OpenChange Progress Report

Julien Kerihuel
<j.kerihuel@openchange.org>

Content

1. General Overview
2. Development tools
3. NSPI Server
4. MAPI Decoding
5. Conclusion

General Overview

What is OpenChange?

- Open Source implementation of Microsoft Exchange Server under Unix platform
- **Provides a MAPI library both for messaging applications and server**
- Native Compatibility with Outlook 2000/2003
- Transparently replaces Microsoft Exchange Server:
  - **Exchange protocol implementation**
  - **No Outlook plugin required** or even needed
  - Relies on Samba4

OpenChange Origins

- Project started in December 2003
- **EPITECH.** End year study project
- **OpenChange company created**:
  - Development supervising
  - Offers a business environment where developers can work on OpenChange.
- **OPENCHANGE IS UNDER GPL LICENSE**
- Use school human resources and technical skills in order to extend the project features.

OpenChange Evolution

BEFORE Samba4 plugin:

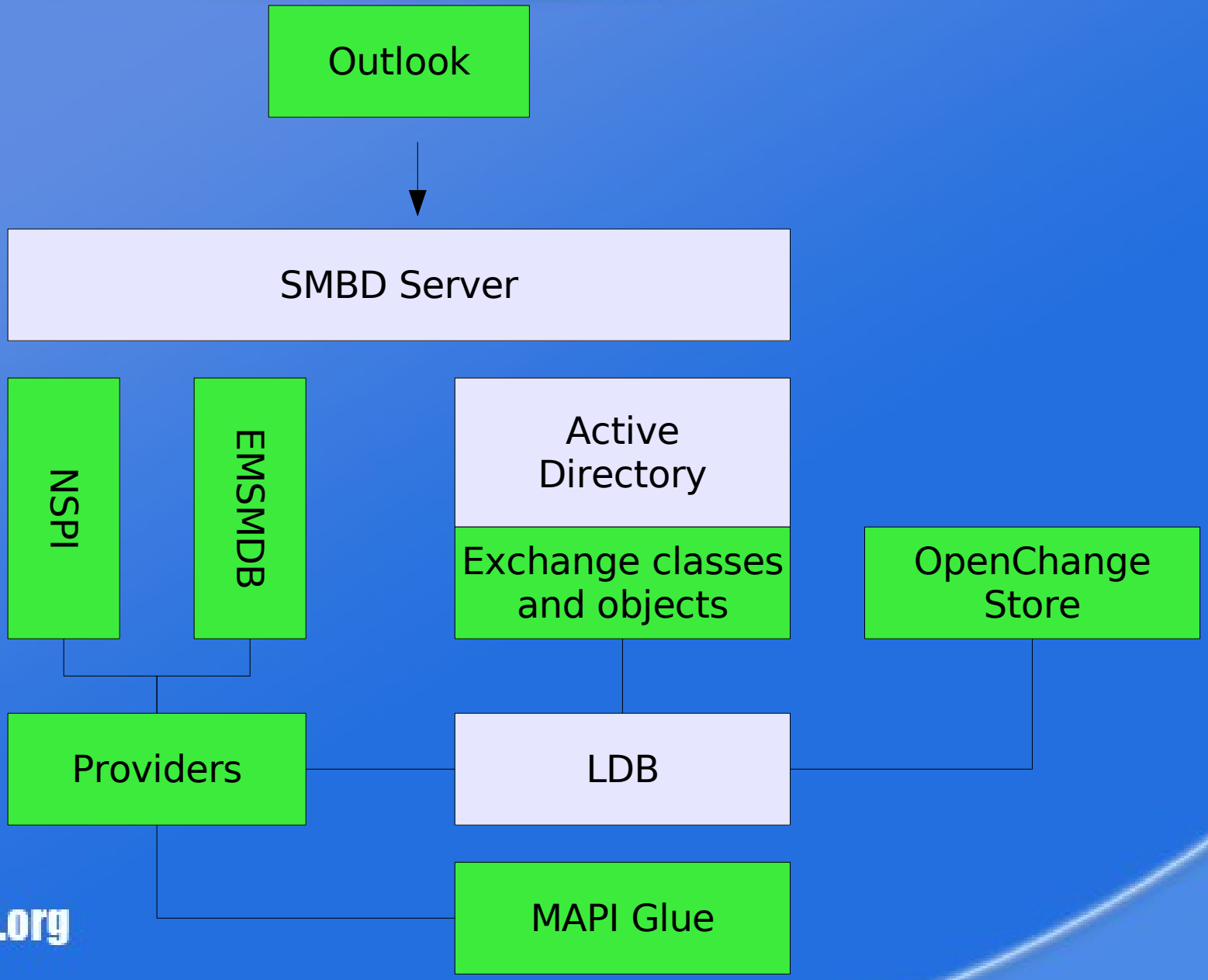
- Friendly fork of Samba4
- SVK + SVN to mirror samba4 sources and have a patched openchange tree on a remote SVN mirror
- Painful to maintain
- Files dispatched in the whole Samba4 tree

OpenChange Evolution

AFTER Samba4 plugin:

- OpenChange is now **developed as a samba4 module**
  - Extends and use Samba4 Active Directory
- **Independent source tree**
- A unique repository to grab openchange source code
- OpenChange intensively uses Samba4 test suite:
  - Ndrdump dumps and analyze
  - Smbtorture tests

OpenChange Evolution

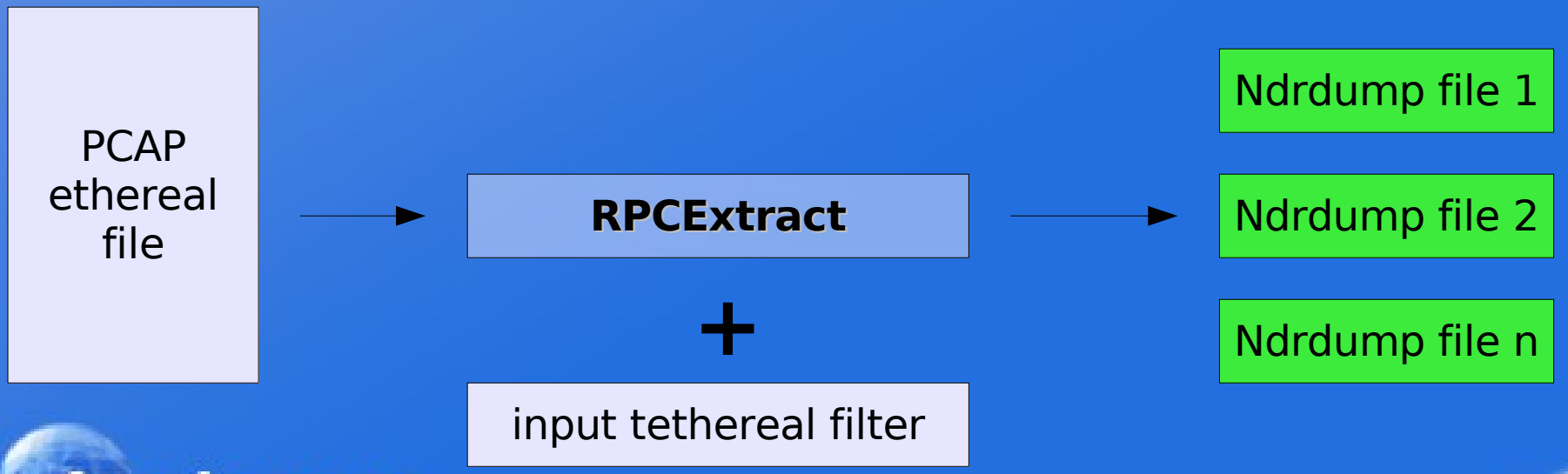


Openchange.org

Development Tools

RPCExtract

- **Features:**
  - Filter out packets from a PCAP file
  - **Payloads found are extracted into separate files**
  - Heavily based on tethereal
  - Integrated into KBPortal



Openchange.org

RPCExtract

- **Limitation:**
  - Based on ethereal 0.10.10
  - Problems with TCP reassembled packets
  - Ethereal filters changed in next version
- **Next release:**
  - Fix the limitations
  - Integrate RPCExtract into ethereal GUI

Knowledge Base Portal

- **What is the KBPortal?**
  - Web application
  - Provide a collaborative way to share experiences and scenarios
- **Features**
  - Integrated browser
  - **mapidump view:** msdn mapitags fetched from msdn and displayed in shell popup with essentials information
  - **rpcextract support** with file uploads
  - download scenario tarball
  - Associate global comments to the scenario or individual files
  - PDF generating
  - Anonymous read-only access

Knowledge Base Portal

- **Which future for KBPortal ?**
  - See how it looks like:
    - **http://kb.openchange.org**
  - **Release of the SAMBAXP release**
  - Fix remaining bugs (need user feedback)
  - Improve the installation process
  - KBPortal runs with 12000 lines of code
  - The current implementation may have shown its limits
  - **Release of KBPortal 1.0**
  - Propose EPITECH students to develop a new KBPortal from scratch written in Ajax or XUL

NSPI Server

What is NSPI ?

- **Name Service Provider Interface**
- Used by Outlook when setting a Microsoft Exchange mail account with the mail applet
- Create and store a profile in the client registry

- NSPI is in charge of:
  - **resolving names** from the Active Directory
  - returns information Outlook needs to contact Microsoft Exchange in further communications.

- **NSPI is the interface between the client and the address book provider**

Research Process

- **RPC-NSPI-PROFILE torture test**
  - Reproduce Outlook behavior when querying Exchange 2000/2003 for the profile
- **torture_create_exchange_user**
  - Extends Windows AD for a user causing:
    - Exchange to create a mailbox for this user
    - Make this user become an Exchange user
    - Use of LDB async code
- **RPC-NSPI-SCANTAGS torture test**
  - Test all MAPITAGS (around 1500) with a single NSPI function
  - See which tags are supported and which are not

Implementation Status

- **The IDL is implemented and working**
- **EMSABP provider implemented at 90%:**
  - EMSABP stands for Extended Messaging System Address Book Provider.
  - It is in charge of the underlying operations:
    - Internal handling of mapitables
    - Fetch and pack information retrieved from the Active Directory
    - Use of the MAPI Glue

Is it working?

- **Almost (-;**
- **It’s a matter of days**
- **While it completes successfully with RPC-NSPI-PROFILE ... Outlook is not that friendly**
- The problem seems to come from the NspiGetHierarchyInfo function which causes:
  - The Mail applet to close unexepectly with Rundll error
  - Loop infinitively on this function

MAPI Decoding

MAPI Decoding

- **99% of MAPI operations are handled by EcDoRpc**
- EcDoRpc obfuscates the data with a **xor 0xa5**
- This xor(ed) content is divided in 2 parts:
  - Content handled by a **TDR layer**
  - **Some kind of signature algorithm**

What is implemented?

- We are at the beginning of MAPI Decoding
- We implemented:
  - empiric signature algorithm
  - RPC-EXCHANGE torture test
  - works until fetching mail headers from an Exchange mailbox

Conclusion

Conclusion

- A lot of work (code and research) still needs to be done

- But we start having results!
- OpenChange SAMBAXP release on the way

- And important parts of the underlying work has been achieved:
  - research
  - design
  - how to plug properly with Samba API

Conclusion

- Join us on IRC:
  - irc.freenode.net #openchange
- Join the development mailing-list
  - openchange-devel@lists.sourceforge.net

Questions/Comments?