

WORCESTER POLYTECHNIC INSTITUTE
CS577/ECE537 ADVANCE COMPUTER NETWORKS
KERBEROS AUTHENTICATION PROTOCOL



Murad Kaplan
mkaplan@wpi.edu

What is Kerberos?

- ▣ Network Authentication Protocol
- ▣ Uses private-key Cryptography
- ▣ Built on Needham/Schroeder Scheme
- ▣ Protects Against
 - Eavesdropping
 - Replay Attacks
- ▣ Trusted third part is required
- ▣ Developed before public-key methods

History

- ▣ Developed at MIT out of Athena Project
 - Athena is a distributed file sharing project
- ▣ Developed based on other protocols with the addition of a timestamp to prevent replay attacks.
- ▣ Implementations
 - MIT
 - Heimdal
 - Sun
 - Microsoft

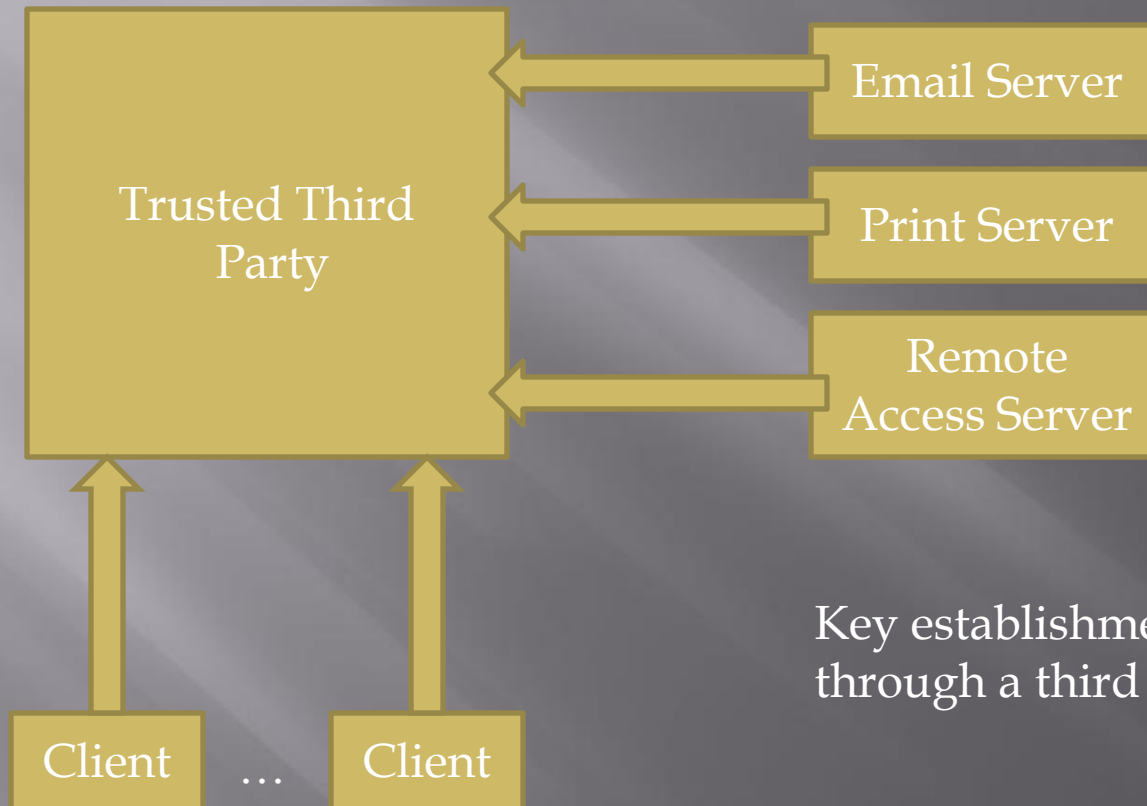
How did it get its name?

- ▣ Kerberos is the three headed dog in Greek mythology (also known as Cerberus)
- ▣ Three Heads
 - Authentication
 - ▣ The users must be able to prove who they are..
 - Authorization
 - ▣ The user must have access to the resource it is trying to get.
 - Accounting
 - ▣ The user cannot deny accessing something, these resources are accounted for.

Why do we need protocols?

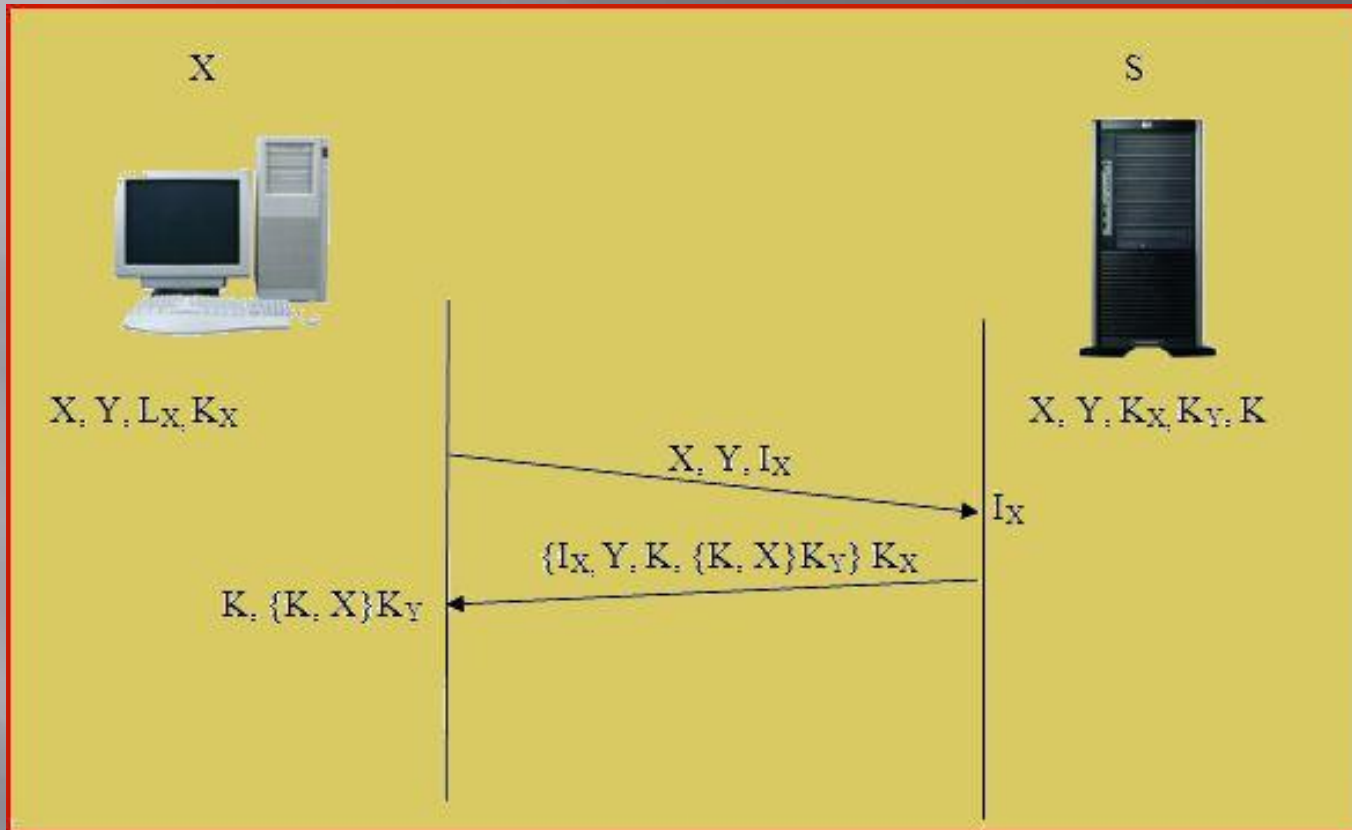
- ▣ Benefits of Kerberos
 - Single sign-on capability
 - ▣ * the user doesn't have to authenticate him/herself for every interaction
 - ▣ Passwords never get sent across the network.
 - Replay Attacks are not possible
 - ▣ This builds upon previous protocols vulnerabilities

Organization



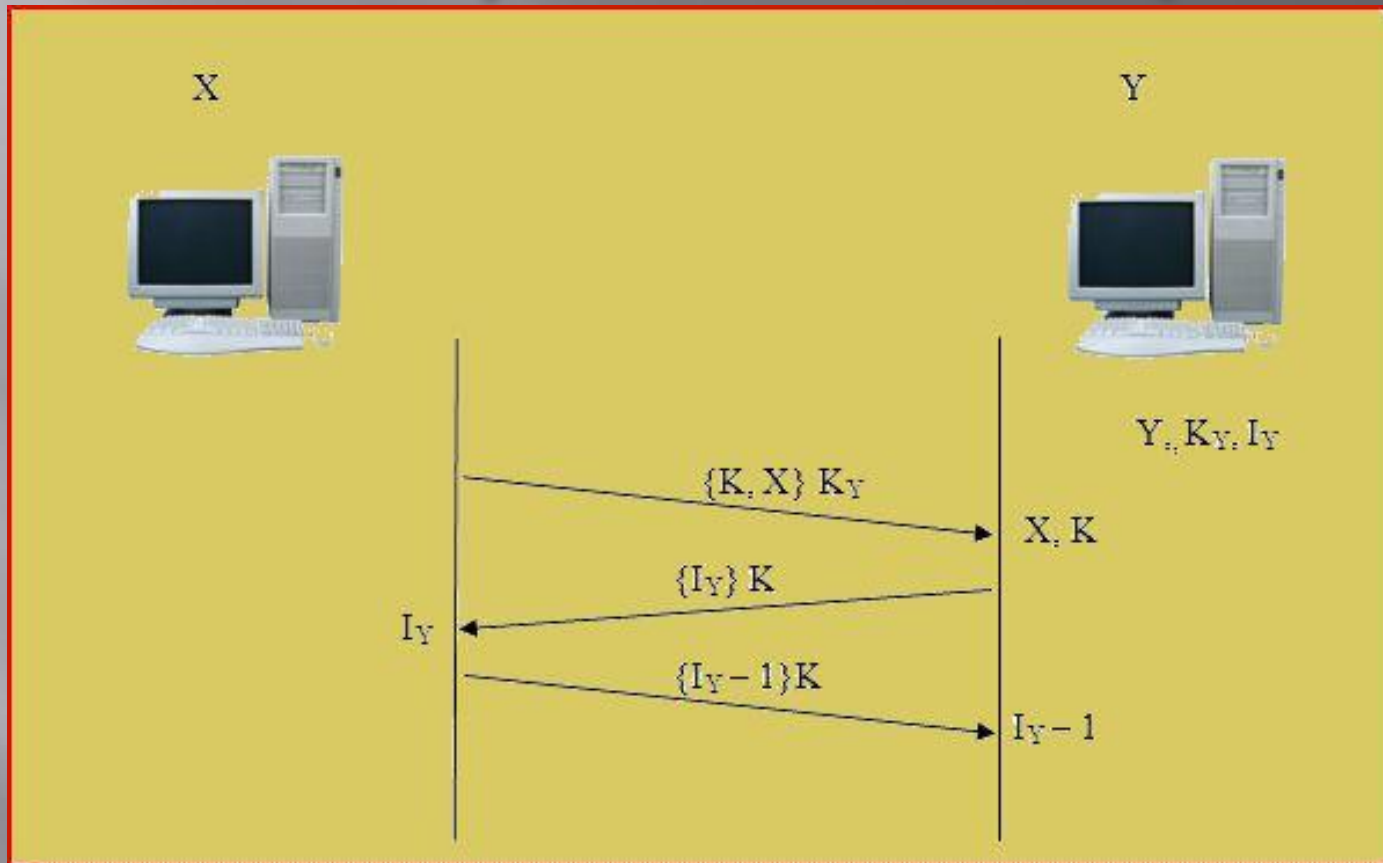
Key establishment is done through a third party.

Needham/Schroeder



Message	Definition
X	Identifier of Client X
Y	Identifier of Client Y
I_X	One time used identifier of X
I_Y	One time used identifier of Y
K_X	Private key of client X
K_Y	Private key of client Y
K	Private session key of X and Y

Needham/Schroeder (con't)

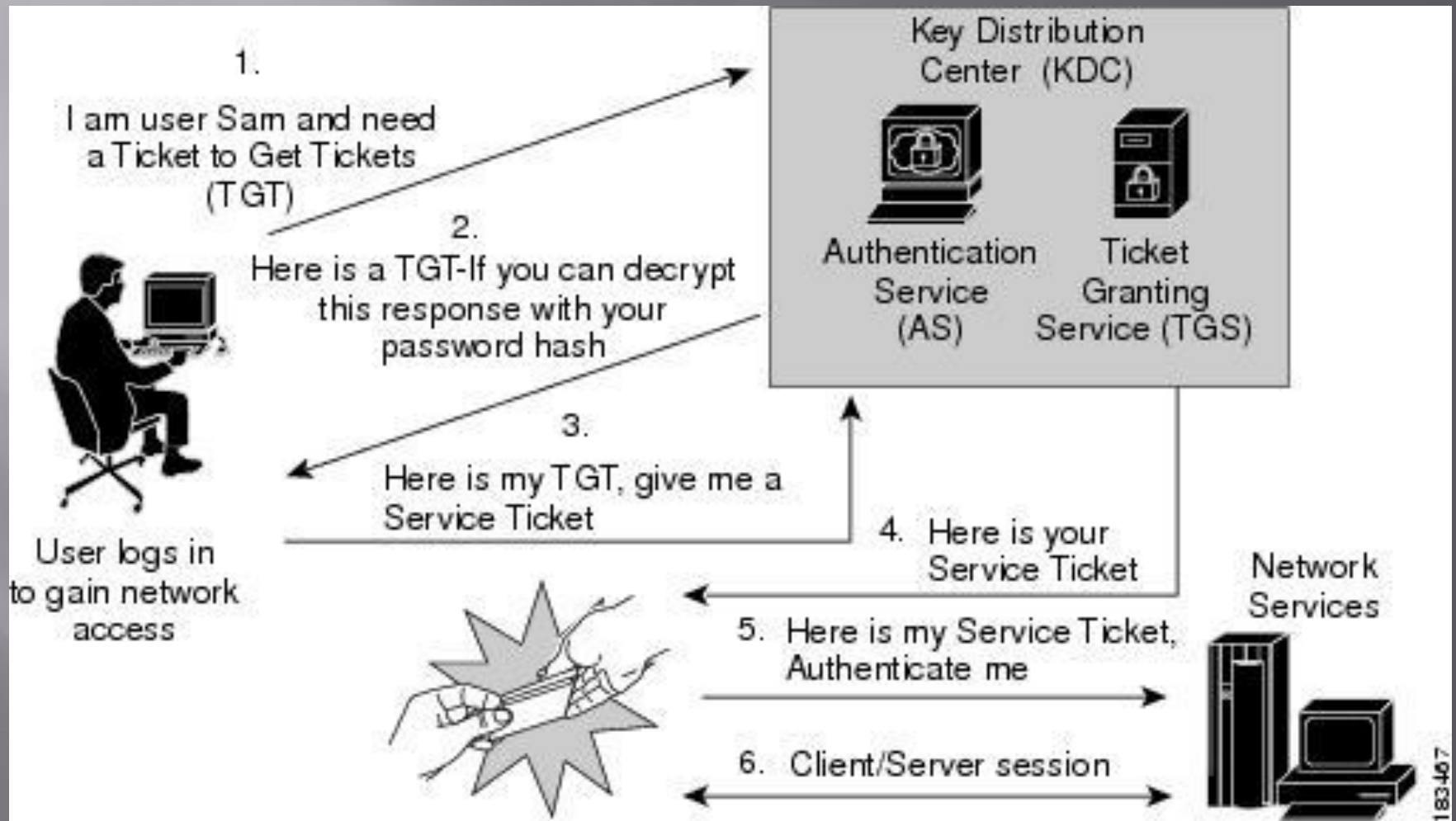


Message	Definition
X	Identifier of Client X
Y	Identifier of Client Y
I_X	One time used identifier of X
I_Y	One time used identifier of Y
K_X	Private key of client X
K_Y	Private key of client Y
K	Private session key of X and Y

Kerberos

- ▣ What is new?
 - Timestamp
 - TGS

Authentication (Ticket Exchange)



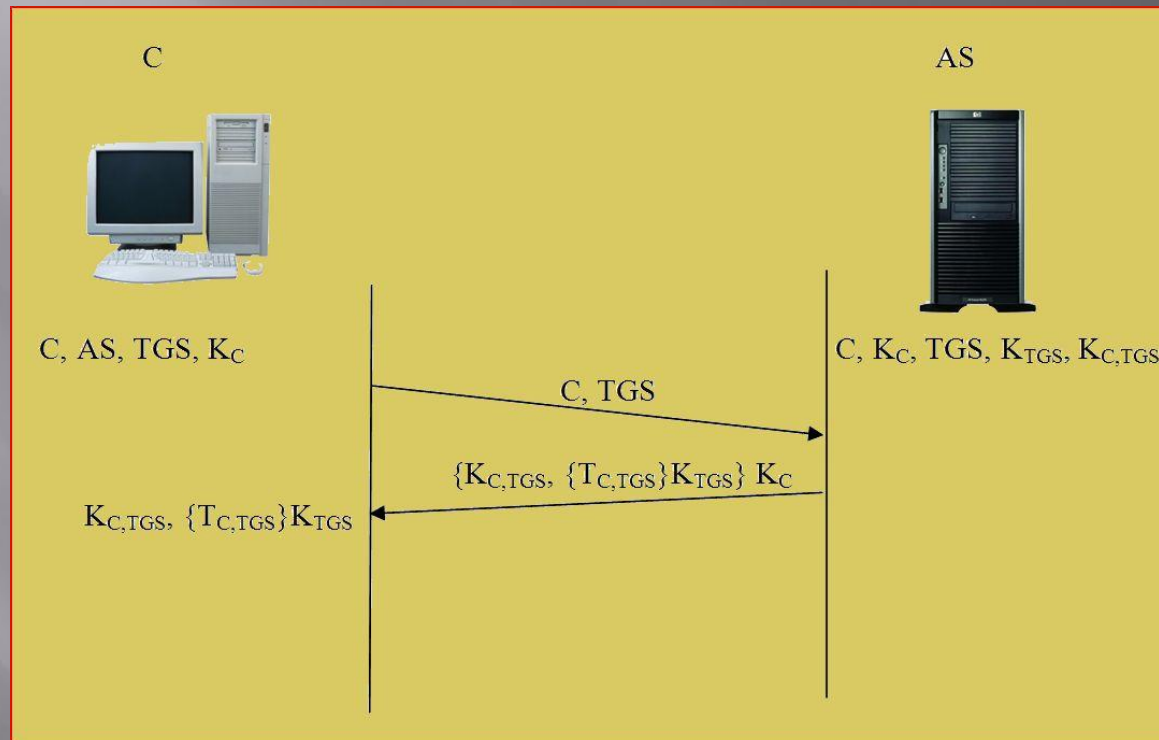
Implementation - Terminology

Term	Definition
Principle	Each entity that uses the Kerberos system
Client (C)	Entity that request service
Server (S)	Entity that provide service
Authentication Server (AS)	Kerberos server that provides initial authentication service
Ticket-granting Server (TGS)	Kerberos server that grants service tickets
Ticket ($T_{X,Y}$)	Identification credential for X to get service from Y
Authenticator (A_X)	One time identification credential generated by X
(K_X)	X's secret key
($K_{X,Y}$)	Session key for X and Y

Message Types

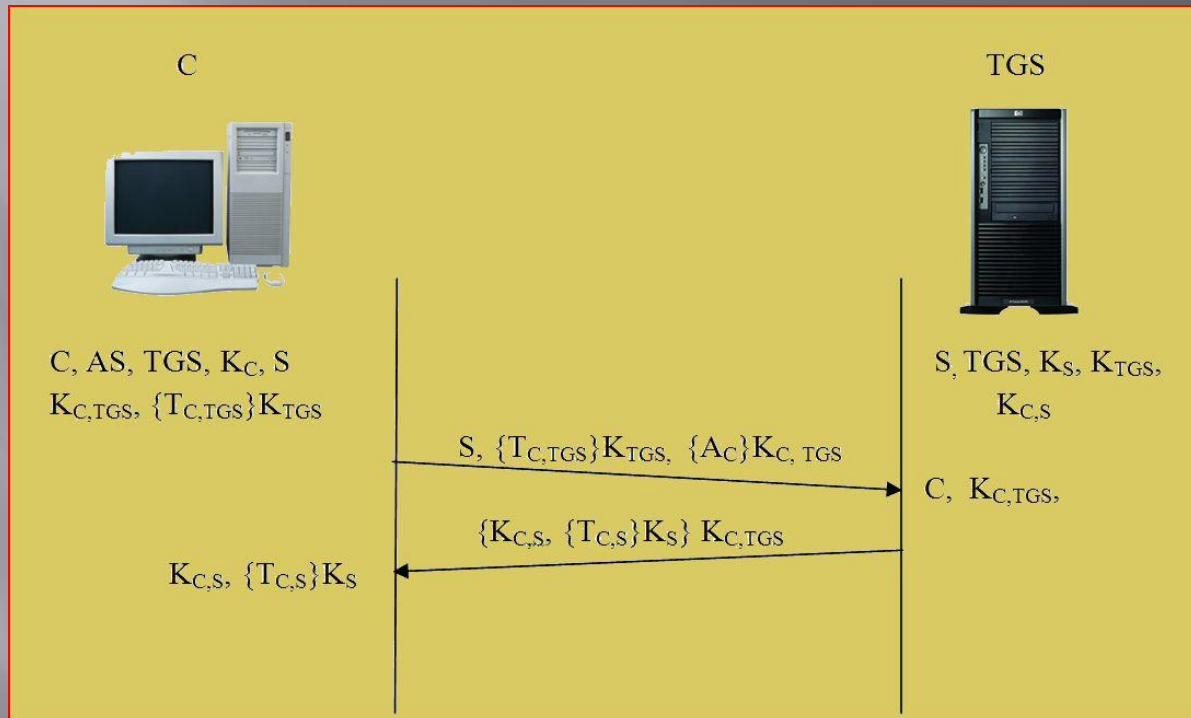
Session	Message types	Directions
The Authentication Service Exchange	KRB_AS_REQ	Client to AS
	KRB_AS_REP	AS to client
The Ticket Granting Service (TGS) Exchange	KRB_TGS_REQ	Client to TGS
	KRB_TGS_REP	TGS to Client
The Client/Server Authentication Exchange	KRB_AP_REQ	Client to Application server
	KRB_AP_REP	[optional] Application server to client

Authentication Service Exchange



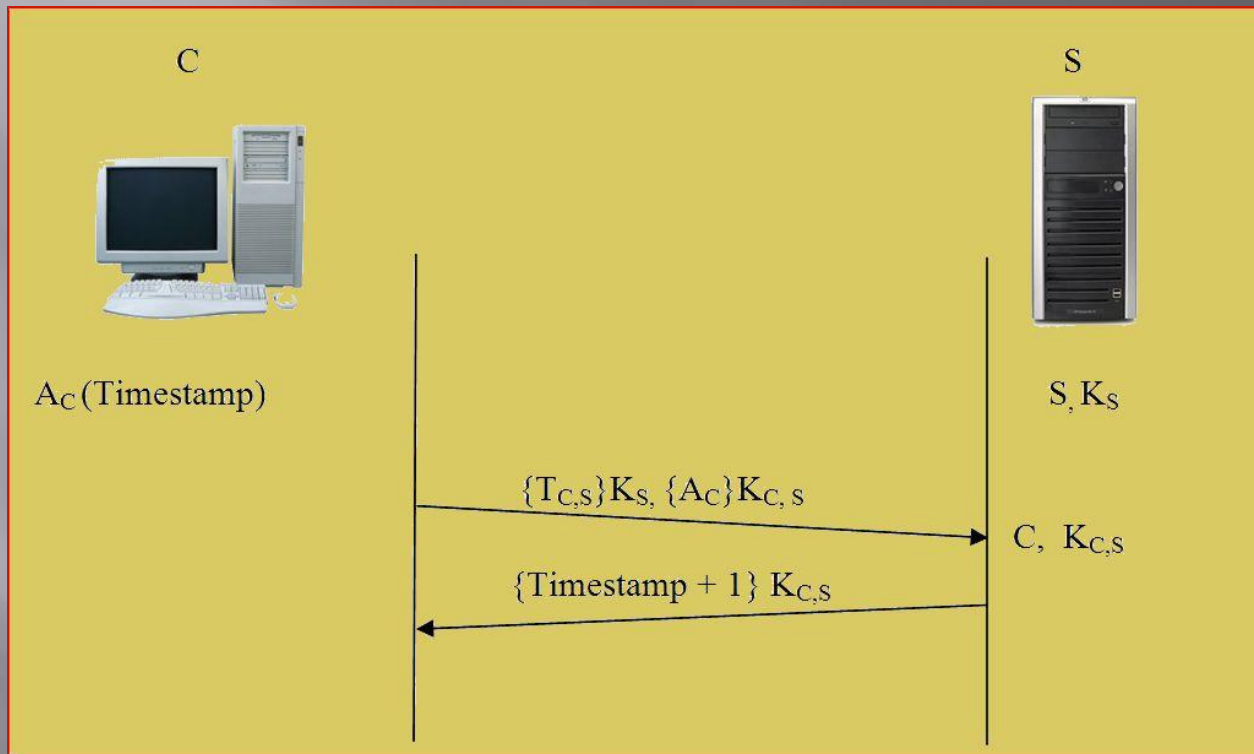
- Client authenticates to the AS once using a long-term shared secret password and receives a ticket from the AS

Ticket Granting Exchange



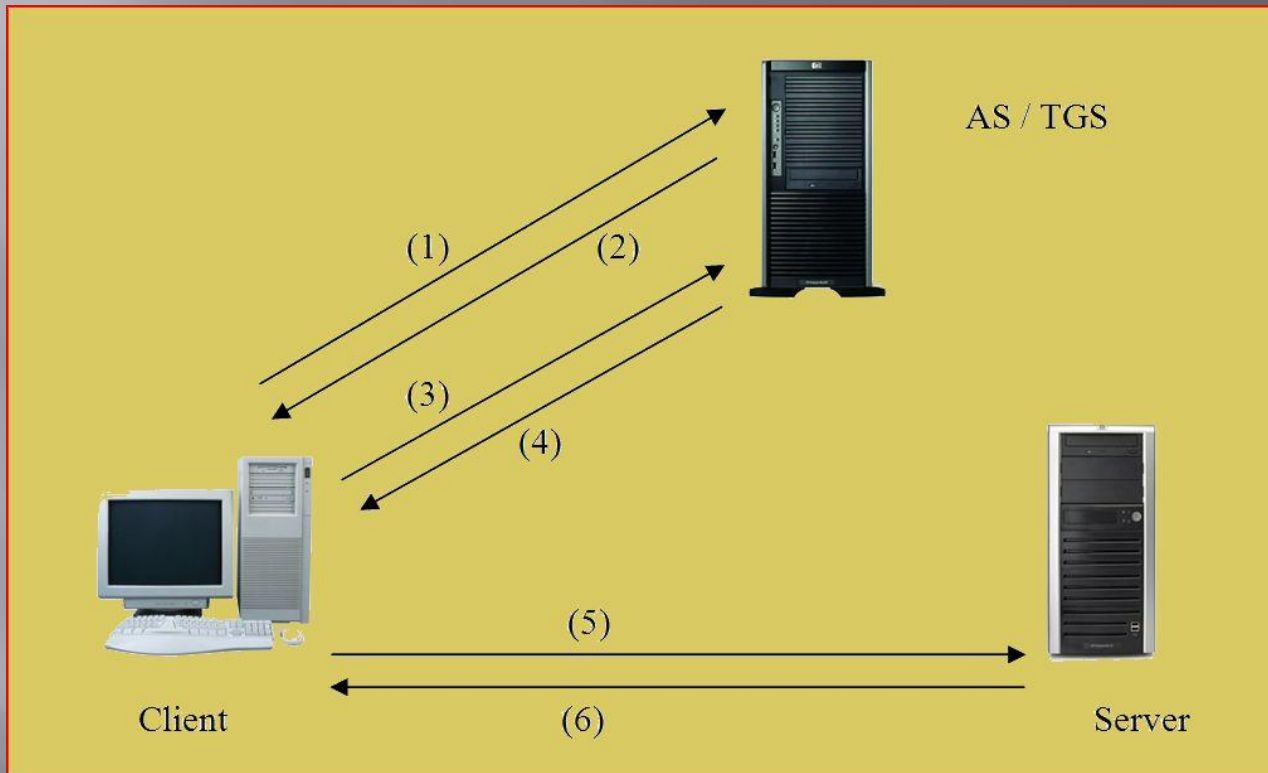
- Client sends the TGS a message composed of the TGT and the name of the requested service.
- The client also sends a message that contains the authenticator, usually a client ID and timestamp
- The TGS decrypts messages using a secret key and sends back a client to server ticket and a client/server session key that is encrypted with the client/TGS session key

Client – Server Exchange



- The client sends the client to server ticket and an authenticator to the Service Server.
- The server checks that everything has been completed correctly and provides the requested service.

Overall Sequence



Number	Message types	Directions
1	KRB_AS_REQ	Client to AS (Authentication Server)
2	KRB_AS_REP	AS to client
3	KRB_TGS_REQ	Client to TGS
4	KRB_TGS_REP	TGS to Client
5	KRB_AP_REQ	Client to Application server
6	KRB_AP_REP	[optional] Application server to client

Environmental Assumptions

- ▣ Applications must be tied into the protocol.
- ▣ "Denial of service" attacks are not solved with Kerberos.
- ▣ Principals must keep their secret keys secret
- ▣ "Password guessing" attacks are not solved by Kerberos.
- ▣ Each host on the network must have a clock which is "loosely synchronized" to the time of the other hosts.

IPSec

Functions and Features:

- ▣ Authentication (using Kerberos)
- ▣ Data integrity
- ▣ Anti-replay
- ▣ Key generation
- ▣ IP Packet filtering

Kerberos and IPSec

	IPSec	Kerberos
Authentication	computer-to-computer	user-to-service
Communications	transfer of IP packets	single log-in
OSI Layer	Network Layer	Application Layer

PKINIT

- ▣ Public Key based initial authentication in Kerberos
- ▣ Used by Microsoft, Cyber safe and Heimdal
- ▣ Uses CA
- ▣ Obviates the human users' burden to manage strong passwords
- ▣ Not recommended for Wireless Networks

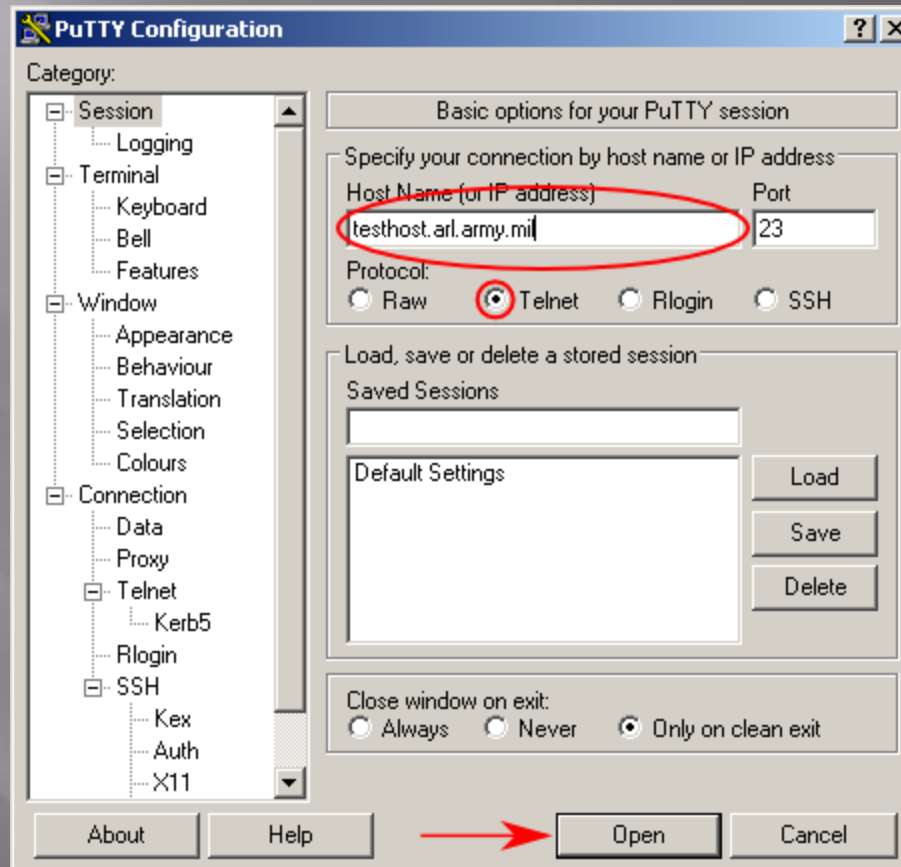
Kerberos in Wireless communications

- ▣ Susceptible, interception of data in transit and eavesdropping are very easy.
- ▣ W-Kerberos
- ▣ Energy consumption !

Kerberos in Real World Use

- ▣ Open Standard
- ▣ Microsoft
- ▣ Unix
- ▣ Oracle
- ▣ US army

Real World Use - Army HPC Access



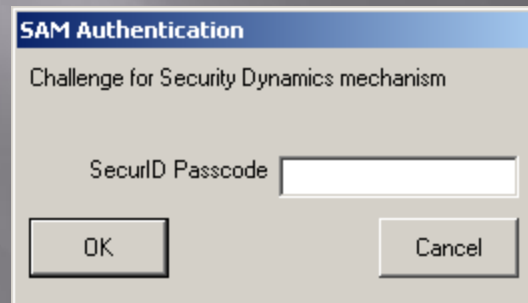
The client can access the server remotely.

HPC Access (con't)

The screenshot shows a window titled "Kerberos" with a menu bar containing "File" and "Help". Below the menu bar, there are three columns labeled "Start Time", "End Time", and "Ticket". A large text area below these columns contains the text "No Tickets". At the bottom of the window, there are three input fields: "Name" with the value "hinman", "Password" with a masked password "*****", and "Realm" with the value "HPCMP.HPC.MIL". Each of these three input fields is circled in red. Below the "Name" field is a "Change Password..." button, below the "Password" field is a "Delete" button, and below the "Realm" field is a "Login" button.

Client enters a username and password.

HPC Access (con't)



The image shows a Windows-style dialog box titled "SAM Authentication". The title bar is blue with the text "SAM Authentication" in white. Below the title bar, the text "Challenge for Security Dynamics mechanism" is displayed. In the center, there is a label "SecurID Passcode" followed by a white text input field. At the bottom of the dialog, there are two buttons: "OK" on the left and "Cancel" on the right.

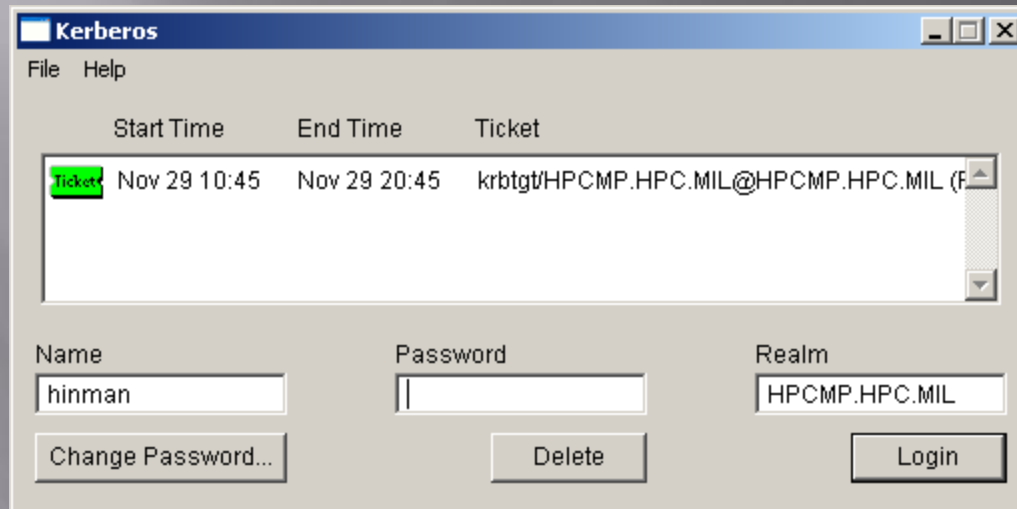
- A code from the SecurID card is entered.
- The TGS checks the client ID, password and SecurID password for validity.

SecurID Card



The SecurID authentication scheme adds in a hardware or software token that generates an authentication code at fixed intervals using a factory-encoded random key.

HPC Acces (con't)



- A ticket (including timestamp) is issued by the TGS. This is used by the service server when granting services to the client.

Other Authentication Protocols

- ▣ Challenge-Handshake Authentication Protocol (CHAP)
 - MS-CHAPv2
- ▣ NT LAN Manager (NTLM)
 - NTLMv2
- ▣ Wi-Fi Protected Access
 - WPA2
- ▣ Remote Authentication Dial In User Service (RADIUS)
- ▣ Diameter
- ▣ Secure Remote Password protocol (SRP)
- ▣ Protected Extensible Authentication Protocol (PEAP)
- ▣ Terminal Access Controller Access-Control System (TACACS)
 - TACACS+

NTLM

- ▣ NET LAN Manager
- ▣ Implemented by Microsoft
- ▣ Was default until Windows NT Server 4.0

Kerberos v.s NTLM in MS

	NTLM	Kerberos
Cryptographic Technology	Symmetric Key	Basic Kerberos: Symmetric Key Cryptography Kerberos PKINIT: Symmetric and Asymmetric Cryptography
Trusted third party	Domain Controller	Basic Kerberos: Domain controller with KDC service Kerberos PKINIT: domain controller with KDC service and Enterprise CA
Microsoft supported platform	Windows 95, Windows 98, Windows ME, Windows NT4, Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008	Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008
Features	Slower authentication because of pass-through authentication	Faster authentication because of unique ticketing system
	No mutual authentication	Mutual authentication
	No support for delegation of authentication	Support of authentication
	Proprietary: Microsoft authentication protocol	Open standard

Weaknesses of Kerberos

- ▣ Design Problems
 - Key Distribution Center (KDC) Vulnerability
 - ▣ Brute force attacks
 - ▣ Denial Of Service (DOS) attacks
- ▣ Protocol Problems
 - Ticket-stealing and replay attacks with multi-user client systems
- ▣ Implementation Problems
 - Client machines and service providers (servers) need to be designed with Kerberos in mind
 - Renewing tickets is a must for long-running processes