Updates from MIT Kerberos

Benjamin Kaduk
kaduk@mit.edu bkaduk@akamai.com

20 August, 2015

While we were gone...

Current release (1.13)

- Security

Coming soon...

- krb5-1.14
- KfW
- On the horizon
- A bit further off

Things you should know about but might have missed

- `KRB5_TRACE`
- kadmin purgekeys for krbtgt rekeying
- `DIR:` ccache type and collection-enabled ccaches
- GSS acceptors can wildcard hostname part of host-based service
- client keytabs

krb5-1.12

Freshly released for EAKC 2014, but a quick recap:

- More plugin interfaces: aname-to-lname, kuserok, host-realm, default-realm
- KDB policy records are more flexible; no refcounts → better performance
- Support principals with no long-term keys (e.g., for OTP/PKINIT)
- KDC support for FAST OTP (RFC 6560)
- Improvents to the `KEYRING:` cache, including collection support
- AES-NI when available
- Experimental KDC audit pluggable interface

Schedule

- Shortened 10-month release cycle (1 year is normal)
- Released on-schedule October 15, 2014
- Should align better with OS releases (Fedora, Ubuntu, etc.)
- (krb5-1.14 is expected in October 2015)

krb5-1.13 features

- HTTP(S) transport — MS-KKDCP HTTP proxy
- Hierarchical iprop
- Support for configuring GSS mechanisms via `/etc/gss/mech.d/*.conf`
- Support for SASL binds in the LDAP KDB backend
- KDC listens on TCP by default
- KCM: cache type for Heimdal (e.g., OS X) compatibility
- Support for unlocked database dumps for the DB2 KDB backend, to allow the KDC and kadmind to continue processing requests during dumps

Late-breaking news in krb5-1.13

- SPNEGO improvements for out-of tree mechs (e.g., NTLM)
- fix build against libressl
- ksu cleanup

Late-breaking news in krb5-1.13

- SPNEGO improvements for out-of tree mechs (e.g., NTLM)
- fix build against libressl
- ksu cleanup (but maybe you shouldn't use ksu)

Late-breaking news in krb5-1.13

- SPNEGO improvements for out-of tree mechs (e.g., NTLM)
- fix build against libressl
- ksu cleanup (but maybe you shouldn't use ksu)
- KDC logging works with redirected stderr
- Incremental improvements to the replay cache performance and correctness

MS-KKDCP

- HTTPS transport, reduces plaintext leakage
- Proxy can in principle filter out bogus requests, and gateway into DMZ
- Lets clients talk to KDCs that might otherwise be unreachable
- Kind of like IAKERB, but...actually deployed

replay cache

Some protocols can be designed to not need a replay cache (by using an acceptor subkey or other key confirmation methods).

For safety and correctness, other protocols need a cache to detect and avoid replay attacks. MIT krb5 supplies such an implementation at the library level, but the implementation is not very performant.

Is replay cache performance an issue for anyone here? Please talk to us!

Security Advisories

MITKRB5-SA-2014-001:

- CVE-2014-4345: Buffer overrun in kadmind with LDAP backend
- `cpw -keepold` triggered miscounting of array size

Security Advisories

MITKRB5-SA-2014-001:

- CVE-2014-4345: Buffer overrun in kadmind with LDAP backend
- `cpw -keepold` triggered miscounting of array size

MITKRB5-SA-2015-001

- CVE-2014-5352: gss_process_context_token() incorrectly frees context

Security Advisories

MITKRB5-SA-2014-001:

- CVE-2014-4345: Buffer overrun in kadmind with LDAP backend
- `cpw -keepold` triggered miscounting of array size

MITKRB5-SA-2015-001

- CVE-2014-5352: gss_process_context_token() incorrectly frees context
- CVE-2014-9421: kadmind doubly frees partial deserialization results

Security Advisories

MITKRB5-SA-2014-001:

- CVE-2014-4345: Buffer overrun in kadmind with LDAP backend
- `cpw -keepold` triggered miscounting of array size

MITKRB5-SA-2015-001

- CVE-2014-5352: gss_process_context_token() incorrectly frees context
- CVE-2014-9421: kadmind doubly frees partial deserialization results
- CVE-2014-9422: kadmind incorrectly validates server principal name

Security Advisories

MITKRB5-SA-2014-001:

- CVE-2014-4345: Buffer overrun in kadmind with LDAP backend
- `cpw -keepold` triggered miscounting of array size

MITKRB5-SA-2015-001

- CVE-2014-5352: gss_process_context_token() incorrectly frees context
- CVE-2014-9421: kadmind doubly frees partial deserialization results
- CVE-2014-9422: kadmind incorrectly validates server principal name
- CVE-2014-9423: libgssrpc server applications leak uninitialized bytes

While we were gone...

Current release (1.13)

- Security

Coming soon...

- krb5-1.14
- KfW
- On the horizon
- A bit further off

Upcoming items from MIT Kerberos

- krb5-1.14 in October
- KfW 4.1 expected . . . sometime this year

krb5-1.14 features

- CAMMAC
- Authentication Indicator
- Hopefully, a reporting-friendly dump format
- gss_acquire_cred_with_password behavior change
- make `FILE:` cache somewhat more efficient
- Don't generate new des3 and arcfour keys by default
- Option for site-specific error message wrapping, and include the `FILE:` ccache name in errors
- Use Linux OFD locks when available

krb5-1.14 features (continued)

- (developers only) note skipped tests in `make check` output
- Incremental improvements to multi-hop preauthentication
- document `FILE:` ccache and keytab file formats
- Support 32-bit kvno keytab extensions
- Log a notice when kadm5.acl fails to parse
- Disallow principal renames with LDAP backend
- Improvements to incremental database propogation
- Limit use of "old" and "wrong" krb5 mechanism OIDs
- Limit use of IAKERB

CAMMAC

- Signed authorization data, originating from KDC
- Can be safely passed back to KDC for processing, unlike AD-KDC-ISSUED
- Generic container, can be used for authentication indicator, PAD, storing other data only available at initial authenticaiton, ...

Authentication Indicator

- Client principals could have multiple usable preauth mechanisms

Authentication Indicator

- Client principals could have multiple usable preauth mechanisms
- Services want to know how (strong) the initial authentication was

Authentication Indicator

- Client principals could have multiple usable preauth mechanisms
- Services want to know how (strong) the initial authentication was
- Encrypted timestamp is fine for mail, but need OTP for payroll access, or PKINIT for making changes in puppet

Authentication Indicator

- Client principals could have multiple usable preauth mechanisms
- Services want to know how (strong) the initial authentication was
- Encrypted timestamp is fine for mail, but need OTP for payroll access, or PKINIT for making changes in puppet
- Carried in a CAMMAC to prevent tampering

Authentication Indicator

- Client principals could have multiple usable preauth mechanisms
- Services want to know how (strong) the initial authentication was
- Encrypted timestamp is fine for mail, but need OTP for payroll access, or PKINIT for making changes in puppet
- Carried in a CAMMAC to prevent tampering
- A string identifier (readable, but "opaque" to machines) for the initial authentication

Authentication Indicator

- Client principals could have multiple usable preauth mechanisms
- Services want to know how (strong) the initial authentication was
- Encrypted timestamp is fine for mail, but need OTP for payroll access, or PKINIT for making changes in puppet
- Carried in a CAMMAC to prevent tampering
- A string identifier (readable, but "opaque" to machines) for the initial authentication
- Different OTP schemes can get different strings (e.g., hardware token vs. app on phone

KfW 4.1 outline

- KfW 4.0 (based off krb5-1.10) was released in 2012
- ~~Time~~ past time for an update
- Based off krb5-1.13
- Waiting for feedback from testers to release
- Please test KfW 4.1 beta 2!

KfW 4.1 features

- Improved support for MSLSA: ccache type
- New library for ribbon interface, more accessible for screen readers
- Registry key for default realm
- Modernization in installer sources
- All the features from krb5 1.11 through krb5 1.13

Candidates for krb5-1.15

- SPAKE preauth
  - prevents offline dictionary attack
  - forward secrecy in generated session keys (with respect to the password-derived key)
  - option for two-factor as part of same exchange
  - For simple second factors, attacker can't tell which factor was wrong

Candidates for krb5-1.15

- SPAKE preauth
  - prevents offline dictionary attack
  - forward secrecy in generated session keys (with respect to the password-derived key)
  - option for two-factor as part of same exchange
  - For simple second factors, attacker can't tell which factor was wrong
- More progress on Python kerberos for testing?
- More progress on moving DNS resolution off clients to the KDC

Ongoing in the IETF

- PAD, akin to the MSFT PAC
- New (faster?) enctypes
- Java GSS bindings updates (streams? no streams?)
- Deprecate des3 and arcfour
- PKINIT algorithm agility
- Extra round trips for AP exchange
- Convince us to take on your idea!

Long-term goals

- Stop relying on the DNS!
- Let the KDC do the resolution, possibly via a local (trusted) copy of the zone file
- Pluggable interface for kadmin ACLs
- API or KCM-like credentials cache
- much more

Thanks!