SAML 2.0 - Kerberos use cases

John Hughes
F2F Sept 8, 2003
High level usage and Scope

- **High Level Use Cases**
  - Intra-domain – using digital signing as basis of trust relationship
  - Inter-domain - using Kerberos as Subject Confirmation Method
  - Bridge Servers

- **Scope**
  - Kerberos V5
  - Microsoft/Kerberos
  - DCE
Use Case: Intra Domain

1. **Authenticate**
2. **SAML Request + ST**
3. **SAML Response (Signed)**
4. **Create Local Identity**
5. **Access Resource + signed SAML Assertion**
Use Case: Inter Domain

For SubjectConfirmation

- Confirmation method set to Kerberos (need separate ones for Windows and DCE??)
- ConfirmationData contains ticket – or a reference to it
- Two uses
  - Use ticket (or reference to it) to authenticate principal
  - Obtain principals attributes (either as PAC/EPAC or Attribute Statements)
Use Case: Inter Domain - Options

- SAML Assertion could contain:
  - Ticket in SubjectConfirmationData
    - Principal TGT
    - Service ticket (between principal and server)
    - Server TGT
  - Attributes
    - As Attribute Statement – already converted
    - As PAC encoded within principal TGT or service ticket within assertion
    - PAC to Attribute Statement conversion service
## Use Case: Inter Domain - Ticket Options

### Principal TGT
- Not possible to directly unpack to extract PAC or session key.
- Need to access KDC to perform authn – would require new protocol message. (Probably SAML based). Would need SAML assertion to also contain \( S_{ku}M_u \) (from cache in principal)
- Would require PAC to be translated to Attribute Statement - possibly as part of new authn protocol

### Service Ticket
- SAML assertion would contain service ticket and authenticator (principal having gone through KRB_AS_REQ and KRB_TGS_REQ process)
- SAML assertion is really replacing KRB_AP_REQ message (and perhaps not supporting equivalent LRB_AP_REP response)
- PAC could be extracted from Service Ticket. However new service could be build that converts PAC into Attribute Statements

### Server TGT
- Doesn’t make sense
Use Case: Inter Domain - using Principal TGT

Authenticate

principal

SAML Assertion
(with principal TGT and \(S_KU^M_u\))

KDC

Auth me
+ TGT and \(S_KU^M_u\)

Attribute
Authority

Confirmation
+ Attribute
Assertion

Server
Use Case: Inter Domain - using Service Ticket

Authenticate

Request Service Ticket

KDC

Attribute Authority

Convert PAC

Attribute Statement

Server

principal

SAML Assertion (with service ticket and authenticator)
Use case: SAML Bridge Server

Notes:

• Virtual Kerberos Client interacts with KDC to register user and/or update reg details. In case of DCE and Windows updates stored user attributes so that PAC received with TGT contains appropriate privileges mapped from supplied Attribute Assertion
• Bridge Server can also perform application protocol conversion, e.g. EJB/RMI to DCE RPC
Use case: Kerberos Bridge Server

Notes:
- In DCE and Windows case the Ticket will contain a PAC. The Bridge Server maps the attributes in the PAC into AttributeStatements or inclusion in the SAML Assertion
Suggested Next Steps

1. Write up this presentation to capture details of use cases
2. Discuss and select any that make sense
3. Produce appropriate profile(s)
Appendix

Kerberos flow
KDC Authentication Service

Ticket Granting Service

1. Request TGT KRB_AS_REQ
   \(\{\text{User}, \text{time}\}_{MU}\)

2. Service Reply with TGT KRB_AS_REP
   \(\{SKU\}_MU \cdot \text{TGT} \quad \text{where TGT} = \{SKU, PAC\}_MK\)

3. Request Ticket to access server KRB_TGS_REQ
   authenticator, TGT where authenticator = \(\{\text{User}, \text{time}\}_{SKU}\)

4. Service Reply with Ticket KRB_TGS_REP
   \(\{S_{US}\}_{SKU} \cdot \text{Ticket} \quad \text{where Ticket} = \{S_{US}, PAC\}_MS\)

5. Application Request KRB_AP_REQ
   authenticator, Ticket where authenticator = \(\{\text{User}, \text{time}\}_{SUS}\)

6. Application Response KRB_AP_REP
   \(\{\text{time}\}_{SUS}\)

\(MU\) Master Key of User: derived from password
\(SKU\) Session key: KDC<->User. Obtained from KDC
\(SUS\) Session key: User<->Server. Obtained from KDC
TGT Ticket Granting Ticket. Obtained from KDC and cached

\(MK\) Master Key of KDC
\(MU\) Master Key of User: derived from password
\(MS\) Master Key of Server: derived from password