Identity management Desktop integration

Alexander Bokovoy • 2016.02.04

Single sign-on everywhere

Use GSSAPI to rely on a single sign-on event:
Logon to the system once

- Obtain Kerberos ticket as result of logon
- Be able to login to VPN with it
- Be able to configure GNOME online accounts with it
- Be able to sign-in to web apps with it

Browsers - Zero Configuration

Effortless configuration

- Use GSSAPI for HTTPS sites without explicit configuration in the browser

Effortless management

- Allow users to control what credentials were used by which sites

Browser - Common flow

HTTPS-enabled site

- For WWW-Authenticate: Negotiate header
- Attempt to obtain ticket to HTTP/<fqdn> for this site
- Initiate GSSAPI authentication in case of success

UX flow

- For first attempt to logon, ask user if single sign-on is allowed, remember the choice
- Use visual indication that single sign-on happened

Browser - Common flow

GSSAPI flow is synchronous

- Don’t block browser’s UI
- Obtaining ticket could take time, visually indicate it
- Bugs in browsers need to be cared for: NTLMSSP support requires it

Multiple identities

- Directory and Kernel keyring credentials caches allow storing tickets for multiple principals
- Allow choosing Kerberos principal intended for use
- Automatic selection is fine for now (libkrb5 has it)

Browser - Common flow

Management

- Which sites were visited
- What identities were used to authenticate
- Add/remove domain or site from the list
- Support black list?

Privacy concerns

Getting HTTP/<fqdn> ticket for all HTTPS sites means

- KDC will know your browsing history to the level of a hostname
- Knowledge of your principal may leak out to browser plugins/extensions

Browsers at war

Firefox - current state

Configuration

- Manual configuration in about:config

User experience

- GSSAPI is locking up the browser UI in case there obtaining ticket is long

Firefox - current state

Management

- No review what sites were provided with single sign-on
- No selection of which principal to use if there are multiple credential caches

Privacy

-

Firefox - current state

Bugs

- Kerberos configuration is ugly:
  - https://bugzilla.mozilla.org/show_bug.cgi?id=520668
- Kerberos authentication is unusably slow when it fails
  - https://bugzilla.mozilla.org/show_bug.cgi?id=890908

Chrom{e,ium} - current state

Configuration

- Machine-wide configuration in /etc
- No user-visible configuration at all
- Command-line configuration

User experience

- No GSSAPI unless explicitly configured
- NTLMSSP processing has bugs that force a pop-up in case no Kerberos ticket is available even if no NTLMSSP is requested

Chrom{e,ium} - current state

Management

-

Privacy

-

Chrom{e,ium} - current state

Bugs

https://code.google.com/p/chromium/issues/list?can=2&q=gssapi

Epiphany - current state

Configuration

- Zero-configuration once https://bugzilla.gnome.org/show_bug.cgi?id=587145 is fixed

User experience

- GSSAPI is locking up the browser UI in case there obtaining ticket is long (need to verify)

Epiphany - current state

Management

- No review what sites were provided with single sign-on
- No selection of which principal to use if there are multiple credential caches

Privacy

-

Epiphany - current state

Bugs

- Main bug (libsoup):
  - https://bugzilla.gnome.org/show_bug.cgi?id=587145
- Google Apps compatibility bug
  - https://bugzilla.gnome.org/show_bug.cgi?id=753610

GNOME Online Accounts

GNOME Online Accounts

Support for GSSAPI

- Transparent with libsoup/WebkitGTK
- Only is added to web services with own logon page

User experience

- Cannot enable single sign-on to Owncloud, for example

GNOME Online Accounts

Management

- Zero details on what principals are in use
- Zero details on what tickets were obtained and how valid they are

User experience

- Current UI for Kerberos details is unusable