redhat

Joining a domain the windows way

Günther Deschner
gd@samba.org

(Red Hat / Samba Team)

Joining before Samba 3.2

- `net rpc join` and `net ads join` implement all join code in the “net” binary monolithically
- Configuration must always have been set appropriately before the join
- 3rd party applications could just do upcalls to the “net” binary, and in case of error, parse stdout return
- We wanted to change this and provide something better

New Joining methods in Samba 3.2

- Support for joining Windows 2008
- Internal library libnetjoin
- Shared library offering a "`NetJoinDomain`" call
- Ability to join with an empty configuration file
- Ability to join remotely
- Ability to be joined remotely
- Example gtk GUI for joining

Joining with an (almost) empty smb.conf

- Samba 3.2 has a new `libsmbconf` internal interface
- Provides read/write access for storing Samba configuration in the local samba registry
- Frontend Samba: `net conf`
- Frontend Windows: `regedit.exe`
- Based on this `libsmbconf`, libnetjoin can join a client with a minimal smb.conf file:

```
[global]
        config backend = registry
```

Live Demo

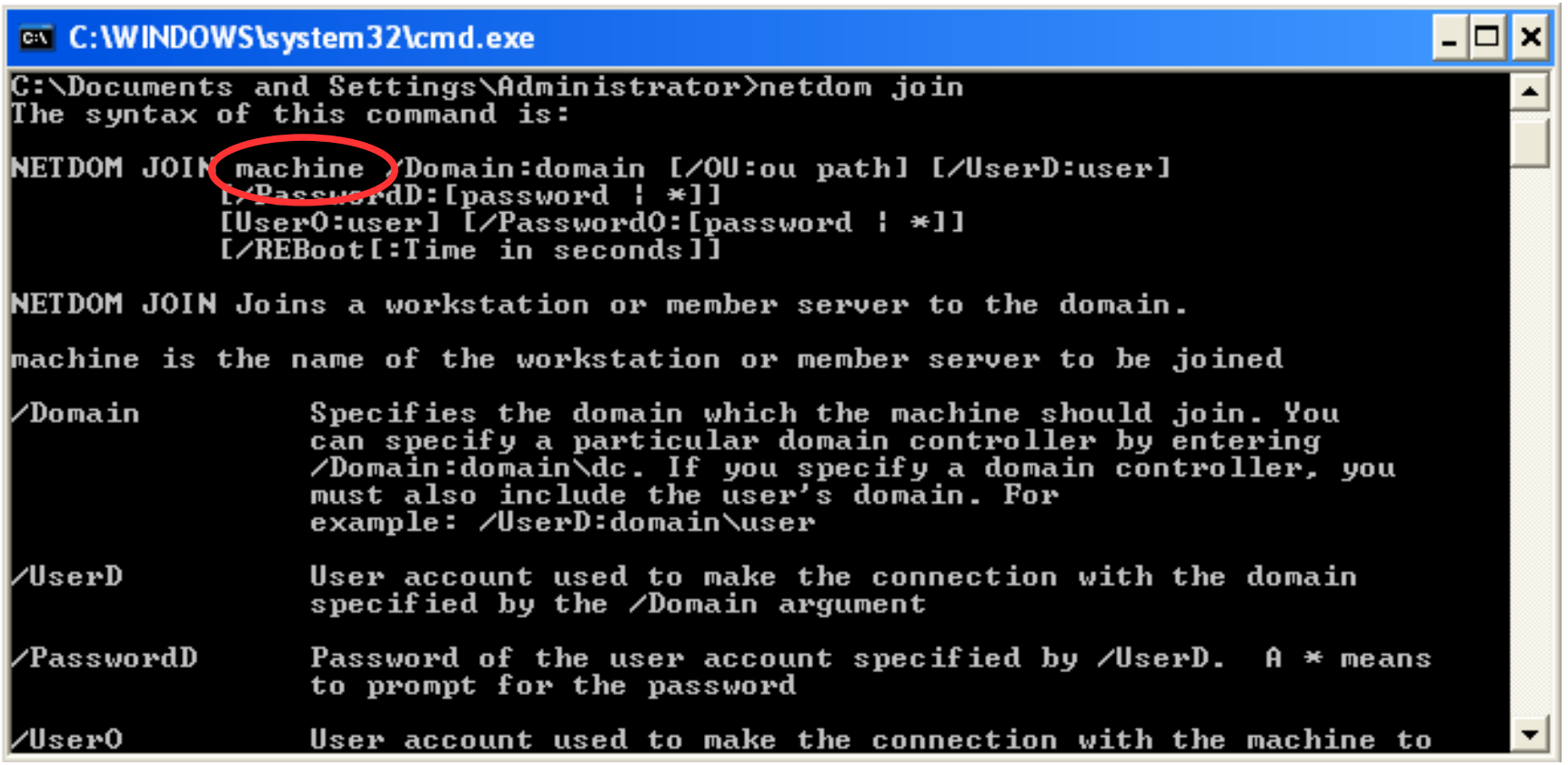
net ads join
&
“config backend = registry”

Joining and Unjoining on Windows ?

- Joining using the gui
- Joining using the command line “netdom join”

Windows netdom join tool

- Windows can join the local or a ***remote*** host to a domain



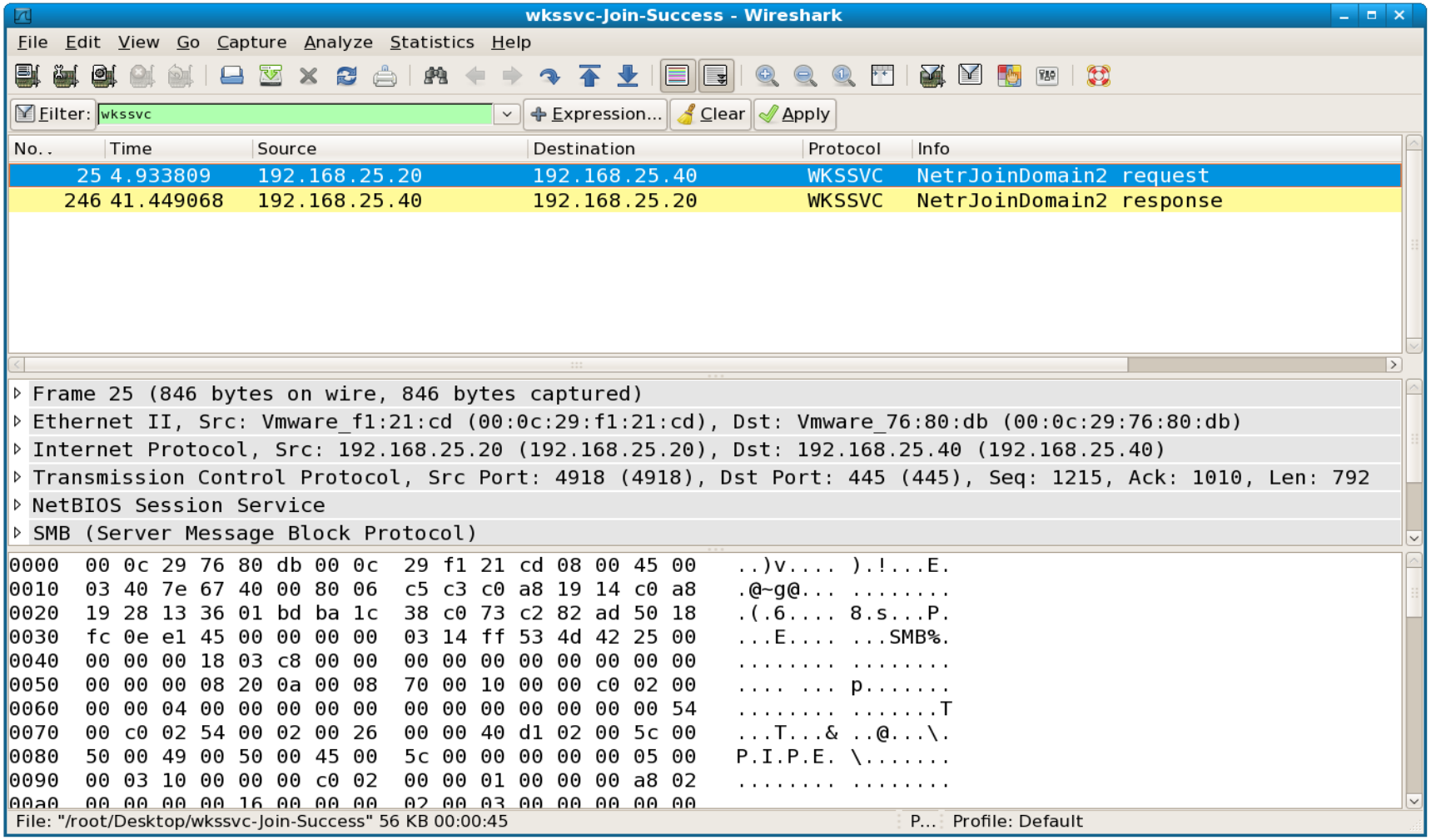
Windows netdom join tool

- At that time there was no documentation available
- We wanted to know:
- How does this actually work?
- How are admin credentials transfered to the remote computer?
- What crypto is being used for this?
- What does that command trigger on the remote computer ?
- And once we have all these answers: can we do this as well ?

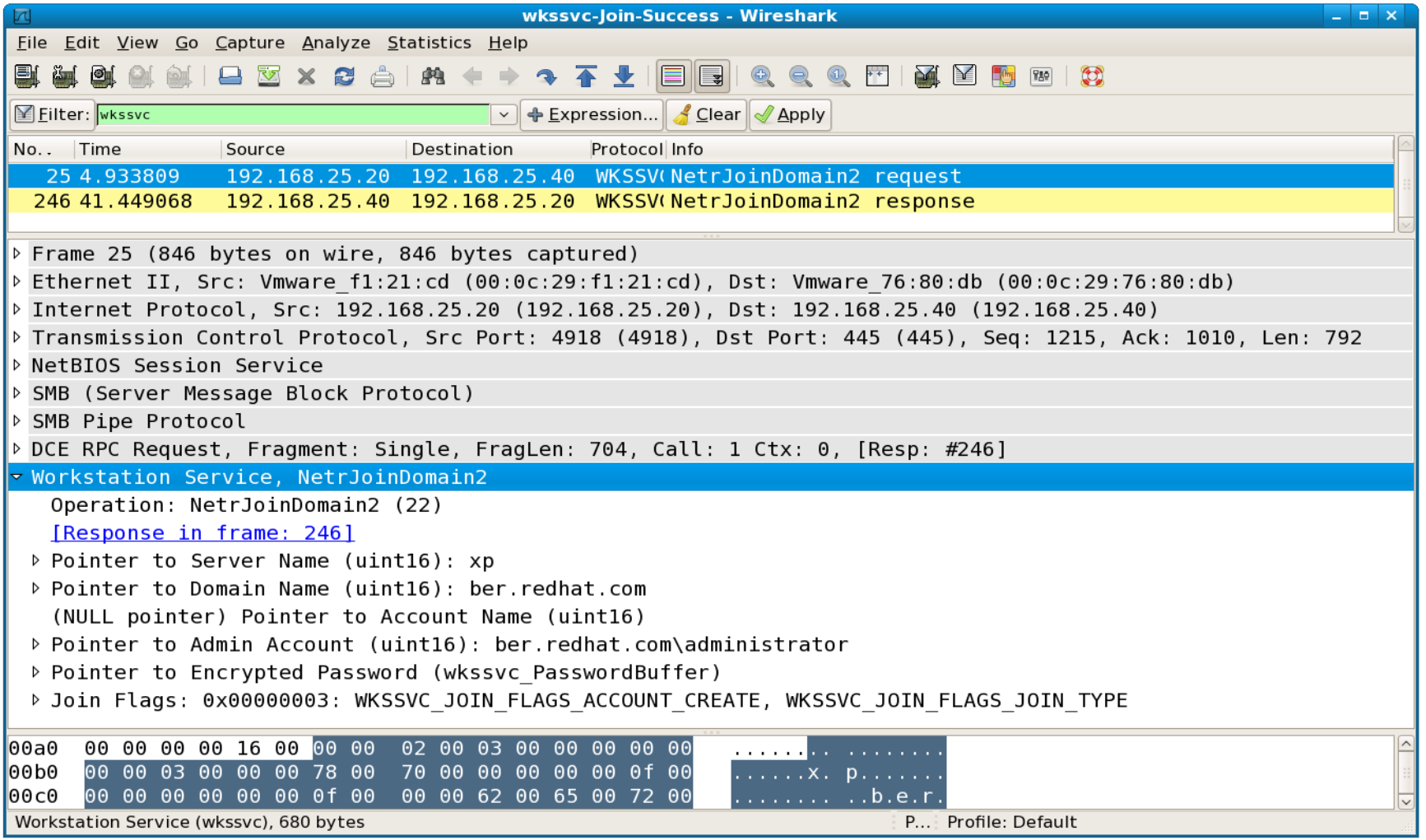
Windows netdom join tool

- Connects to remote computer using current or given credentials
- Opens the remote Workstation Service Named Pipe (`WKSSVC`)
- Calls `NetrJoinDomain2` which transports another set of domain credentials which are used by the remote computer to join the domain
- Also allows to specify Account OU to be joined to
- Once the remote computer receives this request, it gets very active

What NetrJoinDomain2 triggers...



... the mysterious encrypted password



An undocumented 524 byte buffer

- What is the algorithm? Tried all kinds of known and possible combinations using samba4 smbtorture tests
- After some weeks, got WERR_BAD_PASSWORD instead of WERR_LOGON_FAILURE so found the first part of the puzzle
- Final result:
- Cleartext admin password encoded in a 516 byte buffer (like `samr_CryptPassword`)
- 8 byte confounder in front of the 516 byte buffer
- MD5Update *first* called with session_key, *then* with confounder
- Finally encrypted with RC4 using confounded session key

Finding a home for remote domain join

- Samba4 `smbtorture` became able to remotely join clients in a domain
- Long term `smbtorture` was surely not the best place for such a feature
- On Windows NetApi32.lib provides a `NetJoinDomain` call
- The `NetJoinDomain` call looks very similar to `wkssvc_NetrJoinDomain2` as seen on the wire (except the password buffer)
- Started very basic `libnetapi.so` trying to implement this call

`libnetapi` – An API for network management

- Offer similar interface as on windows
- Initially only to support join related calls
- Extended `pidl` version to autogenerate libnetapi based on IDL
- Most calls wrap around rpc call sequences
- Example: `NetUserAdd` on windows calls:
  - `samr_Connect5,`
    `samr_EnumDomains,`
    `samr_LookupDomain,`
    `samr_OpenDomain,`
    `samr_CreateUser2,`
    `samr_QueryUserInfo,`
    `samr_GetUserPwInfo,`
    `samr_SetUserInfo2`

`libnetapi.so` – RPC client library

- Samba 4 IDL based auto-generated rpc client code everywhere
- WKSSVC and WINREG was already done
- migration of LSARPC, SAMR, NETLOGON, DSSETUP and SRVSVC to Samba4 IDL was missing
- Initially only pidl generated *client* was planned but server code needed to be migrated at the same time
- That took some time
- Now fixing or adding new features / infolevels to Samba RPC client or server is much easier

`libnetapi.so` - local vs. remote

- In Windows each Net* call has a `server_name` field as the first argument
- `server_name` is used to distinguish local or remote processing most of the time
- In Samba, local processing could use `LIBSMB_PROG` to talk to the local RPC server.

Implemented calls in libnetapi

- NetJoinDomain
- NetUnjoinDomain
- NetGetJoinInformation
- NetGetJoinableOUs
- NetServerGetInfo
- NetServerSetInfo
- NetGetDCName
- NetGetAnyDCName
- DsGetDcName
- NetUserAdd
- NetUserDel, NetUserEnum, NetQueryDisplayInformation, etc., etc.

NetJoinDomain in netapi.h

- Defined in `netapi.h`
- Very simple call, hides all complexity from the caller
- Does anything required to join the local or a remote computer into a domain
- Admin credentials are given in clear, `NetJoinDomain` takes care of encryption details
- Header:

```
NET_API_STATUS NetJoinDomain(const char * server /* [in] */,
                             const char * domain /* [in] [ref] */,
                             const char * account_ou /* [in] */,
                             const char * account /* [in] */,
                             const char * password /* [in] */,
                             uint32_t join_flags /* [in] */);
```

NetJoinDomain example binaries

- **`netdomjoin` in lib/netapi/examples directory**

```
Usage: netdomjoin hostname
     --ou=ACCOUNT_OU                 Account ou
     --domain=DOMAIN                 Domain name (required)
     --userd=USERNAME                Domain admin account
     --passwordd=PASSWORD            Domain admin password

Help options:
     -?, --help                      Show this help message
     --usage                         Display brief usage message

Common samba netapi example options:
     -U, --user=USERNAME             Username used for connection
     -p, --password=PASSWORD         Password used for connection
     -d, --debuglevel=DEBUGLEVEL     Debuglevel
     -k, --kerberos                  Use Kerberos
```

NetJoinDomain example binaries

- **`net dom join` as a sub command of `net`**

```
usage: net dom join <domain=DOMAIN> <ou=OU> <account=ACCOUNT>
<password=PASSWORD> <reboot>
```

NetJoinDomain locally - libnetjoin

- Needed to abstract all join calls of “net ads join” to make them available outside of the net binary
- Started internal library libnetjoin
- NetJoinDomain calls libnetjoin when server_name is NULL.
- libnetjoin uses IDL for the join and unjoin context

Libnetjoin - input

```
libnet_JoinCtx: struct libnet_JoinCtx
        in: struct libnet_JoinCtx
             dc_name                  : 'w2k3dc-rhber'
             machine_name             : 'MTHELENA'
             domain_name              : *
                  domain_name             : 'BER.REDHAT.COM'
             account_ou               : NULL
             admin_account            : 'administrator'
             admin_password           : 'password'
             machine_password         : NULL
             join_flags               : 0x00000023 (35)
                  0: WKSSVC_JOIN_FLAGS_JOIN_WITH_NEW_NAME
                  0: WKSSVC_JOIN_FLAGS_JOIN_DC_ACCOUNT
                  0: WKSSVC_JOIN_FLAGS_DEFER_SPN
                  0: WKSSVC_JOIN_FLAGS_MACHINE_PWD_PASSED
                  0: WKSSVC_JOIN_FLAGS_JOIN_UNSECURE
                  1: WKSSVC_JOIN_FLAGS_DOMAIN_JOIN_IF_JOINED
                  0: WKSSVC_JOIN_FLAGS_WIN9X_UPGRADE
                  0: WKSSVC_JOIN_FLAGS_ACCOUNT_DELETE
                  1: WKSSVC_JOIN_FLAGS_ACCOUNT_CREATE
                  1: WKSSVC_JOIN_FLAGS_JOIN_TYPE
             os_version               : NULL
             os_name                  : NULL
             create_upn               : 0x00 (0)
             upn                      : NULL
             modify_config            : 0x00 (0)
             ads                      : NULL
             debug                    : 0x01 (1)
             secure_channel_type      : SEC_CHAN_WKSTA (2)
```

Libnetjoin - output

```
libnet_JoinCtx: struct libnet_JoinCtx
        out: struct libnet_JoinCtx
             account_name             : NULL
             netbios_domain_name      : 'BER'
             dns_domain_name          : 'ber.redhat.com'
             dn                       :
                  'CN=mthelena,CN=Computers,DC=ber,DC=redhat,DC=com'
             domain_sid               : *
                  domain_sid              : S-1-5-21-1800104011-1129049609-1243822444
             modified_config          : 0x00 (0)
             error_string             : NULL
             domain_is_ad             : 0x01 (1)
             result                   : WERR_OK
```

Samba 3.2 NetrJoinDomain2 server-side

- Samba 3.2 has also support for remote join and unjoin server side
- Admin credentials need to be provided
- Only members of the Domain Admin and Local Administrators group can call this
- Needs to handle more post-processing
  (local modification, group policy)
- Needs be transaction based

Live Demo

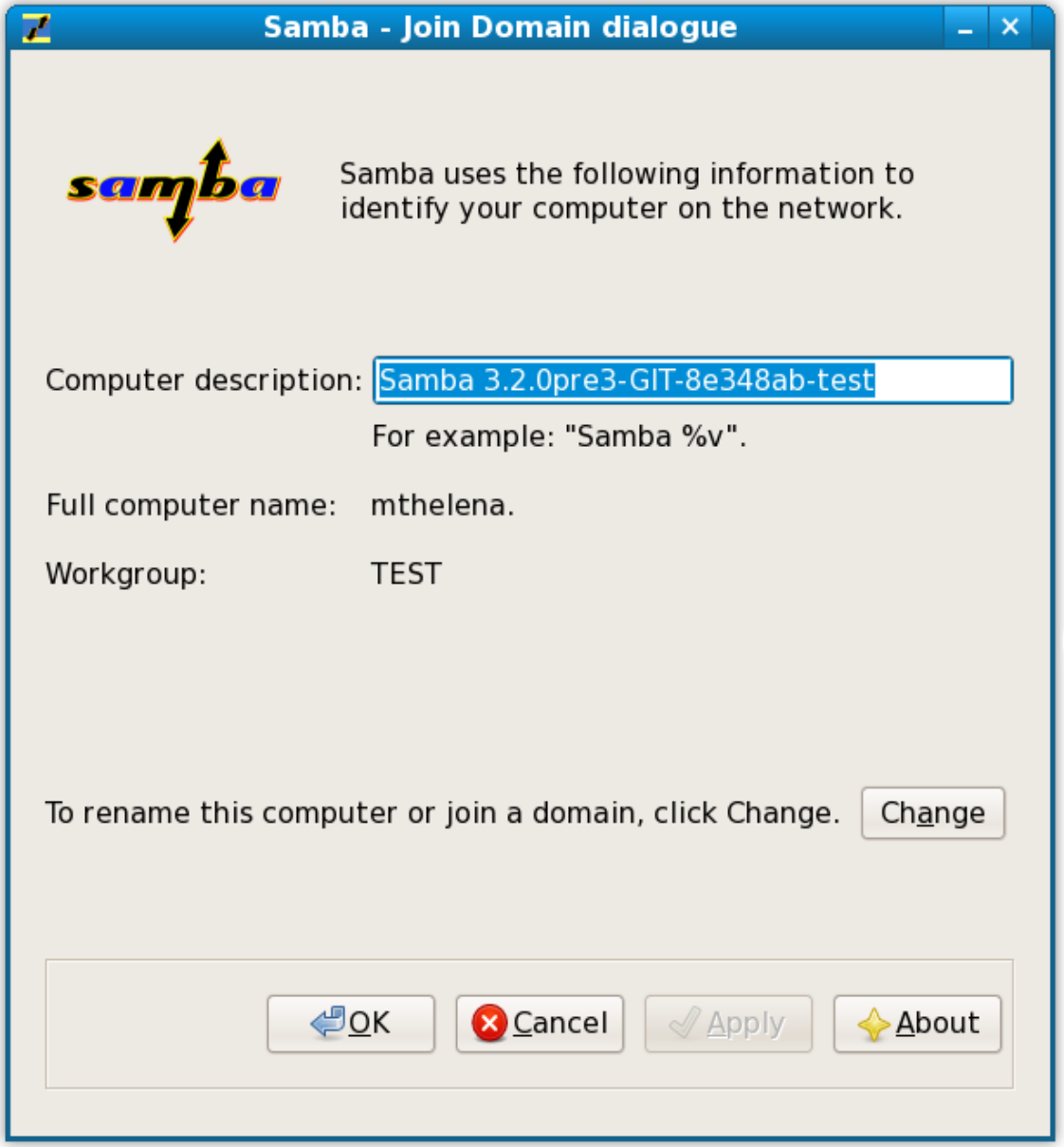
Samba joins XP to W2K3
XP joins Samba to W2K3

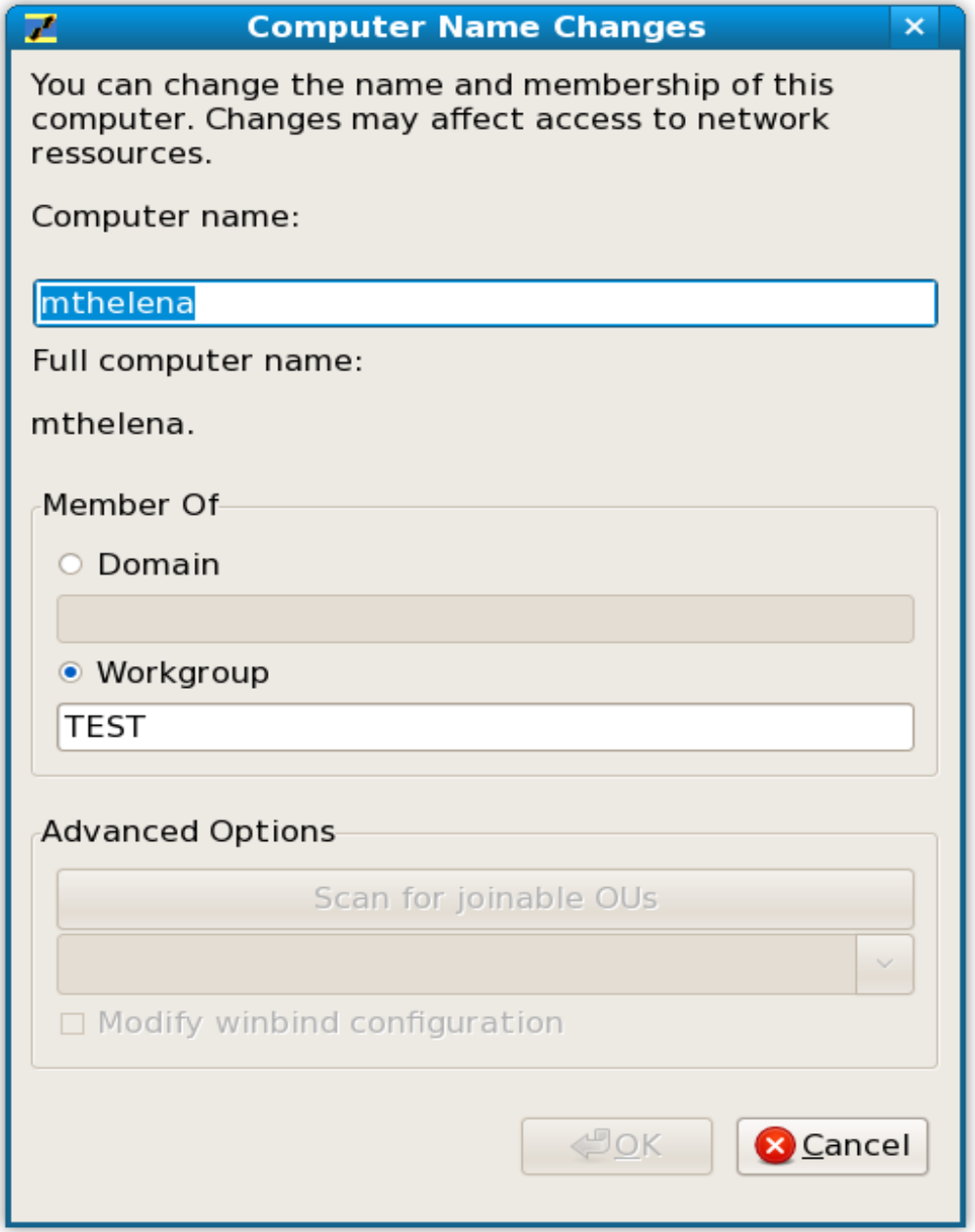
Grow your own...

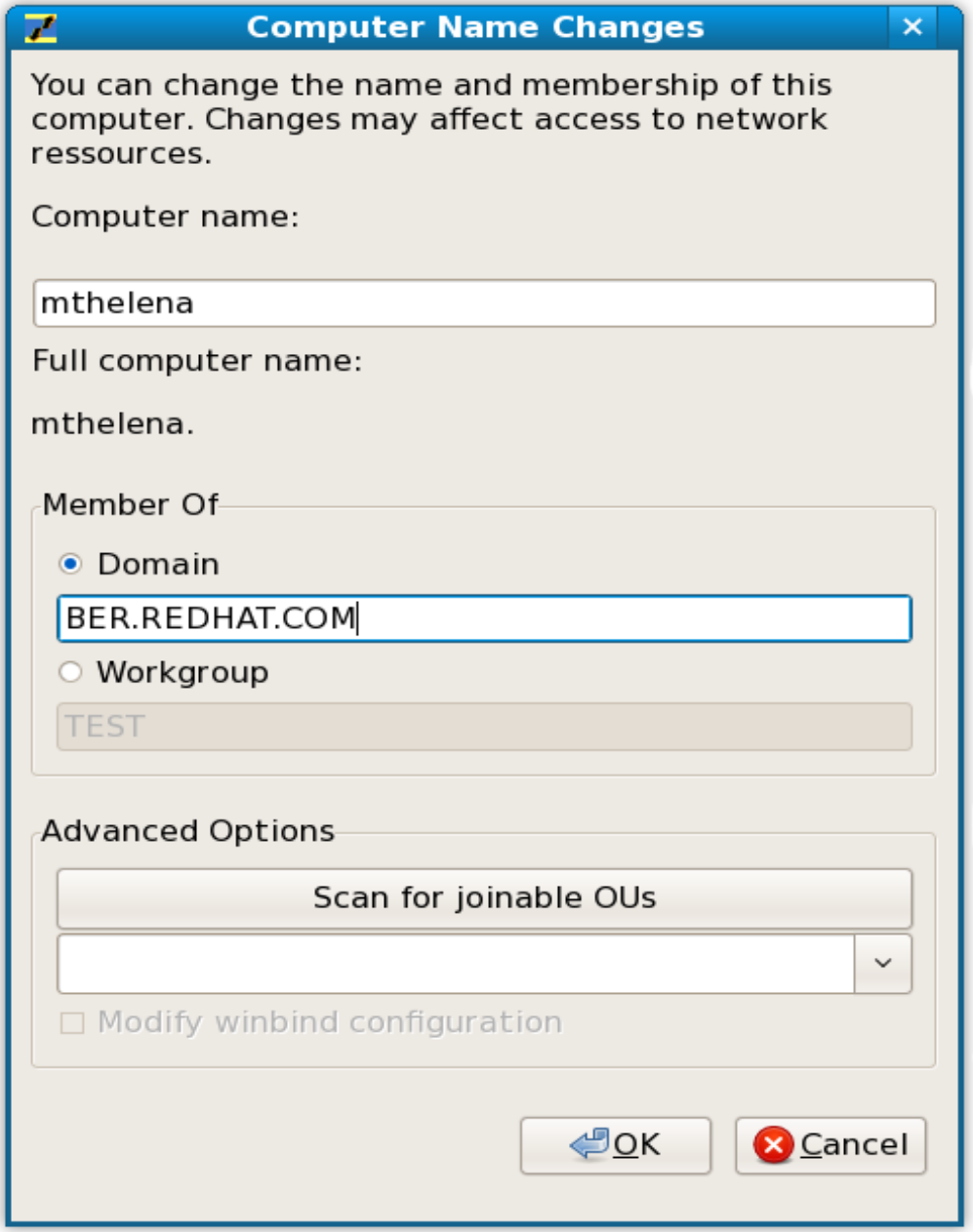
- Now that we had the abstraction in libnetjoin, as well as the abstraction in libnetapi, all kinds of new applications can be written
- One experiment was to offer a Windows-like interface for joining a workstation into a domain
- gtk domainjoin gui in lib/netapi/examples

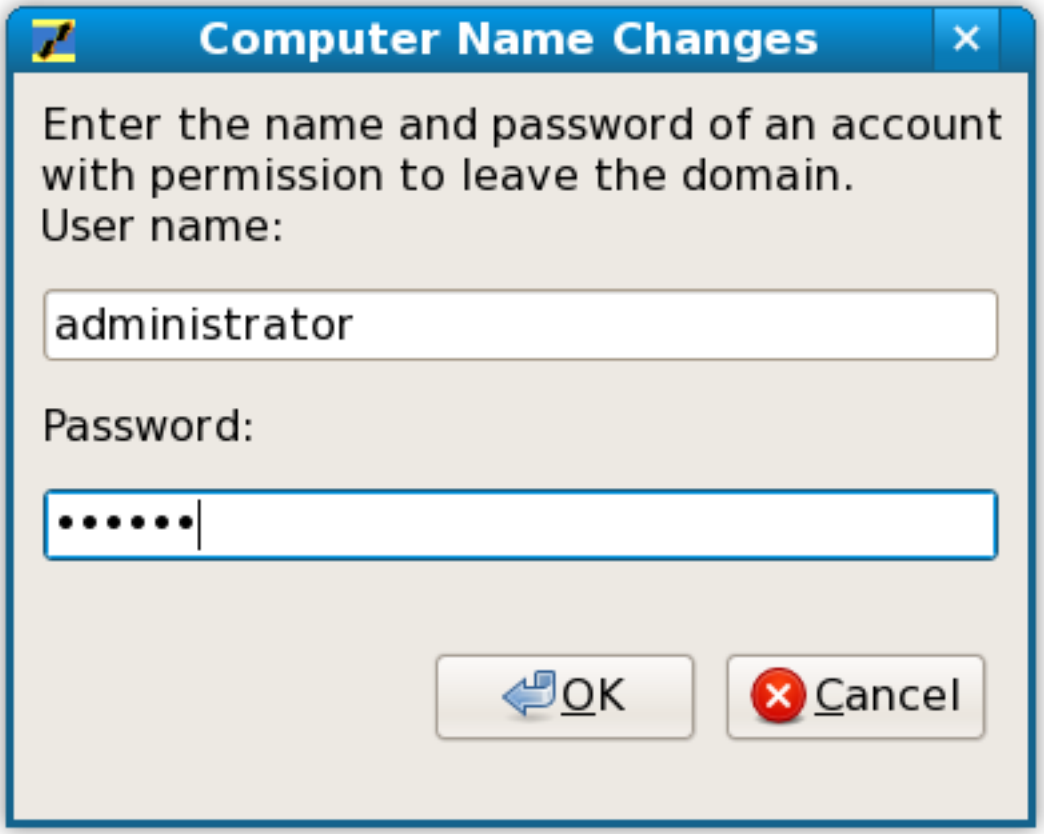
Live Demo

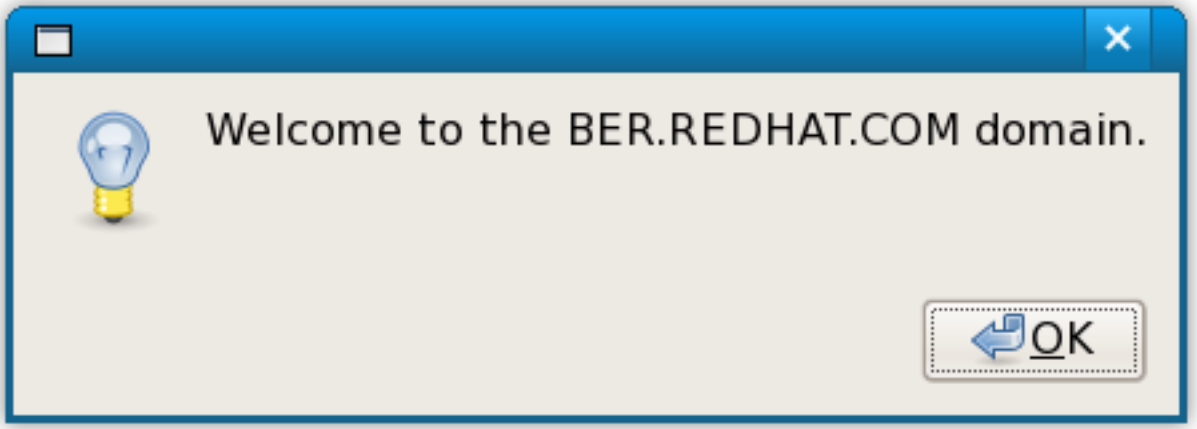
netdomjoin-gui

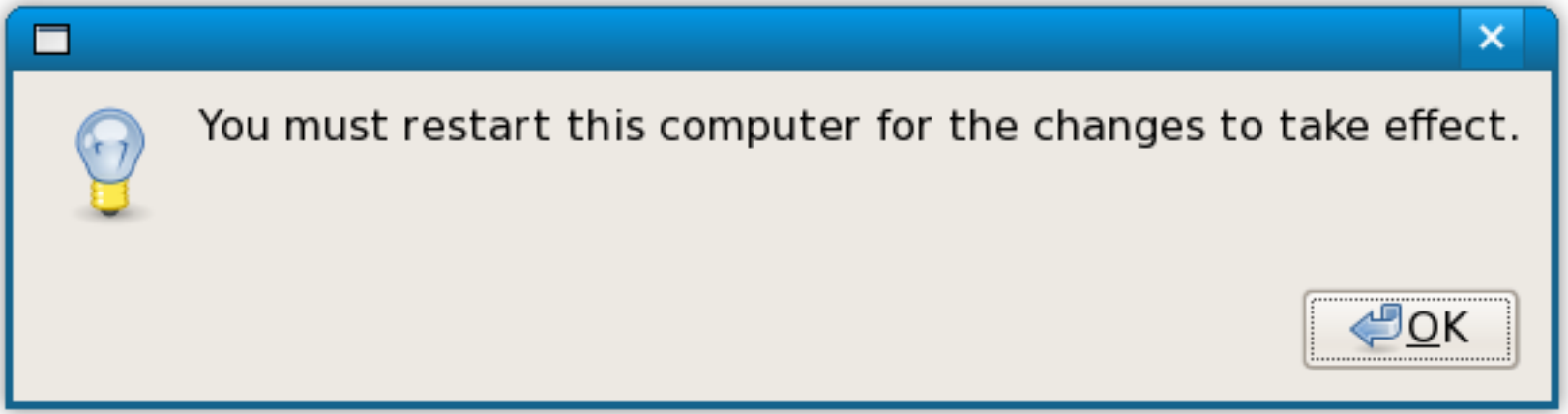

Samba - Join Domain dialogue
Samba uses the following information to identify your computer on the network.
Computer description:
Samba 3.2.0pre3-GIT-8e348ab-test
For example: "Samba %v".
Full computer name:
mthelena.
Workgroup:
TEST
To rename this computer or join a domain, click Change.
Change
OK
Cancel
Apply
About


Computer Name Changes
You can change the name and membership of this computer. Changes may affect access to network ressources.
Computer name:
mthelena
Full computer name:
mthelena.
Member Of
Domain
Workgroup
TEST
Advanced Options
Scan for joinable OUs
Modify winbind configuration
OK
Cancel


Computer Name Changes
You can change the name and membership of this computer. Changes may affect access to network ressources.
Computer name:
mthelena
Full computer name:
mthelena.
Member Of
Domain
BER.REDHAT.COM
Workgroup
TEST
Advanced Options
Scan for joinable OUs
Modify winbind configuration
OK
Cancel


Computer Name Changes
Enter the name and password of an account with permission to leave the domain.
User name:
administrator
Password:
OK
Cancel


Welcome to the BER.REDHAT.COM domain.
OK


You must restart this computer for the changes to take effect.
OK

What's next:

- libnetjoin:
  - joining using vendor extensions (script plugin that vendors use to integrate with local system management frameworks)
  - Set hostname, krb5, ntp, winbind/idmap, nsswitch, pam configuration
  - remote “unsecure” join
- libsmbconf:
  - write support for smb.conf backend in libsmbconf
- libnetapi:
  - make the library less heavyweight
  - python bindings
- start an internal libnet

Thank you for your attention!