Moonshot: Implementing Kitten Technologies

Sam Hartman

Painless Security, LLC

IETF 79

November 9, 2010

Background

- Moonshot is a community project to produce a production-quality federated authentication solution
- Drives work in ABFAB, Kitten and EMU; implements results
- First project meeting held: September 2010 in Copenhagen

Implemented So Far

- Naming Extensions
- GS2 to GSS-API bridge
- SASL channel binding
- A new GSS-API mechanism

Testing with IAKerb

In order to test the GS2 SASL implementation two mechanisms were desired. The Moonshot mechanism and IAkerb were used.

Part I
What Works

SASL Frameworks

- Client applications accessing Moonshot and IAkerb via GS2 bridge with no application knowledge of new mechanisms
- Preliminary channel binding support within framework and mechanisms
- Application needs to understand naming for authorization

Naming Extensions

- Naming extensions expose attributes from multiple sources (AAA and SAML)
- Local attributes as discussed in IETF 78
- Spec work still required

Looking Forward

Desire for Interop Testing

- Multiple GS2 implementations
- Channel binding support in Applications
- Multiple implementations of GSS-EAP
- Target: Second quarter 2010

Learning from IAkerb

- GS2 restricts mechanism behavior
- The first token's OID MUST correspond to what GS2 expects
- Optimizing IAkerb down to Kerberos or similar cannot work in this model
- Needs documentation

RFC 4121 Re-use Made Easy

- Several new mechanisms are re-using RFC 4121
- Desire to conserve RFC 4121 implementations within a system
- Context option or mechanism glue support for RFC 4121 context?

Mechanism Design Considerations

- Name forms used by actual applications
- Kerberos-style optional channel bindings
- DCE style and other extensions
- Defining GS2 name
- Microsoft NegoEx