Kerberos Road Map
Sam Hartman

MIT Kerberos Consortium

April 7, 2008

Goals of Road Map

Priority discussions so far have focused on meeting short or medium term needs. We also need to establish a road map for the future. We should:

- ➜ Prepare Kerberos to meet future challenges so that tomorrow's Kerberos will be attractive in tomorrow's environment.
- ➜ Continue to lead the technology as our sponsors expect.
- ➜ Move forward on all pillars of our strategic vision

Strategic Pillars

We propose to make steady progress in the following areas.

- ➜ Kerberos on the Web
- ➜ Kerberos for Mobile Devices
- ➜ Maintaining and Securing Kerberos
- ➜ Vendor Independence

How We'll Work

- ➜ Report progress on each pillar at board meetings.
- ➜ Requirements analysis, design and standardization of later items proceeds while implementation of earlier items are in progress.

Kerberos on the Web

PRIORITIES

- Understand and analyze Kerberos/web services interactions
  - WS-*
  - Soap
  - XML DSIG/encryption
  - REST
  - SAML
- Gateways between Kerberos, SAML and other federation technologies
- Kerberos through firewalls
- Authentication within the enterprise
- Managing Identity
- Broader Authentication

Web Services

Many Kerberos users are also making a heavy investment in web services. The consortium needs to understand this technology and see where there are gaps it can fill. Examine and Analyze:

- ➜ Protocols
- ➜ How Kerberos is implemented today?
- ➜ Implementation quality and availability

WEB SERVICES

Gap Analysis:

- ➜ Can a Kerberos infrastructure be used to secure all parts of a web services infrastructure?
- ➜ Will extensions to Kerberos break Kerberos integration into web services?
- ➜ Are implementations of these standards sufficiently available to meet customer needs?
- ➜ Is there sufficient documentation?

What We Can Do:

- ➜ Improve standards and documentation.
- ➜ Add necessary support in Kerberos implementation.
- ➜ Identify gaps, but probably not write web services code ourselves.

Gateways to Federation Technology

Kerberos is used alongside SAML and other authentication technologies between organizations. Little thought has been put into making this work in an interoperable manner. There are several challenges.

- ➜ Requesting an authority to convert from one technology to another.
- ➜ Translating information such as entitlements from one format to another
- ➜ Determining trust to assign to an authentication that has crossed mechanism boundaries

KERBEROS THROUGH FIREWALLS

Many companies have developed ad-hoc solutions to allow you to get Kerberos tickets over the same interface that will be used for web traffic.

- ➜ Firewalls near the client and server
- ➜ Kerberos needs to follow same path as application

`http://tools.ietf.org/id/draft-zhu-ws-kerb-04` may be part of the answer.

Authentication within the Enterprise

- ➜ Today, you need to have both a Kerberos and a certificate infrastructure to secure web authentication in the enterprise; work to remove the requirements for two security infrastructures.
- ➜ Improve user experience and configuration
  - ➜ Web browsers all support Kerberos but tend to turn it off by default; find out why.
  - ➜ Make it easier to use Kerberos and other mechanisms on the server side
  - ➜ Work on client configuration issues.

Managing Identity

- ➜ Which identity should be used for a given service (Kerberos IdentityManagement)?
- ➜ Other identity frameworks have a variety of privacy mechanisms; can we take these mechanisms or something similar and use them in Kerberos
- ➜ How do you make this all usable?

What we will do: Continue to work on KIM. Analyze how privacy has been addressed and what the needs are for Kerberos.

Broader Authentication

- ➜ Finish requirements work for web authentication.
- ➜ Participate in discussions of web authentication in standards organizations.
- ➜ Perform market analysis to see where Kerberos used for broader web authentication would benefit people.

MOBILE DEVICES

PRIORITIES

Mobile platforms have relatively limited memory and CPU. Network bandwith is limited, packet loss relatively high and latency very high.

- ➜ Improve Kerberos in high-latency high-packet-loss environments.
- ➜ Reduce memory and CPU footprint.
- ➜ Facilitate Kerberos development for embedded platforms.
- ➜ Credential Management for Mobile Devices

Network Performance

Problems:

- ➜ Lots of DNS traffic
- ➜ Multiple round trips with the KDC

What we can do:

- ➜ Examine caching to reduce DNS traffic and store realm capabilities
- ➜ Advance proposals to have local KDCs perform cross-realm authentication

CPU and Memory

The first step is to profile for memory and CPU usage.

Suspected Targets:

- ➜ Compile time options to strip out unneeded options
- ➜ Use native crypto library
- ➜ Compile out unneeded cache implementations etc.

Facilitate Embedded Development

Kerberos has been ported to VXworks and a number of other embedded operating systems. MIT has little contact with the teams performing these ports.

- ➜ Contact embedded Kerberos users to understand what changes they made and what problems they run into.
- ➜ Understand how Kerberos is used on embedded devices.
- ➜ Propose and prioritize projects as appropriate.

Credential Management for mobile Devices

Typing passwords on cell phones is hard. Storing passwords on cell phones is problematic because they can be stolen.

What we can do::

- ➜ Encourage use of pkinit or single use tokens to avoid dependence on passwords.
- ➜ Study usability of passwords on mobile devices and make recommendations.
- ➜ As appropriate, propose and prioritize projects for extensions to Kerberos that can help.

Maintaining and Securing

PRIORITIES

In order for Kerberos to continue to be a prominent authentication system we need to spend time improving its security and flexibility. Principles:

- ➜ Adopt realistic solutions to security weaknesses
- ➜ Adopt technologies that encourage others to extend Kerberos and use it in new ways

Specific Projects:

- ➜ Finish and implement FAST pre-authentication framework
- ➜ Implement Anonymous Pkinit
- ➜ Implement Mechanism Glue layer
- ➜ Implement PKU2U

FAST Preauth Framework

The FAST preauthentication framework is a necessary first step for any standardized two-factor authentication . FAST will make it much easier to integrate other authentication systems into Kerberos and will fix some long-standing security problems.

Anonymous Pkinit

Anonymous pkinit opens up significant new use cases for Kerberos. It allows a client to know the identity of a server without making its own identity available. It is also relatively easy to implement. We estimate around two months.

PKU2U and Mechanism Glue Layer

These two technologies will enable significant new uses of Kerberos and related security infrastructure.

PKU2U:

- ➜ Mechanism for using certificates in GSS-API
- ➜ Allows application authors to support Kerberos and Certificates using the same code paths and mechanisms
- ➜ Important for NFS

Mechanism Glue:

- ➜ Allows others to create new security mechanisms
- ➜ Significant work on combinations of security mechanisms (pseudomechanisms) that may have long-term value.
- ➜ Demand from one OS vendor already; Sun is already shipping a solution.

VENDOR INDEPENDENCE

The Problem

Kerberos provides many mechanisms for vendor-specific extension. This provides for innovation and product differentiation. Concern for Community:

- ➜ Encouraging vendors to document extensions so others can implement them and maintain interoperability
- ➜ Vendors control the evolution of their extension. What happens when an extension becomes critical and others need to evolve it?

Encouraging Documentation

The Consortium Should:

- ➜ Maintain links to documentation on vendor extensions.
- ➜ Write best practices guidelines for documenting vendor extensions.
- ➜ Work with vendors to encourage them to document extensions and help them in their efforts.

Preserving Open Evolution

The question about what to do in order to avoid single vendors controlling evolution of significant parts of Kerberos is more complicated. Trade Offs:

- ➜ Producing an open alternative to a vendor extension is difficult and at least initially faces significant deployment challenges.
- ➜ However open and competitive evolution has been critical to Kerberos's success.

The consortium has a critical role to play

Preserving Open Evolution

Consortium Role:

- Work with the community to understand where open evolution is critical:
    - Specific examples
    - General requirements and trends
- Find strategies for maintaining open evolution when it is critical.
- Above all, favor interoperability and open evolution; no duplication of work without strong need.