Black Hat Arsenal EU

++

Needle

Marco Lancini

3rd November 2016

MWR LABS

MWR LABS

What is Needle?

+ A tool for auditing iOS Application Security
+ An open source, modular framework
  - streamline the entire process
  - acts as a central hub

needle

MWR LABS

Motivation

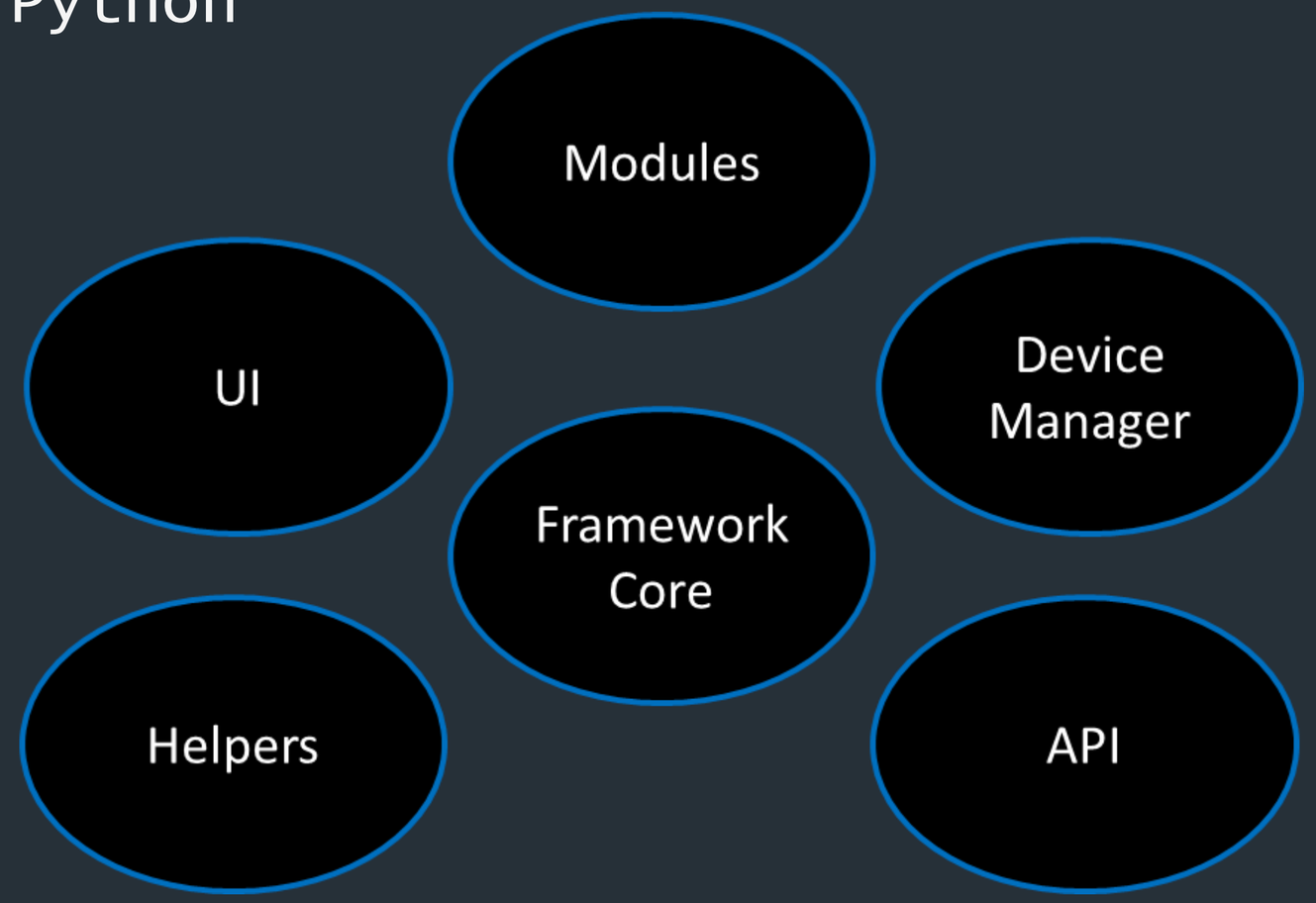
- Beginners: easy to use
- Professionals: save time during assessments
- Developers: quickly test their products

The Architecture

MWR LABS

Architecture

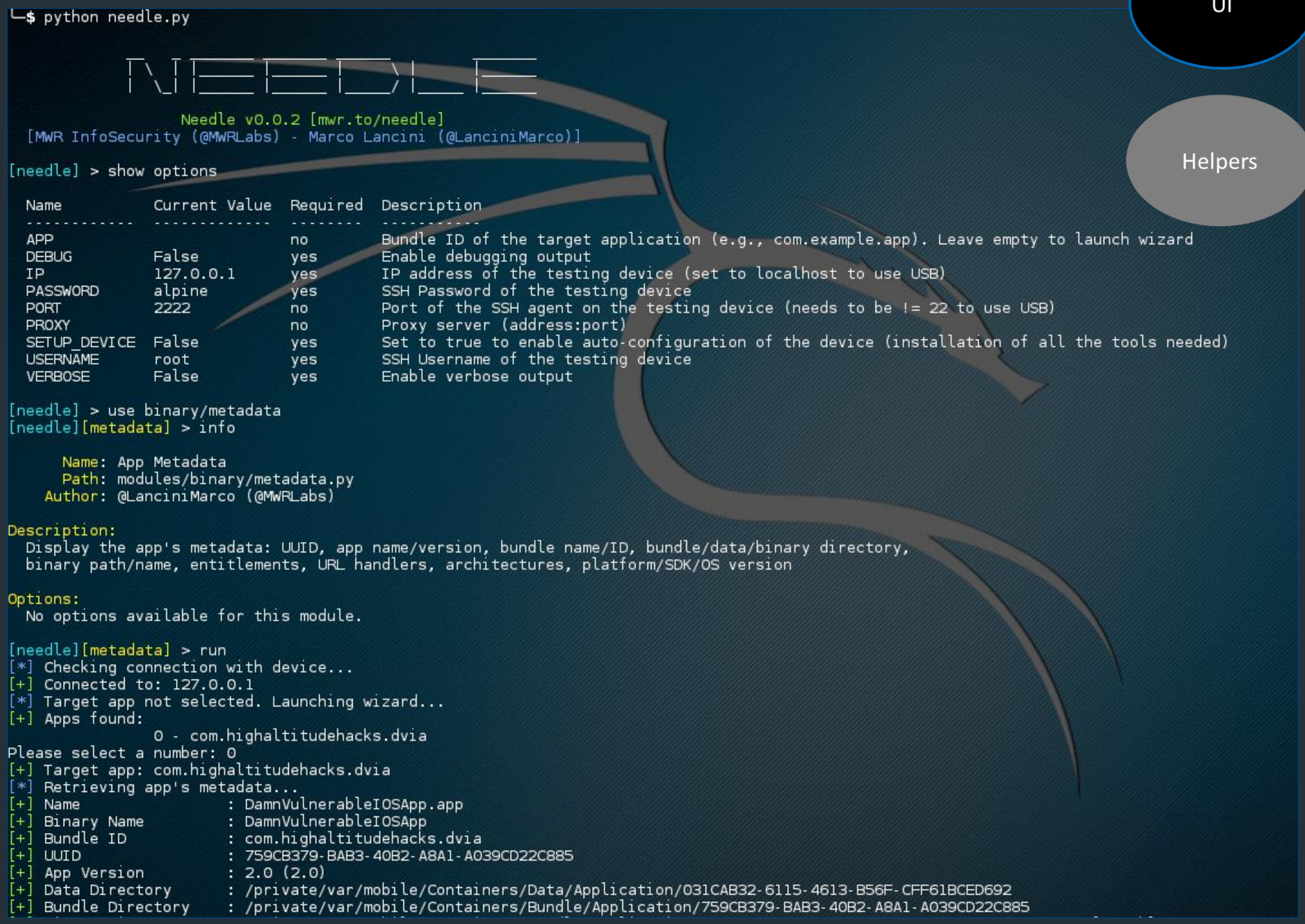
1. Decoupled components
2. Entirely written in Python

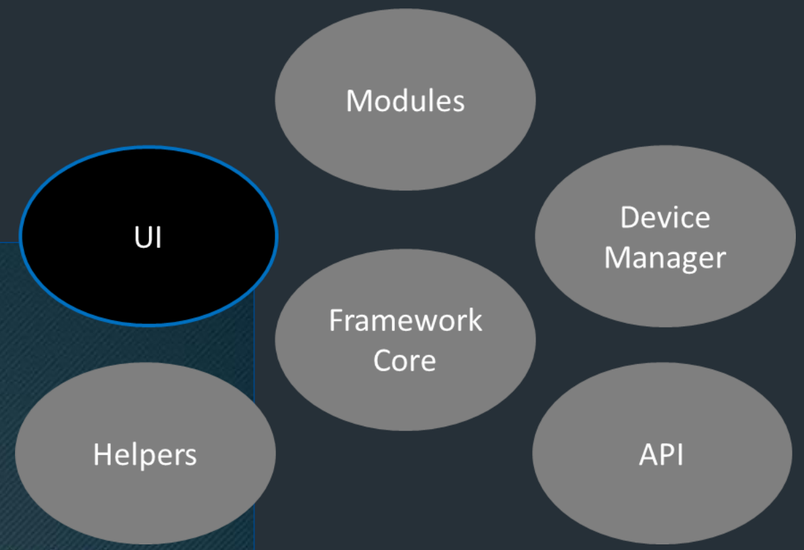


Black Hat Arsenal EU

MWR LABS

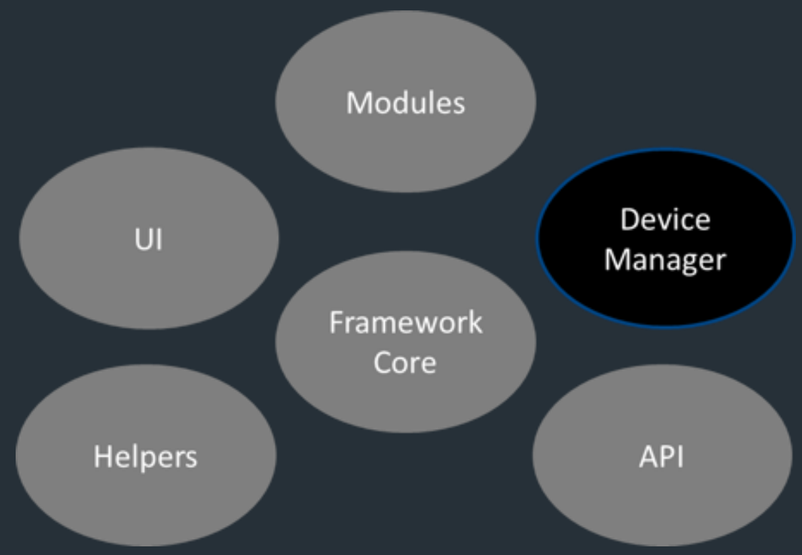
UI





MWR LABS

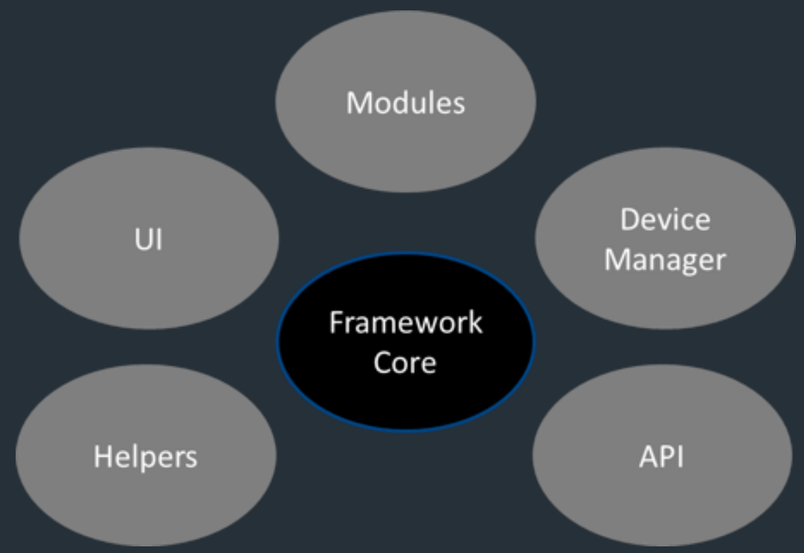
Device Manager



+ Manage connections with the iDevice
  - SSH over Wi-Fi
  - SSH over USB
+ Device setup, port forwarding, cleanup…
+ Basic commands
  - shell, push/pull
+ App management
  - metadata, open, decrypt, data protection…

MWR LABS

Framework Core



+ Initialize and manage all the other components

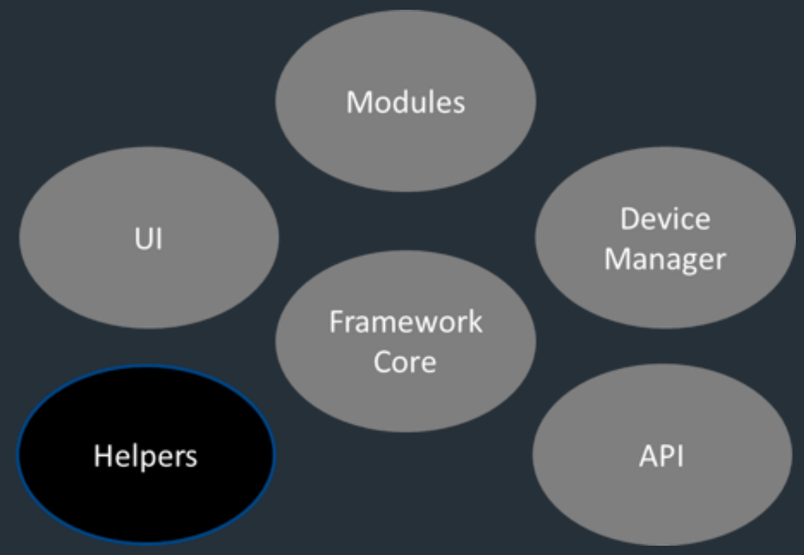
+ Load/execute modules/jobs

+ Maintain status

  - global options, loaded modules, running jobs, device status…
  - pointers to instantiated objects
  - constants

MWR LABS

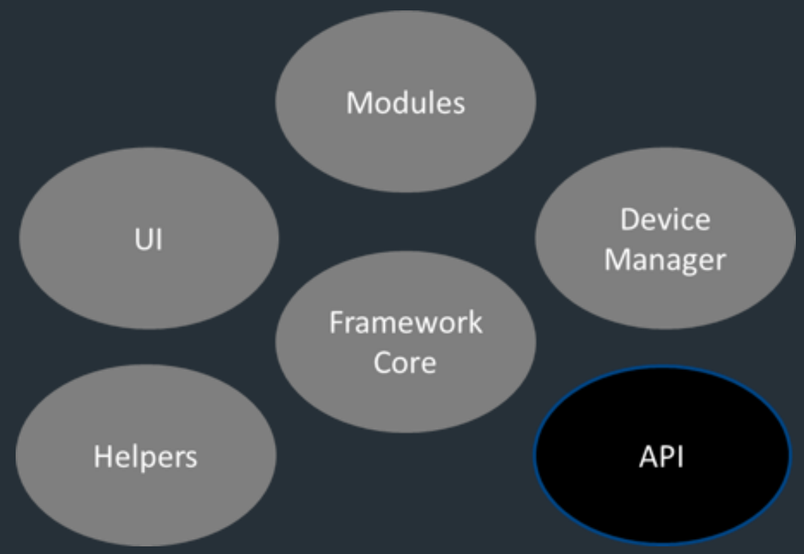
Helpers



+ Common functionalities offered both to the Core and APIs
+ Sanitization, logging, printing…

MWR LABS

API



+ The framework core exposes APIs to interact with the local and remote OS
+ These wraps common functionalities
  - file and data access
  - command execution
  - networking
+ Speed-up creation of new modules

Black Hat Arsenal EU

MWR LABS

API

LOCAL_OP

+file|dir_exist|create|delete(path)
+dir_copy(src, dst)
+dir_is_empty(path)
+dir_reset(path)
+command_subproc_start|stop(cmd|proc)
+command_blocking|interactive(cmd)
+command_background_start(cmd)
+command_background_stop(procname)
+build_output_path_for_file(module, fname)
+build_temp_path_for_file(module, fname)
+delete_temp_file(module, fname)
+cat_file(fname)
+get_ip()
-output_folder_setup|backup(module)

FRAMEWORK

-path_app
-path_core
-path_libs
-path_home
-path_home_temp
-path_home_backup
+printer
+local_op
+device
+APP_METADATA
+TOOLS_LOCAL

+do_x()
+print_x()
+new_connection()
+get_meatdata()

DEVICE

-_frida_server
-_debug_server
#TEMP_FOLDER
#DEVICE_TOOLS
+conn
+app
+installer
+local_op
+remote_op
+printer

-is_usb()
-connect()
-disconnect()
-setup()
-cleanup()
+shell()
+push_pull()

REMOTE_OP

+file|dir_exist|create|delete(path)
+file_copy(src, dst)
+dir_list(path, recursive = False)
+dir_reset(path)
+command_blocking(cmd, internal)
+command_interactive(cmd)
+command_interactive_tty(cmd)
+command_background_start(module, cmd)
+command_background_stop(pid)
+kill_proc(procname)
+download|upload(src, dst, recursive)
+build_temp_path_for_file(fname)
+create_timestamp_file(fname)
+chmod_x(fname)
+parse_plist(plist)
+read_file(fname, grep_args)
+write_file(fname, body)

needle.py

CLI

+init_global_options()
+load_modules()

BaseModule

+print_cmd_output(txt, outfile, silent)

INSTALLER

+configure()

APP

+get_metadata(app_name)
+open(bundle_id)
+search_pid(app_name)
+decrypt(app_metadata)
+get_dataprotection(filelist)
+convert_path_to_filename(fname, metadata)

StaticModule

FridaModule

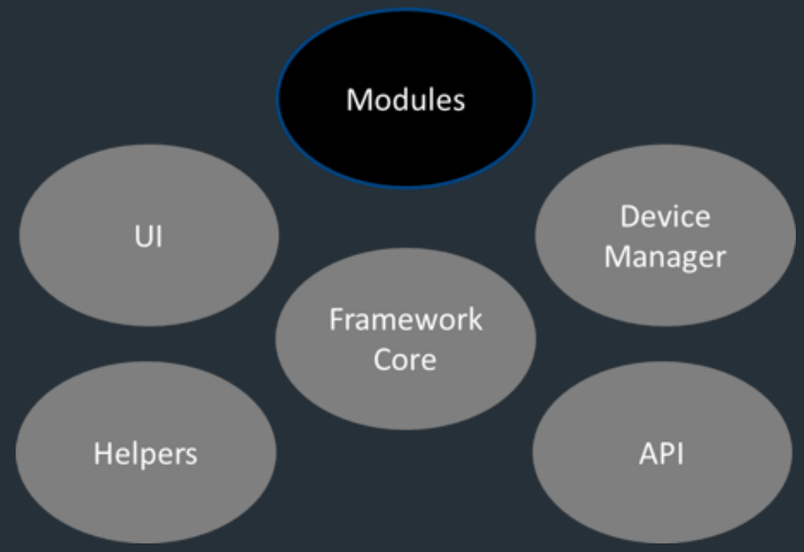
DebugModule

BackgroundModule

FridaScript

MWR LABS

Modules



+ Heart of Needle’s functionalities
+ Collection of python scripts

MWR LABS

Currently Supported Modules

Binary	Storage
• App Metadata • Compilation Checks • Shared Libraries • Strings • Class Dump • Install IPA • Pull IPA	• Binary Cookies • Cache.db Files • Plist Files • SQL Files • Dump Keychain • Screenshot Caching • Keyboard Autocomplete Caching

MWR LABS

Currently Supported Modules

Dynamic
• Jailbreak Detection • URI Handler • Heap Dump • Monitor File changes • Monitor OS Pasteboard • Syslog Monitor • Syslog Watch

Hooking
• Cycript shell • Frida shell • Frida trace • Frida launcher • Enumerate Classes (script) • Enumerate Methods (script) • Enumerate All Methods (script)

MWR LABS

Currently Supported Modules

Comms	Static
• List Installed Certificates • Export Installed Certificates • Import Installed Certificates • Delete Installed Certificates • Install MitmProxy CA Certificate • Intercepting Proxy	• Code Checks

Roadmap

MWR LABS

Roadmap

Agent to deploy on device

- Replace all the dependencies

Support for non-jailbroken devices

New modules

- Substrate integration
- WebView scanner
- Hook Swift methods
- URI handlers fuzzer
- Pinning detection/bypass
- Obfuscation detection

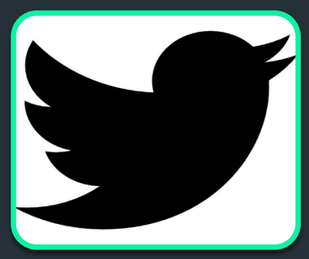
… community based

Black Hat Arsenal EU

MWR LABS

Get Needle

mwr.to/needle



@mwrneedle