Secure Single Sign-On with Apache Directory and Apache Kerberos

Enrique Rodriguez
PMC Member, Apache Directory
PPMC Member, Apache Felix
About the Speaker

- 80's & early 90's VAX, Mac, and Unix
- Mid-90's MCS for Unix-to-NT migrations
- Late-90's Director of Global Systems for Fortune 100, 6 continents, over 100 sites MS migrations
- Summer 2004 Kerberos granted to ASF
- Apache Directory, PMC Member
- Apache Change Password, NTP, DNS
- Safehaus founder (Mobile phone OTP)
- OATH representative (HOTP)
Today's Talk

- Pros & Cons of Kerberos
- Definitions
- General Configuration
- Scenario 1: Apache Directory as KDC
- Scenario 2: Apache Directory as KDC
Why not Kerberos?

- “Not firewall friendly.”
- Requires servers
- Difficult concepts
- “Relies on passwords.”
Why Kerberos?

- Adoption
  - Microsoft
  - SSO for Linux, Mac, Windows
  - Application support

- Robust
  - RFC 1510 Kerberos V5 1993
  - RFC 4120 July 2005
    - Clarifications
    - Extension point for authorization data
    - Stronger encryption
Why Directory-Backed?

- Tool support
  - Remote management
  - Interchange format (LDIF)
- Hierarchical
  - Subtrees
  - Access Control
  - Collective attributes
  - Replication
- Catalog configuration
  - DNS zones
  - Kerberos realms
Definitions

- Principal
  - Kerberos Principal (User, Service)
- Realm (Kerberos)
  - Zone (DNS)
  - Domain (Realm + Zone)
- Ticket
  - TGT (Authentication Service)
  - Service Ticket (Ticket-Granting Service)
- Symmetric key (secret)
- KDC (AS and TGS)
- SSO
- Realm Control
Definition: SSO

- Sign-on
- Single
- Secure
  - Confounder, checksum, symmetric keys, IP addresses, timestamps
  - Service-oriented
  - Passwords do not traverse the network
Windows Log On - Kerberos

User name: erodriguez
Password: *********
Log on to: EXAMPLE.COM (Kerberos Realm)
Windows Security

Logon Information
You are logged on as EXAMPLE.COM\\erodriguez.

Logon Date: 10/4/2005 3:34:53 PM

Use the Task Manager to close an application that is not responding.

- Lock Computer
- Log Off...
- Shut Down...
- Change Password...
- Task Manager
- Cancel
Change Password

User name: erodriguez
Log on to: EXAMPLE.COM (Kerberos Realm)
Old Password: 
New Password: 
Confirm New Password: 

OK 
Cancel
Definition: Realm Control

workstation

EXAMPLE.COM

1. NTP
2. DNS
3. Kerberos
4. Changepw
5. LDAP

Apache Directory
Configuration Overview

- Service Configuration
- Catalog Configuration
- Principal Configuration
- Password Policy
- KDC Discovery
Service Configuration

- All protocols
  - Service Factory
    - OC apacheFactoryConfiguration
    - MUST AT apacheServicePid
  - Service
    - OC apacheServiceConfiguration
    - MUST AT apacheServicePid
    - MAY AT apacheServiceFactoryPid
  - Protocol
    - ipPort
    - ipAddress
Catalog Configuration

- Kerberos, Change Password, DNS
- Location of entries
  - entryBaseDn (dc=example,dc=com)
  - catalogBaseDn
- Per-service configuration
  - apacheCatalogEntry
    - apacheCatalogEntryName
      - EXAMPLE.COM
    - apacheCatalogEntryBaseDn
      - dc=example,dc=com,ou=Zones,dc=apache,dc=com,
Kerberos Configuration

- Server instances
  - service.pid: org.apache.kerberos.1
    - IP address: 192.168.0.1, port: 88
    - search base: dc=example,dc=com
  - service.pid: org.apache.kerberos.2
    - IP address: 10.0.0.1, port: 88
    - search base: dc=apache,dc=org
Configuration via LDAP
Kerberos Services

- [1] JNDI EventDirContext
- [2] OSGi ManagedServiceFactory
- [4] MINA NIO Library
- [5] JNDI DirContext
- [6] MINA NIO Library

![Diagram](image-url)
Kerberos Principal Schema

- ou=Users,dc=example,dc=com
- krb5kdc.schema
  - krb5KDCEntry
    - krb5PrincipalName
    - krb5Key
    - krb5EncryptionType
    - krb5KeyVersionNumber
Change Password Properties

- `changepw.password.length`
  - 6 characters
  - Minimum password length

- `changepw.category.count`
  - 3 (out of 4)
  - Number of character categories required (A-Z), (a-z), (0-9), non-alphanumeric (!, $, #, %, ...)

- `changepw.token.size`
  - 3 characters
  - Password must not contain tokens larger than 3 characters that occur in the user's principal name.
KDC Discovery (DNS)

- SRV record
- A record

Windows 2000:
C:> Ksetup

default realm = EXAMPLE.COM (external)
EXAMPLE.COM:
  (no kdc entries for this realm)
  Realm Flags = 0x0 none
Mapping erodriguez@EXAMPLE.COM to administrator.

DNS Query:
Name: _kerberos._udp.EXAMPLE.COM
Type: SRV (Service location)
Class: IN (0x0001)

DNS Response:
_kerberos._udp.example.com SRV service location:
priority = 0
weight = 0
port = 88
svr hostname = kerberos.example.com
Configuration Review

- Service Configuration
- Catalog Configuration
- Principal Configuration
- Password Policy
- KDC Discovery
Interoperability Scenarios

- Windows domain without a Microsoft KDC
- Kerberos clients in a Windows domain
- Kerberos servers in a Windows domain
- Standalone Windows systems in a Kerberos realm
- Using a Kerberos realm as a resource domain
- Using a Kerberos realm as an account domain
Apache-Centric Scenarios

- **Scenario 1**
  - Apache Directory is KDC
  - Windows Clients
  - Linux Clients

- **Scenario 2**
  - Apache Directory is KDC
  - Windows Resource Domain
  - Windows Domain trusts Apache Realm
  - Windows Clients
  - Linux Clients
Non-windwos Kerberos users use their Apache Directory accounts

- Setup the /etc/krb5.conf
- Users login with their Apache Directory account (kinit, PAM)
/etc/krb5.conf

[libdefaults]
default_realm = EXAMPLE.COM
default_tkt_enctypes = des-cbc-md5
default_tgs_enctypes = des-cbc-md5

[realms]
EXAMPLE.COM = {
    kdc = kerberos.example.com:88
    kpasswd_server = kerberos.example.com:464
}
Windows users also use their Apache Directory accounts

- Configure system as standalone (no domain)
- Use Ksetup to configure the realm
- Use Ksetup to establish the local account mapping
- Logon to Kerberos realm

EXAMPLE.COM

Windows

Linux
Windows Configuration 2/3

- Default no-domain, Windows 2003 installation.
  - Computer name 'www'.
- Windows 2003 CD-ROM Support Tools
  - support\tools\suptools.msi
- Set the domain/realm:
  - C:> Ksetup /setdomain EXAMPLE.COM
- Note the full computer name:
  - www.EXAMPLE.COM
  - krb5PrincipalName:
    - host/www.example.com@example.COM
Windows Configuration 3/3

- Set the local machine account password
  - DIT userpassword: randall
  - `C:> Ksetup /setmachpassword randall`

- Add KDC's
  - Specific KDC:
    - `C:> Ksetup /addkdc EXAMPLE.COM`
    - `C:> Ksetup /addkdc kerberos.example.com`

- Point to DNS for "KDC Discovery":
  - `C:> Ksetup /addkdc EXAMPLE.COM`

- Map users:
  - `C:> Ksetup /mapuser erodriguez@EXAMPLE.COM administrator`
Windows Change Pswd 1/2

- Set an Apache Change Password server:
  - Specific:
    - C:> Ksetup /addkpasswd EXAMPLE.COM kerberos.example.com
  - DNS:
    - C:> Ksetup /addkpasswd EXAMPLE.COM

- Change a password using at a prompt:
  - C:> Ksetup /domain /changepassword <old-password> <new-password>
Change a password using Windows Security:

1. After logging on, press CTRL+ALT+DEL.
2. Click on the button labeled "Change Password ..."
3. Enter the Old Password and New Password (twice) and click OK.
Scenario 2: Cross-Realm Operation (Trusts)

- Why use trusts?
  - Trusts address scalability
  - Trusts address admin boundaries
  - Trusts allow a work-around for MS authz data

- Overview
  - Regular Cross-Realm Operation
  - Trust Relationship with MS Domain
Cross-Realm Concepts

- Kerberos uses symmetric key crypto.
- Kerberos is “service-oriented.”
- krbtgt/“accepting realm” @ “issuing realm”
  - krbtgt/EXAMPLE.COM@EXAMPLE.COM
  - krbtgt/EU.EXAMPLE.COM@EXAMPLE.COM
- A “trust” = “inter-realm” key
- 2 one-way trusts = one 2-way trust
Cross-Realm Config 1/2

- Principal Identifiers in a Local Realm
  - ou=Users, dc=example, dc=com
  - erodriguez@EXAMPLE.COM (local user)
  - krbtgt/EXAMPLE.COM@EXAMPLE.COM (local KDC)
  - krbtgt/EU.EXAMPLE.COM@EXAMPLE.COM (inter-realm key, EU.EXAMPLE.COM "trusts" EXAMPLE.COM)
Cross-Realm Config 2/2

- **Principal Identifiers in a Remote Realm**
  - `ou=Users, dc=eu, dc=example, dc=com`
  - `krbtgt/EU.EXAMPLE.COM@EU.EXAMPLE.COM` (remote KDC)
  - `krbtgt/EU.EXAMPLE.COM@example.com` (inter-realm key, EU.EXAMPLE.COM "trusts" EXAMPLE.COM)
  - `host/WWW.EXAMPLE.COM@EU.EXAMPLE.COM` (remote service to access)
Cross-Realm Workflow 1/2

- Client authenticates normally to local realm
  - erodriguez@EXAMPLE.COM
  - krbtgt/EXAMPLE.COM@EXAMPLE.COM

- Client requests access to service in remote realm
  - krbtgt/EXAMPLE.COM@EXAMPLE.COM
  - host/WWW.EXAMPLE.COM@EU.EXAMPLE.COM
Cross-Realm Workflow 2/2

- Client receives ticket grant (TGT) for remote realm (EU) from local realm
  - krbtgt/EU.EXAMPLE.COM@EXAMPLE.COM
- Client presents TGT to EU realm KDC for service ticket to access web server
  - krbtgt/EU.EXAMPLE.COM@EXAMPLE.COM
  - host/WWW.EXAMPLE.COM@EU.EXAMPLE.COM
- Client presents service ticket to web server
Cross-Realm Authentication

EXAMPLE.COM

EU.EXAMPLE.COM

Apache KDC

TGT

TGT

Linux

Windows Server

www.EXAMPLE.COM

TICKET
Windows Authorization 1/2

- Kerberos supports authz data in tickets
- Windows KDC supplies authz data in tickets
  - At interactive logon (AS exchange):
    - User, global, universal group SIDs
  - At session ticket request (TGS exchange)
    - Domain local group SIDs
- Interoperability issues are minimum
  - Windows authz data ignored by non-Windows implementations
Mapping is contained in the AltSecurityIdentities

- Win2K account:
  - erodriguez@WINDOWS.EXAMPLE.COM
- altSecurityIdentities entry:
  - Kerberos:erodriguez@EXAMPLE.COM
Apache KDC, Windows Authz

1. TGT
2. TGT
3. TGT
4. TGT

EXAMPLE.COM
EU.EXAMPLE.COM

Apache KDC
Windows KDC

Windows

With NT Auth Data

Name Mapping to NT account
Windows 2000 domain without a Microsoft KDC

- Not a supported scenario
- Windows domain security model depends on authorization
- Microsoft KDC is tightly integrated with Active Directory
- Support for down-level services (NTLM)
What's Next? 1/2

- Apache Directory
  - Triggers / stored procedures
    - Symmetric key derivation
  - Round-out DNS
  - DHCP
- Apache Felix
  - Incubator graduation
  - LDAP-backed OSGi services to Felix
  - 1.1 Release with Felix
What's Next? 2/2

- Standardization Efforts
  - OATH – IETF
    - SAM RFC for Kerberos
    - Provisioning
  - IDFusion authorization mechanism
    - Kerberos Authorization Data
    - LDAP schema
More Information

- Apache Directory Project
  - http://directory.apache.org
- Apache Felix Project
- OSGi
  - http://www.osgi.org
- Safehaus HausKeys, Mitosis, TripleSec
  - http://www.safehaus.org
- OATH
- IETF