User Authentication Protocols

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-14/

Overview

1. Remote User Authentication Using Secret Keys
2. Kerberos V4
3. Kerberos V5
4. Remote User Authentication Using Public Keys
5. Federated Identity Management

These slides are based partly on Lawrie Brown's slides supplied with William Stallings's book "Cryptography and Network Security: Principles and Practice," 6th Ed, 2013.

User Authentication

- Four means of authenticating user's identity: Based on something the individual
  1. Knows - e.g., password, PIN
  2. Possesses - e.g., key, token, smartcard
  3. Is (static biometrics) - e.g., fingerprint, retina
  4. Does (dynamic biometrics) - e.g., voice, sign
- Can use alone or combined. All have issues
- May be one-way or mutual
- Key issues are
  - Confidentiality – to protect session keys
  - Timeliness – to prevent replay attacks

Ref: http://en.wikipedia.org/wiki/Mutual_authentication

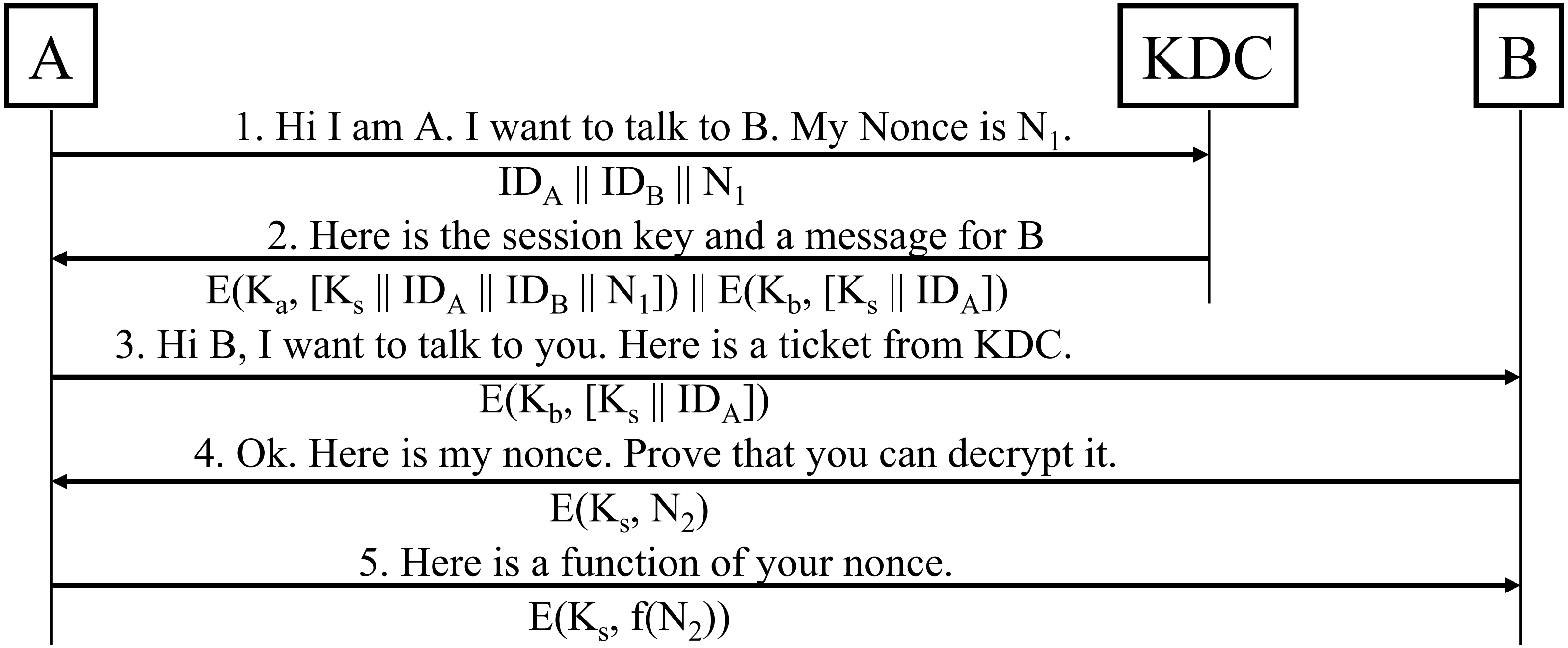
Replay Attacks

- A valid signed message is copied and later resent. Examples:
  - Simple replay: No timestamp
  - Repetition that can be logged: time stamped message within valid time
  - Repetition that cannot be detected: Original message replaced with a new message
  - Backward replay without modification: Source's message back to the source
- Countermeasures include
  - Use of sequence numbers (generally impractical)
  - Timestamps (needs synchronized clocks)
  - Challenge/response (using unique nonce)

Ref: http://en.wikipedia.org/wiki/Replay_attack, http://en.wikipedia.org/wiki/Reflection_attack

Needham Schroeder Protocol

- Everyone has a shared secret key with KDC
- KDC generates session keys



A

KDC

B

1. Hi I am A. I want to talk to B. My Nonce is N_1.

$ID_A \| ID_B \| N_1$

2. Here is the session key and a message for B

$E(K_a, [K_s \| ID_A \| ID_B \| N_1]) \| E(K_b, [K_s \| ID_A])$

3. Hi B, I want to talk to you. Here is a ticket from KDC.

$E(K_b, [K_s \| ID_A])$

4. Ok. Here is my nonce. Prove that you can decrypt it.

$E(K_s, N_2)$

5. Here is a function of your nonce.

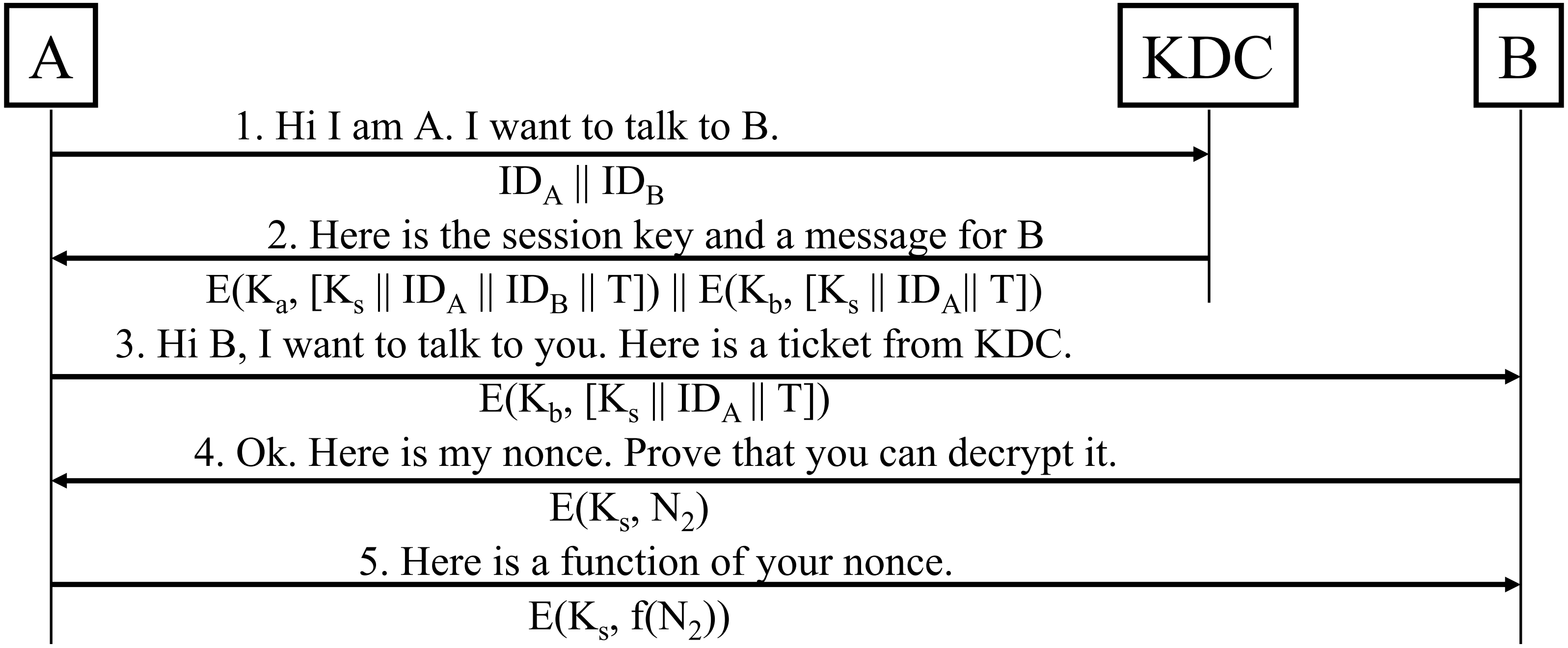
$E(K_s, f(N_2))$

- If someone can crack one K_S, he can replay 3, block 4. Then masquerade as A.

Ref: http://en.wikipedia.org/wiki/Needham%E2%80%93Schroeder_protocol

Denning's Modification

- Include timestamps



A

KDC

B

1. Hi I am A. I want to talk to B.

$ID_A \| ID_B$

2. Here is the session key and a message for B

$E(K_a, [K_s \| ID_A \| ID_B \| T]) \| E(K_b, [K_s \| ID_A\| T])$

3. Hi B, I want to talk to you. Here is a ticket from KDC.

$E(K_b, [K_s \| ID_A \| T])$

4. Ok. Here is my nonce. Prove that you can decrypt it.

$E(K_s, N_2)$

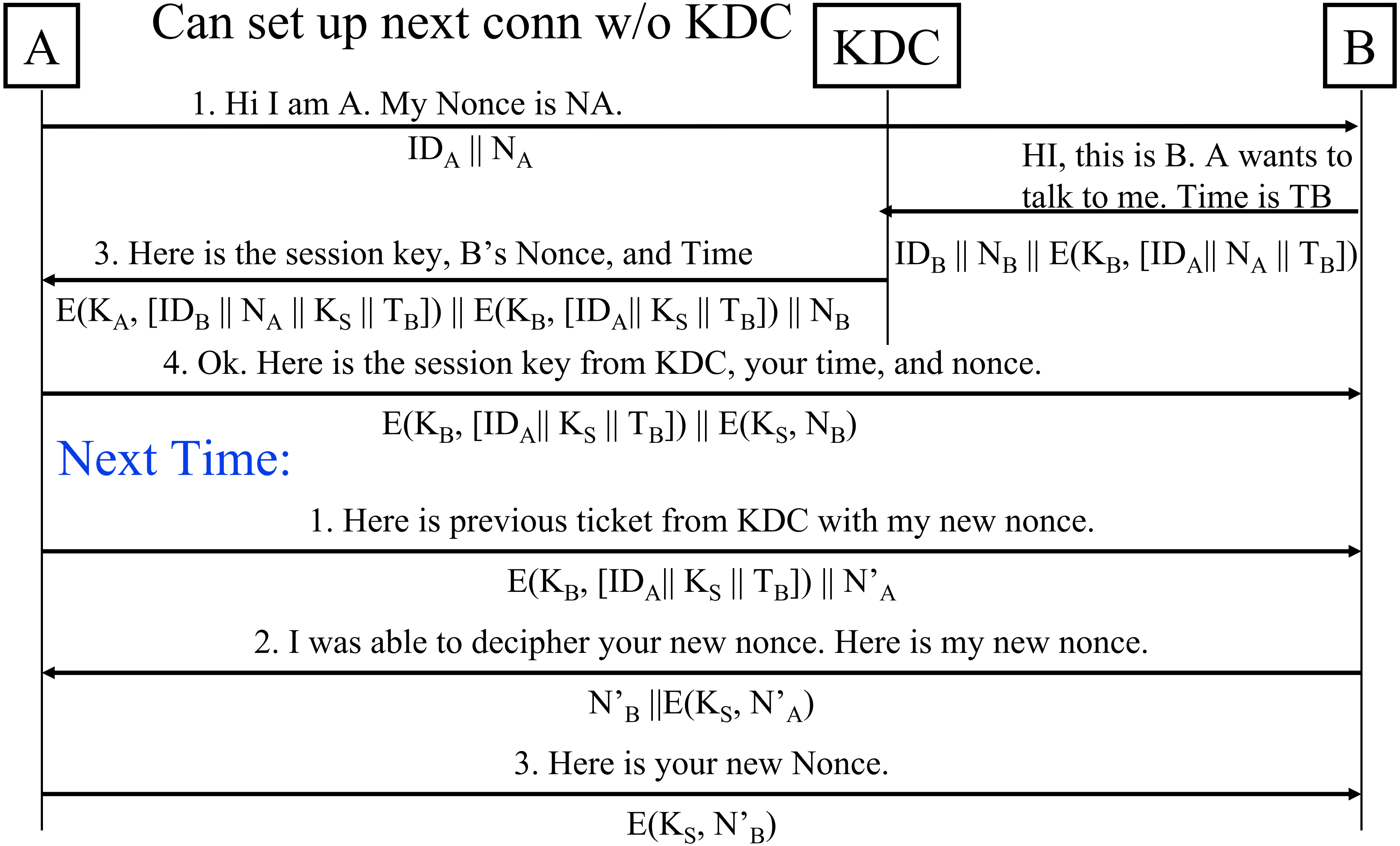
5. Here is a function of your nonce.

$E(K_s, f(N_2))$

- Needs synchronized clocks.

Corrected Protocol

- Include timestamps and nonce.
  Can set up next conn w/o KDC



1. Hi I am A. My Nonce is NA.

$ID_A \| N_A$

HI, this is B. A wants to talk to me. Time is TB

$ID_B \| N_B \| E(K_B, [ID_A \| N_A \| T_B])$

3. Here is the session key, B's Nonce, and Time

$E(K_A, [ID_B \| N_A \| K_S \| T_B]) \| E(K_B, [ID_A \| K_S \| T_B]) \| N_B$

4. Ok. Here is the session key from KDC, your time, and nonce.

$E(K_B, [ID_A \| K_S \| T_B]) \| E(K_S, N_B)$

Next Time:

1. Here is previous ticket from KDC with my new nonce.

$E(K_B, [ID_A \| K_S \| T_B]) \| N'_A$

2. I was able to decipher your new nonce. Here is my new nonce.

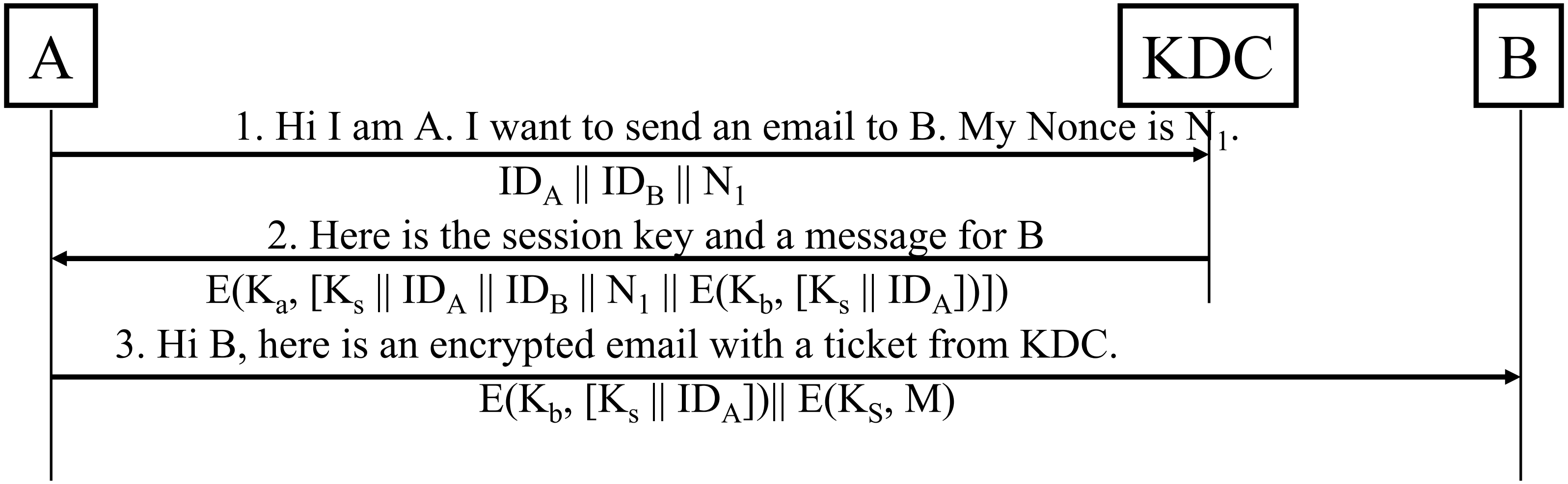
$N'_B \| E(K_S, N'_A)$

3. Here is your new Nonce.

$E(K_S, N'_B)$

One-Way Authentication for Email

- B is not up, when A wants to send email


A
KDC
B
1. Hi I am A. I want to send an email to B. My Nonce is N_1.
$ID_A \| ID_B \| N_1$
2. Here is the session key and a message for B
$E(K_a, [K_s \| ID_A \| ID_B \| N_1 \| E(K_b, [K_s \| ID_A])])$
3. Hi B, here is an encrypted email with a ticket from KDC.
$E(K_b, [K_s \| ID_A])\| E(K_S, M)$

- Only B can read the message.
- Authenticates that A sent the message.

Ref: http://en.wikipedia.org/wiki/E-mail_authentication

Overview of Kerberos

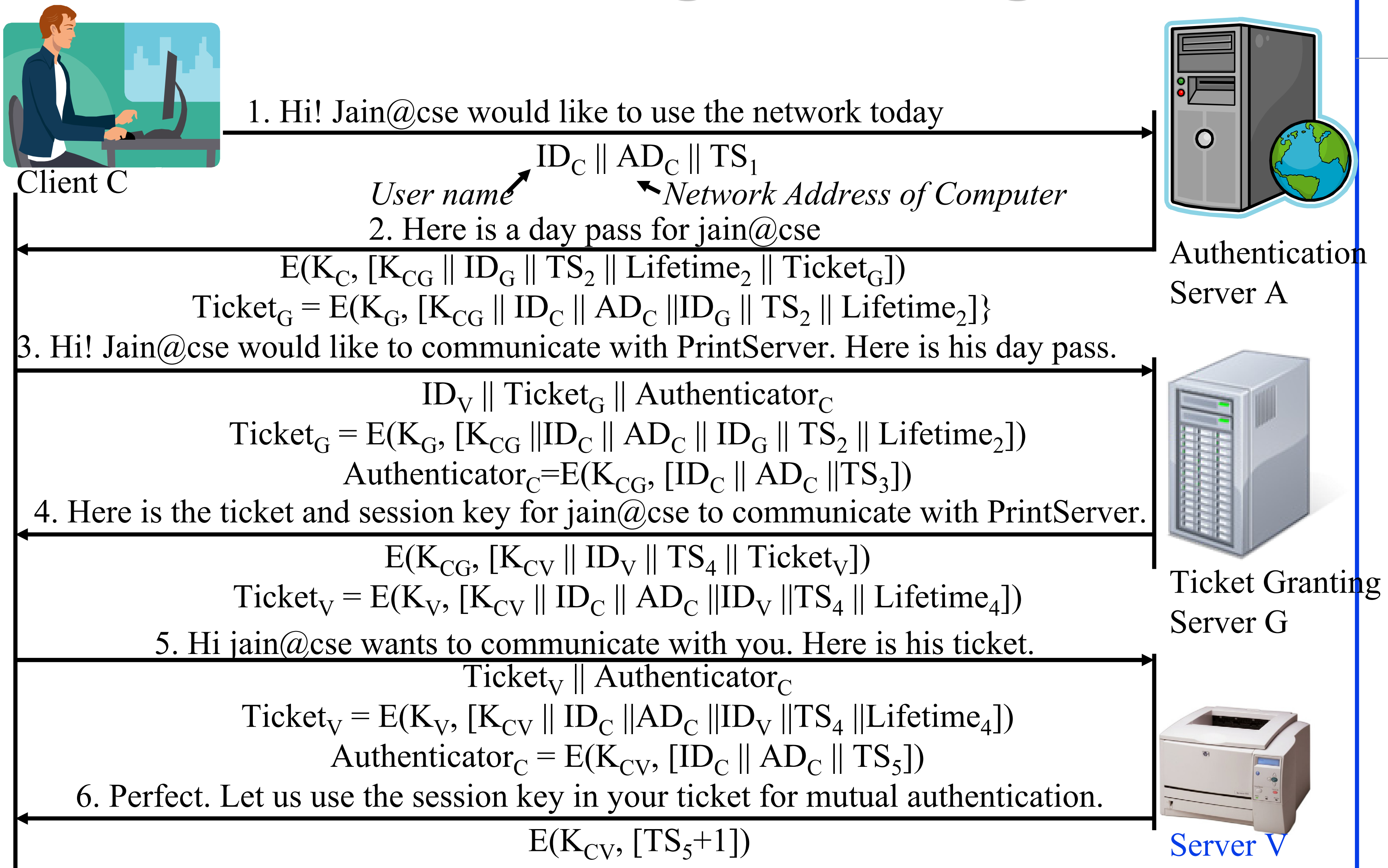
- Allows two users (or client and server) to authenticate each other over an insecure network
- Named after the Greek mythological character *Kerberos* (or *Cerberus*), known in Greek mythology as being the *monstrous three-headed guard dog of Hades*
- Designed originally for Project Athena at M.I.T.
- Implementation freely available from M.I.T.
- V5 is an Internet Standard (RFC 4120)
- Windows 2000/XP/Server 2003/Vista use Kerberos as their default authentication mechanism
- Apple's Mac OS X clients and servers also use Kerberos
- Apache HTTP Server, Eudora, NFS, OpenSSH, rcp (remote copy), rsh, X window system allow using Kerberos for authentication.

Overview (Cont)

- Protects against eavesdropping and replay attacks
- Uses a trusted third party (Authentication Server) and symmetric key cryptography
- First 3 versions are no longer in use.
- V5 is a generalization of V4 with several problems fixed and additional features.
- It is easier to understand V5 if you know V4
- Learn V4's features and mistakes

Ref: http://en.wikipedia.org/wiki/Kerberos_(protocol)

Kerberos V4 Message Exchange



1. Hi! Jain@cse would like to use the network today

$ID_C \| AD_C \| TS_1$

User name *Network Address of Computer*

2. Here is a day pass for jain@cse

$E(K_C, [K_{CG} \| ID_G \| TS_2 \| \text{Lifetime}_2 \| \text{Ticket}_G])$

$\text{Ticket}_G = E(K_G, [K_{CG} \| ID_C \| AD_C \| ID_G \| TS_2 \| \text{Lifetime}_2]\}$

3. Hi! Jain@cse would like to communicate with PrintServer. Here is his day pass.

$ID_V \| \text{Ticket}_G \| \text{Authenticator}_C$

$\text{Ticket}_G = E(K_G, [K_{CG} \| ID_C \| AD_C \| ID_G \| TS_2 \| \text{Lifetime}_2])$

$\text{Authenticator}_C = E(K_{CG}, [ID_C \| AD_C \| TS_3])$

4. Here is the ticket and session key for jain@cse to communicate with PrintServer.

$E(K_{CG}, [K_{CV} \| ID_V \| TS_4 \| \text{Ticket}_V])$

$\text{Ticket}_V = E(K_V, [K_{CV} \| ID_C \| AD_C \| ID_V \| TS_4 \| \text{Lifetime}_4])$

5. Hi jain@cse wants to communicate with you. Here is his ticket.

$\text{Ticket}_V \| \text{Authenticator}_C$

$\text{Ticket}_V = E(K_V, [K_{CV} \| ID_C \| AD_C \| ID_V \| TS_4 \| \text{Lifetime}_4])$

$\text{Authenticator}_C = E(K_{CV}, [ID_C \| AD_C \| TS_5])$

6. Perfect. Let us use the session key in your ticket for mutual authentication.

$E(K_{CV}, [TS_5+1])$

Kerberos V4 Concepts

- **Authentication Server (AS):** Physically secure node with complete authentication database
- **Principal**: Authentication Server A, Ticket Granting Server G, Client (Computer) C, User (Human) U, Server V
- **Ticket Granting Server (TGS)**
- **Keys**: K_{cg}, K_{cv}, K_{ag}, K_{u}, K_{gv}
- **Ticket**: Encrypted information. All current V4 implementations use DES.
- **Ticket Granting Ticket (TGT):** Allows user to get tickets from TGS

Concepts (Cont)

- **Authenticator**: Name and time encrypted with a session key. Sent from client to server with the ticket and from server to client.
- **Credentials**: Session key + Ticket
- User enters a name and password. Client converts the password to a key K_u.
- TGT and the session key are good for a limited time (21 hours).

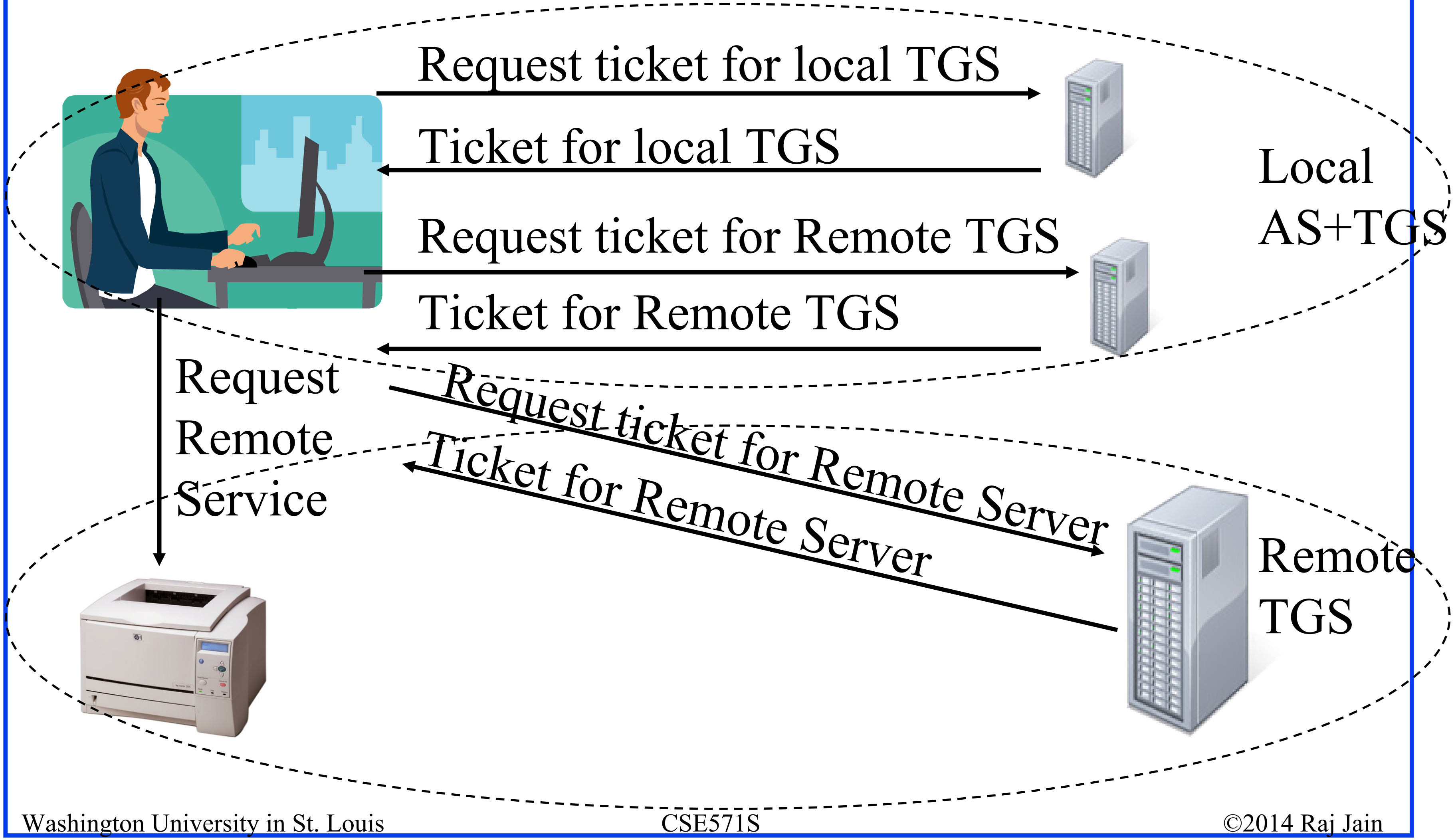
Key Design Principles

1. The network is open ⇒ Need a proper secret key to understand the messages received
(except message 1, which is in clear)
2. Every client and server has a pre-shared secret with the AS.
3. AS and Ticket Granting Server (TGS) are logically separate but share a secret key
4. Both AS and TGS are stateless and do not need to remember the permissions granted. All the state is in the tickets. (Day pass is just a longer term ticket)
5. Longer term secrets are used less frequently. Short term secrets are created and destroyed after a limited use.

Ref: http://en.wikipedia.org/wiki/Ticket_Granting_Ticket

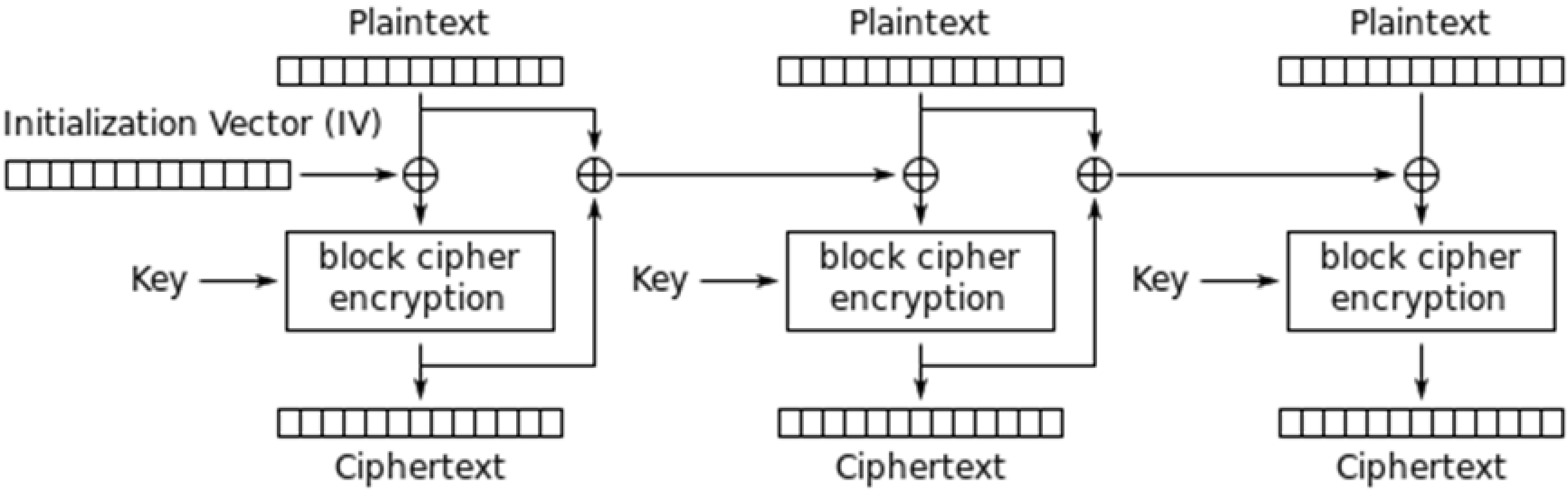
Inter-Realm Authentication

- Realm: One AS and its clients and servers



Privacy and Integrity

- Kerberos V4 uses an extension to CBC
- With CBC, only two blocks are affected by a change.
- **Propagating Cipher Block Chaining** (PCBC) causes all blocks to change.



Source: Wikipedia

Ref: http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Kerberos V4 Issues

1. Names, Instance, Realm (non standard). Limited to 40 Char.
2. Only DES encryption. Not strong.
3. Only IPv4 addresses. No IPv6 or ISO CLNP addresses.
4. Byte ordering indicated in the message (ASN.1 better)
5. Maximum life time limited to 21 hours: 8 bit life time in units of 5 minutes
6. No delegation. A server cannot access another server on behalf of the client.
7. Inter-realm authentication limited to pairs ⇒ N^2 pairs
8. Double encryption of the ticket: $K_{client}[K_{server}[\ldots]]$
9. Propagating Cipher Block Chaining (PCBC) does not detect interchange of cipher blocks
10. No subsession keys for long sessions
11. Brute force password attack

ASN.1

- Abstract Syntax Notation One
- Joint ISO and ITU-T standard, Original 1984, latest 2008.
- Used to specify protocol data structures
- X.400 electronic mail, X.500 and LDAP directory services, H.323 VOIP, SNMP, etc use ASN.1
- Pre-Defined: 1=Boolean, 2=Integer, 3=Bit String, 4=Octet String, 5=Null, 6=Object Identifier, 9=Real
- Constructed: SEQUENCE (structure), SEQUENCE OF (lists), CHOICE, ...

Ref: http://en.wikipedia.org/wiki/Abstract_Syntax_Notation_One

ASN.1 Example

```
AddressType ::= SEQUENCE {
name        OCTET STRING,
number      INTEGER,
street      OCTET STRING,
city        OCTET STRING,
state       OCTET STRING,
zipCode     INTEGER
}
```

Encoding Rules

- ASN.1 only specifies the structure.
- Encoding rules indicate how to encode the structure in to bits on the wire.
- Examples: Basic Encoding Rules (BER), Packed Encoding Rules (PER), XML Encoding rules (XER), Distinguished Encoding Rules (DER), ...
- In BER, everything is encoded as Tag-Length-Value.

BER Example

- John Miller, 126 Main Street, Big City, MO 63130

30	2F	04	0B	4A	6F	68	6E	20	4D	69	6C	6C	65	72
Seq.	Len	Oct Str	Len	J	o	h	n		M	i	l	l	e	r

02	01	7E
Int	Len	126

04	0B	4D	61	69	6E	20	53	74	72	65	65	74
Oct str	Len	M	a	i	n		S	t	r	e	e	t

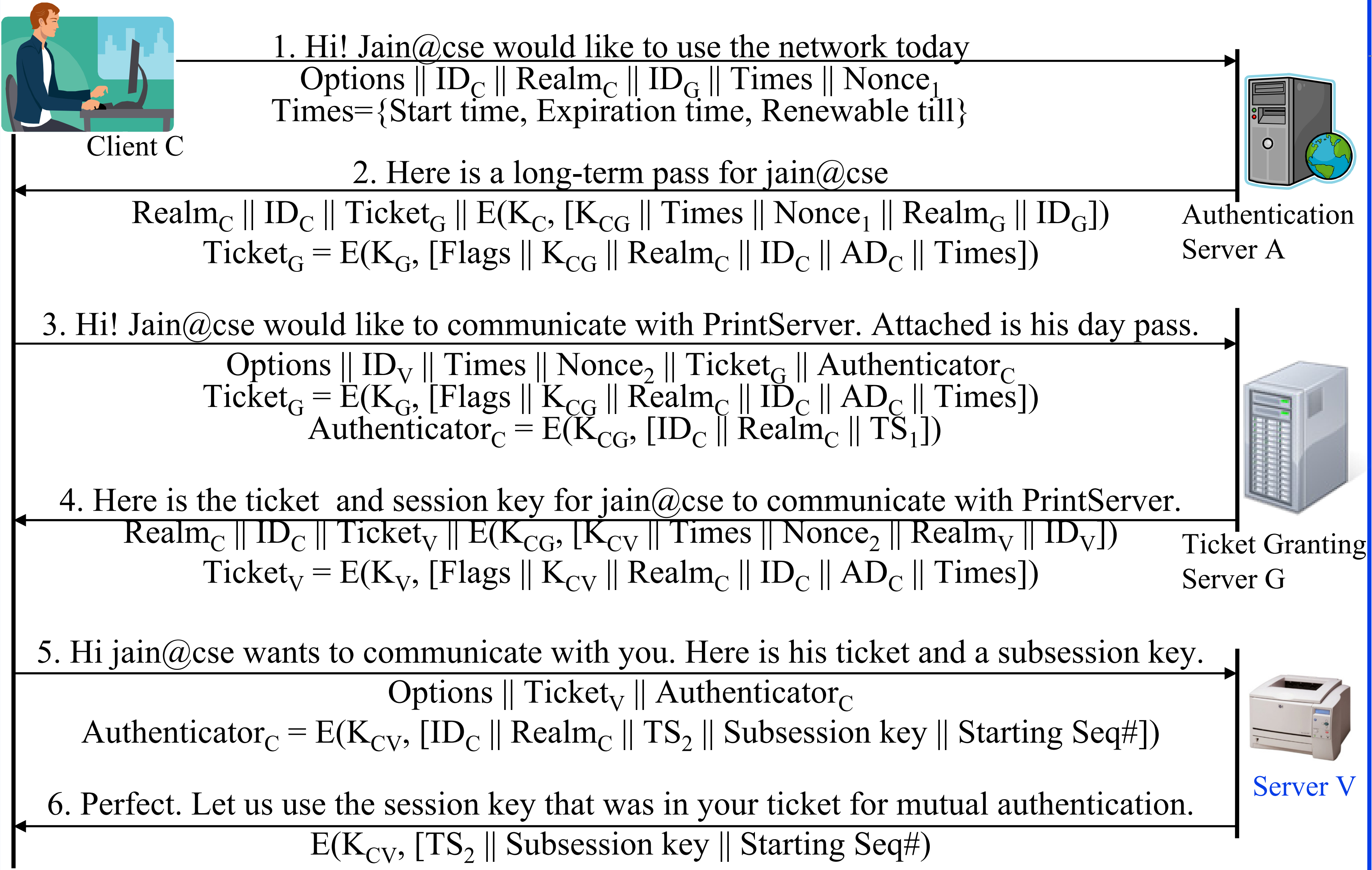
04	08	42	69	67	20	43	69	74	79
Oct Str	Len	B	i	g		C	i	t	y

04	02	4D	4F	02	02	F6	9A	0
Oct Str	Len	M	O	Int	len	63130		Null

Kerberos V5

1. Names, Instance, Realm have ASN.1 names. Can be any length.
2. Any encryption. Encryption scheme coded.
3. Any type of addresses. Address type specified.
4. ASN.1 Byte ordering
5. Explicit Start time and End time. Can have arbitrary life times.
6. Delegation possible by requesting proxy able tickets.
7. Inter-realm authentication hierarchy
8. No Double encryption of the ticket
9. Explicit integrity mechanism detects block interchange
10. Subsession keys for long sessions
11. Password attack made difficult by a pre-authentication mechanism

Kerberos V5 Messages



Client C

1. Hi! Jain@cse would like to use the network today

Options || ID_C || $Realm_C$ || ID_G || Times || $Nonce_1$

Times={Start time, Expiration time, Renewable till}

Authentication Server A

2. Here is a long-term pass for jain@cse

$Realm_C$ || ID_C || $Ticket_G$ || E(K_C, [K_{CG} || Times || $Nonce_1$ || $Realm_G$ || ID_G])

$Ticket_G$ = E(K_G, [Flags || K_{CG} || $Realm_C$ || ID_C || AD_C || Times])

3. Hi! Jain@cse would like to communicate with PrintServer. Attached is his day pass.

Options || ID_V || Times || $Nonce_2$ || $Ticket_G$ || $Authenticator_C$

$Ticket_G$ = E(K_G, [Flags || K_{CG} || $Realm_C$ || ID_C || AD_C || Times])

$Authenticator_C$ = E(K_{CG}, [ID_C || $Realm_C$ || TS_1])

Ticket Granting Server G

4. Here is the ticket and session key for jain@cse to communicate with PrintServer.

$Realm_C$ || ID_C || $Ticket_V$ || E(K_{CG}, [K_{CV} || Times || $Nonce_2$ || $Realm_V$ || ID_V])

$Ticket_V$ = E(K_V, [Flags || K_{CV} || $Realm_C$ || ID_C || AD_C || Times])

5. Hi jain@cse wants to communicate with you. Here is his ticket and a subsession key.

Options || $Ticket_V$ || $Authenticator_C$

$Authenticator_C$ = E(K_{CV}, [ID_C || $Realm_C$ || TS_2 || Subsession key || Starting Seq#])

Server V

6. Perfect. Let us use the session key that was in your ticket for mutual authentication.

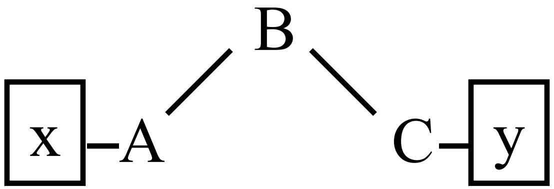
E(K_{CV}, [TS_2 || Subsession key || Starting Seq#)

Kerberos V5 Flags

- **Initial**: Ticket issued by AS (not by TGT)
- **Pre-Authent**: The client was pre-authenticated by AS before a ticket was issued
- **HW-Authent**: Pre-authenticated using hardware (e.g., smart card) possessed solely by name client
- **Renewable**: TGS can issue a new ticket that expires at a later date. Allows long life time.
- **May-Postdate**: TGS can issue a post-dated ticket
- **Postdated**: This ticket is postdated. Check authentication time field for original authentication time

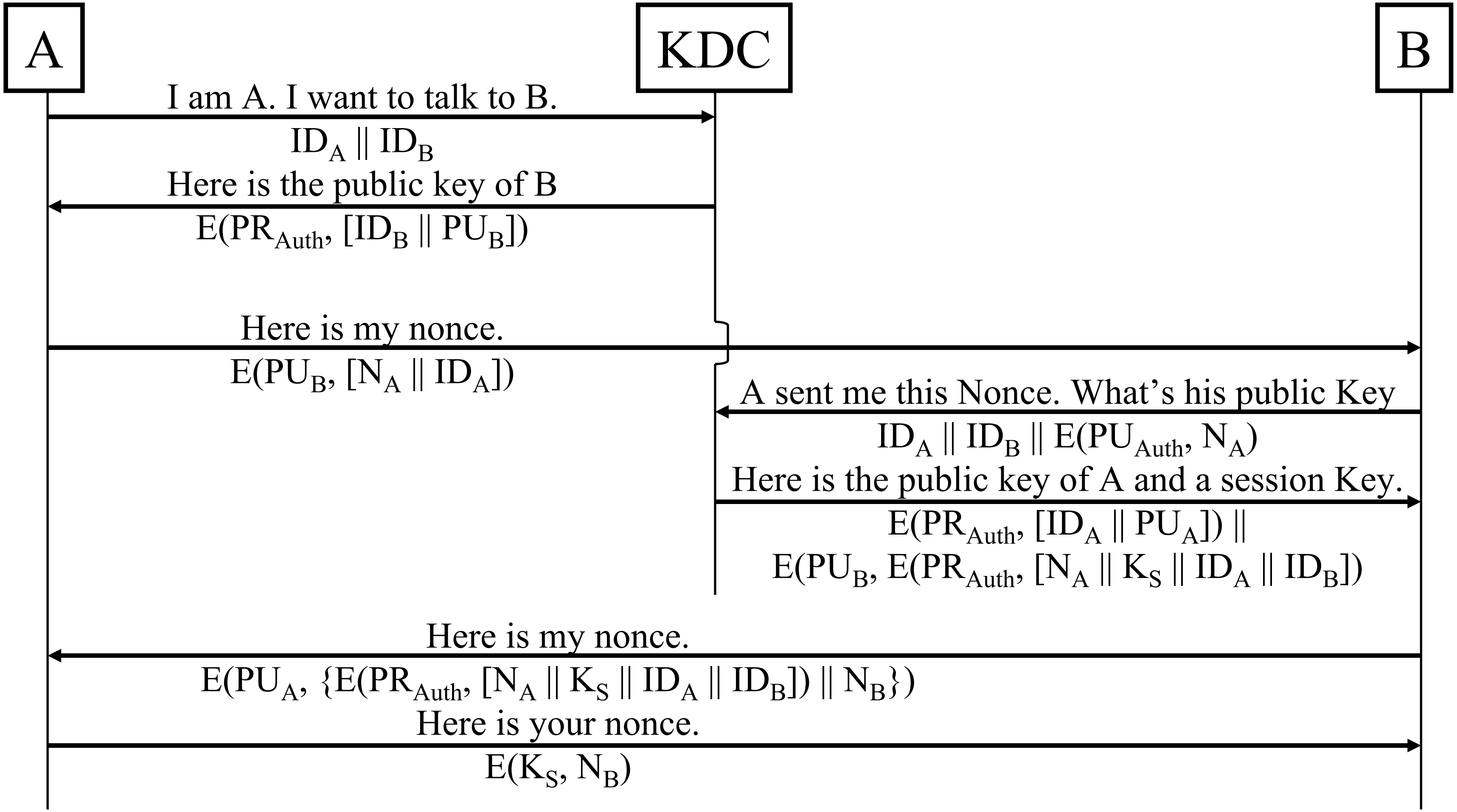
Kerberos V5 Flags (Cont)

- **Invalid**: This ticket is invalid and must be validated by TGS before use. Used with postdated tickets.
- **Proxiable**: TGS can issue a new service granting ticket with a different network address
- **Proxy**: Indicates that this ticket is a proxy
- **Forwardable**: TGS can issue a ticket with a different address for use in a different realm.
- **Forwarded**: This ticket has been forwarded or was issued based on a forwardable TGT. x@A can get to y@C via B. List of all transited realms is put in the ticket.



Remote User Authentication Using Public Keys

- KDC can be used to provide public keys for mutual authentication



A

KDC

B

I am A. I want to talk to B.

$ID_A \| ID_B$

Here is the public key of B

$E(PR_{Auth}, [ID_B \| PU_B])$

Here is my nonce.

$E(PU_B, [N_A \| ID_A])$

A sent me this Nonce. What's his public Key

$ID_A \| ID_B \| E(PU_{Auth}, N_A)$

Here is the public key of A and a session Key.

$E(PR_{Auth}, [ID_A \| PU_A]) \|$

$E(PU_B, E(PR_{Auth}, [N_A \| K_S \| ID_A \| ID_B])$

Here is my nonce.

$E(PU_A, \{E(PR_{Auth}, [N_A \| K_S \| ID_A \| ID_B]) \| N_B\})$

Here is your nonce.

$E(K_S, N_B)$

Remote User Authentication Using Public Keys (Cont)

One-Way Authentication: Required for Email

- Can use public keys for encryption and authentication
- Long message ⇒ Computation complexity
- For encryption, better to use a secret key and send the secret key using public key

$$A \rightarrow B: E(PU_B, K_S)||E(K_S, M)$$

- For authentication, use a digital signature

$$A \rightarrow B: M \,||\, E(PR_A, H(M))$$

Note: Someone else can replace the signature
⇒Encrypt the message and signature:

$$A \rightarrow B: E(PU_B, [M \,||\, E(PR_A, H(M))])$$

- Recipient B must know A's public key
⇒ A can send its certificate with the message

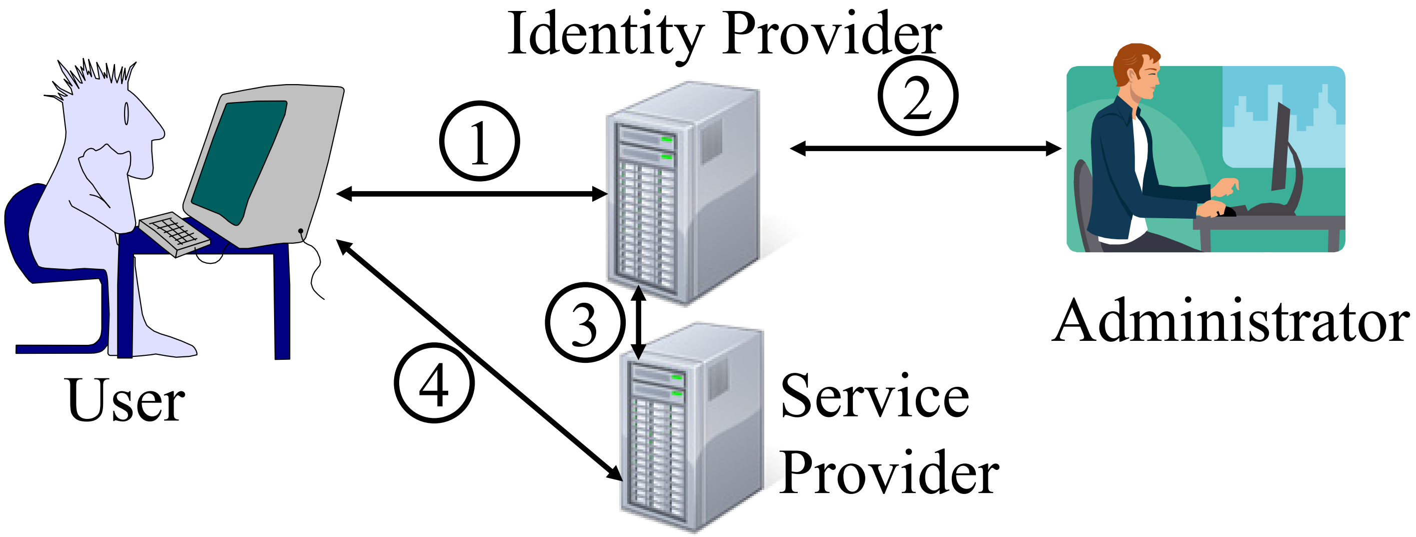
Federated Identity Management

- Generalization of **Single-Sign on**
- User is authenticated once and then can use resources at other partner organizations across multiple security domains
- Examples:
  - Employees accessing purchasing sites
  - Health insurance providers
  - Purchasing sites to shipping sites
- Identity Management is more general than authentication
  - Authentication, authorization, accounting, provisioning, workflow automation, delegated administration, password synchronization, self-service password reset, federation
- Kerberos contains many of these elements

Ref: http://en.wikipedia.org/wiki/Federated_identity, http://en.wikipedia.org/wiki/Federated_identity_management, http://en.wikipedia.org/wiki/Identity_management, http://en.wikipedia.org/wiki/Category:Identity_management_systems

Federated Identity Operation

1. End user authenticates with the identity provider, e.g., Facebook
2. Administrator associates attributes with each user or each role
3. Identity provider passes the id, attributes, and authentication to service provider
4. Service provider opens session with the user



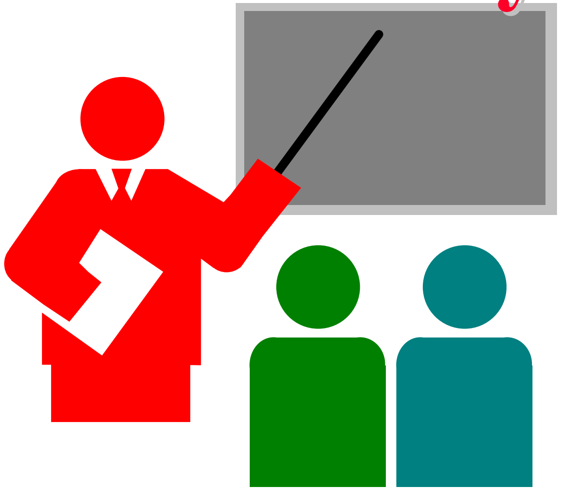
Ref: http://en.wikipedia.org/wiki/Identity_Assurance_Framework

Standards for Federated ID Management

- Security Assertion Markup Language (SAML)
  - XML-based language for exchange of security information between online business partners
- Part of OASIS (Organization for the Advancement of Structured Information Standards) standards for federated identity management

Ref: http://en.wikipedia.org/wiki/SAML, http://en.wikipedia.org/wiki/Web_Single_Sign-On_Metadata_Exchange_Protocol http://en.wikipedia.org/wiki/OpenID

Summary



- Kerberos is a symmetric key authentication system. Uses Authentication Server and ticket granting server.
- Kerberos V4 is widely deployed. V5 generalizes the design. Generalized ASN.1 names, General encryption, addresses, names. Allows delegation, post-dated tickets, renewals, Inter-realm authentication
- Federated identity management allows users to authenticate once and use resources on other partner organizations.
- Security Assertion Markup Language (SAML) is used to pass on security tokens for federated identity management.

Homework 15

A. In Kerberos V4, when Bob receives a Ticket from Alice:

a. How does he know that it is genuine?

b. How does he know that it came from Alice?

c. When Alice receives a reply, how does she know that it is not a replay of an earlier message from Bob?

d. What does the Ticket contain that allows Alice and Bob to talk securely

Limit your answer to one sentence each.

B. What would be the BER encoding of {firstname "Ed"} {weight 259}? ASN.1 type for octet strings is 4 and for integers it is 2.