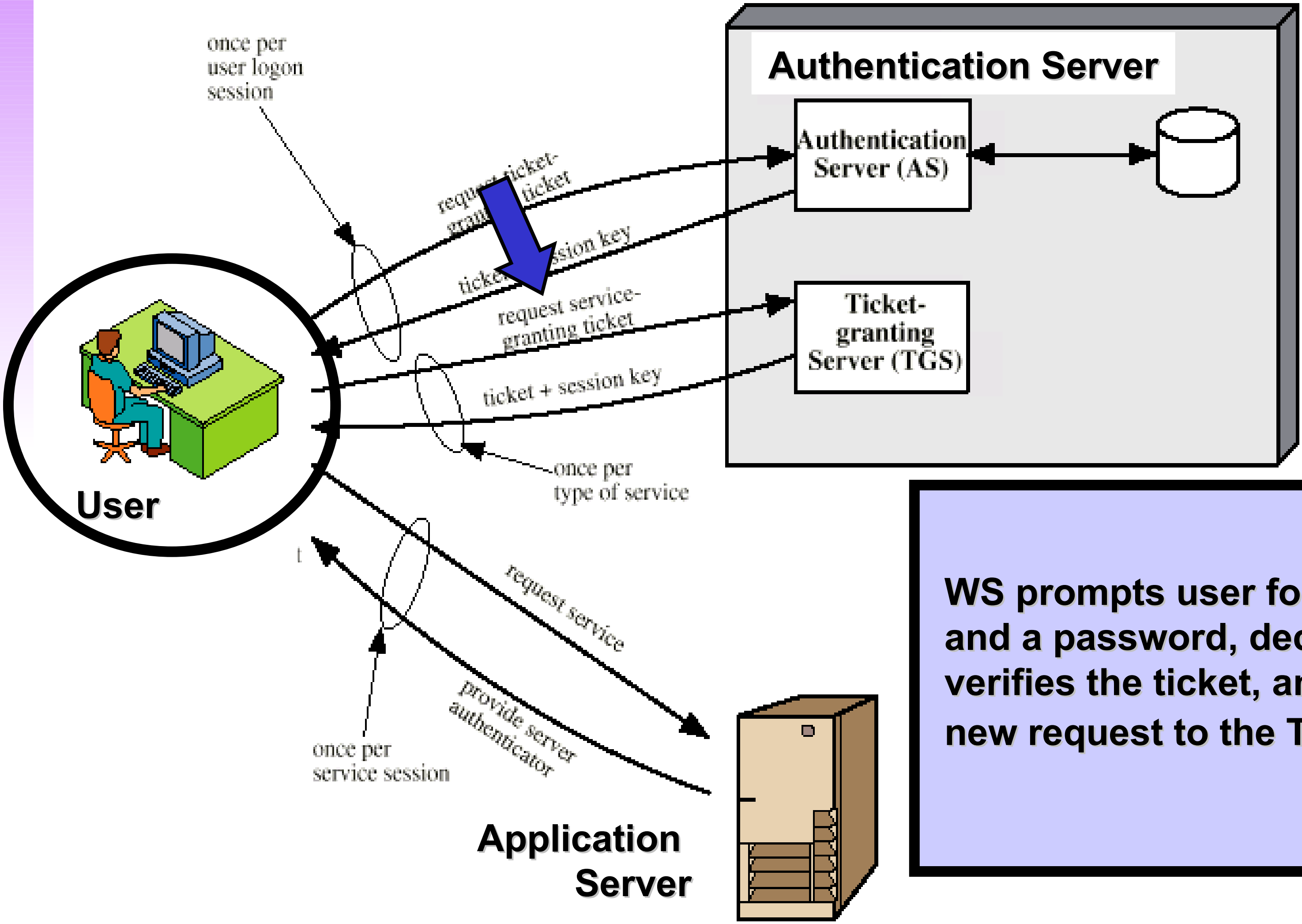
UCSC
kasun@cmb.ac.lk

Kerberos – Message 2



**AS verifies user access rights,
creates TG ticket and session key, encrypts using key derived from user's password and sends back to user**

Kerberos – Message 3

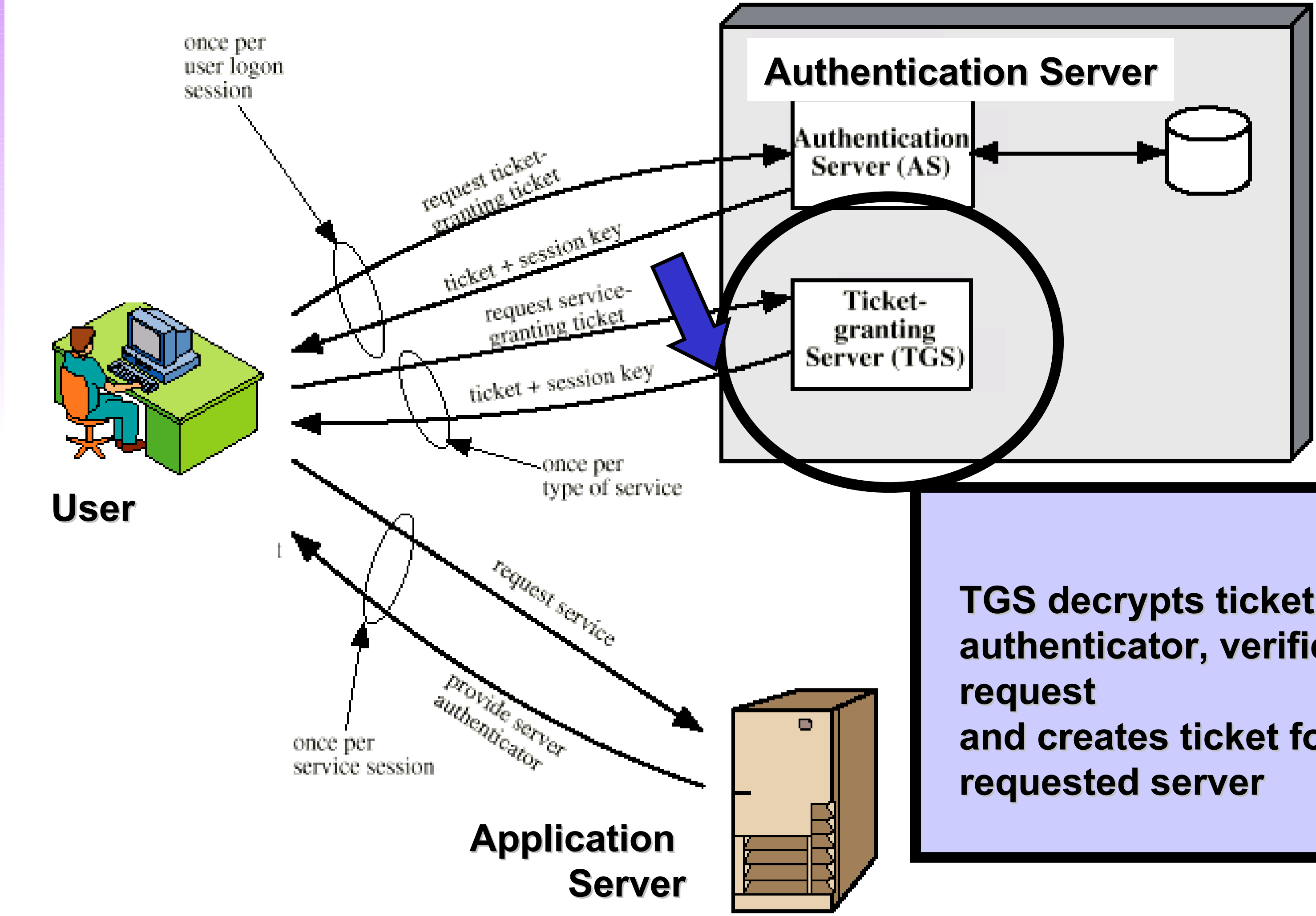

once per user logon session
Authentication Server
Authentication Server (AS)
request ticket-granting ticket
ticket + session key
request service-granting ticket
Ticket-granting Server (TGS)
ticket + session key
once per type of service
User
request service
provide server authenticator
once per service session
Application Server

WS prompts user for userID and a password, decrypts and verifies the ticket, and sends new request to the TGS

UCSC

kasun@cmb.ac.lk

Kerberos – Message 4

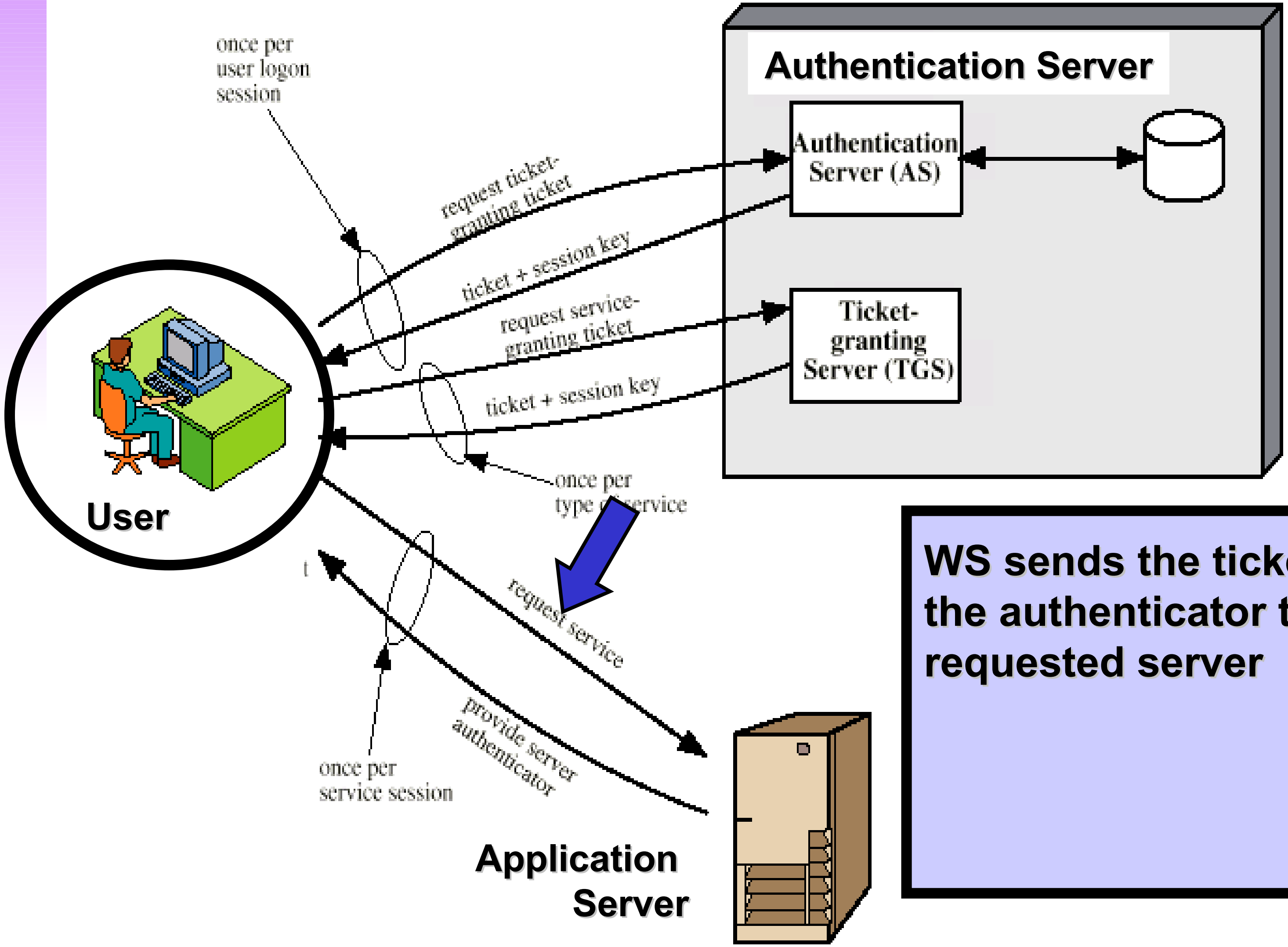


TGS decrypts ticket and authenticator, verifies request
and creates ticket for the requested server

UCSC

kasun@cmb.ac.lk

Kerberos – Message 5

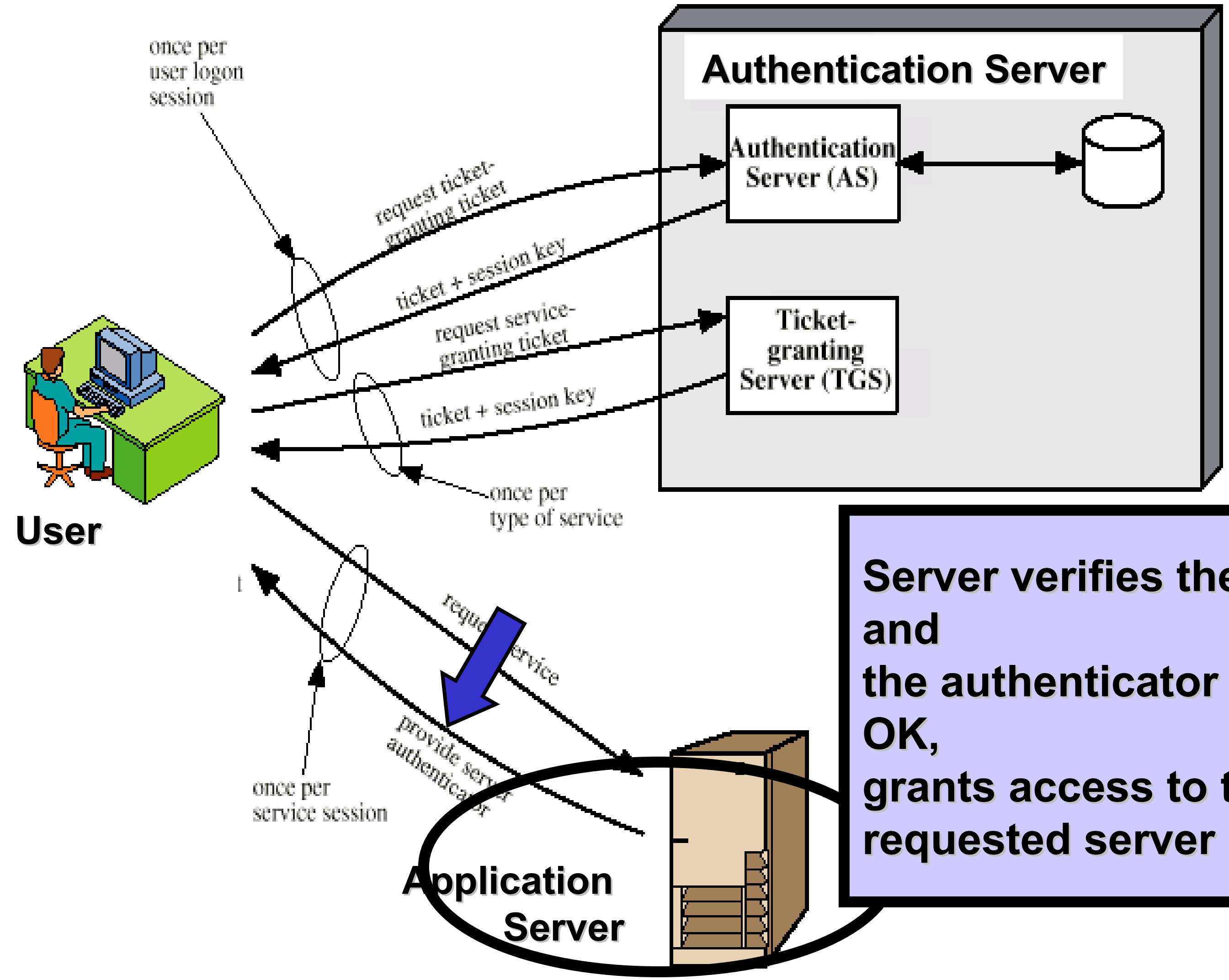


WS sends the ticket and the authenticator to the requested server

UCSC

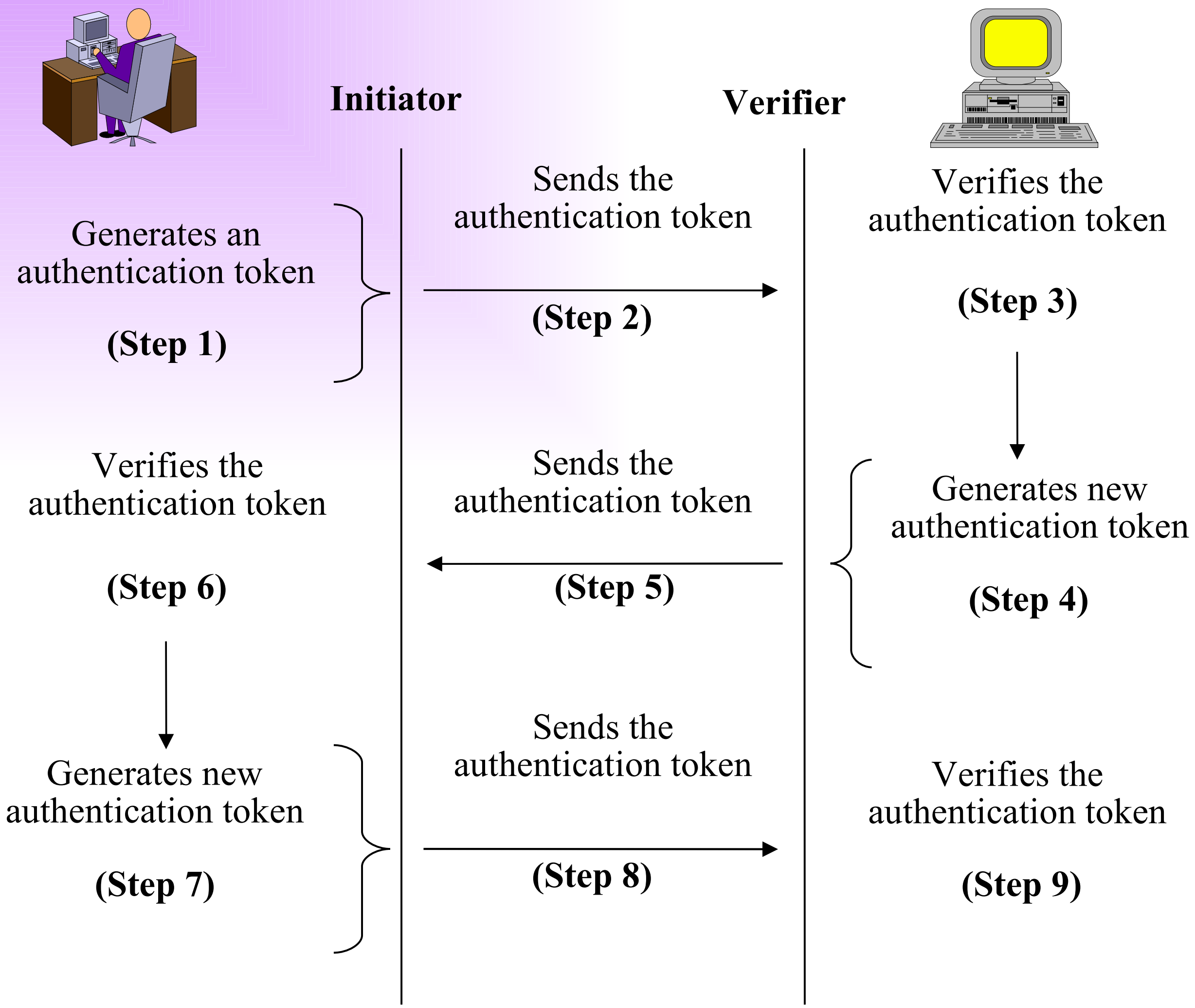
kasun@cmb.ac.lk

Kerberos – Message 6


once per user logon session
request ticket-granting ticket
ticket + session key
request service-granting ticket
ticket + session key
once per type of service
Authentication Server
Authentication Server (AS)
Ticket-granting Server (TGS)
User
once per service session
Application Server

Server verifies the ticket and
the authenticator and if OK,
grants access to the requested server

Strong Authentication Protocol



Initiator

Verifier

Generates an authentication token

(Step 1)

Sends the authentication token

(Step 2)

Verifies the authentication token

(Step 3)

Generates new authentication token

(Step 4)

Sends the authentication token

(Step 5)

Verifies the authentication token

(Step 6)

Generates new authentication token

(Step 7)

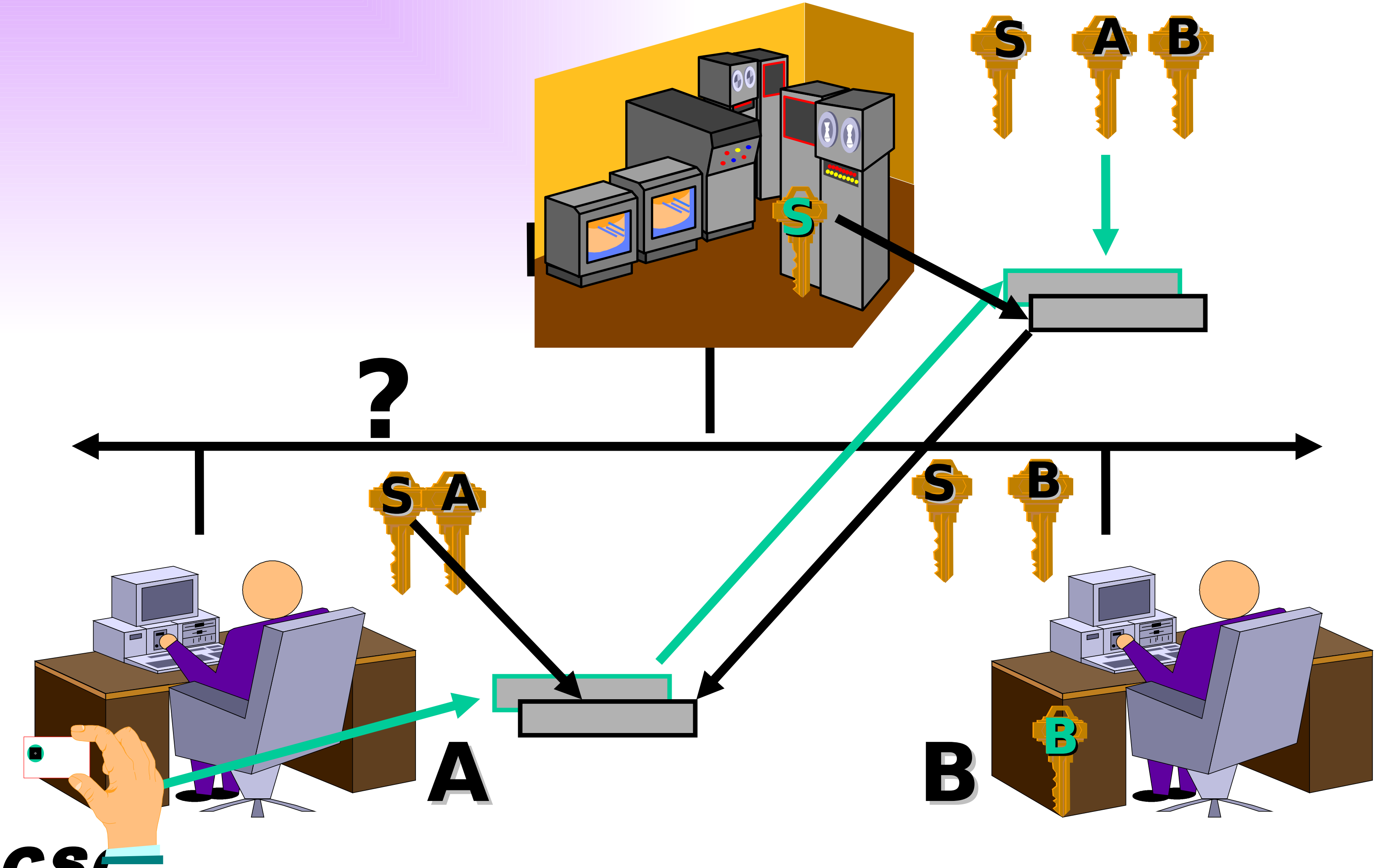
Sends the authentication token

(Step 8)

Verifies the authentication token

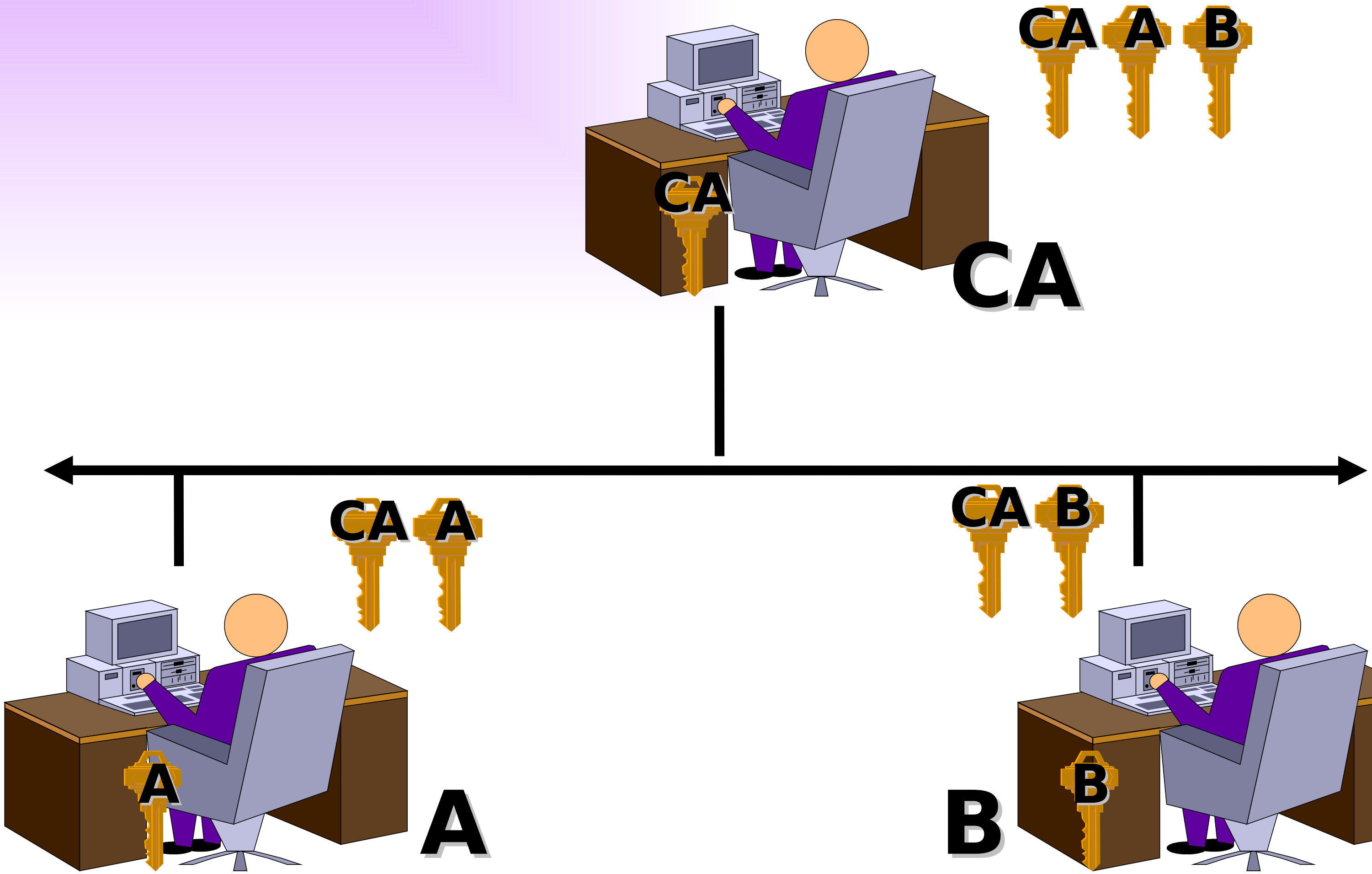
(Step 9)

Authenticity of Public Keys



kasun@cmb.ac.lk

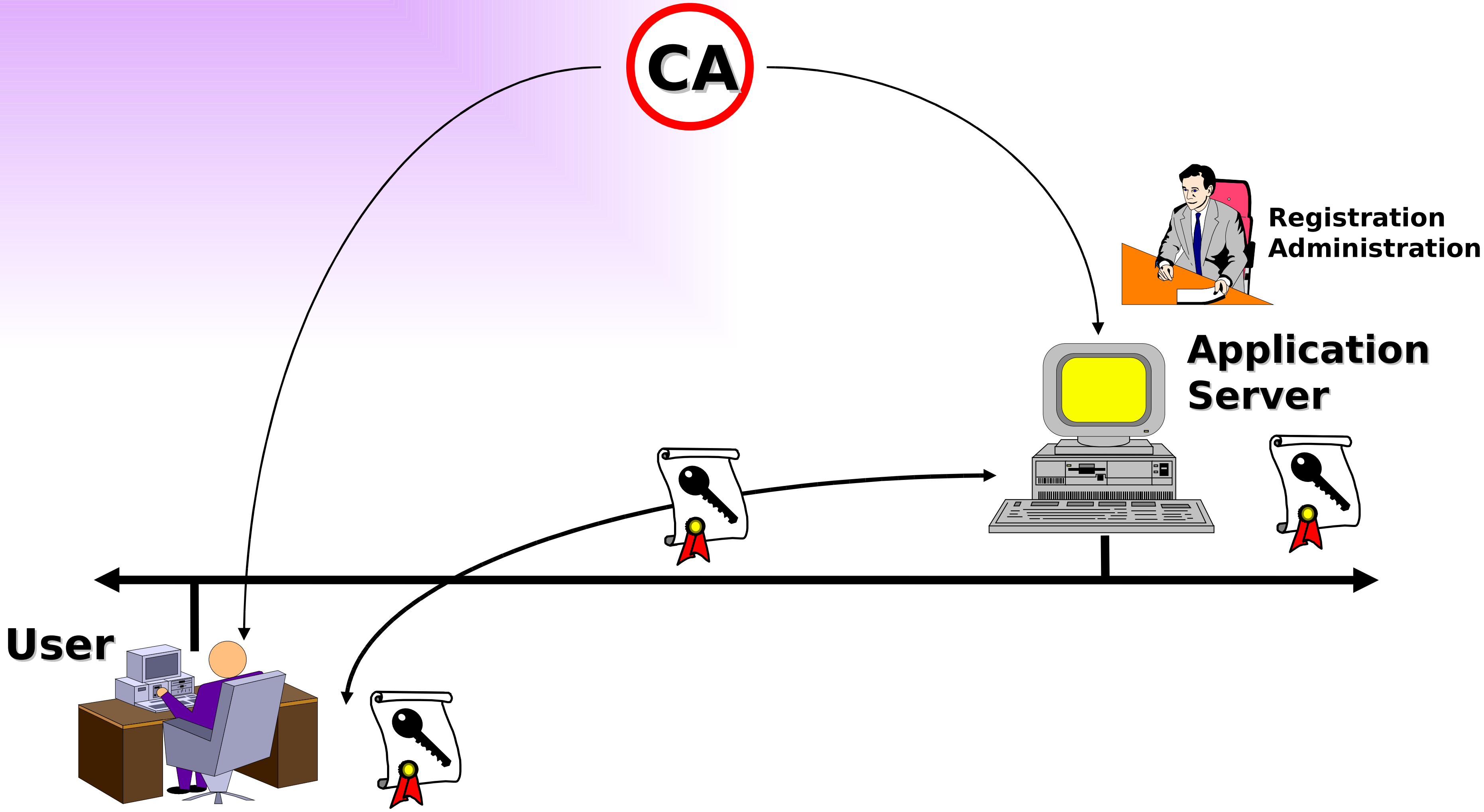
Authentication in Open Networks – Certificates



UCSC

kasun@cmb.ac.lk

Remote Authentication



UCSC

kasun@cmb.ac.lk

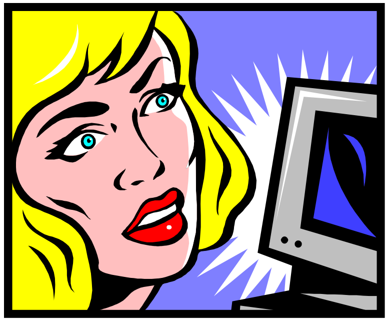
All rights reserved. No part of this material may be reproduced and sold.

Authentication with Biometrics

- Automated methods of identity verification or identification based on the principle of measurable physiological or behavioral characteristics.

  Example: Fingerprint, an iris pattern, a voice sample.

- Biometric characteristics should be unique and not plicable or transferable.



What is a Firewall?

- A choke point of control and monitoring
- interconnects networks with differing trust
- imposes restrictions on network services
- only authorized traffic is allowed
- auditing and controlling access
- can implement alarms for abnormal behavior
- is (supposedly) itself immune to penetration
- provides perimeter defense

kasun@cmb.ac.lk

Purpose of a Firewall

Basically, a firewall does three things to protect the network:

- **It blocks incoming data that might contain a hacker attack.**
- **Hide internal addresses from Internet hackers. This is called NAT.**
- **It screens outgoing traffic to limit Internet use and/or access to remote sites.**

Limitation of a Firewall

- Cannot protect from attacks bypassing it

- Cannot protect against internal threats
  - E.g. disgruntled employee

- Cannot protect against transfer of all virus infected programs or files because of huge range of O/S & file types

Types of Firewall

- Packet Filters
- Stateful Packet Filters
- Application Level Gateway
- Circuit Level Gateway

kasun@cmb.ac.lk

Packet Filter Firewalls

- Simple concept
- Examine each IP packet (no context) and permit or deny according to rules
- Restrict access to services (ports)
- Possible default policies:
  - that not expressly permitted is prohibited
  - that not expressly prohibited is permitted

Attacks on Packet Filters

- IP address spoofing
  - Fake source address to be a trusted one
  - Countermeasure: Discard packets with inside source address arriving on an external interface
- Source routing attacks
  - Attacker sets a route other than default
  - Countermeasure: Block source routed packets
- Tiny fragment attacks
  - Split header info over several tiny packets to circumvent
  - rules that depend on TCP header information
  - Countermeasure: Either discard or reassemble before check

kasun@cmb.ac.lk

Stateful Packet Filters

- Examine each IP packet in context
  - keeps tracks of client-server sessions
  - checks each packet validly belongs to one

- Better able to detect bogus packets out of context

- E.g. permit ftp data connection from outside the firewall to inside, provided the corresponding control connection from inside to outside is still open between same machines and on expected ports.

Application-level Gateway (proxy)

- Use an application specific gateway/proxy
- Has full access to protocol
  - User requests service from proxy
  - Proxy validates request as legal
  - Then forwards request and returns result to user
- Need separate proxies for each service
  - some services naturally support proxying
  - others are more problematic
  - custom services generally not supported
  - Ex: HTTP for Web

    FTP for file transfers

    SMTP/POP3 for e-mail

kasun@cmb.ac.lk

Circuit Level Gateway

- Relays two TCP connections
- Imposes security by limiting which connections are allowed
- Once created, usually relays traffic without examining contents
- Typically used, when it trusts internal users by allowing general outbound connections
  - E.g. SOCKS server

Features and Functionality

- **A wide range of additional features and functionalities are being integrated into standard firewall products.**

These are

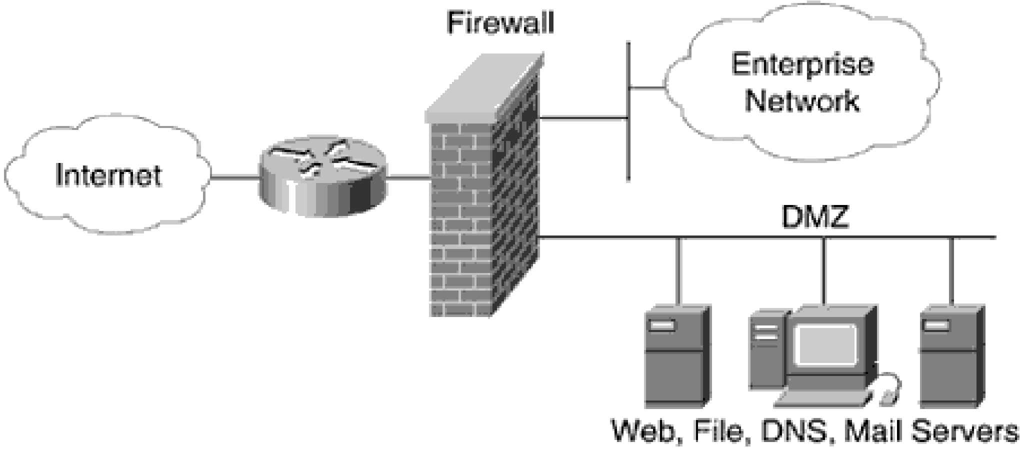
  - **Demilitarized zone (DMZ)**
  - **Content filtering**
  - **Virtual private networking (VPN).**

kasun@cmb.ac.lk

Demilitarized Zone Firewalls

- A secure system that supports a limited number of applications for use by outsiders.
- For example, a company that hosts a Web site or sells its products or services over the Internet

A DMZ Topology



d.

kasun@cmb.ac.lk

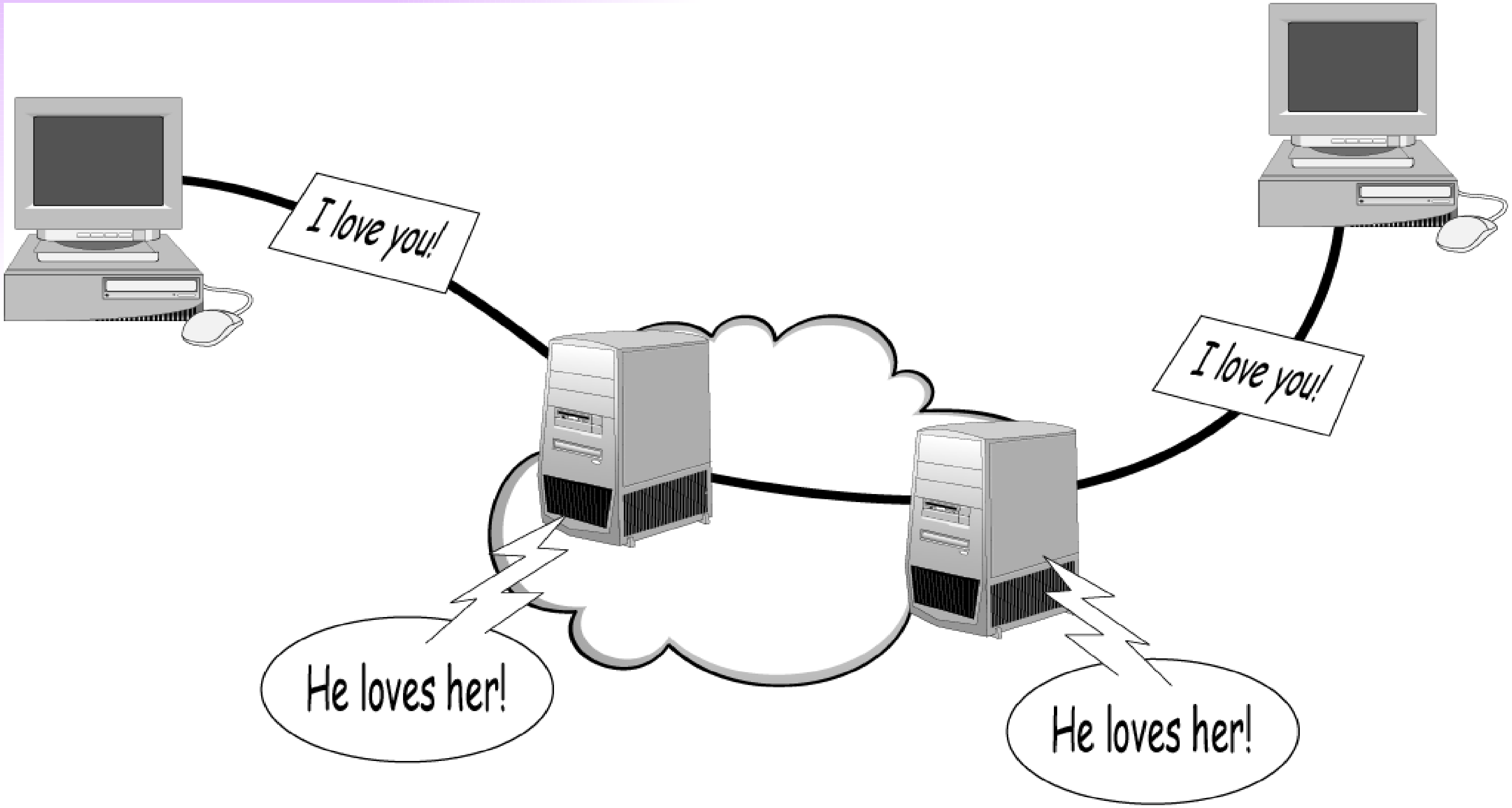
Security in Networks and Distributed Systems

5.2 Web Security

- Solving Privacy Problems
- Solving Authentication Problems
- Secure Socket Layer (SSL) Protocol
- Secure Electronic Transaction (SET) Protocol
- Safe Guarding Web Servers

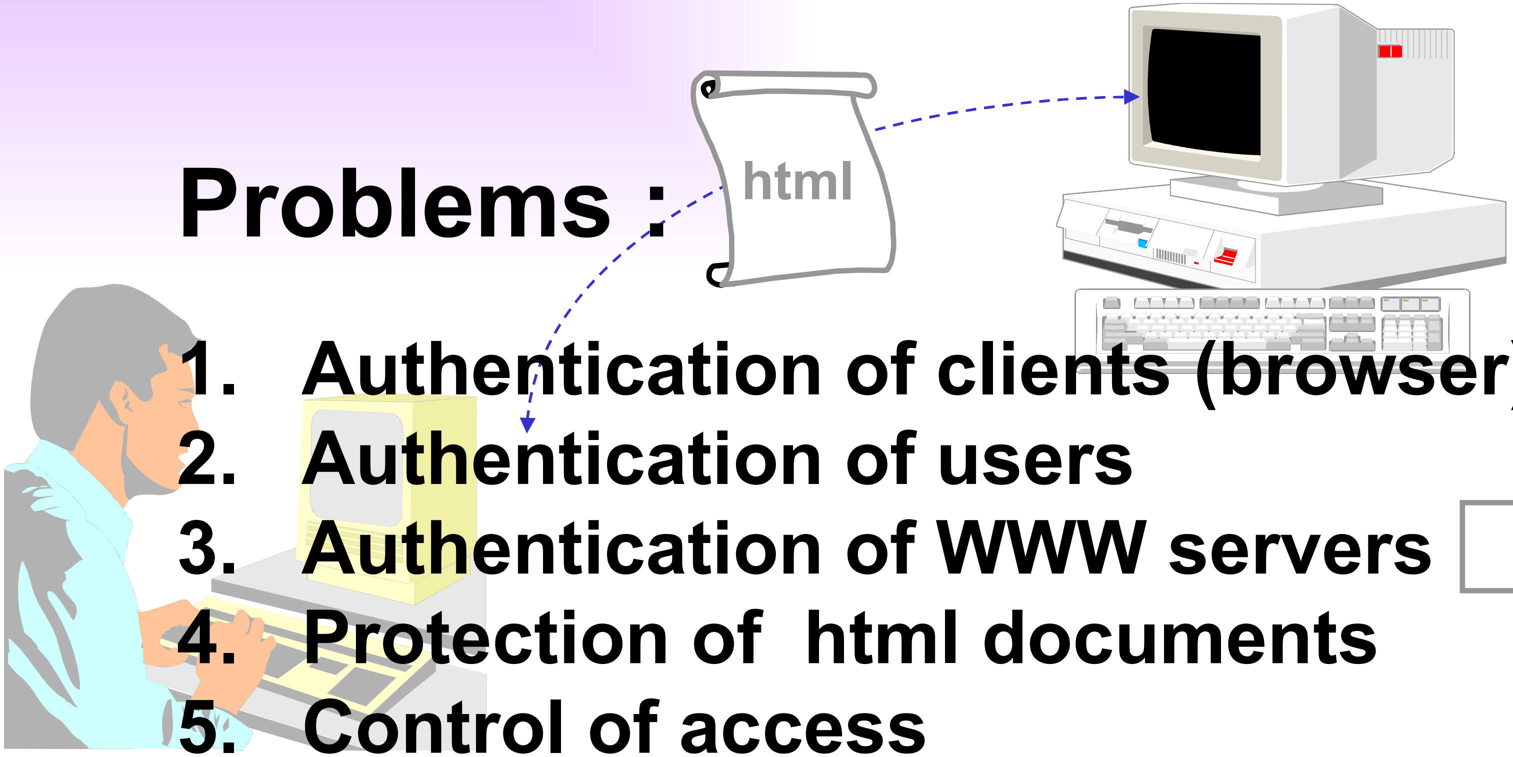
kasun@cmb.ac.lk

How the Internet Works -2



Stateless protocol

Problems :



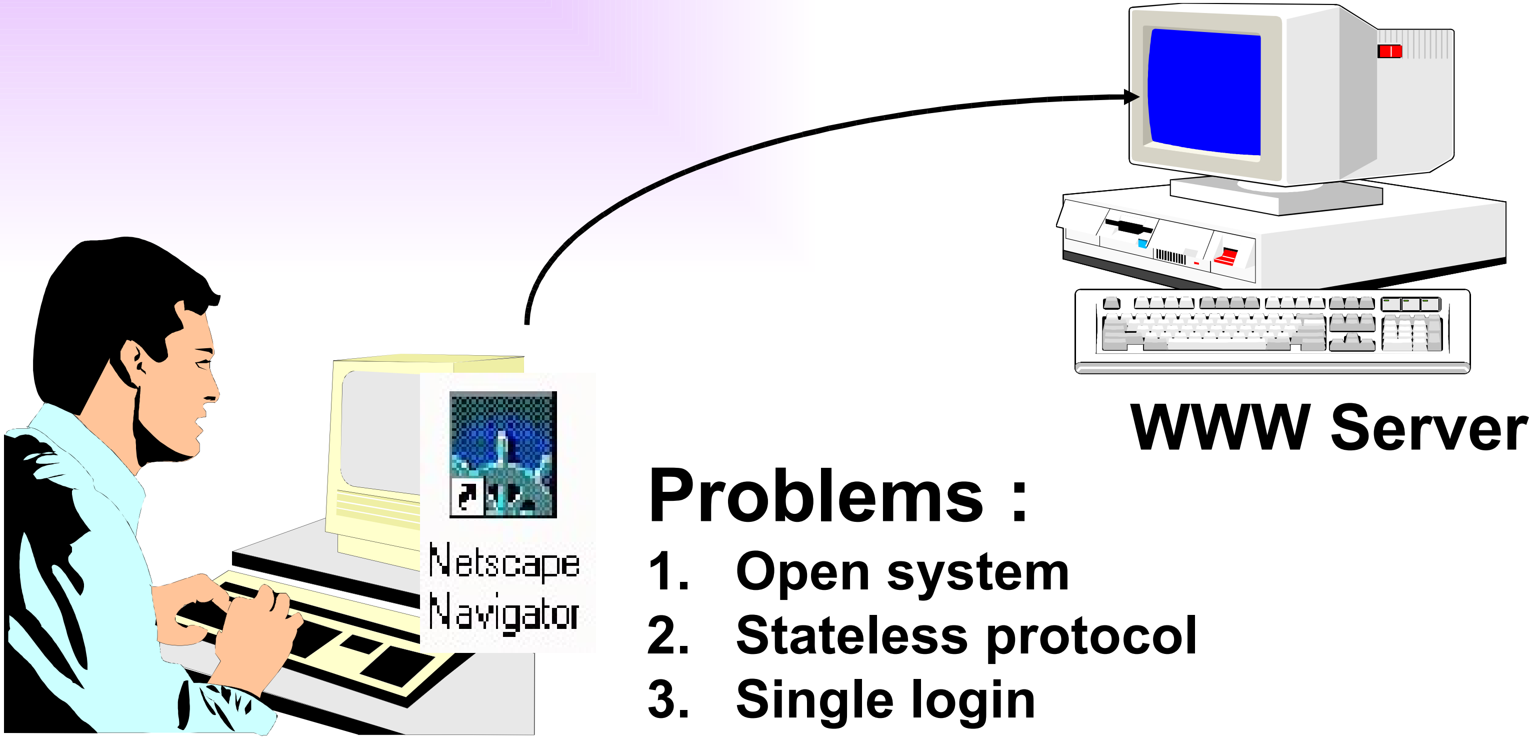
1. Authentication of clients (browser)
2. Authentication of users
3. Authentication of WWW servers
4. Protection of html documents
5. Control of access

CGI

UCSC

kasun@cmb.ac.lk

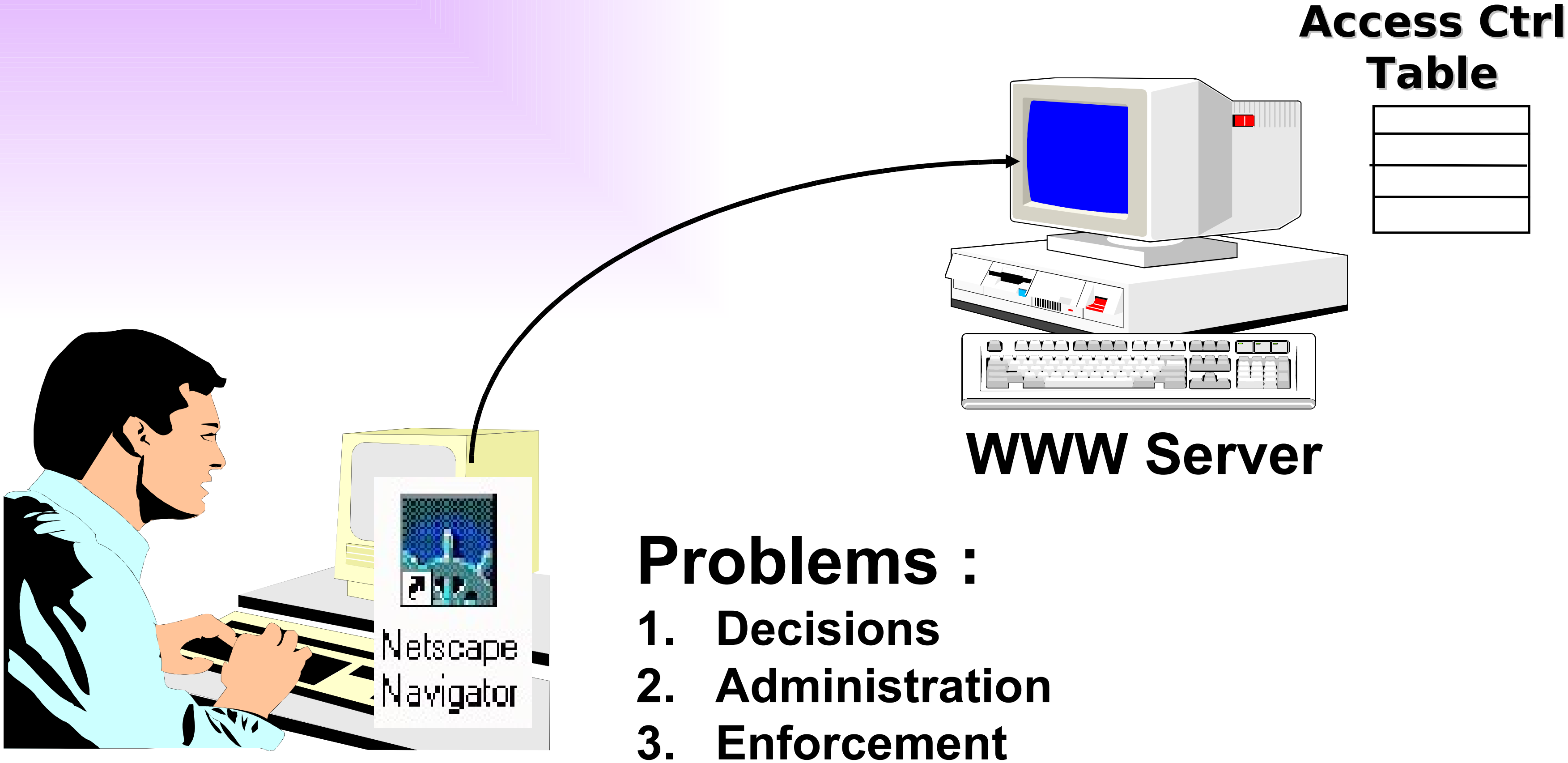
Remote login



Problems :

1. Open system
2. Stateless protocol
3. Single login

Access Control for Users

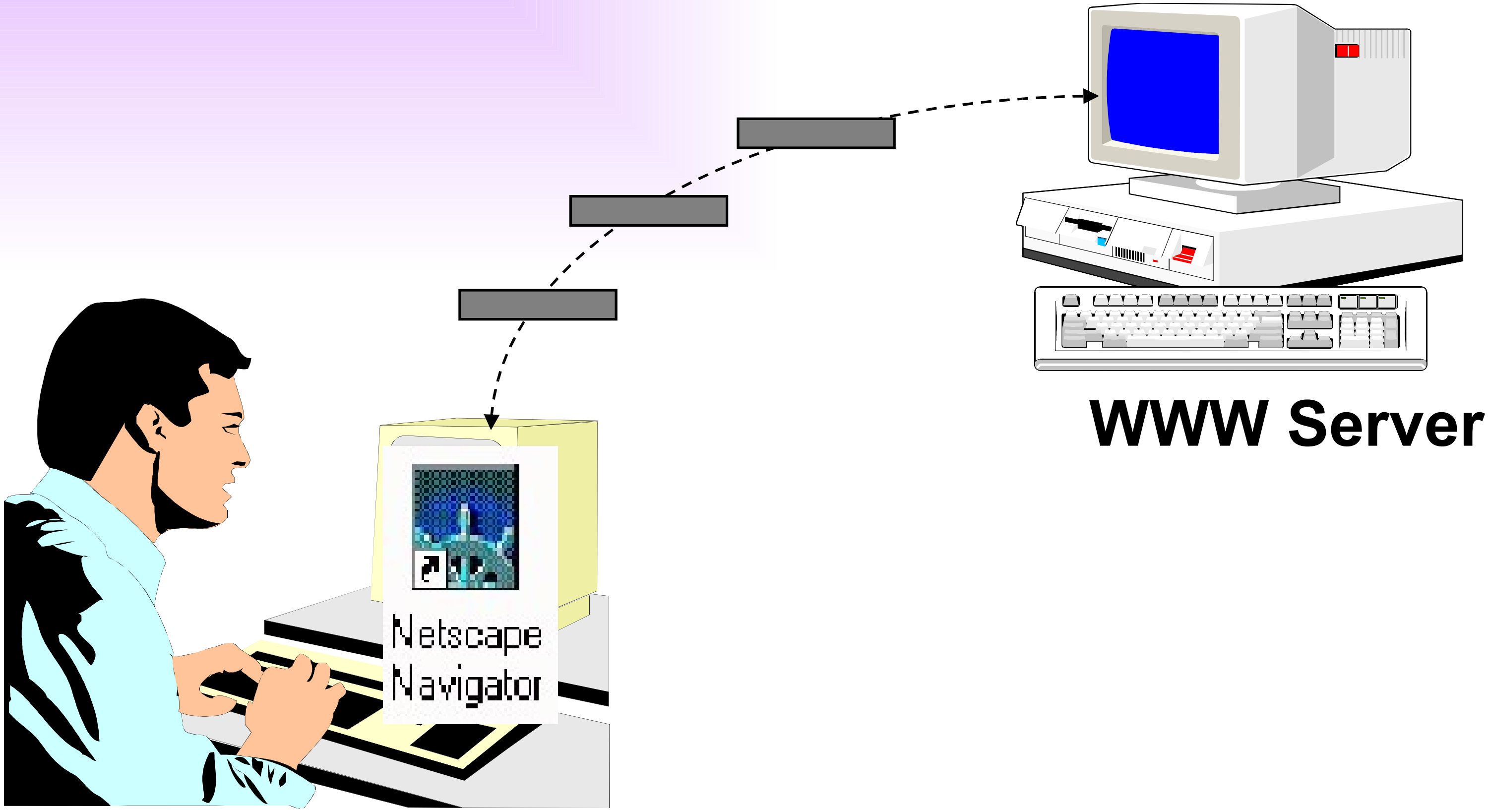


Problems :

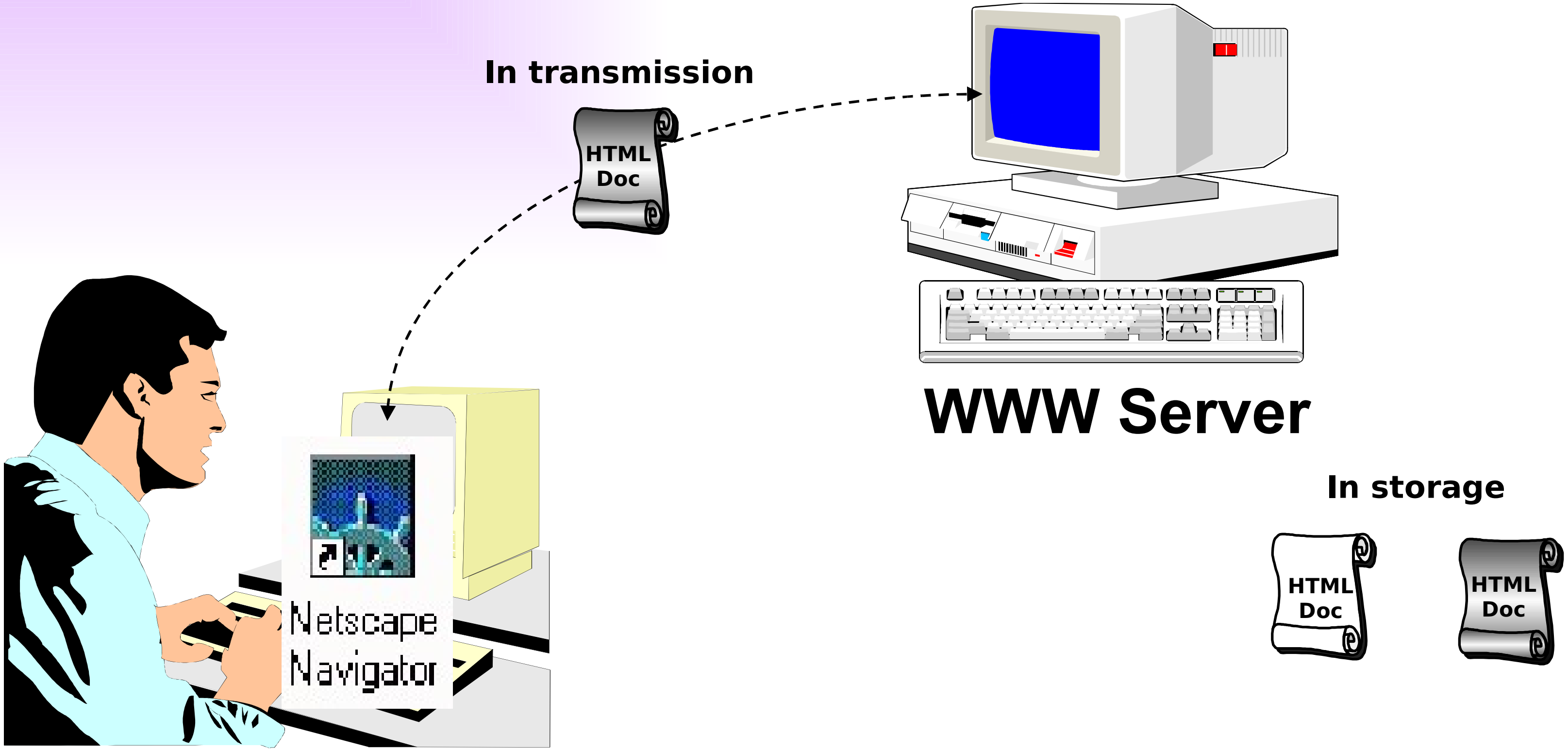
1. Decisions
2. Administration
3. Enforcement

UCSC
kasun@cmb.ac.lk

Protection of Messages



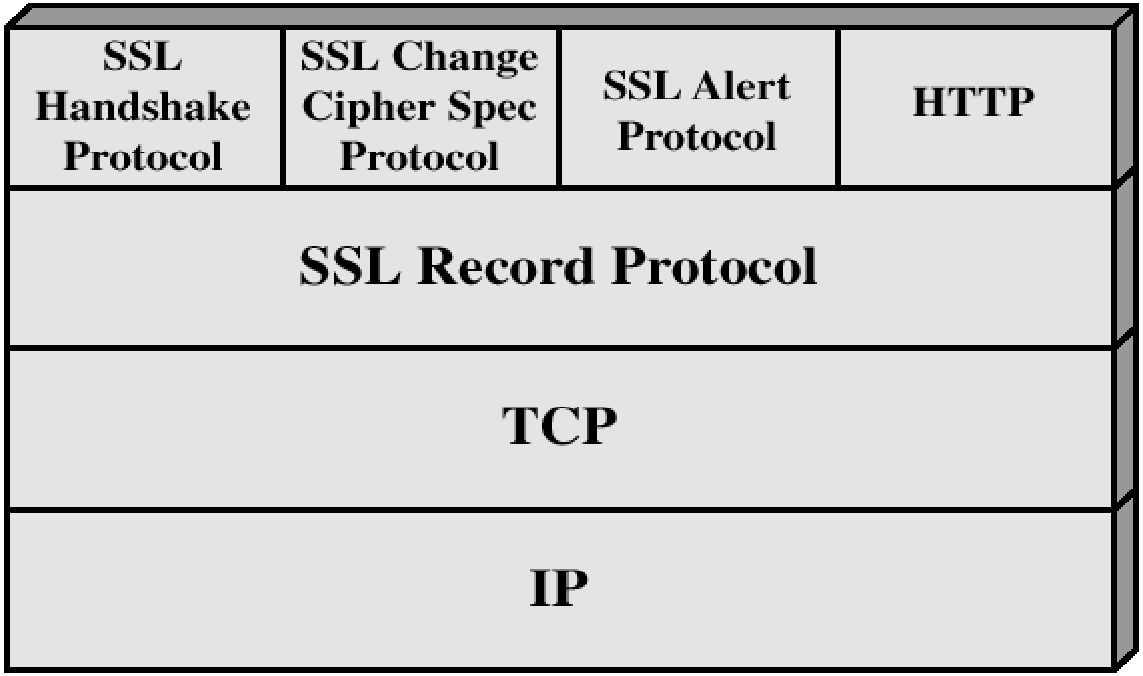
Protection of Documents



SSL and TLS

- SSL was originated by Netscape
- TLS working group was formed within IETF
- First version of TLS can be viewed as an SSLv3.1

SSL Architecture



SSL Handshake Protocol | SSL Change Cipher Spec Protocol | SSL Alert Protocol | HTTP

SSL Record Protocol

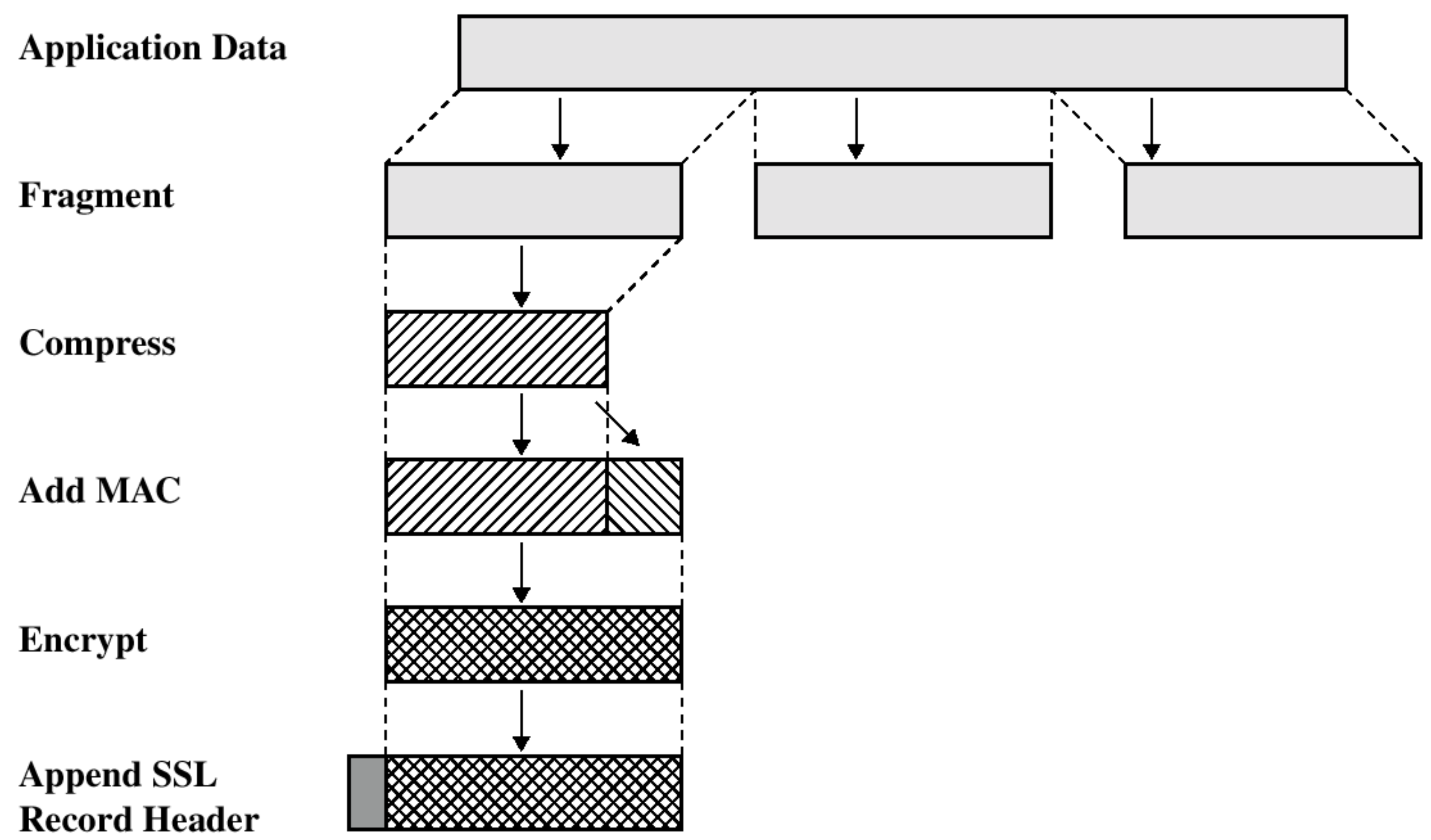
TCP

IP

Figure 7.2 SSL Protocol Stack

kasun@cmb.ac.lk

SSL Record Protocol Operation



Handshake Protocol

- The most complex part of SSL.
- Allows the server and client to authenticate each other.
- Negotiate encryption, MAC algorithm and cryptographic keys.
- Used before any application data are transmitted.

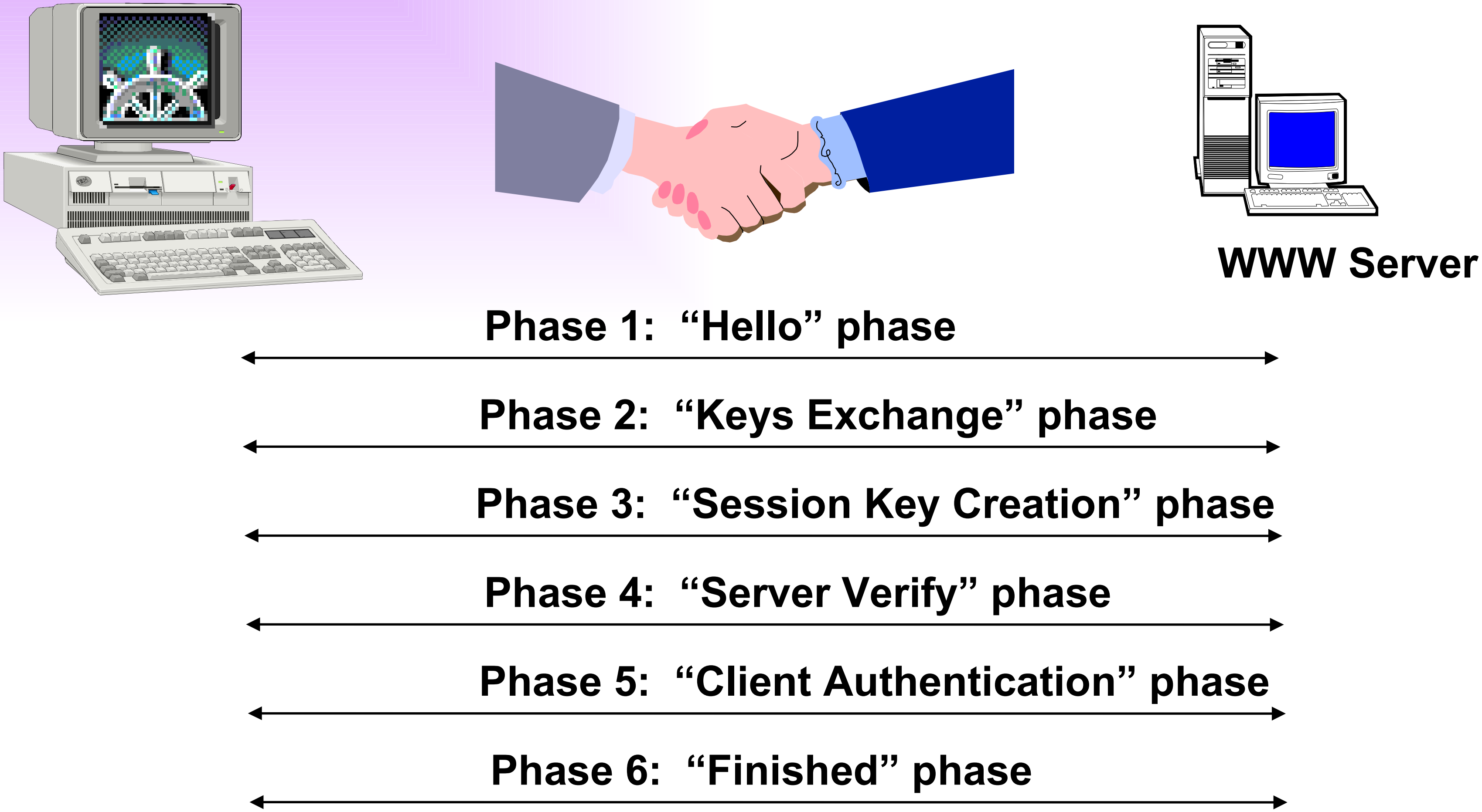
kasun@cmb.ac.lk

Secure WWW (SSL)

Secure client/server (WWW) protocol:

1. Server Authentication
2. Client Authentication (optional)
3. Negotiation of the encryption algorithm
4. Establishment of the session key
5. Encryption of http messages (DES, RC4, etc.)
6. Integrity of http messages (MD2)

Secure WWW (SSL)



WWW Server

Phase 1: “Hello” phase

Phase 2: “Keys Exchange” phase

Phase 3: “Session Key Creation” phase

Phase 4: “Server Verify” phase

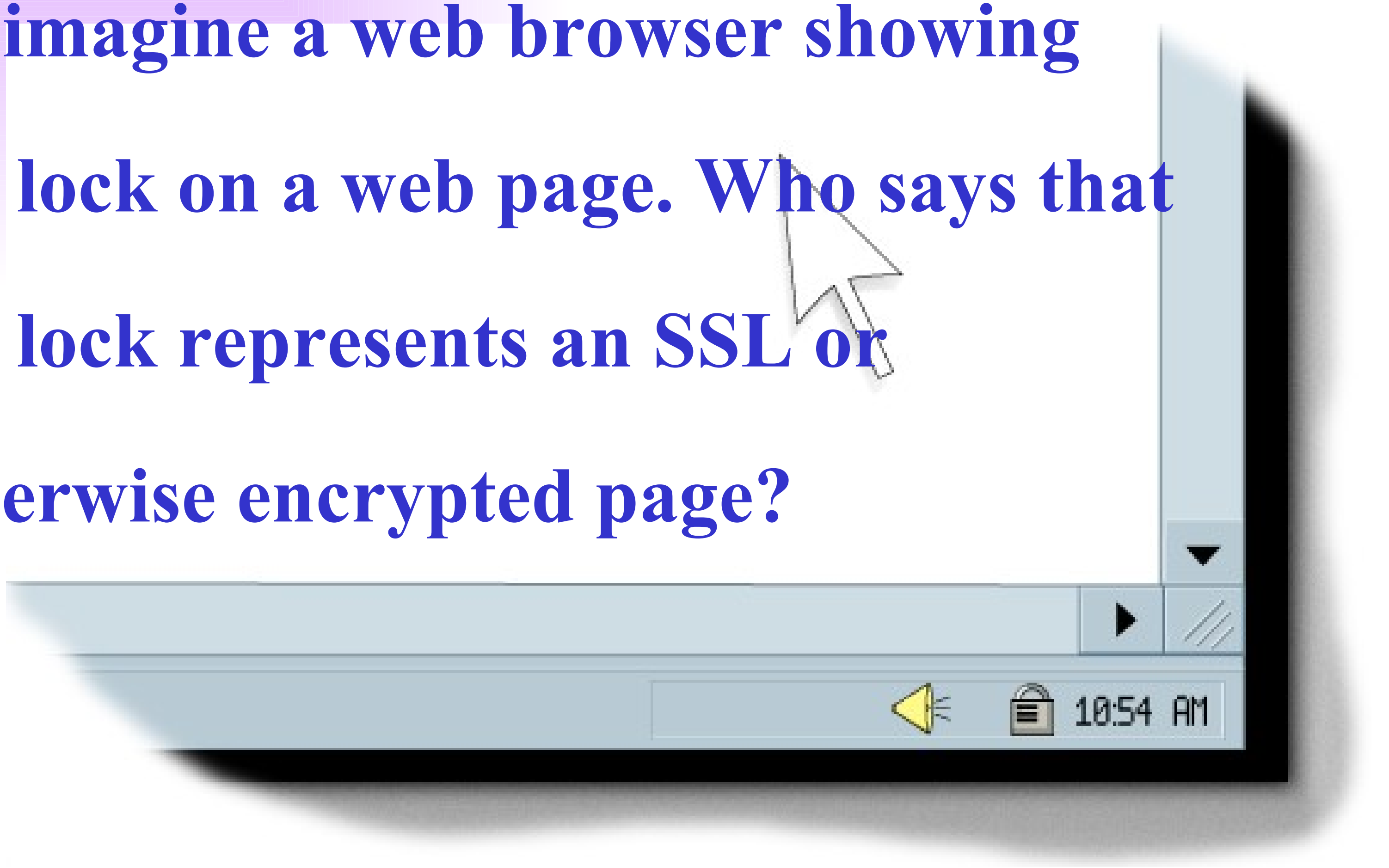
Phase 5: “Client Authentication” phase

Phase 6: “Finished” phase

Transport Layer Security

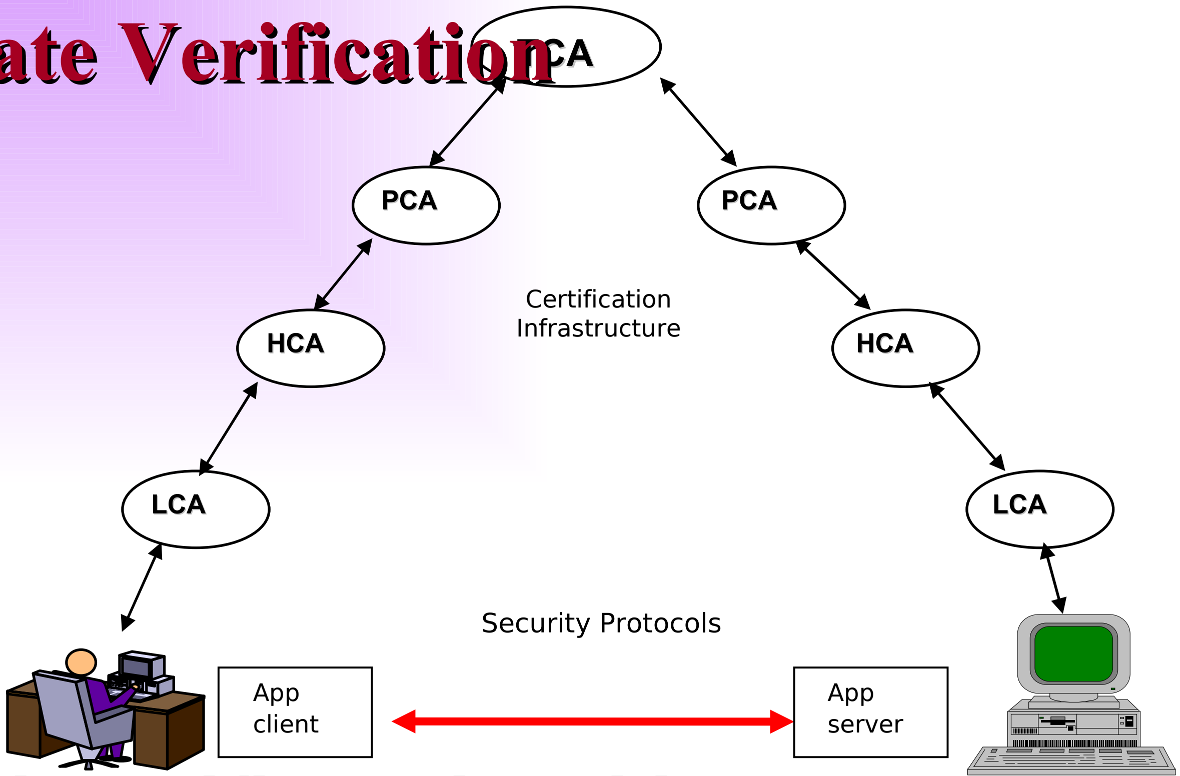
- The same record format as the SSL record format.
- Defined in RFC 2246.
- Similar to SSLv3.
- Differences in the:
  - version number
  - message authentication code
  - pseudorandom function
  - alert codes
  - cipher suites
  - client certificate types
  - certificate_verify and finished message
  - cryptographic computations
  - padding

Trust



Now imagine a web browser showing the lock on a web page. Who says that the lock represents an SSL or otherwise encrypted page?

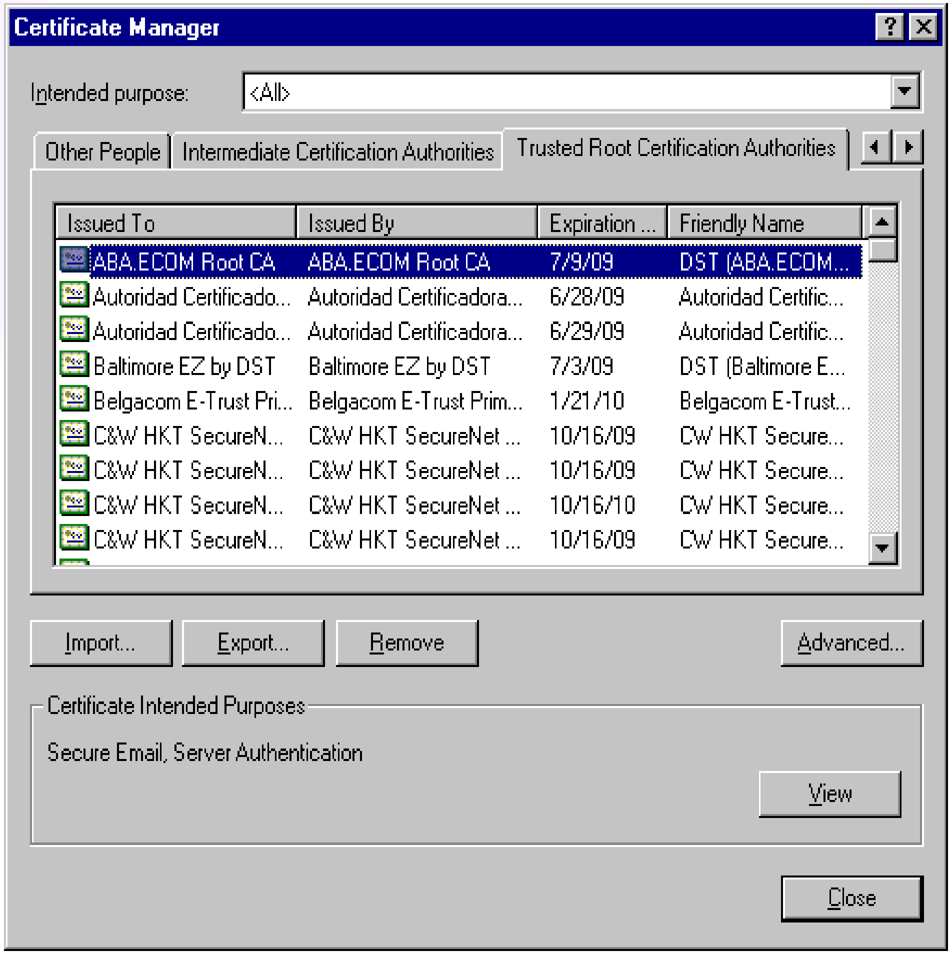
Certificate Verification



- **Trusted certificate handling**
- **Certificate chain verification**
- **Certificate Revocation List (CRL) handling**
- **Certificate extension verification**

(Un)Trusted Certificates

- Pre-installed trusted certificates
- Week key length certificates
- Could be replaced


Certificate Manager
Other People
Intermediate Certification Authorities
Trusted Root Certification Authorities
Import...
Export...
Remove
Advanced...
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiration ...	Friendly Name
ABA.ECOM Root CA	ABA.ECOM Root CA	7/9/09	DST (ABA.ECOM...
Autoridad Certificado...	Autoridad Certificadora...	6/28/09	Autoridad Certific...
Autoridad Certificado...	Autoridad Certificadora...	6/29/09	Autoridad Certific...
Baltimore EZ by DST	Baltimore EZ by DST	7/3/09	DST (Baltimore E...
Belgacom E-Trust Pri...	Belgacom E-Trust Prim...	1/21/10	Belgacom E-Trust...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/09	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/09	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/10	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	10/16/09	CW HKT Secure...

Certificate Intended Purposes

Secure Email, Server Authentication

Secure Sockets Layer – Apache

- Compile and install mod_ssl module.
- Create a public/private key pair.
- Get public key signed by certificate authority, yielding a certificate.
- Install certificate and configure Apache to find it.
- Restart

Create Self-signed Certificate

You can generate a self-signed host certificate using the following command:

```
openssl req -new -x509 -out host.pem
```

(Your private key will be saved to privkey.pem file and self-signed certificate will be saved to host.pem file.)

kasun@cmb.ac.lk

Creating a Certificate Request

To create a certificate request, use the following command:

```
openssl req -new -nodes -out req.pem -keyout key.pem
```

(Your private key will be saved to key.pem file and certificate request will be saved to req.pem file.)

req.pem:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBlDCB/gIBADBVMQswCQYDVQQGEwJMSzEQMA4GA1UEBxMHQ29sb21ibzEMMAoG
A1UEChMDQ01CMQ0wCwYDVQQLEwRVQ1NDMRcwFQYDVQQDEw51Y3NjLmNtYi5hYy5s
azCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA9XZEtFxoVbGhH9nrWKRi1avK
lMKKobVkgS99b9bcwnJ6zh7ZXwoiNBO1UNyDUuWrxxlZxcChnzds0UvEHVJatPYM
8+XwQpOmobIK/3E9f9SYh6OVbNxAIoLAXXoHBzV8YysyuxqEPFqmZW94TnfTUFWC
TTuwKPIourOZI1zhyW8CAwEAAaAAMA0GCSqGSIb3DQEBBAUAA4GBABBDlwxgDxqd
wpnfGUuRiIsp2C5KxHFAsVKvVwpRhlgdihcrYXpY2xNq1OTnqqS2dts2pO+xPuEP
nAREnFABPxsqn95/mr+T91bah/2eBuhbJ9TjzxY9wWebTNMrk9CFygqlYldniizd
mhWMWQuqSnXSS5oC/+itEtAd64hWHv0Q
-----END CERTIFICATE REQUEST-----
```

kasun@cmb.ac.lk

Obtaining a Server Certificate

Convince a Certificate Authority to Sign your Certificate:

- Submit the req.pem file to Verisign or Thawte for signing (pay the fee) or
- Submit the req.pem file to **www.cacert.org** or **ca.cmb.ac.lk** **(Free)**.

They will eventually mail you back a signed certificate.

Authenticating with SSL

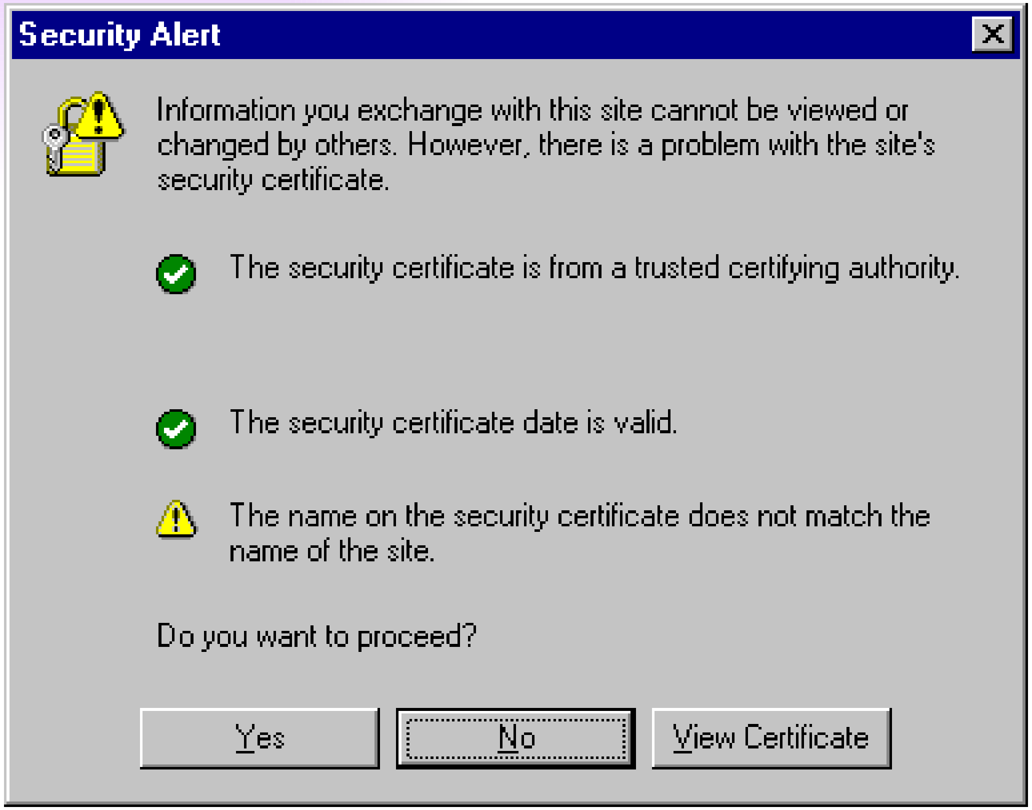
Give users of your intranet client certificates to authenticate with.
Advantages: No passwords to mess around with.
Disadvantages: Certificate management is **hard**.

Creating Client Certificates
OpenSSL will do that.

kasun@cmb.ac.lk

Secure Socket Layer (SSL)

- **Optional user authentication**
- **No document level protection**
- **No Non-repudiation**



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

✓ The security certificate is from a trusted certifying authority.

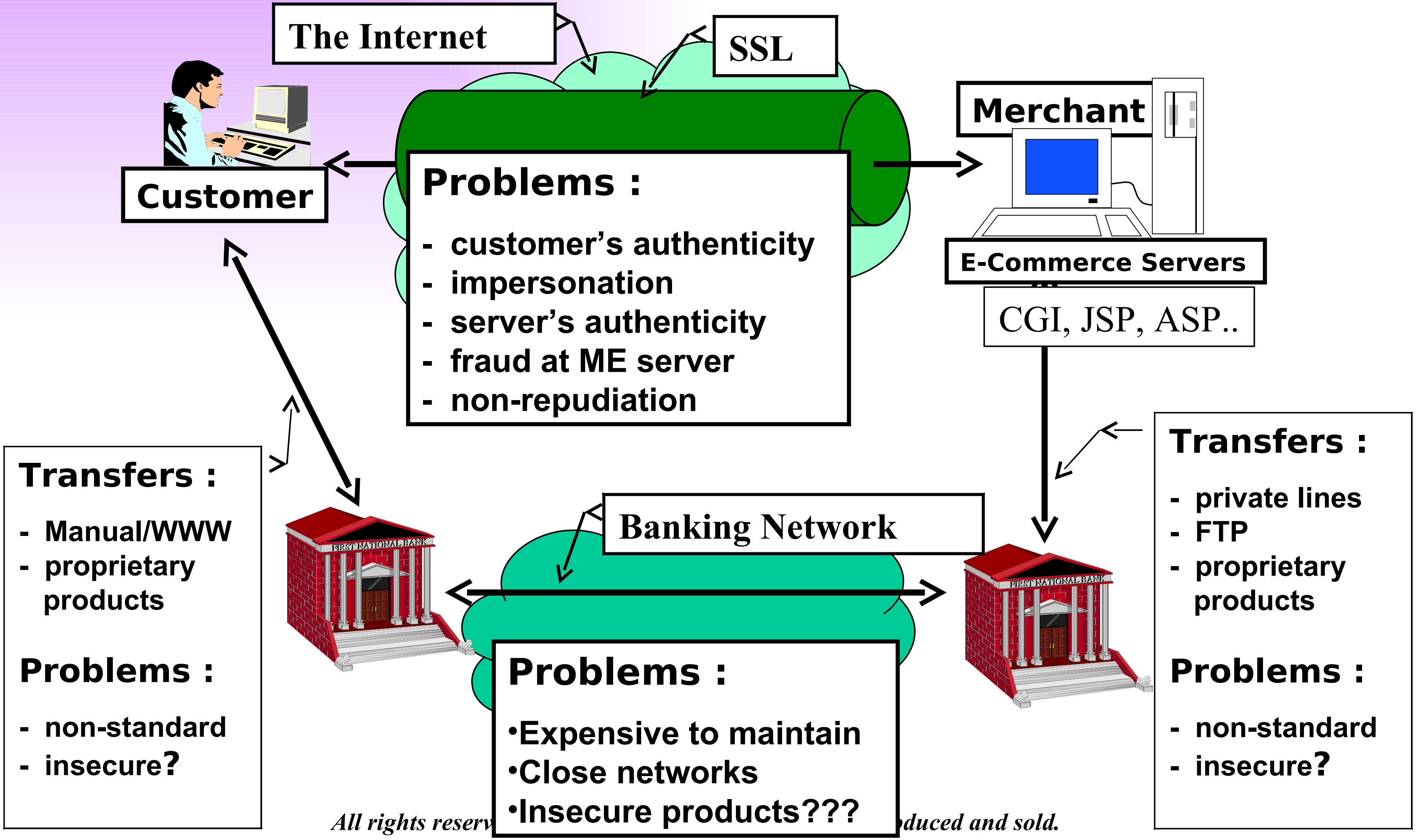
✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?

kasun@cmb.ac.lk

Secure Credit Card Payments (SSL)



Problems :

- customer’s authenticity
- impersonation
- server’s authenticity
- fraud at ME server
- non-repudiation

Transfers :

- Manual/WWW
- proprietary products

Problems :

- non-standard
- insecure?

Problems :

•Expensive to maintain
•Close networks
•Insecure products???

Transfers :

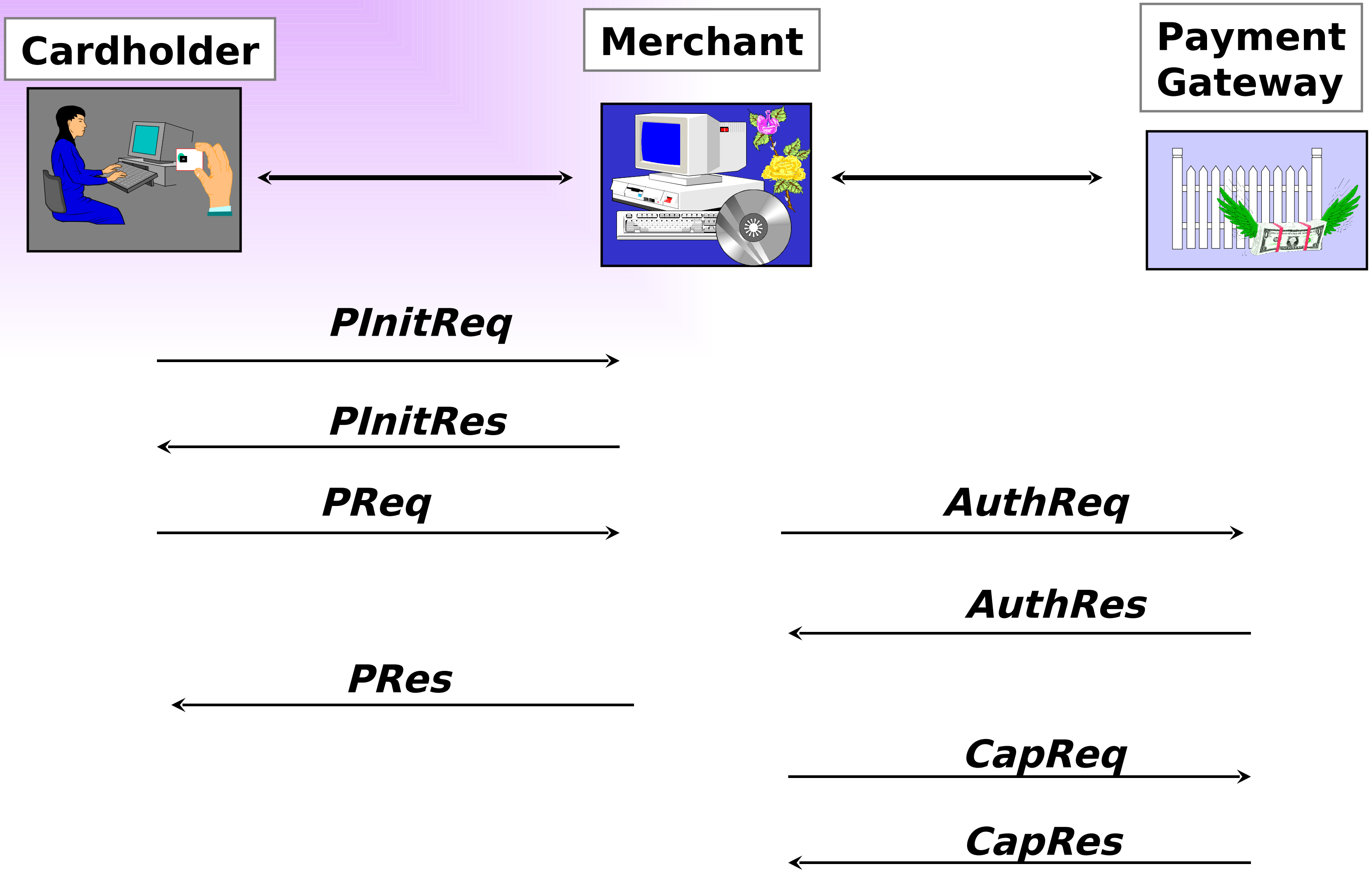
- private lines
- FTP
- proprietary products

Problems :

- non-standard
- insecure?

kasun@cmb.ac.lk

SET Payment System



Cardholder

Merchant

Payment Gateway

PInitReq

PInitRes

PReq

AuthReq

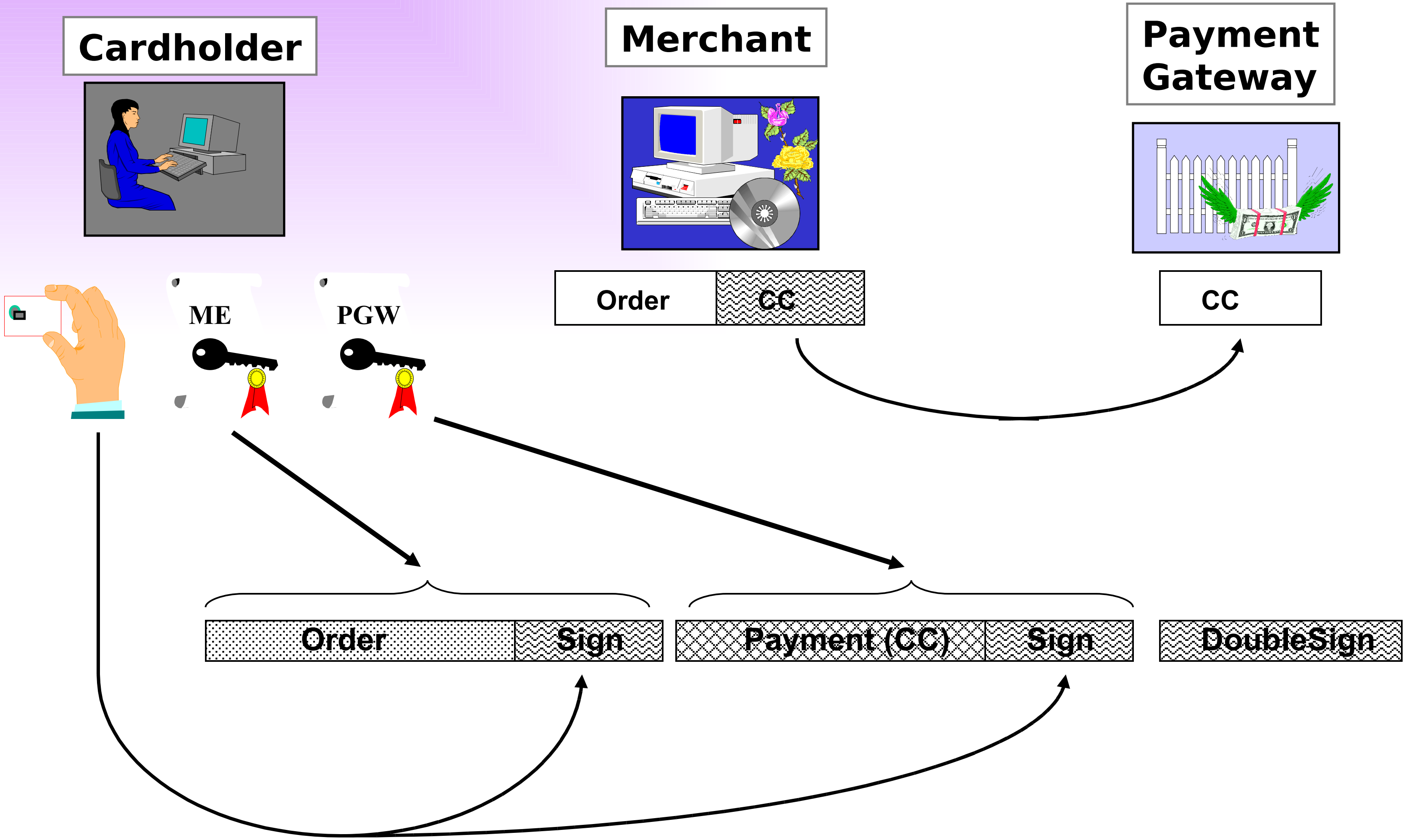
AuthRes

PRes

CapReq

CapRes

SET PReq Message



Cardholder

Merchant

Payment Gateway

ME

PGW

Order | CC

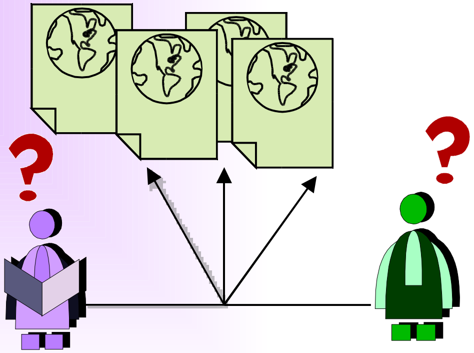
CC

Order | Sign

Payment (CC) | Sign

DoubleSign

Problems of Single Sign–On



Solution → Once login Multiple services → **Single Sign-on**

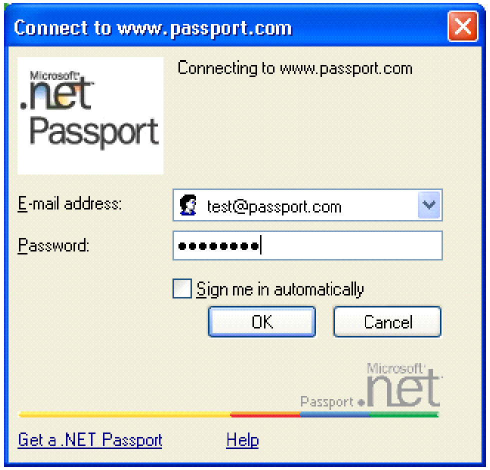
- **Different web sites are under completely different administrative control**
- *Microsoft Passport* – **Microsoft's ambitious attempt to provide this service**

UCSC

kasun@cmb.ac.lk

Microsoft .NET Passport

- **Centralized identity system based on symmetric cryptography.**
  - **Designed to use existing web technologies**
    - HTTP redirects,JavaScript, Cookies,SSL



Connect to www.passport.com

Connecting to www.passport.com

E-mail address: test@passport.com

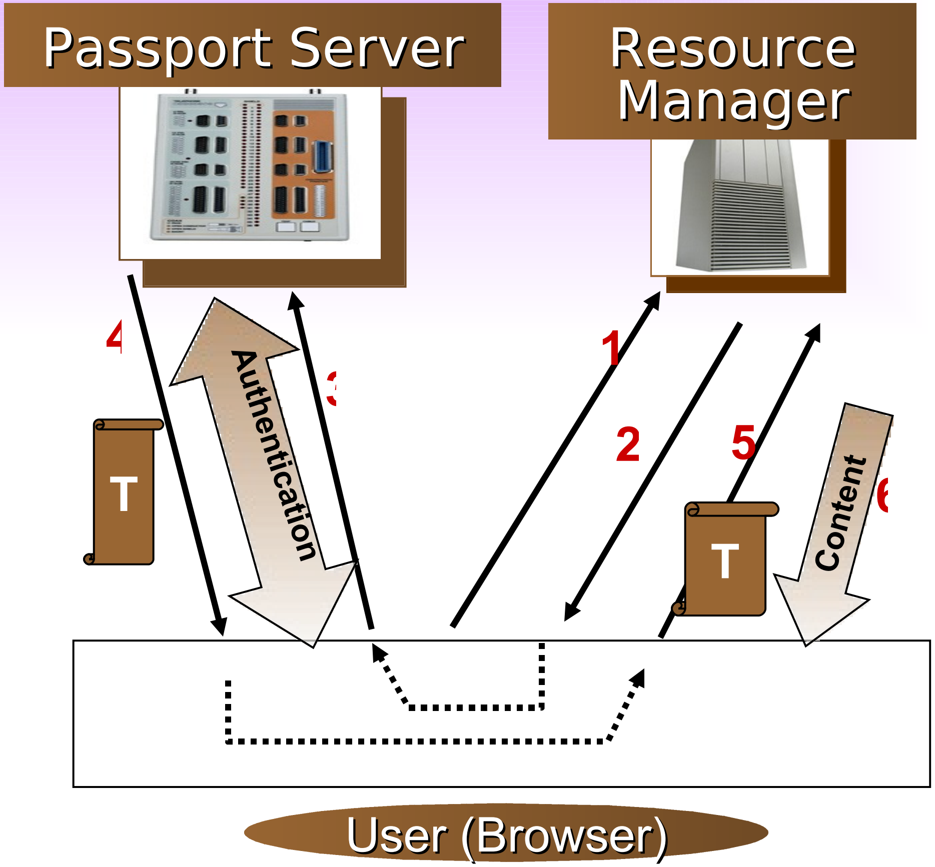
Password: ••••••••

☐ Sign me in automatically

- Heart of the entire system - A single system located in the passport.com internet domain
- Unique identifier for every user
- This is sent back in the form of an encrypted "ticket".

kasun@cmb.ac.lk

How .NET Passport Works?



1. Initial resource request

1. Redirect to passport

1. Passport authentication request

1. Authentication response

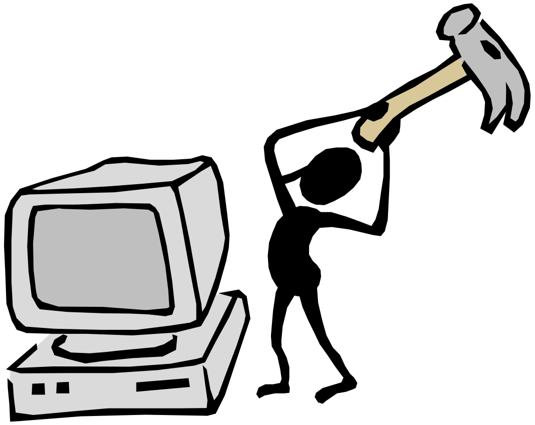
1. Authenticated resource request

6. Content delivery.

kasun@cmb.ac.lk

Risks of Passport?

- Global centralization
- Lack of documentation
- Passport uses a simple password authentication mechanism
- Problem of encryption algorithm
- Problems with SSL protocol

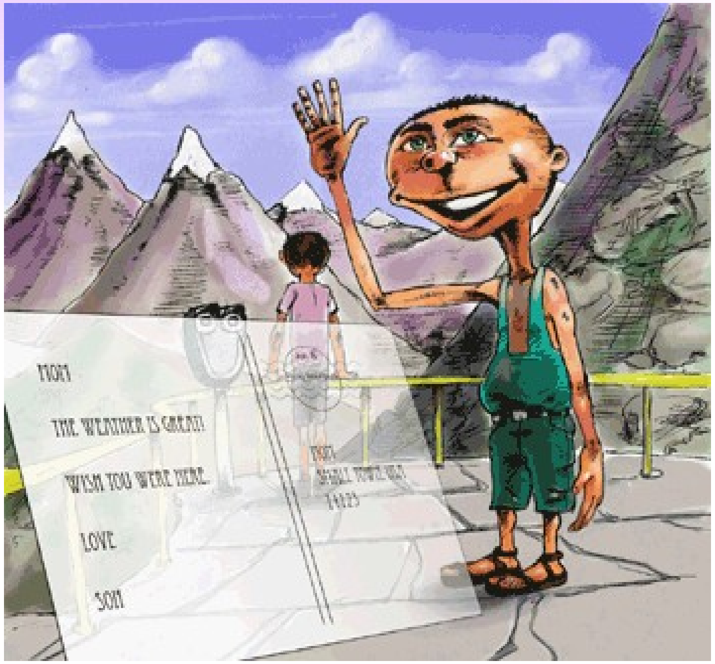


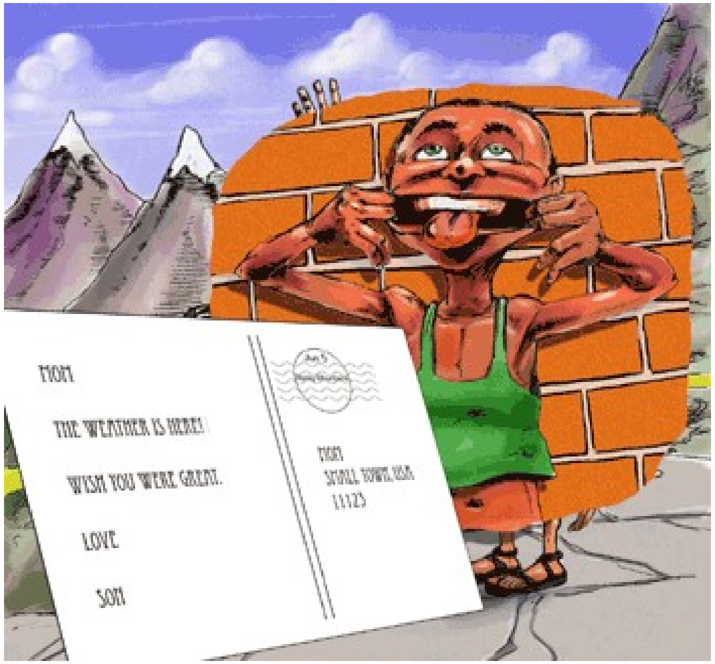
5.3 Secure Electronic Mail

- Privacy Enhanced Email (PEM)
- Pretty Good Privacy (PGP)
- Public Key Cryptography Standards-PKCS#7
- Secure/Multipurpose Internet Mail Extensions (S/MIME)

Email is in the Clear

Email – A Postcard Written in Pencil





http://www.cert.org/homeusers/email_postcard.html

E-mail Security

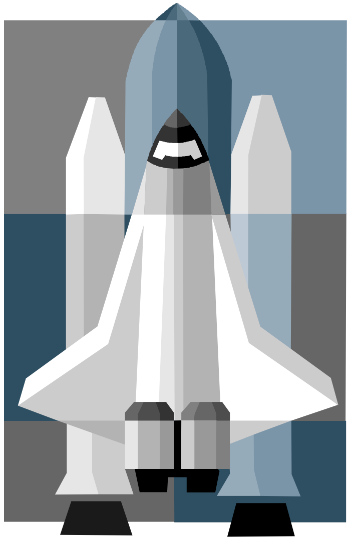
- Pretty Good Privacy (PGP) (www.pgp.com)
  - Philip R. Zimmerman is the creator of PGP.
  - PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.
- S/MIME
  - Secure/Multipurpose Internet Mail Extension
  - S/MIME will probably emerge as the industry standard.
  - PGP for personal e-mail security

Why Is PGP Popular?

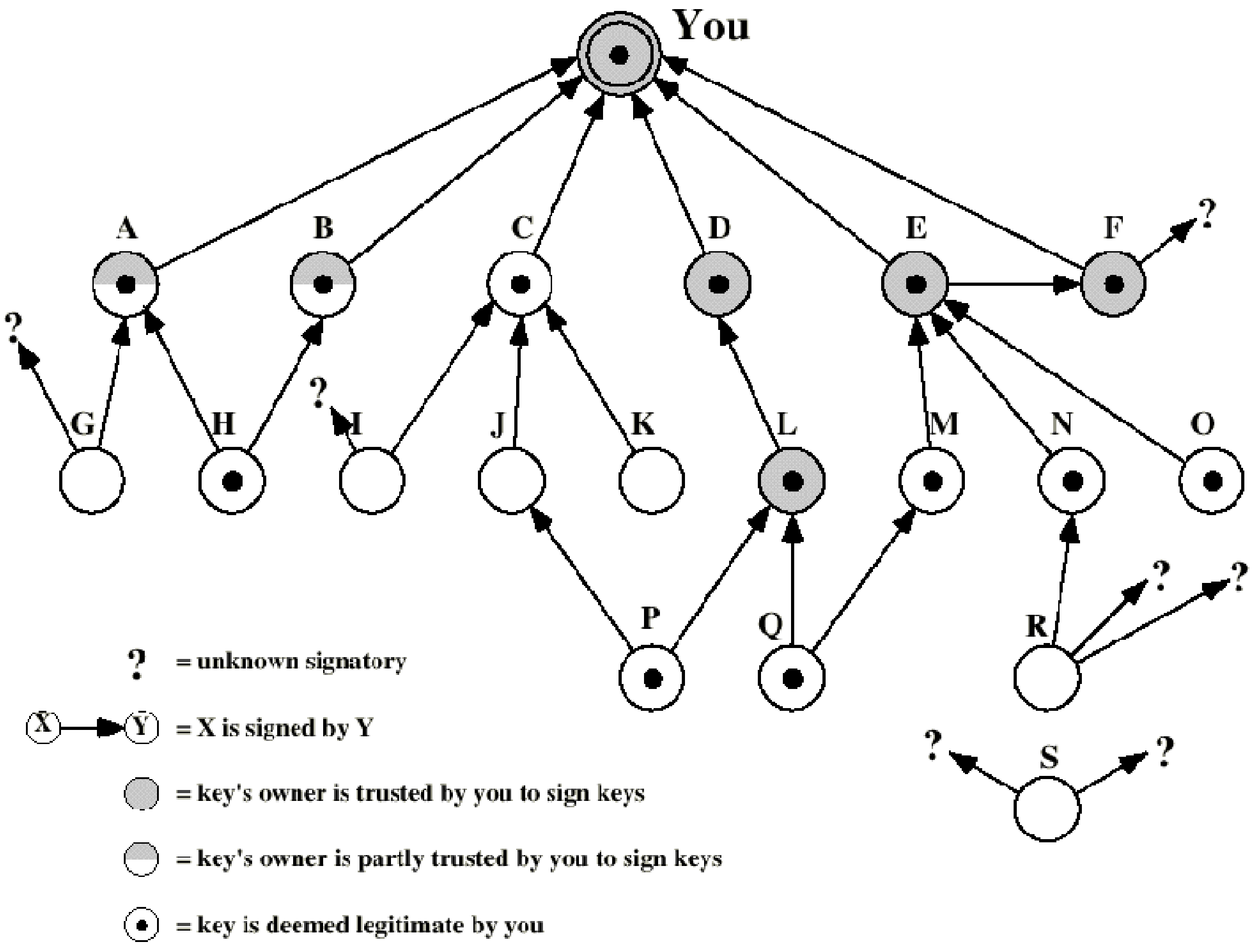
- **It is availiable free on a variety of platforms.**
- **Based on well known algorithms.**
- **Wide range of applicability**
- **Not developed or controlled by governmental or standards organizations**

Operational Description

- Consist of five services:
  - Authentication
  - Confidentiality
  - Compression
  - E-mail compatibility
  - Segmentation



PGP Public Keys


You
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
?
? = unknown signatory
X → Y = X is signed by Y
= key's owner is trusted by you to sign keys
= key's owner is partly trusted by you to sign keys
= key is deemed legitimate by you

kasun@cmb.ac.lk

MIME content (mixed)

MIME content headers

text/plain
text/richtext
multipart/mixed
multipart/parallel
multipart/alternative
multipart/digest
message/rfc822
message/partial
message/external-body
image/jpeg
image/gif
video/mpeg
audio/basic
application/postscript
application/octet-stream

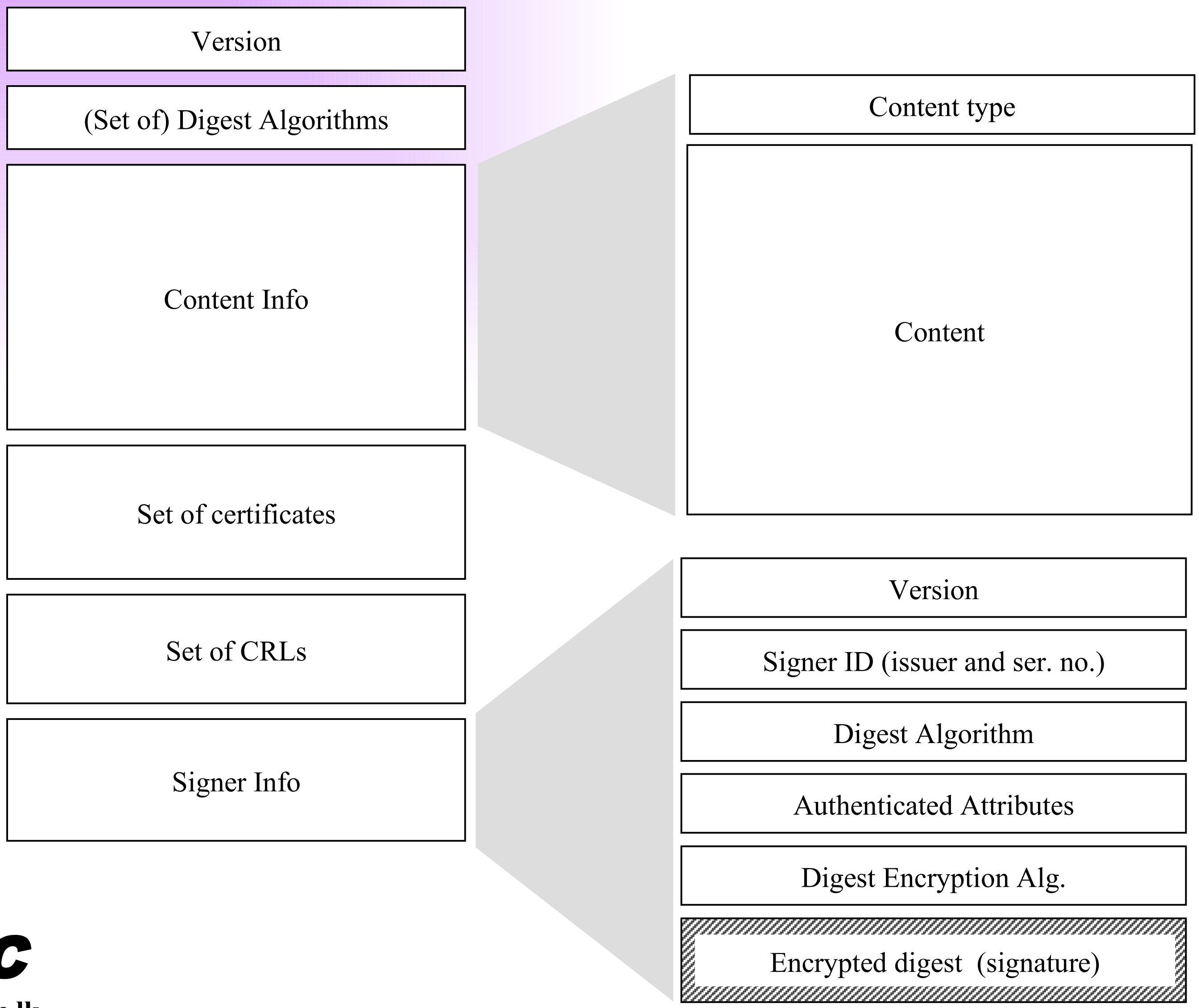
MIME content headers

```
From: Dr William Buchanan
<w.buchanan@napier.ac.uk>
MIME-Version: 1.0
To: w.buchanan@napier.ac.uk
Subject: Any subject
Content-Type: multipart/mixed;
boundary="boundary name"
This part of the message will be ignored.
-- boundary name
Content-Type: multipart/mixed;
boundary="boundary name"
This is the first mail message part.
-- boundary name
And this is the second mail message part.
-- boundary name --
```

Securing a MIME entity

- MIME entity is prepared according to the normal rules for MIME message preparation
- prepared MIME entity is processed by S/MIME to produce a PKCS object
- the PKCS object is treated as message content and wrapped in MIME

PKCS7 “signed data”



Version

(Set of) Digest Algorithms

Content Info

- Content type
- Content

Set of certificates

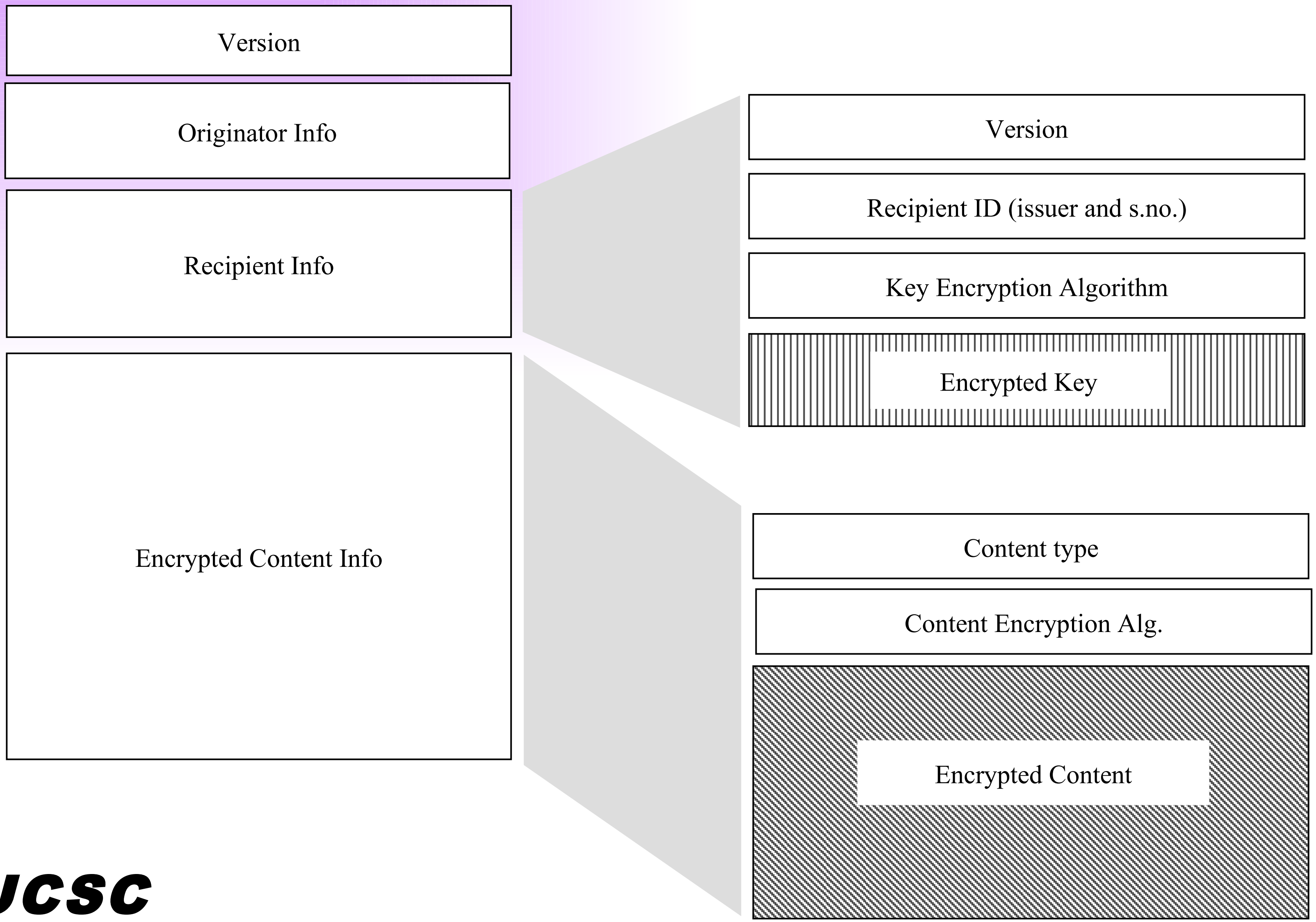
Set of CRLs

Signer Info

- Version
- Signer ID (issuer and ser. no.)
- Digest Algorithm
- Authenticated Attributes
- Digest Encryption Alg.
- Encrypted digest (signature)

UCSC
kasun@cmb.ac.lk

PKCS7 “enveloped data”



Version

Originator Info

Recipient Info

Encrypted Content Info

Version

Recipient ID (issuer and s.no.)

Key Encryption Algorithm

Encrypted Key

Content type

Content Encryption Alg.

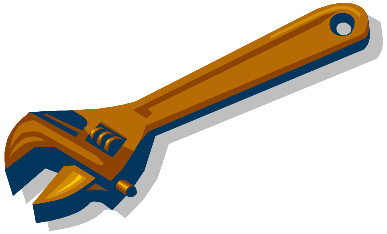
Encrypted Content

S/MIME Functions

- Enveloped Data: **Encrypted content and encrypted session keys for recipients.**
- Signed Data: **Message Digest encrypted with private key of “signer.”**
- Clear-Signed Data: **Signed but not encrypted.**
- Signed and Enveloped Data: **Various orderings for encrypting and signing.**

Algorithms Used

- Message Digesting: **SHA-1 and MDS**
- Digital Signatures: **DSS**
- Secret-Key Encryption: **Triple-DES, RC2/40 (exportable)**
- Public-Private Key Encryption: **RSA with key sizes of 512 and 1024 bits, and Diffie-Hellman (for session keys).**



User Agent Role

- **S/MIME uses Public-Key Certificates - X.509 version 3 signed by Certification Authority**
- **Functions:**
  - Key Generation **- Diffie-Hellman, DSS, and RSA key-pairs.**
  - Registration **- Public keys must be registered with X.509 CA.**
  - Certificate Storage **- Local (as in browser application) for different services.**
  - Signed and Enveloped Data **- Various orderings for encrypting and signing.**

kasun@cmb.ac.lk

Attachments

- Computer viruses and other malicious software are often spread through email attachments.
- If a file attached to an email contains a virus, it is often launched when you open (or double-click) the attachment.
- Don’t open email attachments unless you know whom it is from and you were expecting it.

Should you open attachments?

If it is suspicious, do not open it!

- What is suspicious?
  - Not work-related.
  - The email containing the attachment was not addressed to you, specifically, by name.
  - Incorrect or suspicious filename.
  - Unexpected attachments.
  - Attachments with suspicious or unknown file extensions (e.g., .exe, .vbs, .bin, .com, .pif, or .zzx)
  - Unusual topic lines: “Your car?”; “Oh!”; “Nice Pic!”; “Family Update!”; “Very Funny!”

Email best practices

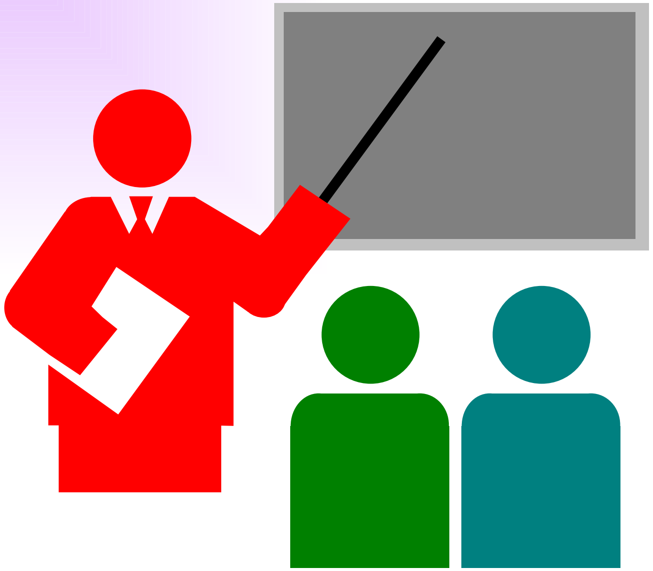
- Use the BCC field when sending to large distribution lists.
  - Protects recipients email addresses
  - Prevents Reply to All issues
- Avoid use of large distribution lists unless legitimate business purpose.
  - E.g., All Faculty/Staff list
  - Use TCU Announce instead
- Beware of Reply to All button
- Don't forward chain email letters.

OKAY! ALRIGHT!! I PROMISE! - I'LL NEVER FORWARD A GROUP EMAIL AGAIN WITHOUT USING BCC!!
Louder.
Pirillo & Fitz
© BLAUGH.COM · FITZ & PIRILLO · SAVE 10% AT GODADDY BY USING THE COUPON CODE "BLAUGH"

What is spam?

- Spam is anonymous, unsolicited junk email sent indiscriminately to huge numbers of recipients.
- What for?
  - Advertising goods and services (often of a dubious nature)
  - Quasi-charity appeals
  - Financial scams
  - Chain letters
  - Phishing attempts
  - Spread malware and viruses

Questions?



kasun@cmb.ac.lk