The Kerberos Protocol

Ron Burback

Lecture 8

The Talk

- Definitions
- Authenticating to the Security Service
- Authenticating to another Service.
- Acquiring Permissions
- Authenticating to another Service with Permissions
- Authenticating Challenge

Definitions

- Principal: The name of a person or server.
- Password: A secret string known only to the owner.
- Key: The parameter used in an encryption or decryption algorithm.
- Pass Key: A password is converted to a pass key with a one-way encryption.

Definitions

- Session Key: A key used for a short period of time.
- Authenticating: The act of validating a principal's identity.
- Authorization: The act of granting permissions.

Definitions

- PAC: Privilege Attribute Certificate. The list of a principal’s capabilities.
- ACL: Access Control List. The list of principals and groups granting various permissions to a resource.
- Clear Text: Traditional text.
- Cipher Text: Encoded text.

Definitions

- Encryption: The act of taking clear text into cipher text.
- Decryption: The act of taking cipher text into clear text.
- One way Encryption: A message is encrypted in a fashion which is not reversible.

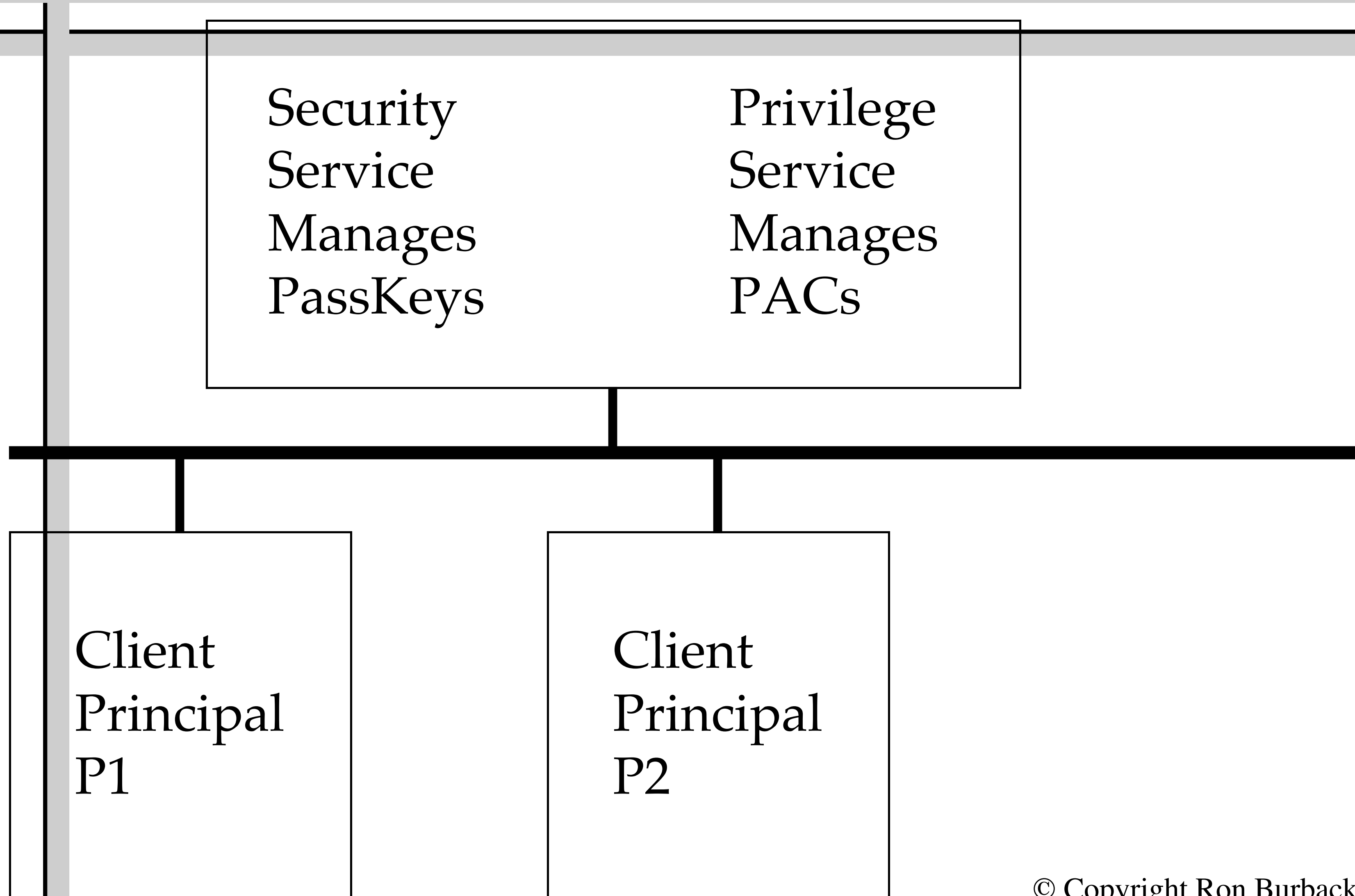
Definitions

- Ticket: A message from the security service, always encrypted, granting authorization or authenticating.

Definitions

- Secret (Private) Key Algorithm: One key is used to both encrypt and decrypt text.
- Public Key Algorithm: Two keys are used. One key, a secret key, to encrypt text and a different key, a public key, to decrypt the text.
- Registry: The pass key database for a secret key algorithm.

Services Involved in Security



Two Important Tickets

- TGT (Ticket Granting Ticket) - authenticates a principal.
- STkt (Service Ticket) - authenticates one principal to communicate with another principal. Principal to principal authentication.

TGT

<Security Service's Key>
Principal's Name
Session Key
Expiration Time

The TGT authenticates a principal. It includes the principal's name, a session key used for communication between the principal and the security service, and a expiration time. All encrypted with the Security Service's Key.

STkt - P1 wants to talk to P2

<Principal P2's Key>
Principal P1
Session Key
Expiration Time

The STkt authenticate a principal P1 to another Principal P2. It includes the principal P1's name, a session key used for communication between the principal P1 and principal P2, and a expiration time. All encrypted with the Principal P2's Key.

Understanding the graphics

Message, M, is encrypted with Key, K, and contains Data, D, is sent from Principal, P1 to Principal, P2. Note that Key, K, is not part of the message.

Authenticating to the Registry Step 1

Message: M1 →

Principal: P1

Principal P1 would like to authenticate.

Security Service

The Principal sends the account name, in the clear, to the Security Service.

Authenticating to the Registry Step 2

Principal:
P1

Message: M2

< Principal's Pass Key >
S1, TGT

Security
Service

Ticket:TGT (Ticket Granting Ticket)

<Security Service's Pass Key>
S1, P1, lifetime

The Security Service creates a new session key, S1, and constructs the Ticket Granting Ticket, TGT. The TGT contains the session key, the principal's name, and a lifetime all encrypted in the Security Service's Pass Key. This message is encrypted in the Principal's Pass Key and sent back to the Principal.

Authenticating to the Registry Step 3

- The Principal types in the pass word.
- This is converted to a pass key.
- The pass key is used to decrypt the message and obtain the TGT.
- The Principal now has the session key and is authenticated to the security service.

List of Tickets, so far

- TGT, Ticket Granting Ticket with Session Key S1

Authenticating to another service

- Principal P1 would like to talk to another service. In this example, P1 would like to talk to the Privilege Service. The Privilege Service will eventually grant privileges to P1. The Privilege Service will authorize P1. The Privilege Service is really just a component of the security service.

Authenticating to another service: Step 1

Principal:
P1

Message

<Key: S1>

P1 would like to talk to the Privilege Service.
TGT

Security
Service

The Principal, P1, sends a message to the Security Service, encrypted in the session key granted in the TGT, asking for permission to talk to the Privilege Service.

Authenticating to another service: Step 2

- The Security Service decrypts the message and discovers the TGT.
- The Security Service decrypts the TGT and validates this request.
- A new session key, S2, is created.
- A STkt ticket is constructed consisting of P1 and S2 encrypted in Privilege Service's key.

Authenticating to another service: Step 3

Principal: P1

Security Service

<Key: S1>
Session Key : S2
STkt

STkt: Service Ticket Granting Ticket

<Privilege Service's Pass Key>
S2, P1, lifetime

The Security Service creates a new session key S2, and a STkt ticket with S2 and P1 encrypted in Privilege Service's pass key. The Security Service then encrypts the ticket in the session key S1.

Authenticating to another service: Step 4

- P1 decrypts the message and discovers the key S2 and the STkt for Privilege Service.
- We now have a ticket to talk to Privilege Service.

List of Tickets, so far

- TGT, Ticket Granting Ticket, Key S1
- STkt, Service ticket for the Privilege Service, Session Key S2

A Principal P1 has authenticated to the security service and is authorized to talk to the Privilege service.

Next, we will get the PAC.

Two More Important Tickets

- PTGT (Privilege Ticket Granting Ticket) - authorizes a principal by using a PAC. Just a TGT with a PAC.
- PSTkt (Service Ticket) - authorizes one principal to communicate with another principal including a PAC. Principal to principal authorization. Just at STkt with a PAC.

PTGT

<Security Service's Key>
- Privilege Service Name
- Session Key
- Expiration Time
- PAC of the Principal

The PTGT authorizes a principal. It includes the privilege service's name, a session key used for communication between the principal and the privilege service, a expiration time, and the PAC. All encrypted with the Security Service's Key. Note the use of the Privilege Service Name.

PSTkt - P1 wants to talk to P2 with authorization.

<Principal P2's Key>
Privilege Service
Session Key
Expiration Time
PAC of P1

The PSTkt authorizes a principal P1 to another Principal P2. It includes the privilege service's name, a session key used for communication between the principal P1 and principal P2, a expiration time, and the PAC of P1. All encrypted with the Principal P2's Key.

Acquiring Permissions

- At this time the principal has been authenticated and has a TGT.
- The principal has requested a service ticket to the Privilege Service and has a STkt.
- We know want to obtain a PTGT with a PAC from the Privilege Service.

Acquiring Permissions: Step 1

Principal:
P1

Message →

<Session Key S2>
STkt
P1 would like a PTGT

Privilege
Service

The Principal P1 sends the request for a PTGT to the Privileged Service and includes the STkt all encrypted in the S2 session key.

Acquiring Permissions: Step 2

Message

Principal:
P1

<Session Key S2>
Session Key S3
PTGT

Privilege
Service

The Privilege Service creates the PTGT and a new session key S3 and returns the information back to the Principal all encrypted in the session key S2.

Acquiring Permissions: Step 3

Principal P1 now decrypts the message, discovers the PTGT and the new session key. P1 now has the PAC. Recall that the PTGT is encrypted with the Security Service's Key.

List of Tickets, so far

- TGT, Ticket Granting Ticket, Key S1
- STkt, Service ticket for the Privilege Service, Session Key S2
- PGTG, TGT with PAC, Session Key S3

Next, we will get the PAC to another service.

Authenticating to another service with PAC: Step 1

Message

Principal: P1

<Key: S3>

P1 would like to talk to the P2 include a PAC.
PTGT

Privilege Service

The Principal, P1, sends a message to the Security Service, encrypted in the session key granted in the PTGT, asking for permission to talk to the P2.

Authenticating to another service with PAC: Step 2

- The Security Service decrypts the message and discovers the PTGT.
- The Security Service decrypts the PTGT and validates this request.
- A new session key, S4, is created.
- A PSTkt ticket is constructed consisting of P1 and S4 encrypted in Security Service's key. The PAC is copied into the PSTkt.

Authenticating to another service: Step 3

Principal: P1

<Key: S3>
Session Key : S4
PSTkt

Security Service

PSTkt: PAC Service Ticket Granting Ticket

<Security Service's Pass Key>
S4, P1, lifetime, PAC

The Security Service creates a new session key S4, and a PSTkt ticket with S4 and P1 encrypted in Security Service's pass key. The Security Service then encrypts the ticket in the session key S3.

List of Tickets, so far

- TGT, Ticket Granting Ticket, Key S1
- STkt, Service ticket for the Privilege Service, Session Key S2
- PGTG, TGT with PAC, Session Key S3
- PSTkt, PAC Service Ticket for P2, Session Key S4.

Authentication Challenge

- At anytime a client process can challenge another client process even if a valid STkt or PSTkt has been presented.

Authentication Challenge:

- P1 has given P2 a STkt.
- P2 challenges the ticket by generating a random number and sending it in the clear to P1. If P1 is really on the other end of the connection, P1 can reply to this challenge with the same random number encrypted in the STkt's session key. If P2 gets back the same random number then it really is P1 at the other end.

Public Key Extensions

- We can use the same protocol with an RSA based public key algorithm. The protocol, the tickets, and the session keys all remain the same. What changes is the encryption algorithm.
- Communication with a Principal is done with the Principal's public key

TGT - if public key was used

<Security Service's Public Key>

Principal's Name
Session Key
Expiration Time

Only the Security Service would be able to decrypt this ticket. The other ticket are similar.

Summary

- Authentication vs Authorization
- Tickets - Architecture Foundation
- Request, Encrypt, Challenge protocols
- Public vs Private