Kerberos V5

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/cse571-07/

Overview

❑ Kerberos V4 Issues

❑ ASN.1 and BER

❑ Names, Delegation of Rights

❑ Ticket Lifetimes

❑ Cryptographic Algorithms

❑ Hierarchy of Realms

Kerberos V4 Issues

1. Names, Instance, Realm (non standard)

1. Only DES encryption

2. Only IPv4 addresses

3. Byte ordering indicated in the message (ASN.1 better)

4. Maximum life time limited to 21 hours: 8 bit life time in units of 5 minutes

5. No delegation

6. Inter-realm authentication limited to pairs $\Rightarrow N^2$ pairs

7. Double encryption of the ticket: $K_{client}[K_{server}[...]]$

8. PCBC does not detect interchange of cipher blocks

9. No subsession keys for long sessions

10. Brute force password attack

ASN.1

❑ Abstract Syntax Notation One

❑ Joint ISO and ITU-T standard, Original 1984, latest 2002.

❑ 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: INTEGER, BOOLEAN, BIT STRING, OCTET STRING

❑ Constructed: SEQUENCE (structure), SEQUENCE OF (lists), CHOICE, ...

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	80	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	FE
Int	Len	123

04	0B	4D	61	69	6E	20	53	74	72	65	65	74
Oct str	11	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	96	0
Oct Str	Len	M	O	Int	len	63130		Null

Names

❑ V4: Name, Instance, Realm
(40 character each. Null terminated). Dot "." is illegal.

❑ V5: Name can contain dot and can have many parts.,
e.g., jain.raj

❑ V4: Realms are DNS names.

❑ V5: Realms can be DNS names, X.500 names, etc

Delegation of Rights

- **Need**: Backup job requires operators to access files
- V5 allows requesting a TGT with a different address
- Can include many addresses or no addresses $\Rightarrow$ Anyone.
- TGT with operator's address can then be passed to the operator.
- Can also request to include application specific restrictions in the TGT
- These restrictions are copied in the tickets
- Can request that TGT be *forwardable* $\Rightarrow$ One operator can pass it to another operator.
- Can request that TGT be *proxiable* $\Rightarrow$ Alice can request a ticket from TGT for use by the operator.
- Allowing delegation, forwarding, proxy, many addresses, no addresses are **policy decisions**

Ticket Lifetimes

❑ V4: Lifetime is one octet
  $\Rightarrow$ max 256 in units of 5 minutes $\Rightarrow$ Max 21 hours

❑ V5: Many timestamps, each in ASN.1 format
  (17 bytes in s)

❑ Start Time

❑ End Time

❑ Auth Time: Time at which initial TGT was obtained

❑ Renew Till: Must renew after this time

❑ Start Time < End Time < Renew Till

Renewable Tickets

❑ Tickets cannot be invalidated

❑ Long term use permitted only if renewed frequently

❑ Expired tickets cannot be renewed
$\Rightarrow$ KDC does not have to remember revoked tickets for long time

Postdated Tickets

❑ Start Time in future

❑ Pre-invalidated ⇒ Must be validated at the start time
   ⇒ Allows revoking the authentication

❑ May-Postdate flag in TGT
   ⇒ TGS can issue post-dated tickets

Key Versions

- Allows principals to change keys
- Multiple versions of keys are kept at KDC and TGS
- Each key is stored as
  <Key, Principal_KeyVersionNo, KDC_KeyVersionNo>
  $\Rightarrow$ Allows the possibility of KDC changing its key
- Helpful for renewable and post-dated tickets
- Renewal Tickets are issued with the latest keys

Master Keys in Different Realms

❑ Password-to-key hash function uses realm name also

❑ Attacker cannot use the same key in multiple realms (Attacker can still use the same password in multiple realms)

Optimizations

❑ V4: Ticket is encrypted with client's key
   Ticket is already encrypted with Server's key
    $\Rightarrow$ Double encryption

❑ V5: Ticket is not encrypted again

❑ V4: Target's name inside the ticket
❑ V5: No name inside the ticket

Cryptographic Algorithms

❑ V4: DES

❑ V5: Encryption field is type-value encoded
  $\Rightarrow$ Any encryption

Integrity-Only Algorithm

❑ V4: Jueneman Checksum

❑ V5: Choice of algorithms

  ➢ rsa-md5-des

  ➢ des-mac

  ➢ des-mac-k

  ➢ res-md4-des (optional)

  ➢ rsa-md4-des-k (Optional)

Encryption for Privacy and Integrity

❑ Choice: des-cbc-crc, des-cbc-md4, des-cbc-md5

❑ Checksum is combined with the message and then encrypted with DES in CBC mode.

Hierarchy of Realms

- ❏ V4: Limits to pairs

- ❏ V5: Transition allowed.

- ❏ B is registered with A and C is registered with B

- ❏ x@A can get to y@C via B

- ❏ List of all transited KDC's is put in the ticket

- ❏ It is the applications responsibility to decide if some transited KDC is trustworthy

```
              A
           /     \
         B         C
        / \       / \
       D   E     F   G
```
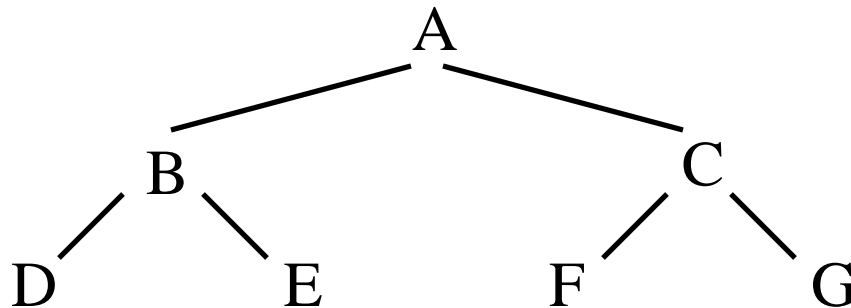
Password Attacks

❑ V4: Initial request in clear. Anyone can request TGT for president@whitehouse.gov

❑ and use it for offline attack.

❑ V5: Need to send pre-authentication data. Current time encrypted by user's key.

❑ One can still do offline analysis of tickets received for another user.

❑ V5 does not allow tickets for human users.

❑ Attackers can still monitor pre-authenticated data and analyze it offline.

Key Inside Authenticator

- ❑ Alice having two conversations with Bob
- ❑ Attacker can inter-mingle packets and confuse
- ❑ V5 allows Alice to use two different keys.
- ❑ Alice puts a key in the authenticator along with the ticket.
- ❑ Bob uses Alice-bob session key to decrypt the authenticator and then uses the key proposed by Alice to continue the conversation.

Double TGT Authentication

❑ User's workstation get a TGT for the user and discard the master key generated from the password.

❑ Xwindows applications need to authenticate to the user in order to write to his windows.

❑ These tickets are encrypted with user's master keys

❑ The workstation can send the user's TGT and the tickets to TGS and get back tickets encrypted with session key.

Public Keys for Users

❑ Users can send a certificate to the KDC and get a reply encrypted with their public key.

❑ KDC also keep a translation table to translate X.500 names in the certificate to Kerberos style names.

❑ Kerberos style names are used in the tickets.

❑ User can then send the ticket to older servers that do not know about public key.

❑ This is called PKINIT

Summary
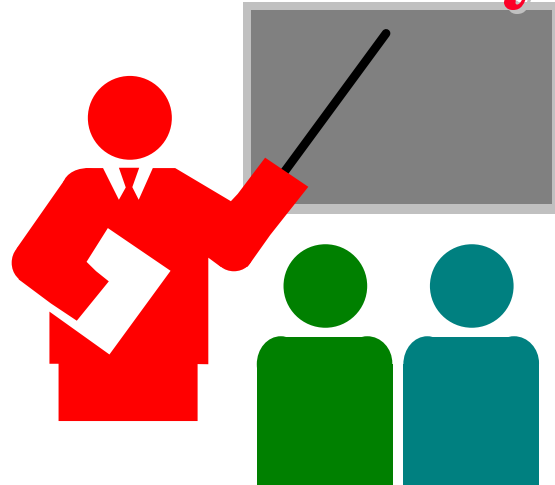
- Kerberos V5 is design follows ISO ASN.1 $\Rightarrow$ General
- General encryption, addresses, names
- Allows delegation, post-dated tickets, renewals
- Inter-realm authentication
- Public Keys for users

Homework 11

❑ Read chapter 14 of the text book

❑ Submit answer to the following exercises:

➢ **Exercise 14.1**: Suppose the Kerberos V5 password to key conversion function is identical to V4 but then takes the output that V4 would compute and xors it with the realm name. This would produce a different key in each realm, as desired. What is wrong with this algorithm?

➢ **Exercise 14.2**: Consider the following variant of Kerberos. Instead of having postdated or renewable tickets, a server which notes that the authorization time is older than some limit presents the ticket to the TGS and asks if it should believe the ticket. What are the trade-offs of this approach relative to the Kerberos V5 approach. Hint: Compare TGS's work and consider revoked authentications.