

Implementing PKINIT

Olga Kornievskaja
CITI, University of Michigan

PKINIT: Public Key based initial authentication in Kerberos

- Authentication protocol where both parties are authenticated via X509 certificates
 - Provides two key establishment mechanisms (DH-based, RSA-based)
 - AS_REQ (PA_DATA) contains Alice's signature
 - AS_REP (PA_DATA) contains KDC's signature
- Standards Track IETF RFC4556 (Kerberos working group)

PKINIT implementation history

- Earlier draft implemented by Microsoft (Win2K) and Apple
- Last week Heimdal released version 0.8 which includes PKINIT support
- Microsoft is working toward an RFC-based implementation (Vista)
- RedHat is working on a PKINIT implementation using MIT's preauthentication plug-in

CITI's PKINIT efforts

- Sponsored by Sandia National Labs, CITI has implemented PKINIT and working toward having it included in MIT's Kerberos distribution
- MIT plans to include CITI's PKINIT in their 1.7 release
- Code is currently available in MIT's subversion

CITI's PKINIT implementation

- Support RFC-based PKINIT and Windows-compatible version
- Uses MIT's preauthentication plug-in interface
- Provides modular cryptographic interface
 - CITI's implementation uses OpenSSL crypto
- Provides configurable and modular credential storage

PKINIT interoperability

- Preliminary testing
 - CITI, Heimdal, RedHat implementations interoperate
 - All unix clients interoperate with Win2K KDC
 - Vista (PKINIT client) and Longhorn (PKINIT server) are broken
 - CITI and Heimdal KDCs support Win2K clients but we were unable to test Win2K client against a unix KDC
- CITI is hosting an interoperability event in May

PKINIT w/ smartcards

- Window's PKINIT only supports smartcards-based PKINIT
- Heimdal and CITI's PKINIT support various credential storage locations and modular interface to retrieving them
 - PKCS11 (Smartcards, soft tokens)
 - File system

PKINIT testing

- ActivCard, Cryptoflex, Coolkey, CAC (any open-sc supported cards)
 - Buggy ActivCard
- Platforms tested (includes 32&64-bit):
 - Linux, Solaris, MacOS (Ken Renard)

Naming in PKINIT

- Client identity
 - Kerberos principal name encoded in an X509 SAN
 - Mapping facility at the KDC (ie, file, ldap)
 - MUST have X509 EKU fields
- KDC identity (win2k)
 - KDC's hostname is encoded in an dnsName SAN
- Implementation needs a modular name mapping design

PKINIT Summary

- <http://www.citi.umich.edu/projects/pkinit>
- PKINIT interoperability event May 30th&31th

NFSv4 PKi GSS mechanism

- SPKM3 is out
- Public key user-to-user authentication (PK2U) might be in
 - It's "PKINIT without KDC"
 - IETF draft (Larry Zhu, Microsoft)
 - <http://www.ietf.org/internet-drafts/draft-zhu-pku2u-01.txt>
 - Microsoft is working on an implementation