IDfusion
An Open-Architecture for Kerberos based Authorization

Dr. Greg Wettstein, Ph.D., John Grosen, MS

Information Technology Services
North Dakota State University

Enrique Rodriguez
Safehaus/Apache Software Foundation
Background

• 1997 - Identity based architecture.
  – Hurderos Project
• Host centric to service centric transition.
  – Everything is a service
• Integrated management and provisioning
  – Uberware
Why Authorization?

- What people want is authorization.
- No standardized protocol or scheme for implementing authorization.
- Lack of a standard hinders use of authorization.
- Open Standards = Open Architectures
Why emphasize standards?

“At the end of the day the only thing that matters in information delivery is who is consuming information and what information can they consume. He who controls that controls everything.”

Wettstein's Theorem on the Transcendency of Identity Management
Goals

• Simple and flexible.
• Synergistic combination of the strengths of Kerberos and LDAP.
• Inherent security from the perspective of the directory.
• Consistent with services oriented architectures.
Rethinking Authorization

• Phases of authorization.
• Identity intersection model.
Authorization Phases

• Execution
  – Application specific process based on user attribute information.

• Implementation
  – Infrastructure to support execution of authorization decision.
Identity Intersection Model

User Uii
Service Sii

Service Authorization Instance Identity Slii
Model Implementation

- N-bit vectors used for intrinsic identities.
- Cryptographic hash with message size $m=N$ used to implement 'fusioning'.

$$S_{lii} = H_m(U_{ii}, S_{ii})$$
Kerberos Model

- Define service authentication identity.
  - svc/SERVICE@REALM
- Use HMAC derivative of fusioning hash with authentication identity key Kn.
- Publish HMAC identity for Slii.

\[ Slii = HmKn(Uii,Sii) \]
Example Publications

Service Identities:
- dn: service=IDENTITY,dc=org,dc=NNN
- kvno: 3
- sii: [0-9a-f]{Lm}
- state: enabled|disabled

Service Instance Identities:
- dn: Slii=[0-9a-f]{Lm},dc=org,dc=NNN
- cn: GoldenS St. Ignatius
- sn: Wettstein
- iid: Iggy.Wettstein
- uid: k9
- title: Corporate Retriever
- Uii: [0-9a-f]{Lm}
- state: enabled|disabled

- dn: service=KERBEROS,dc=org,dc=NNN
- kvno: 4
- Sii: [0-9a-f]{Lm}
- state: enabled|disabled

- dn: Siii=[0-9a-f]{Lm},dc=org,dc=NNN
- krb5RealmName: ORG.NNN
- krb5PrincipalName: bark1
- state: enabled|disabled
- preauth: IDfusion|OTP
Kerberos Protocol Extensions

• Authorization payload field holds intrinsic identities.
  – Ticket granting ticket: Uii
  – Service ticket: Slii

• Application uses payload field as a pointer into the directory.
AS_REQ Procedure

• Lookup and validate KERBEROS service object.
• Lookup and validate IDENTITY service object.
• Load binary representation of Uii in authorization payload field of TGT.
TGS_REQ

- Load Uii from credential (TGT).
- Lookup and validate Sii based on service name from svc/SVCNAME principal.
- Compute and validate Slii.
- Store binary representation of Slii in service ticket.
Reference Implementation - KDC

• Shared library plugin for MIT 1.4.3.
• Methods:

  init
  destroy
  as_req
  as_req_authz
  tgs_req
  tgs_req_authz
Administrative Support

• Plugin for kadmind.
• Methods:
  – pwd_update
  – acl_check
• Implementing support for KRBAADM service.
Integrated Management

• ISME
  – identity generation and management engine.
  – service provisioning.

• GOOI
  – graphical representation and control of identity heirarchy.
Demo
  FM Dog Obedience
    Iggy.Wettstein
      IDENTITY
      KERBEROS
  North Dakota State University
    john.grosen
      IDENTITY
Demo
North Dakota State University
  KERBEROS
    Linux Server: server2.hurderos.com
  IDENTITY
FM Dog Obedience
  KERBEROS
    Linux Server: server2.hurderos.com
  IDENTITY
    Linux Server: server2.hurderos.com
In Our Spare Time

- Apache integration.
- IDfusion based two-factor authentication.
- Host ticket propagation of Slii's.
- API development.
- Delegated management.
- Client support.
Thank You

- John Grosen, Enrique Rodriguez
- NDSU and ITS