T&I Incubator: OIDC Support for SSH under Windows

Final demo – 21st September 2021

Dmytro Dehtyarov
Agenda

• Motivation & Background
• Port oidc-agent to Windows
• Communication with oidc-agent
• Integration with putty
• Outlook
Agenda

• Motivation & Background
• Port oidc-agent to Windows
• Communication with oidc-agent
• Integration with putty
• Outlook
Motivation

• SSH Key Management
• Risks of untracked and unmanaged SSH Keys
• 90% of keys are no longer used [1]
Motivation

Access Tokens!

Identity Provider

Request access token

Access userinfo

private/public keys

SSH

...
Goals

- High-Level: Integrate OIDC with SSH (client-side) under **Windows**
  - Port oidc-agent to Windows
  - Integrate oidc-agent into SSH client Putty
  - Extend putty for access token based authentication
High-Level Architecture

• oidc-agent VS. ssh-agent

1. Obtain access token
   (Refresh access token)

2. OIDC Workflow

3. SSH

4. Access userinfo

OIDC-capable SSH Server
Agenda

• Motivation & Background
• Port oidc-agent to Windows
• Communication with oidc-agent
• Integration with putty
• Outlook
oidc-agent

• Command-line tools
  • oidc-agent
  • oidc-gen
  • oidc-add
  • oidc-token

• Available for Linux and MacOS

https://github.com/indigo-dc/oidc-agent
Possibilities to port oidc-agent

✗ • Windows Subsystem for Linux 2
  • No changes to source code
  • Not user-friendly

✗ • Build natively
  • Rewrite platform-dependent code (IPC, pthreads, etc)

✓ • POSIX emulation layer – Cygwin, MSYS
  • Moderate changes to source code
  • Semi-native approach
Build oidc-agent with MSYS2

• Source code modifications
  • Using compiler directives
  • Excluded functionalities
  • Implemented registry connector
  • Adapted building procedures

• Build with ’make’
  • Same codebase
  • Produces .exe binaries

• Build&Installation script

```c
#ifdef __MSYS__
#include <windows.h>
#endif
```
oidc-agent on Windows

• Github
  • https://github.com/indigo-dc/oidc-agent/tree/windows

Demo
oidc-agent on Windows
Agenda

• Motivation & Background
• Port oidc-agent to Windows
• Communication with oidc-agent
• Integration with putty
• Outlook
liboidc-agent API

- Static/dynamic library
  - Unix Domain Sockets
  - Requires compatibility layer!
- Goal: compile API library natively
Native liboidc-agent API library

- Reimplemented IPC using winsock
- Talk directly with emulated sockets
  - Authentication handshake
- Compiled using mingw-w64 (MSYS2 or cross-compile on Linux)
Native liboidc-agent API library

• Originally only for oidc-token
• Refactored & extended for other tools
• Following endpoints available:
  • getAccessToken
  • getAccessTokenForIssuer
  • getLoadedAccountsList
Agenda

• Motivation & Background
• Port oidc-agent to Windows
• Communication with oidc-agent
• Integration with putty
• Outlook
Putty

- Client for **SSH**, Telnet, ...
- Putty, Plink, PSFTP, PSCP
- Originally written for Windows
- Supports authentication:
  - no-auth
  - password
  - public key
  - Gssapi
  - keyboard-interactive
  - ... OIDC access tokens
OIDC Based Authentication

• Server:
  • SSH server with pam-ssh-oidc
  • Mapping daemon motley_cue

1. Retrieve access token
2. Deploy local account/get username
3. Input access token when prompted
   • Subtype of keyboard-interactive auth
OIDC Based Authentication

• Available for:
  • Putty
  • Plink
  • PSFTP
  • PSCP

• Built using mingw-w64
  • Windows (MSYS2 – mingw32)
  • Cross-compile on Linux
OIDC Based Authentication

• Git:
  • https://git.scc.kit.edu/m-team/putty/-/tree/oidc-support

Demo
OIDC based authentication
Agenda

• Motivation & Background
• Port oidc-agent to Windows
• Communication with oidc-agent
• Integration with putty
• Outlook
Outlook

• Provide installer for oidc-agent
  • Better user-experience
• Build liboidc-agent.lib for Windows environment (MSVC)
• Provide OIDC support for Putty under supported compilers
  • Clang
  • MSVC
  • LCC
• Discuss and publish putty extension
Summary

• All requirements satisfied
• oidc-agent runs on Windows
• liboidc-agent works on Windows
• Putty supports authentication with access tokens for SSH

Requirements
• oidc-agent obtains/manages access tokens on Windows
• oidc-agent must be easy-to-install on Windows
• oidc-agent runs as a daemon (Windows Service) providing an API
• putty allows to select between ssh-keys and oidc-tokens (pageant VS. oidc-agent)
• putty supports authentication&authorization with oidc-tokens against supported ssh-server
• putty obtains valid access tokens from oidc-agent
• putty provides a simple GUI for oidc-gen
Thank you

Any questions?

www.geant.org
References

[1] https://www.ssh.com/academy/iam/ssh-key-management
[5] https://images.app.goo.gl/bUgQzq5YaTPamEXP8
[12] https://images.app.goo.gl/M1eHHZSzY1cc9X37A
[13] https://docs.google.com/presentation/d/17HM11YjafC5VA4_o2EjNrtbRqJGgQP0q92C_uqFAM6A/edit