

# AFS and PAM

Russ Allbery

May 1, 2007

# Contents

- What is PAM?
- The PAM Groups
- PAM for Login
- PAM for Screen Savers
- AFS PAM Modules
- Problems with pam\_afs
- Working with pam\_krb5
- SSH Challenges
- Linux PAM Examples

## What is PAM?

- Pluggable Authentication Modules
- Abstracts the user authentication and session setup process
- Only does authentication and simple authorization
- Developed originally on Solaris
- Enhanced but mostly compatible version on Linux
- Now used by many UNIXes, but implementation varies

## The PAM Groups

- PAM divides the login process into groups
  - auth: Prompts for and verifies password
  - account: Simple authorization decisions (only for login)
  - session: Prepares for an interactive session
  - password: Handles authentication token changes
- setcred, the odd step-child
- setcred vs. open\_session: who knows? who cares?

## PAM for Login

- auth group prompts for password, does basic authentication
  - Store the credentials in a separate temporary cache
  - Don't chown credential cache until setcred
- account group does basic authorization
- setcred stores credentials and adds supplemental groups
- session group creates a login session
- When the user logs out, session group closes the login session

## PAM for Screen Savers

- auth group prompts for password, does basic authentication
- account group could do authorization, but frequently ignored
- setcred to refresh credentials (REINITIALIZE/REFRESH)
- session group not called
- Bad screen savers don't call setcred and thereby lose

## AFS PAM modules

- Authentication and AFS modules
  - pam\_afs and pam\_afs.krb (OpenAFS)
  - Heimdal pam\_krb4 (requires Heimdal)
  - pam\_krb5afs from Sourceforge (requires Heimdal)
- AFS session modules
  - pam\_afs2 from Douglas Engert
  - Sam's pam\_openafs\_session
  - My pam\_afs\_session
- Using Heimdal vs. forking an external aklog

## Problems with pam\_afs

- Kerberos v4 and kserver only
- Does all of its work in the auth group
  - Doesn't work with SSH privilege separation
  - Doesn't support token renewal from screen savers
- Forks by default to avoid thread leaks
- Pulling AFS libraries into applications is very ugly
- Requires hacks to build shared on non-x86 Linux



## Working with pam\_krb5

- Merging the Kerberos auth module and AFS tokens is problematic
  - Vendor Kerberos v5 modules are common, often don't do AFS
  - AFS is conceptually separate
  - Easier to debug separate modules
- pam\_krb5 responsible for getting tickets, AFS module for getting tokens afterwards
- AFS runs as a session module
- Ideally also want a setcred hook

## SSH Challenges

- auth group run in a separate subprocess
- PAM data not passed out of authentication hook
- ChallengeResponseAuthentication required for prompting
- Threading issues
- Broken session/setcred behavior in older versions

## Linux PAM Examples

```
auth      [success=ok default=1] pam_krb5.so
auth      [default=done]         pam_afs_session.so
auth      required               pam_unix.so try_first_pass
session   optional               pam_krb5.so
session   required               pam_afs_session.so

auth      sufficient              pam_unix.so
auth      [success=ok default=die] pam_krb5.so use_first_pass
auth      [default=done]         pam_afs_session.so
session   optional               pam_krb5.so
session   optional               pam_afs_session.so
```