Stanford Web Authentication Overview

Russ Allbery

June 6, 2006

Contents

- Stanford WebAuth Design Goals
- WebAuth Strengths
- WebAuth Weaknesses
- Future Direction
- HTTP Negotiate Introduction
- HTTP Negotiate Deployment Challenges
- Shibboleth
- Fitting It Together

Stanford WebAuth Design Goals

- No central state for simple scalability
- Use browser cookie jar as a credential store
- Support credential delegation
- Support backward compatibility
- Extensible protocol without authentication assumptions
- LDAP integration (with backward compatibility)
- No central server required after initial authentication

WebAuth Strengths

- Very widespread deployment at Stanford
- Well-tested and stable in production
- Extensible protocol based strongly on Kerberos
- Extensive documentation
- Strong LDAP integration
- Easily scalable, good support for load-balanced pools

WebAuth Weaknesses

- Protocol inherently incapable of doing central logout
- No official Windows IIS support
- Not as widely used, so smaller development community
- Complex protocol

Future Direction

- HTTP Negotiate for initial sign-on
- Cannot replace WebAuth, Cosign looks great, can we merge?
  - Support Cosign authentication in WebAuth module
  - LDAP module could support any authentication type
  - Weblogin server could log users into both systems
- IIS security contexts
- Shibboleth for Windows IIS authentication
- Shibboleth integration into Weblogin display
- More minor cleanup, particularly better WebKDC logging

HTTP Negotiate Introduction

- Kerberos GSS-API authentication over HTTP protocol
- Relationship to SPNEGO
- Right idea, questionable implementation
- Seems to be the best thing currently available
- Two Apache module implementations with different problems
- Need local patches to mod_auth_kerb

HTTP Negotiate Deployment Challenges

- Browser support mostly there but annoying:
  - IE configuration stupidity
  - Safari's principal of the week
  - Firefox library loading bugs
  - Opera seems to just lose
- Windows cross-realm and Exchange breakage
- User freakout about any change
- HTTP Negotiate hard to explain
- Solution: Make it optional and hide it a little

Shibboleth

- Solving a different problem: federated identity
- Good solution for hard edge cases
- Can be used for intranet authentication, but complex
- Doesn't support credential delegation
- *Does* support IIS
- Looks like your other web authentication system to users

Fitting It Together

- Separate user interface from authentication protocol
- Different systems have pluses and minuses — support them all!
- Shibboleth seems the only widely deployed solution to its problem
- LDAP integration is more important than you might think
- Authorization is hard but LDAP groups seem the most flexible
- This technology area is still very immature