State of the Technology

Sam Hartman
MIT Kerberos Consortium
December 11, 2007

Kerberos consortium
www.kerberos.org

Current Activities

* Kerberos 1.7 release
* Improving transparency of MIT Kerberos
* Examining Kerberos and the web
* Exploring Kerberos on mobile devices

Things to Start Now

Absent objections from the board, we will:

* Bring in consultant to work on white papers and best practices for Kerberos
* API and administrator documentation
* Reduce time spent maintaining infrastructure
* Bring in consultants for tightly scoped technical projects to build pool of resources

Potential Opportunities

* Work with Microsoft on FAST -- next generation project to improve Kerberos security
* Put together project to get one-time password support in Kerberos; interest from RSA

What We're Doing

Exploring Kerberos on Mobile Devices

Kerberos on the Web

Transparency of MIT Kerberos

Exploring Kerberos on Mobile Devices

* Strong interest from Apple
* Problems: network performance, ease of use, code size
* Early stage exploration

Kerberos on the Web

* Two aspects:
  - Kerberos and web services
  - Improved use of Kerberos for web mutual authentication
* Ongoing work on the second aspect to be presented at the FSTC later this week
* No resources currently available to explore web services or to implement design for web authentication once completed

Transparency of MIT Kerberos

* Develop policies and procedures for transparent evaluation of projects.
* Recruit additional contributors outside of MIT

Potential Opportunities

Kerberos and FAST

Kerberos and One Time Passwords

Kerberos and FAST

* Joint MIT Microsoft proposal to improve Kerberos security and to work on
* Microsoft is probably significantly ahead in implementation
* Recommendation: continue the protocol work and estimate engineering required for this project

Kerberos and One Time Passwords

* Approached by RSA; interest in adding well-designed support for Secure ID and other tokens
* Tokens heavily used in government and financial sector as well as at MIT
* Recommendation: involve board in finding funding for project; discuss with board whether this would be a priority if funding became available