view
scan
script
xor eax,*

re|search();

reverse engineering research environment

Open-Source Project

2012, Mario Schallner

A set of specialized tools and technologies for research in the fields of reverse code engineering and low level binary analysis
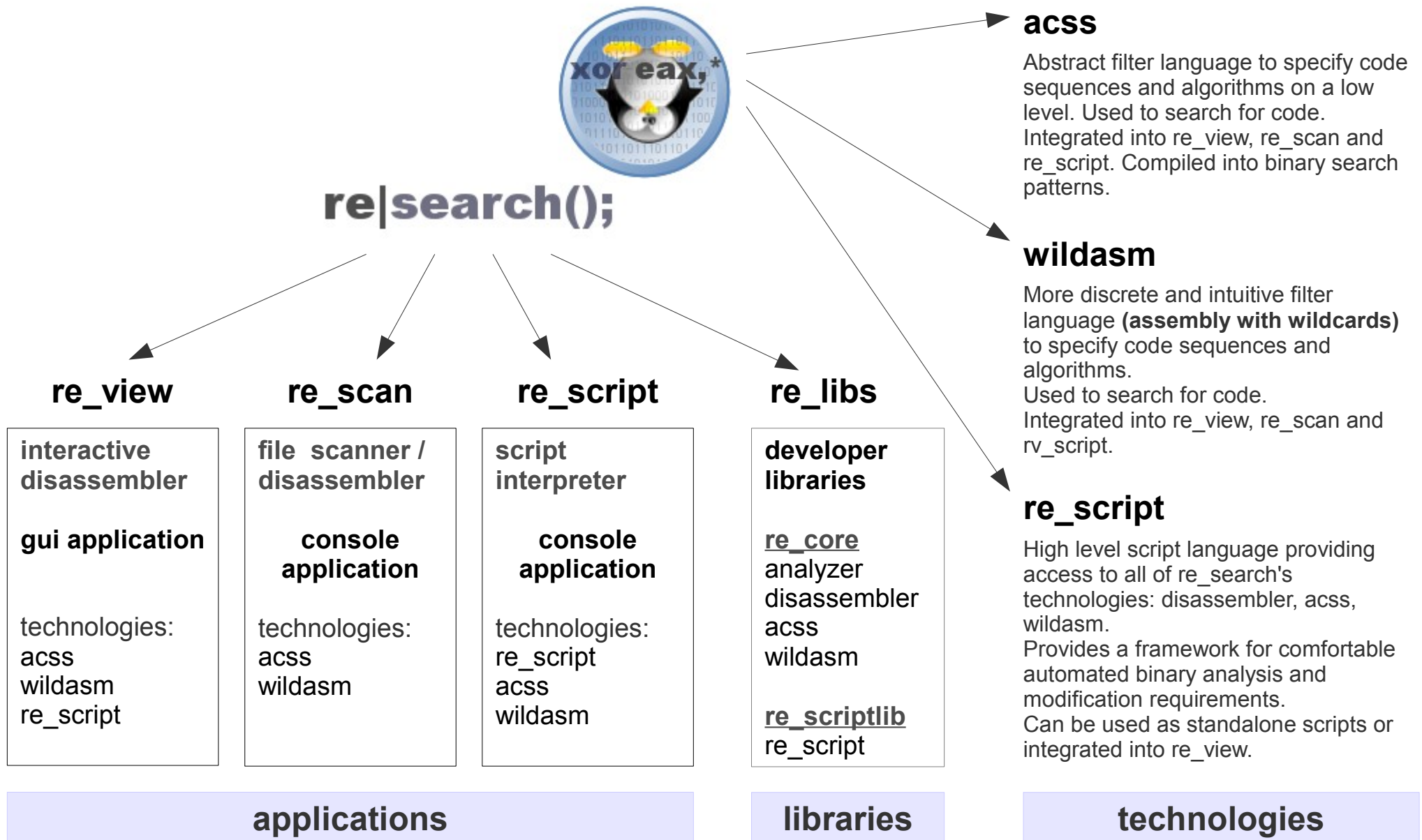
Intended purpose, operational area
- General low level code analysis, malware analysis, binary auditing, education
- Security business, professional trainings, schools and universities, software-developers, ...

Tools, technologies
- Interactive disassembler, commandline disassembler / analyzer / scanner
- Specialized object oriented scripting language, standalone script interpreter
- Integrated abstract code sequence / algorithm search facilities on 2 abstraction levels – stronger and more flexible than any existing antivirus scan engine
- Shared libraries providing all functionality of **re|search();** for building derived own software easily

Open Source, platform independent, free

acss

Abstract filter language to specify code sequences and algorithms on a low level. Used to search for code. Integrated into re_view, re_scan and re_script. Compiled into binary search patterns.

wildasm

More discrete and intuitive filter language **(assembly with wildcards)** to specify code sequences and algorithms.
Used to search for code.
Integrated into re_view, re_scan and rv_script.

re_script

High level script language providing access to all of re_search's technologies: disassembler, acss, wildasm.
Provides a framework for comfortable automated binary analysis and modification requirements.
Can be used as standalone scripts or integrated into re_view.

re|search();

re_view

interactive disassembler

gui application

technologies:
acss
wildasm
re_script

re_scan

file scanner / disassembler

console application

technologies:
acss
wildasm

re_script

script interpreter

console application

technologies:
re_script
acss
wildasm

re_libs

developer libraries

re_core
analyzer
disassembler
acss
wildasm

re_scriptlib
re_script

applications

libraries

technologies

re_core

re_logger	re_acss_expression	re_wildasm_expression
re_file	re_acss_compiler	re_wildasm_compiler
re_file_elf32	re_acss_library	re_wildasm_library
re_file_pe32		
re_file_raw32	re_acss_syntaxhighlighter	re_wildasm_syntaxhighlighter
re_target		
re_disassembler	re_disasm_thread	re_address_descriptor

re_scriptlib

re_script_engine   re_script   re_script_highlighter

re_view

rv_target	rv_disasm_model	rv_elf32_shdr_model	rv_dynview_xrefs
rv_disasm_view	rv_hexedit_model	rv_elf32_phdr_model	rv_dynview_insn
	rv_fileinfo_model	rv_elf32_ehdr_model	rv_dynview_hexdump
	rv_tag_processor	rv_pe32_nthdr_model	rv_tag_delegate
	rv_comment_processor	rv_pe32_shdr_model	rv_tag_editor
	rv_acss_lib_processor	rv_wildasm_lib_processor	

re_scan | ...

re_script | ...