K4-5 Upgrade: The Saga Continues

Trials and Tribulations of Kerberos Transition at the University of Michigan

or

How to Prepare for the Next Upgrade
Overview

In next half an hour we will:

- Present a general outline of the Kerberos upgrade project in the context of the large and diverse University of Michigan environment,
- Discuss organizational and technical issues we have encountered,
- Offer insights into what we have learned.
Kerberos History at the University of Michigan

- **Prehistory:**
  - Kerberos was in production at the University of Michigan in 1990. It became popular in 1992.
  - In 1998 MIT released K5: we upgraded our Kerberos servers almost immediately.
  - In 2000 we turned on triple DES and added one more Kerberos server.
Kerberos History at the University of Michigan

- More recent events
  - In 2002 University of Michigan Internal Risk assessment group audited Kerberos infrastructure and recommended we turn on preauthentication and turn off K4.
  - In 2005 MIT announced plans to discontinue support for Kerberos 4.
  - In 2005 ITSS was established and IT Commons initiatives was started: improving Kerberos became an IT management priority.
  - Current team was assembled January 2006 and project was fast-tracked.
Kerberos 4-5 Upgrade Summary

- **Project Objectives**
  - Provide more secure authentication mechanism while making sure there is a minimal impact on the end user.

- **Project Goals**
  - Replace Kerberos 4 with Kerberos 5 services.
  - Turn on preauthentication for all Kerberos users.
  - Prepare for the switch to AES encryption.

- **Project Timeline**
  - Upgrade project started in 1998.
  - Projected finish date: mid 2007.
Upgrade Obstacles

- Environment size, complexity and decentralization.
- Pervasive use of Kerberos authentication.
- Shooting moving target: emergence of new services that use initial Kerberos authentication - analysis data obsolete within a week.
- Existence of multiple authentication environments within the university.
- Competing timelines with other initiatives.
The University of Michigan

Users

- **Campus locations and number of schools and colleges:**
  - Ann Arbor: 19
  - Dearborn: 4
  - Flint: 5
- **Total student enrollment:** 55,028
- **Instructional staff:** 7,830
- **Regular non-instructional staff:** 28,201
- **Living degree holders:** 456,381

from "Budget Update" *(http://www.umich.edu/~urel/budget/bg.html)*

9 June 2006

mdw@umich.edu
kkit@umich.edu
Kerberos Use Data

- ~395,350 Kerberos principals
- In the last six months: authentication attempts made against ~173,200 principals
- In a non-session day (June 5th, 2006) we had:
  - 1,499,943 initial authentication attempts for 87,334 unique users
  - 1,176,580 service tickets requests for 1252 unique services:
    - 844977 mail
    - 101730 cosign
    - 35812 krbtgt
    - 31876 afs
    - 120 directory

Uniqname Creation 1993-2005

9 June 2006
mdw@umich.edu
kkit@umich.edu
Kerberos 4-5 Project Major Milestones

- Turn off Kerberos 4
  - Upgrade Kerberos 4 services/clients: 30% completed – completion target Fall 2006
  - Implement external filtering: completed April 2006
  - Expire antique passwords: 95% complete - completion target July 2006
- Turn off DES: completion target mid 2007.
Turn off Kerberos 4:
Upgrade Kerberos 4 services/clients

- Find services dependent on Kerberos authentication
- Communicate plan to the campus providers and negotiate K4-5 migration
- Provide resources
  - Documentation
  - Examples
  - Support: debug problems, help with testing, coding...
- IT providers: upgrade to K5
Turn off Kerberos 4: Implement filtering

- Facilitate staged withdrawal of service
- Prevent new services from being deployed with K4 dependencies

Steps:

- Matt Bing (ITSS) developed wrapper script with “host deny” and “host allow” logic
- Tested and deployed wrapper script
- Defined external Vs. internal (to UM) IP ranges
- Analyzed K4 usage by IP address to isolate external IP ranges
- Turned off external K4 service in a staged fashion
Turn off Kerberos 4: Expire antique passwords

- More than 100,000 passwords last changed before 1998: AFS 3 salts and only one key.

**Steps:**

- Identified active principals:
  - >100,000 principals,
  - ~20,000 active,
  - ~10,000 could be reached via email.

- Launched “password change” communication campaign
  - 40% users contacted changed their password before expiration date.

- Marcus Watts developed a script that expires antique passwords.
- Kevin McGowan developed a Web application that allows users to change their expired password on the Web.
Staging Preauthentication

- We are analyzing Kerberos logs to identify services that do initial authentication.
- We will test each service with preauthentication:
  - We are finding pilot groups of users to test preauthentication.
- We will turn preauthentication on:
  - By default for newly created uniqnames,
  - For remaining uniqnames in a staged fashion.
Future Direction

- **Turn off DES**
  - Required:
    - Windows support for AES,
    - AFS to support triple DES or AES.

- **Turn off triple DES**
  - Required:
    - AFS support for AES.
Measurements of Success

- Legacy cases (Kerberos 4, no preauthentication and use of DES) turned off before MIT officially stops the support.
- Little or no user surprise:
  - No production outage due to the upgrade.
  - Tolerable number of Kerberos support questions.
Lessons Learned

- Turning on K5 was relatively easy - turning off K4 is a challenge:
  - Organization size and culture.
  - Pervasive use of Kerberos authentication.

- Change of this type and magnitude requires upper management support.

- Never underestimate the power of communication and education.

- Make sure you have access to the right technical talent and expertise.

- Leverage all technical capabilities and tools.

- It is important to collaborate with other units: offer and provide technical support and expertise to IT providers campus wide.

- Research Kerberos usage: analyze logs weekly, monthly, quarterly, as a standard production support procedure.
QUESTIONS?