Kerberos

In greek mythology, Kerberos is the dog that guards the entry to Hades
In Harry Potter, this dog is known as "Fluffy"

Background for Kerberos

- Project Athena at MIT (mid to late 1980s)
- Hundreds of diskless workstations
  - open terminal access, no physical security
  - insecure network
- Few servers (programs, files, print, ...)
  - physically secure

Simple Authentication

- One password per service is infeasible
- New authentication service (AS) introduced
- Both users and services have passwords
- AS identifies user by password
- AS returns a "ticket" to the user
  - ticket includes identity encrypted with the service's password
  - if the ticket decrypts properly, access to the service is granted

Stronger Authentication

- Include service name in the ticket to prove that it was properly encrypted
- Include client workstation address to prevent network sniffers
- Remaining problems:
  - re-authentication every time a new service is contacted
  - password sent across the network in the clear

Ticket Granting Service (TGS)

- TGS has access to the AS database
- TGS provides service tickets to users with a TGS ticket (eliminate resubmitting password)
- Users obtain ticket granting tickets from AS
- User sends username, receives TGS ticket encrypted with user's password
- Tickets can be reused

Insecure Workstations

- What happens to tickets after a user has logged out?
  - an opponent could log on to the workstation and use the tickets
  - could be explicitly destroyed when user logs out
  - sniffer could be used to capture tickets, hacker may then login to the same workstation and use the tickets (*replay session*)
- This is especially a problem with small mobile devices that are easily stolen

Limiting Ticket Lifespan

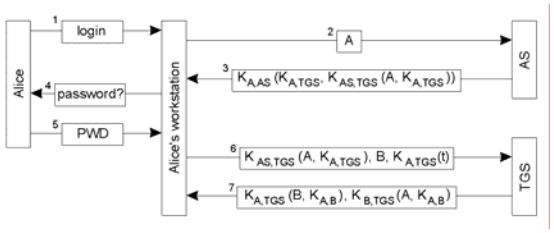
- AS timestamps ticket when it is issued
- AS includes lifespan along with timestamp
- Remaining problems:
  - workstation clocks must be synchronized
  - what should the lifespan of a ticket be?

Verifying Tickets

- Authentication relies on the following tests:
  - can the service decrypt the ticket?
  - has the ticket expired?
  - do the username and workstation address correspond?
- The tests prove:
  - the ticket came from AS
  - the ticket is still valid
  - failure proves that the ticket is false, success does not prove a thing, tickets can be stolen and reused on the same workstation

Authentication in Kerberos

Summary I



Setting up a secure channel in Kerberos

Summary II