Objective

We have to defeat the enemies
and save the earth!!

Our contributions

- Introduce a **new concept of analysis framework** to use easily
  - perform analysis of normal application by using web proxy
- Introduce methodologies for implementing our concept
  - pros and cons of the methodologies
- Demonstrate use cases

Define Keyword

- **Web Application**
  - consist of usually script languages
  - operate based on web server/client
- **Normal Application**
  - executable binary except for web applicaton
  - PE, ELF, etc.
- **Web Proxy**
  - a tool for web application analysis
  - Burp suite, paros, fiddler, etc.

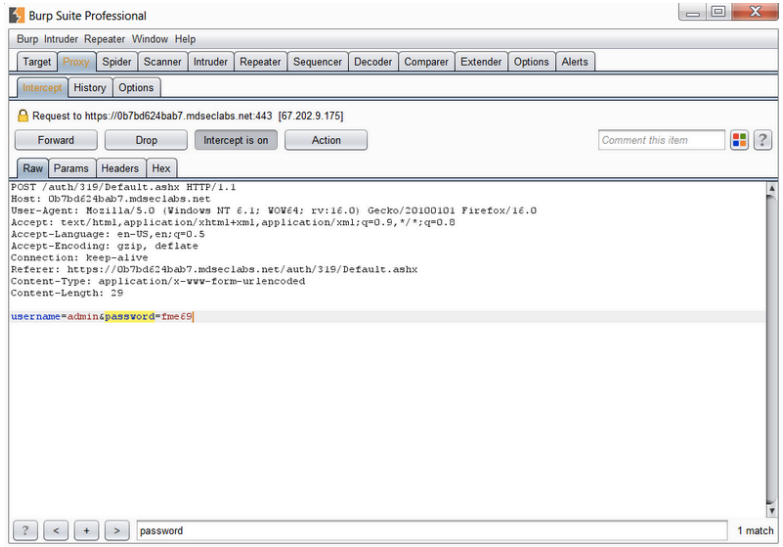
What's wrong?

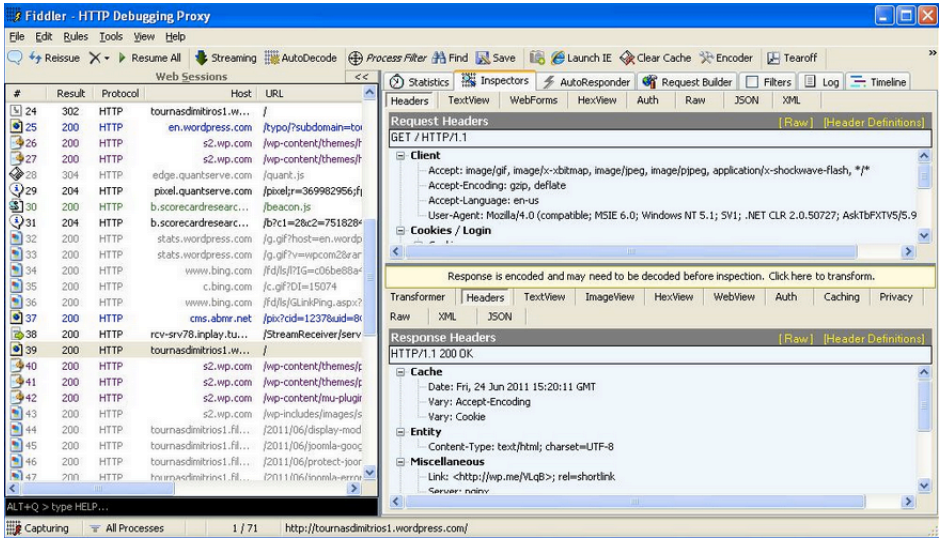
Background

Existing methodologies/tools for application analysis

Web Application analysis

- easy to use and operate using a web proxy (burp, paros, fiddler, etc.)
- monitor and modify the contents without difficulty

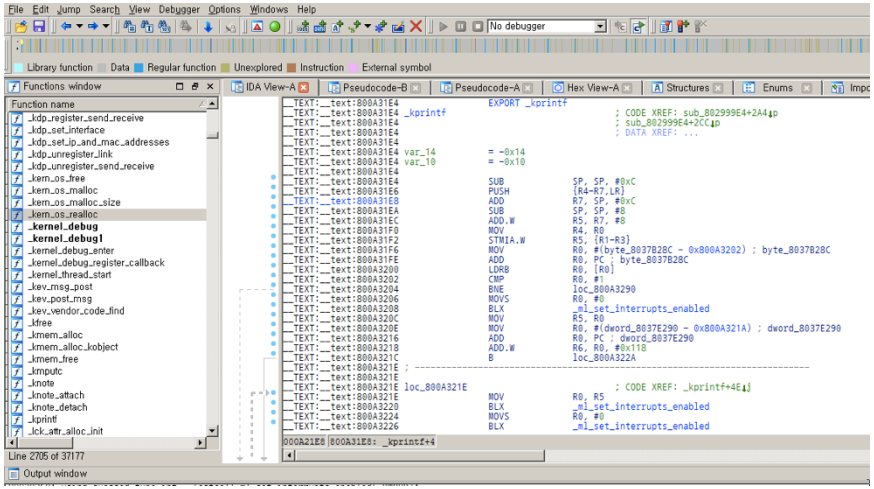


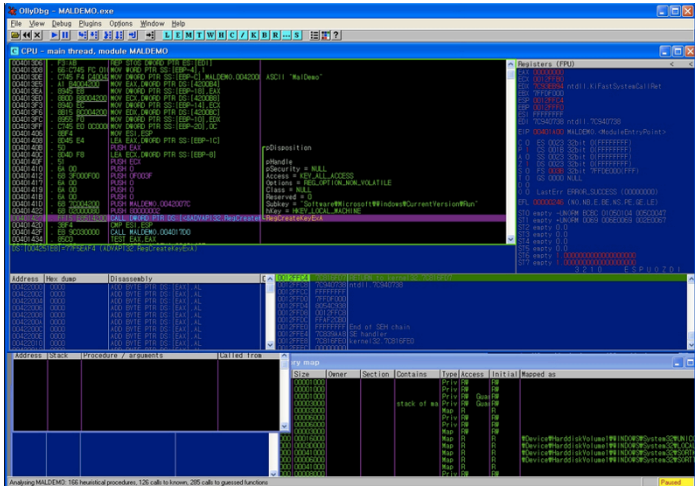


Existing methodologies/tools (cont'd)

Normal Application(excutables) analysis

- much harder and complex than web application(GDB, IDA, Ollydbg, windbg, etc.)
- In secure channel, how can we check the contents?





Challenges for application analysis

We cannot

save the earth

using our resources

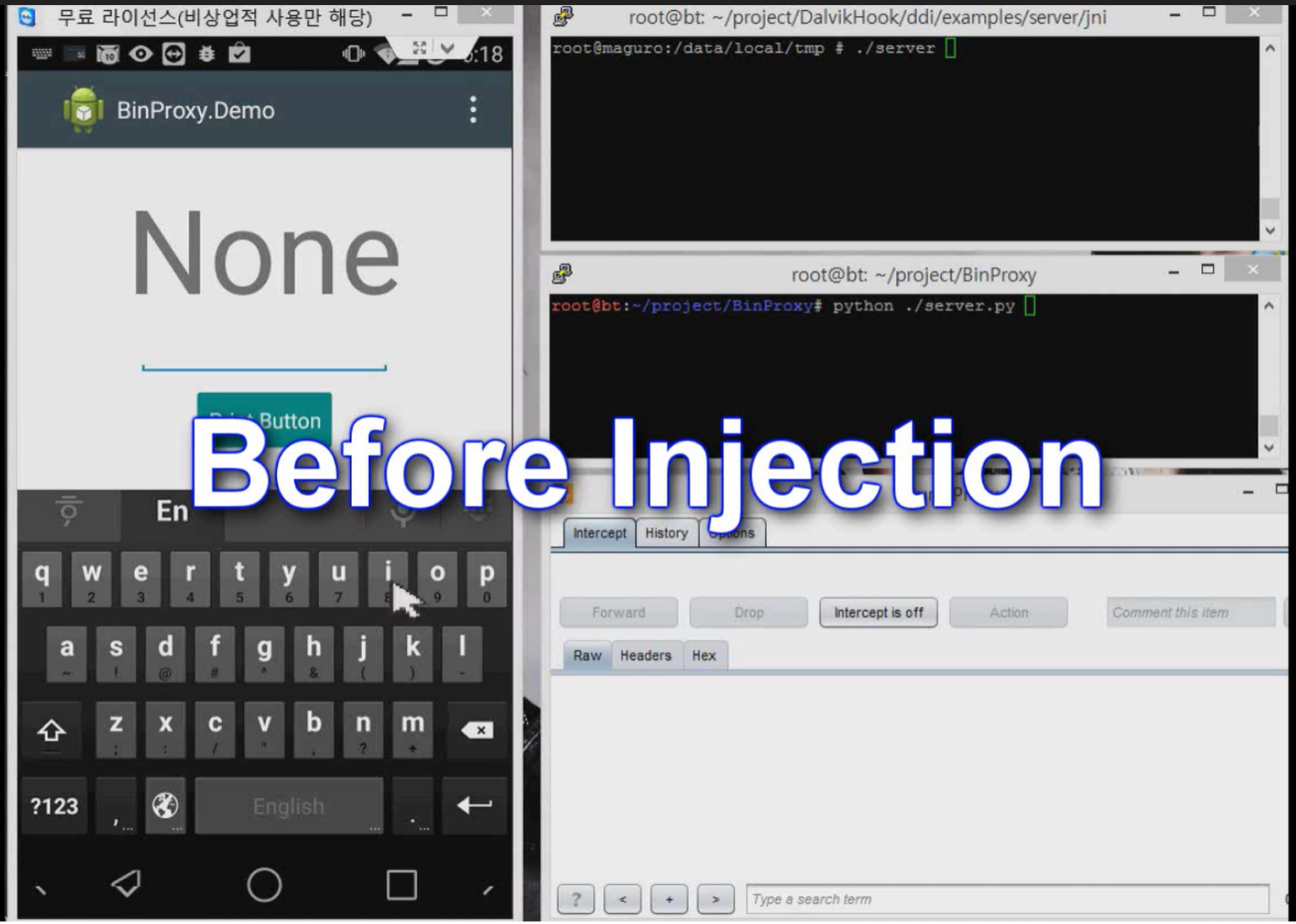
Lack of time and manpower

How to solve a problem?

Need a EASY tool

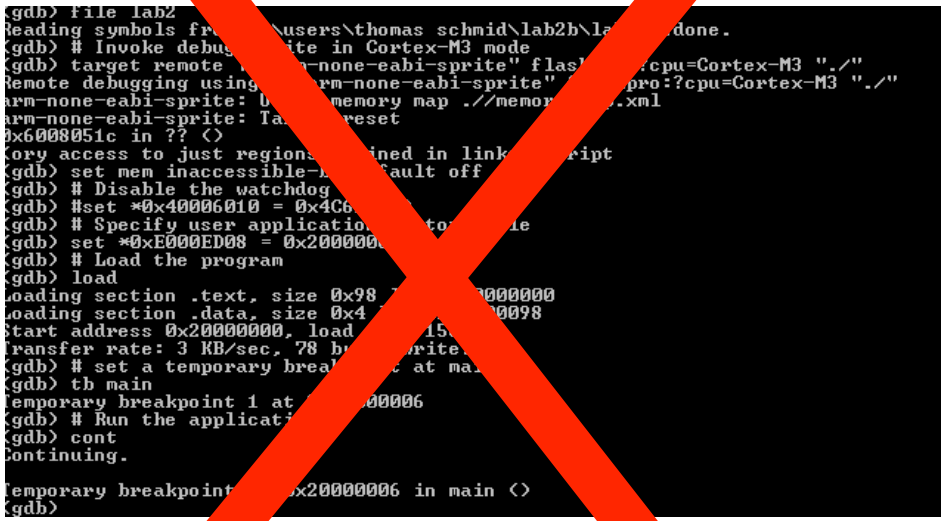
So what??

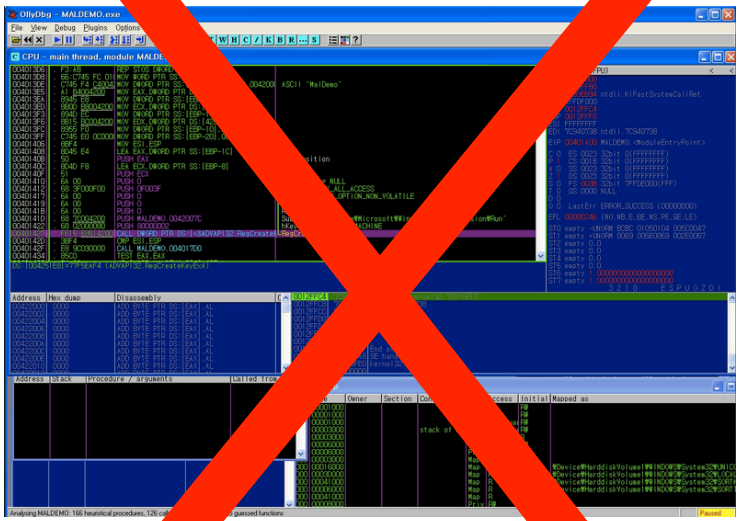
BinProxy : A New Paradigm for Binary Analysis


무료 라이선스(비상업적 사용만 해당)
BinProxy.Demo
None
Button
root@bt: ~/project/DalvikHook/ddi/examples/server/jni
root@maguro:/data/local/tmp # ./server
root@bt: ~/project/BinProxy
root@bt:~/project/BinProxy# python ./server.py
Intercept
History
Forward
Drop
Intercept is off
Action
Comment this item
Raw
Headers
Hex
Type a search term
Before Injection

Key Features

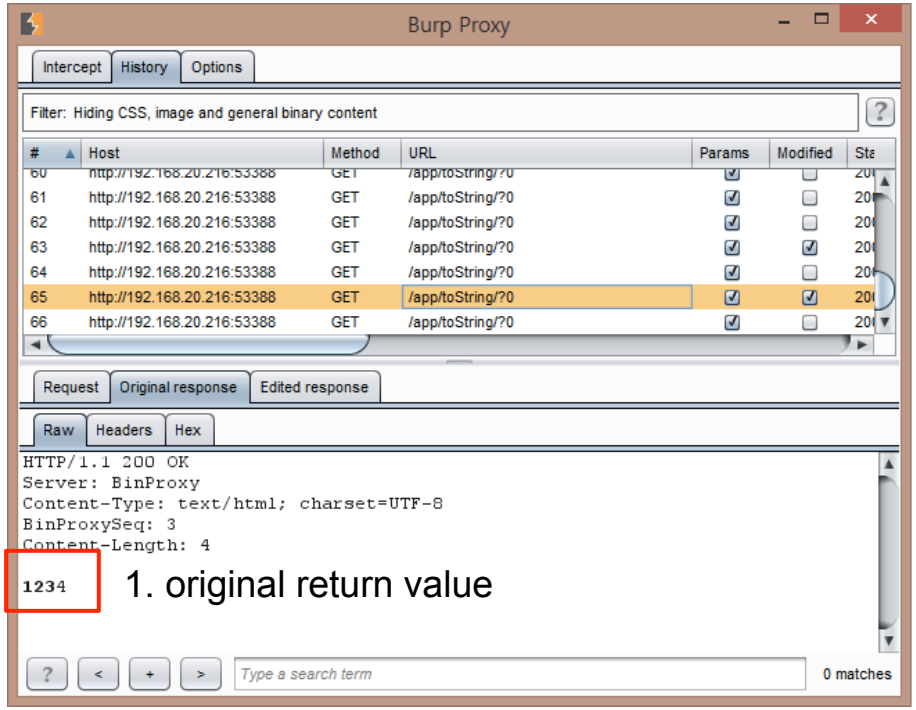
We do not need gdb and ollydbg
to analyze applications any more.



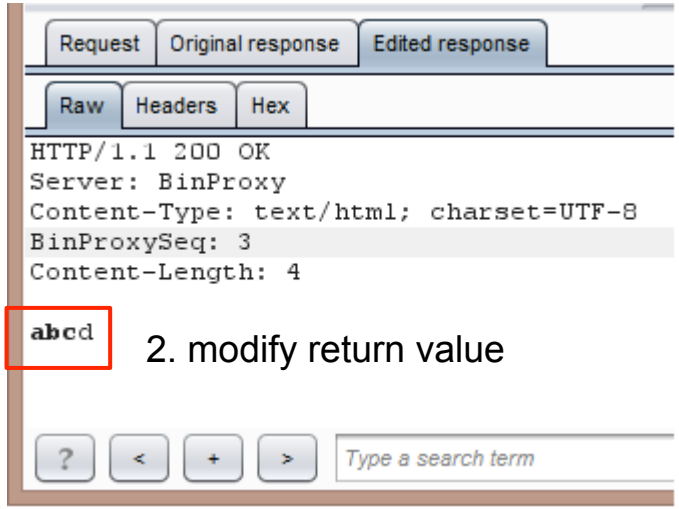


Key Features (cont'd)

Should we use the difficult tools for **simple analysis**?
You can monitor and control the normal applications
with your favorite web proxy



1. original return value

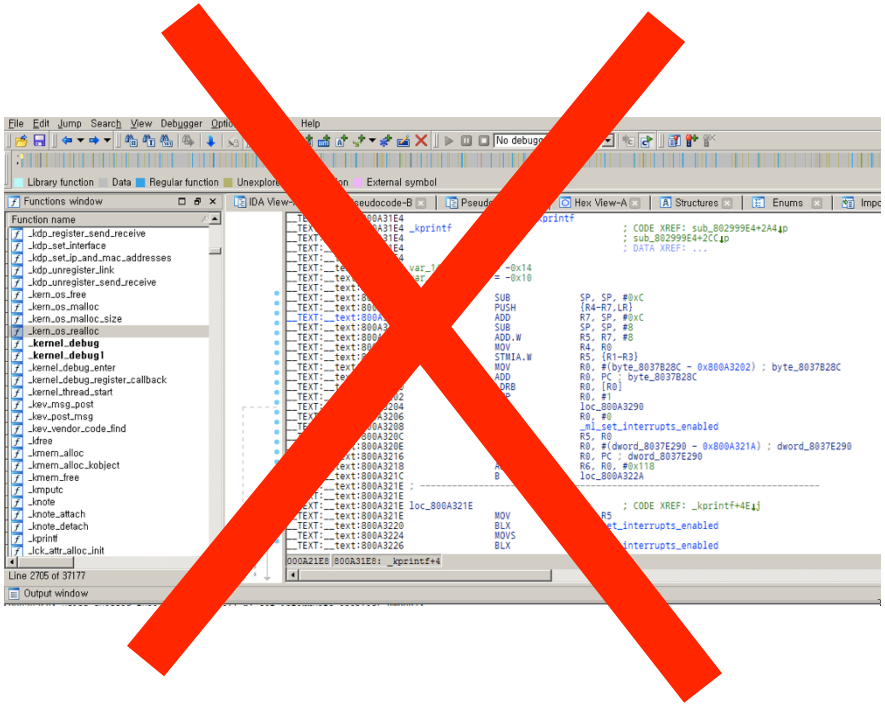


2. modify return value

3. Click Forward Button

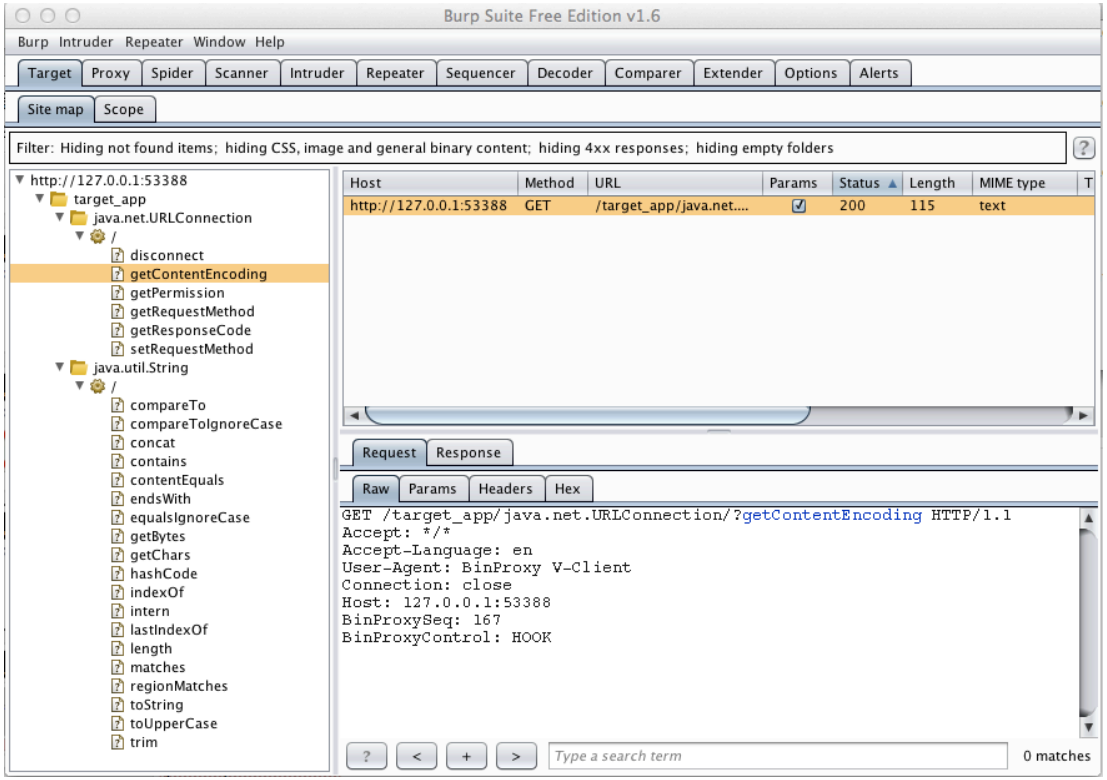
Key Features (cont'd)

We do not want to use difficult IDA tool to analyze applications any more.

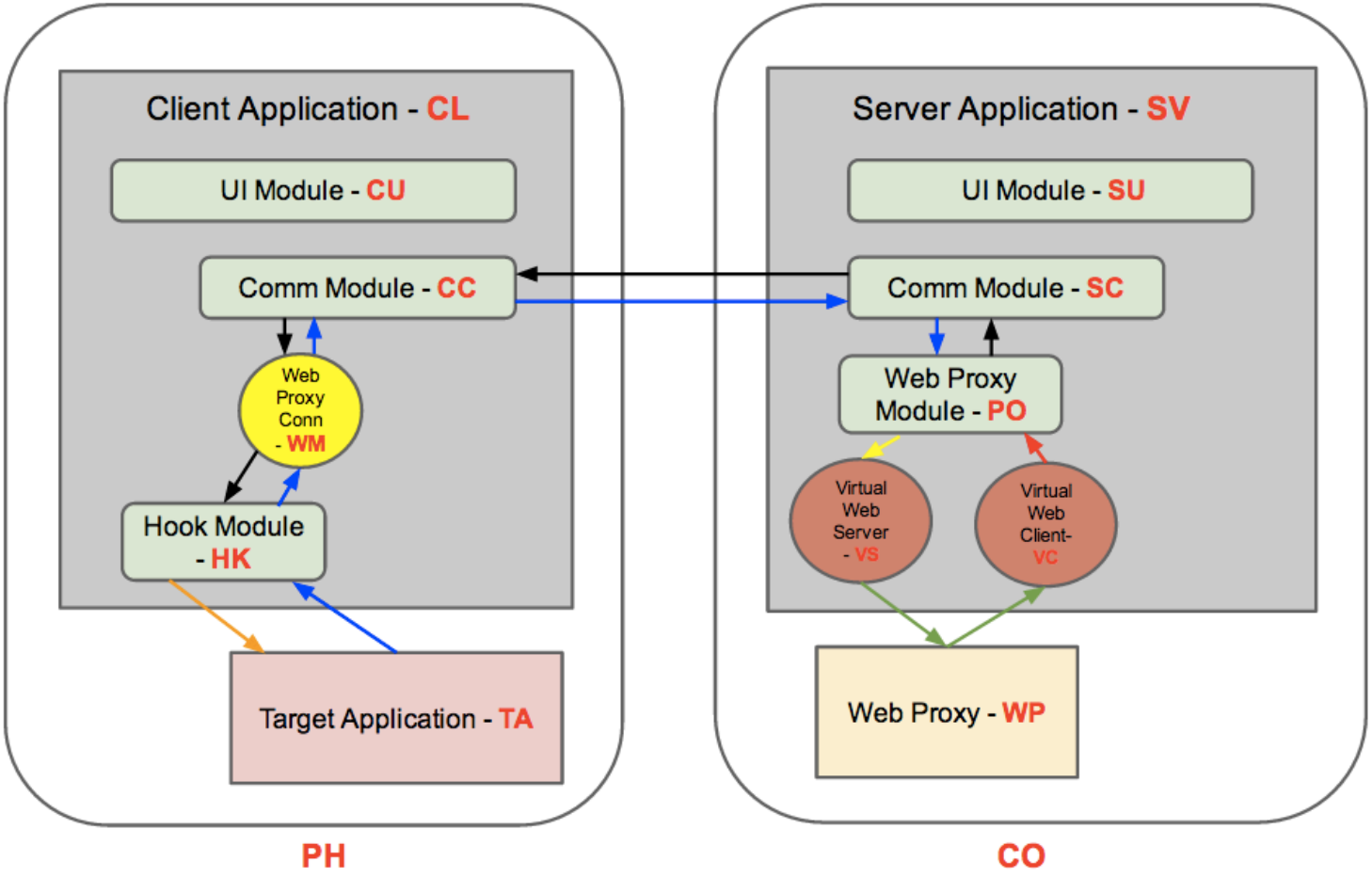


Key Features (cont'd)

You can know what functions are existed in target apps and what functions can be monitored.



Overall Achitecture



Components

- Target application
  - smart phone apps, excutable program based on Windows, OSX and etc.
- Web Proxy
  - A user-friendly proxy to be used for analysis (ex. burp, paros, ..)
- BinProxy Client
  - is Operated in the target application is installed
  - communication module : communicate with BinProxy server
  - hooking module : modify the flow of functions.
- BinProxy Server
  - is Operated in the web proxy is installed
  - communication module : communicate with BinProxy client and web proxy

What You Need

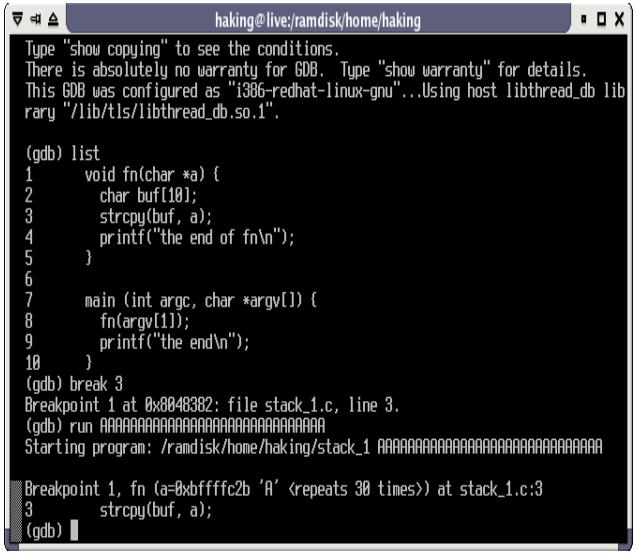
Need things to make BinProxy

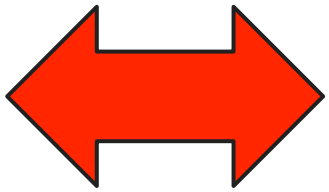
Intercept function call & Forward it to a Web proxy

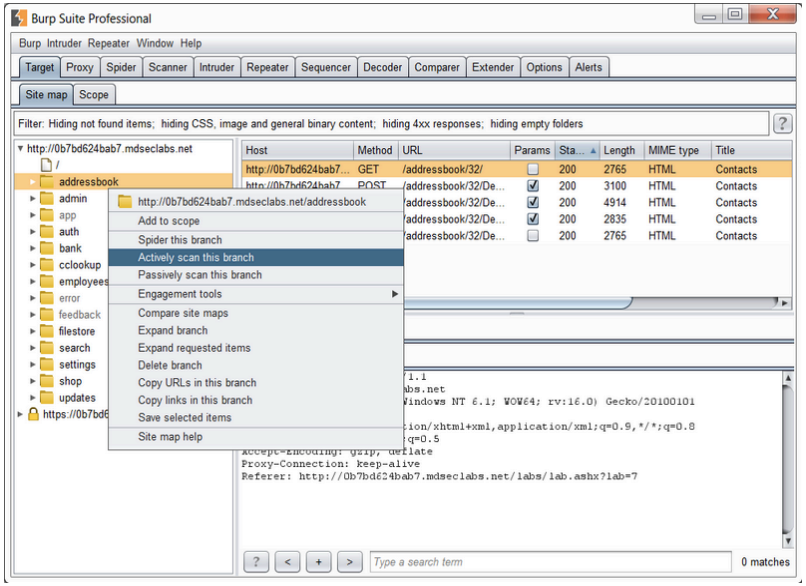
Main techniques for implementation

how to control function calls by using web proxy

Convert Functions







Function monitoring and Function Controlling

Main techniques for implementation (cont'd)

API / User-defined function

Hooking

Function monitoring and Function Controlling

Main techniques for implementation (cont'd)

Dynamic function Hooking

No need a pre-compiled hooking code

Dynamic target function selection

Function monitoring and Function Controlling

Main techniques for implementation (cont'd)

Return value,

primitive / refernce

type arguments

Target function selection

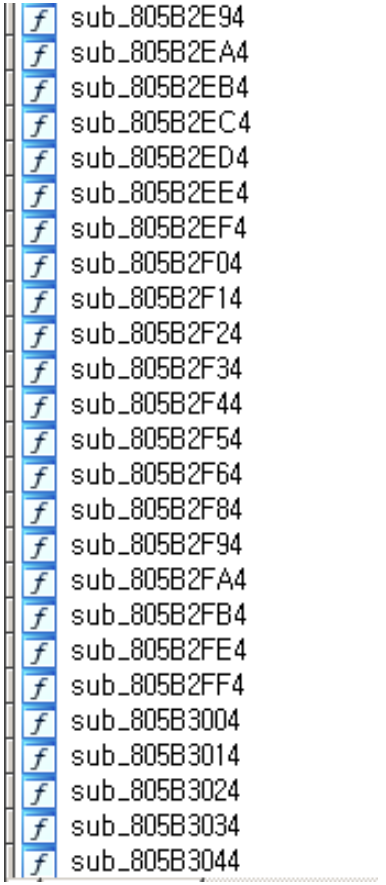
Main techniques for implementation (cont'd)

Extraction API lists

Target function selection (cont'd)

Extracting user-defined fuctions and Finding out Args and Types

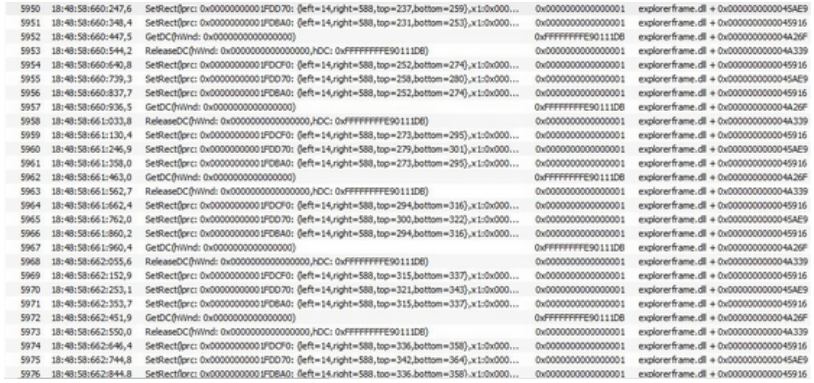
```
1  int __fastcall sub_805D2CE0(int a1, int a2, int a3, int a4, int a5, int a6)
2  {
3    int v6; // r4@1
4    int v7; // r0@1
5    int v8; // r1@1
6    int v9; // r0@2
7    int v11; // [sp+8h] [bp-18h]@1
8    int v12; // [sp+Ch] [bp-14h]@1
9    int v13; // [sp+10h] [bp-10h]@1
10   int v14; // [sp+14h] [bp-Ch]@1
11   int v15; // [sp+18h] [bp-8h]@1
```



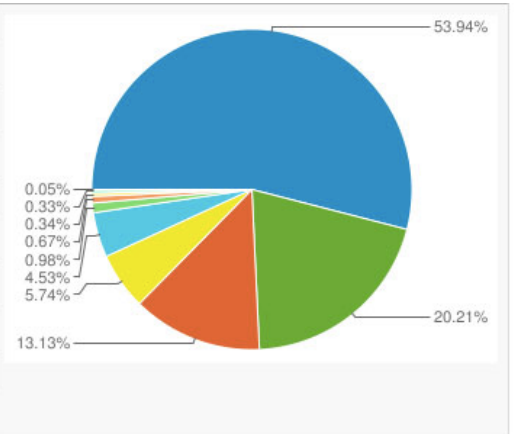
Target function selection (cont'd)

Monitoring function calls and statistics

-> Selecting target functions easily



1.	Internet Explorer	53.94%
2.	Safari	20.21%
3.	Chrome	13.13%
4.	Firefox	5.74%
5.	Mozilla Compatible Agent	4.53%
6.	Android Browser	0.98%
7.	Opera	0.67%
8.	IE with Chrome Frame	0.34%
9.	NaverCafe	0.33%
10.	RockMelt	0.05%



How to make?

the way of building BinProxy

How to interwork with a web proxy - BinProxy Client

```
int hooked_func(arg1, arg2, ...)
{
    arg_string = make_arg_string(original_arg1, original_arg2, ...);

    new_arg_string = send_to_server_and_wait("
        HOOK_INFO^^before_call^^#{original_function_name}^^#{arg_string}");
```

* hooked_func send before_call message to BinProxy Server through communication module.
* before_call message = function name + the value of arguments

* After sending a before_call message, the hooked_func will be blocked until getting response from BinProxy Server.

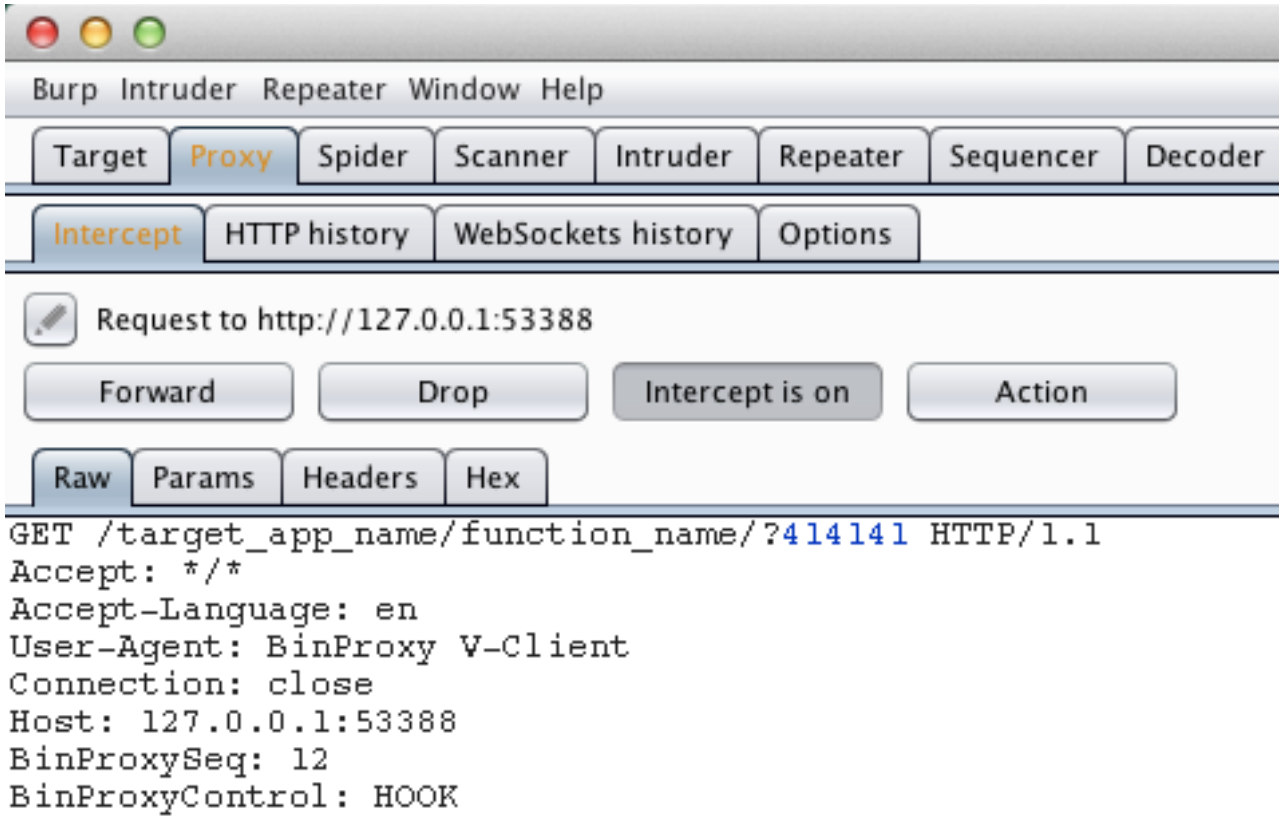
```
    if( new_ret_string == ret_string )
        return ret;
    else
        return parse(new_ret_string, 1);
}
```

How to interwork with a web proxy - BinProxy Server

BinProxy Server convert a before_call message into HTTP request format for delivering the message to Web Proxy.

```
POST http://127.0.0.1:53388/function_name
Host: target_app_name
User-Agent: BinProxy

01_414141
```

How to interwork with a web proxy - Web Proxy



How to interwork with a web proxy - BinProxy Client

```
int hooked_func(arg1, arg2, ...)
{
    arg_string = make_arg_string(orig

    new_arg_string = send_to_server_a
        HOOK_INFO^^before_call^^#{ori                    ame}^^#{arg_string}");

    if( new_arg_string == arg_string )
        ret = original_func(original_arg1, original_arg2, ...);
    else
        ret = original_func(parse(new_arg_string, 1), parse(new_arg_string, 2
            ), ...);

    ret_string = make_ret_string(ret);

    new_ret_string = send_to_server_and_wait("
        HOOK_INFO^^after_call^^#{original_function_name}^^#{ret_string}");
}
```

execute an original function

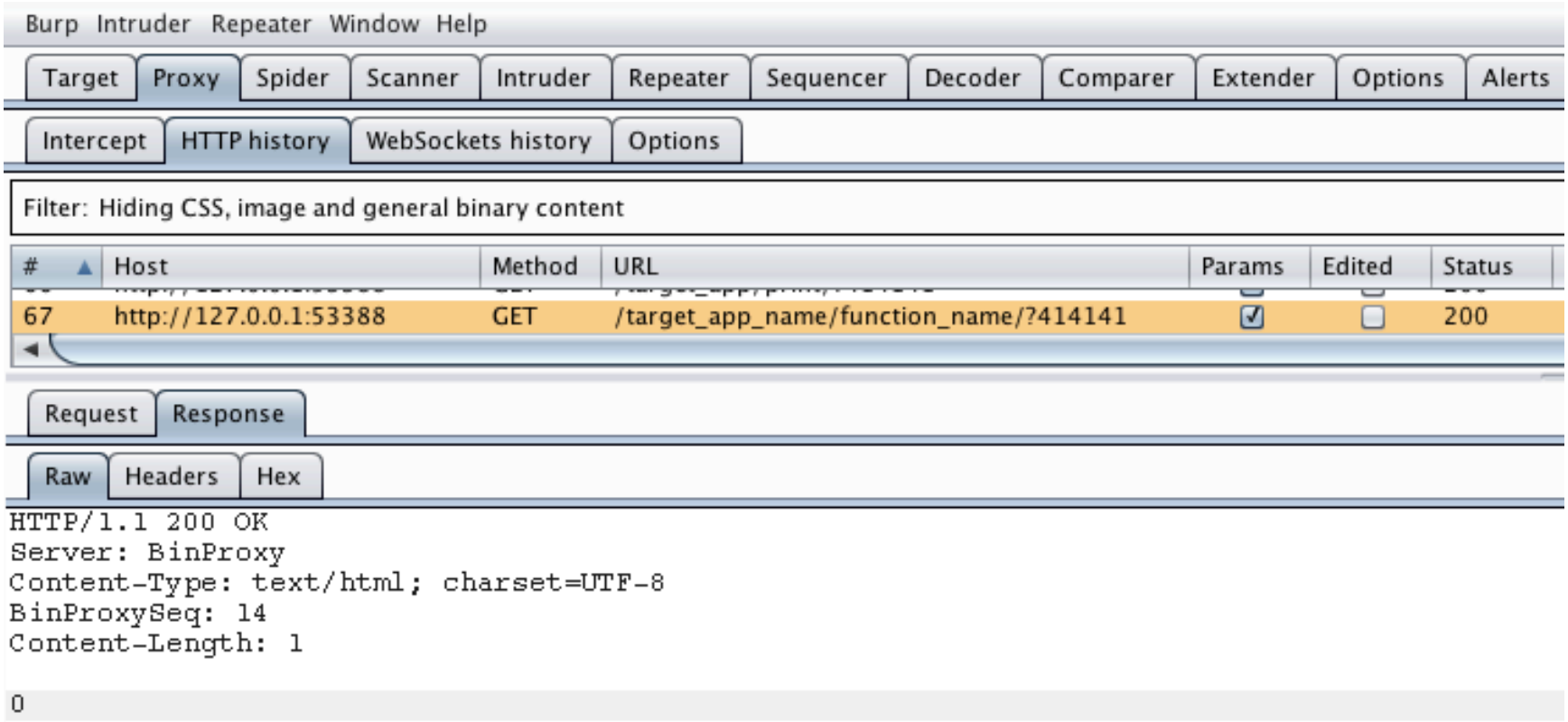
After sending an after_call message,
hooked_func will be blocked until getting response from BinProxy Server.

How to interwork with a web proxy - BinProxy Server

BinProxy Server convert a after_call message into HTTP response format for delivering the message to Web Proxy.

```
HTTP/1.1 200 OK
Date: Mon, 04 Aug 2014 17:22:59 GMT
Server: BinProxy
Content-Length: 1
Connection: close
Content-Type: application/return

0
```

How to interwork with a web proxy - Web Proxy



How to interwork with a web proxy - BinProxy Client

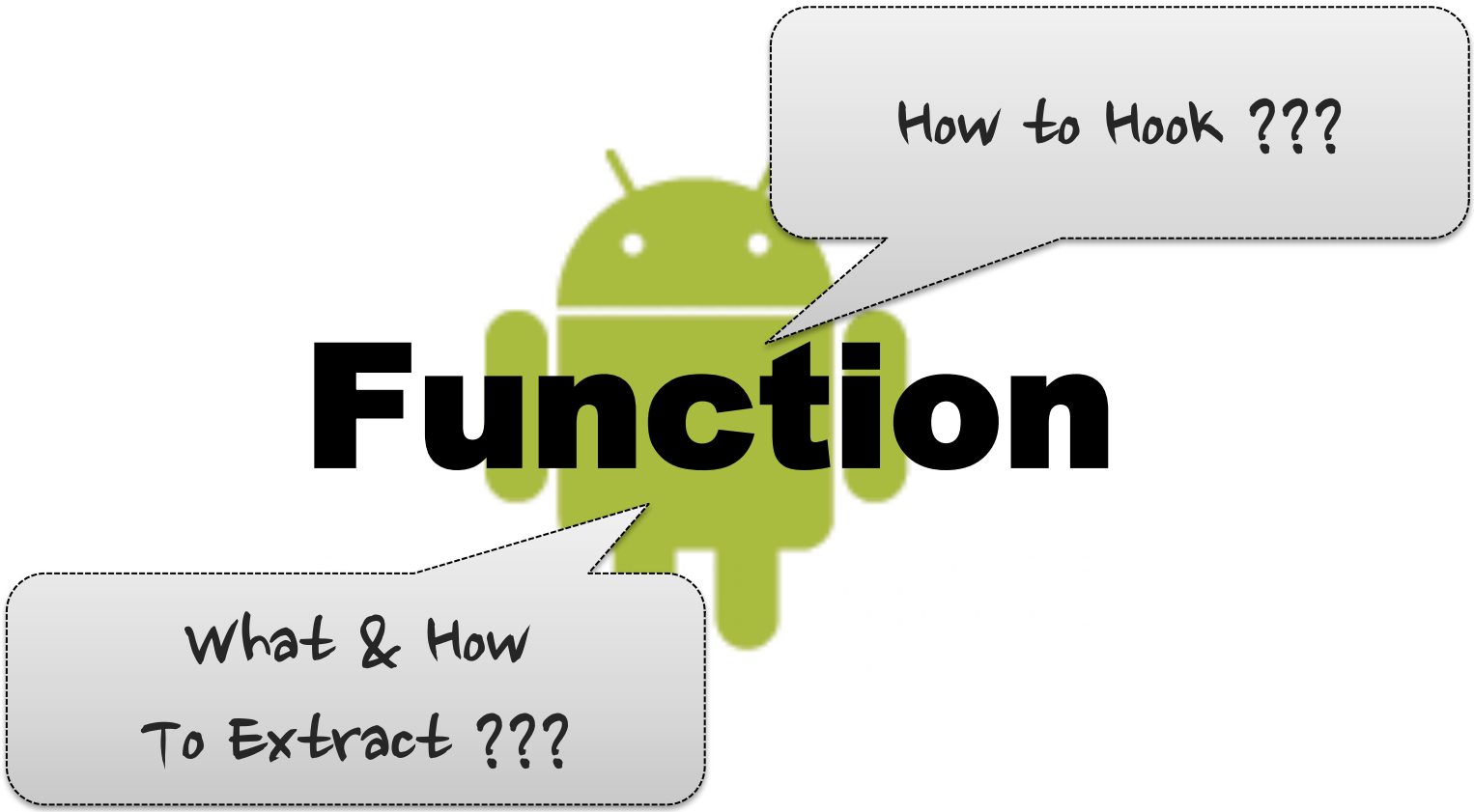
```
int hooked_func(arg1, arg2, ...)
{
    arg_string = make_arg_string(original_arg1, original_arg2, ...);

    new_arg_string = send_to_server_and_wait("
        HOOK_INFO^^before_call^^#{original_function_name}^^#{arg_string}");

    if( new_arg_string == arg_string )
        ret = original_func(original_arg1, original_arg2, ...);
    else
        ret = original_func(parse(new_arg_string, 1), parse(new_arg_string, 2
            ), ...);

    ret_string = make_ret_string(ret);

    new_ret_string = send_to_server_and_w
        HOOK_INFO^^after_call^^#{original                    tring}");

    if( new_ret_string == ret_string )
        return ret;
    else
        return parse(new_ret_string, 1);
}
```

return the value

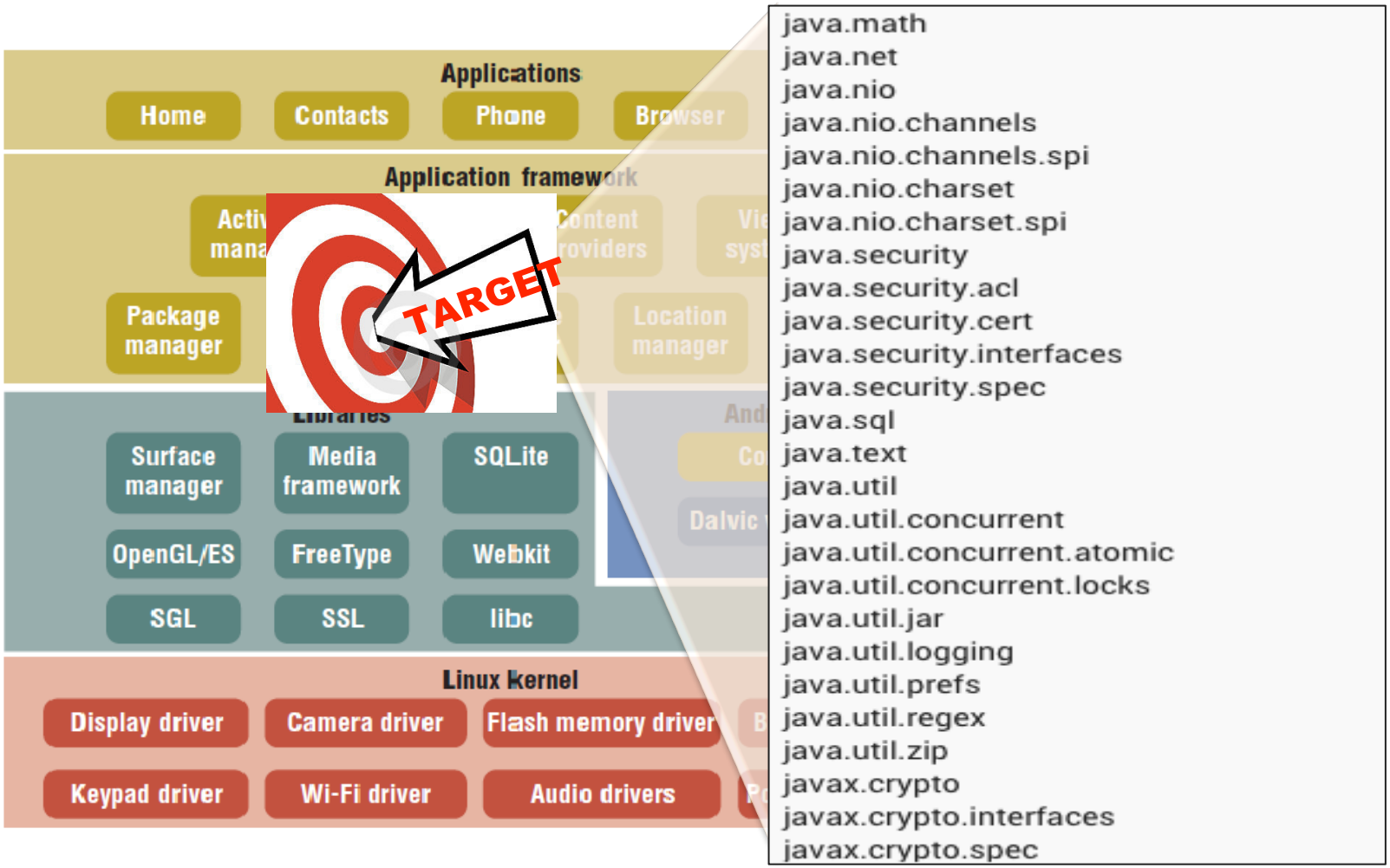
How to make?

Ways of build android client & PoC

Key Requirements



Key Requirements
- What & How To extract ..

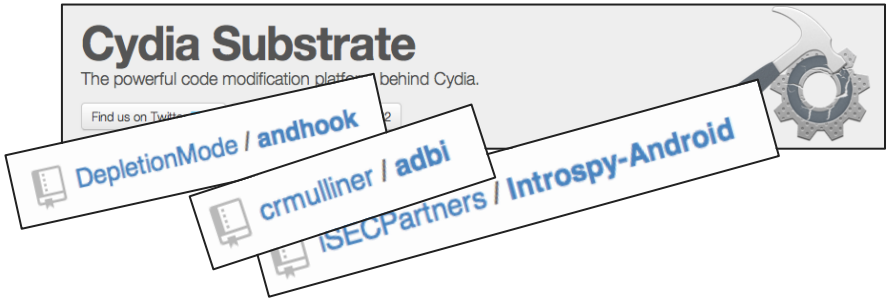


Key Requirements
- What & How To extract ..

We can use for hooking in Android :

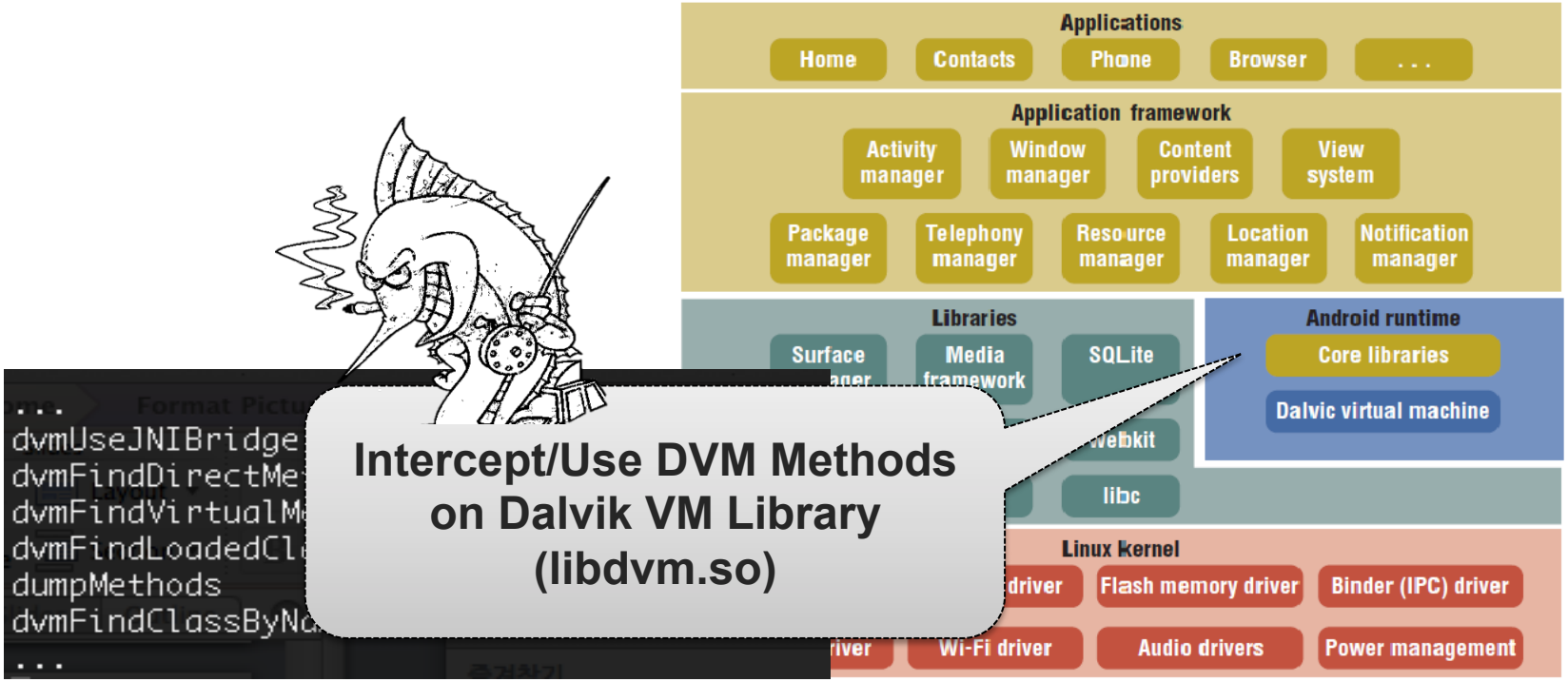
- Cydia substrate for Android
- Introspy-Android (GUI Interface + Cydia Substrate)
- AndHook(Android Hooking Framework)
- ADBI(Android Dynamic Binary Instrumentation Toolkit)
- [Paper] Hooking on Android -2014 CodeEngn Conference

….

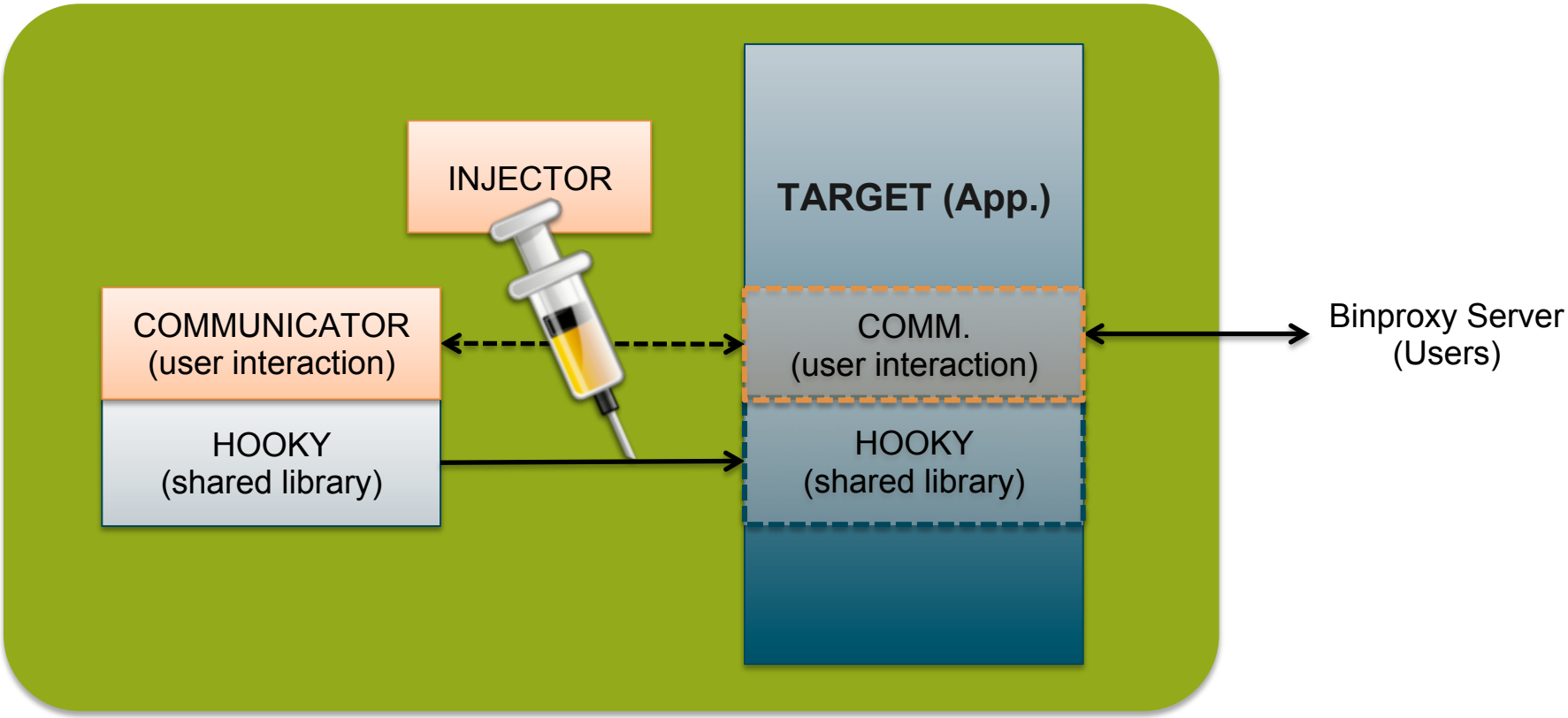


ADBI
(Android Binary Instrumentation Toolkit)

Dynamic Dalvik Instrumentation Framework for Android (old)
 - Collin Mulliner, SummerCon 2013.
https://github.com/crmulliner/adbi (current)



Binproxy Client modules for Android



Binproxy Client modules … (cont'd)

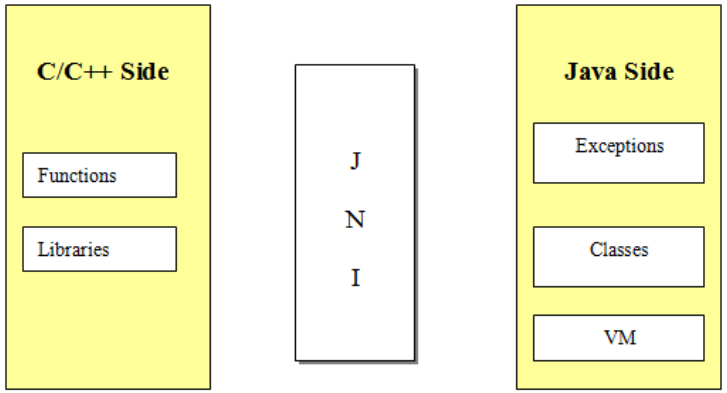
- INJECTOR
  : Inject the HOOKER(.so) into Target App.(running process)

- HOOKER
  : Hook the java/Android standard API for analysis.
  : loaded as the shared library(so) developed using JNI

- COMMUNICATOR
  : Interactive interface for communication with user
  : Send/receive values for Hooking, Monitoring, Modifying

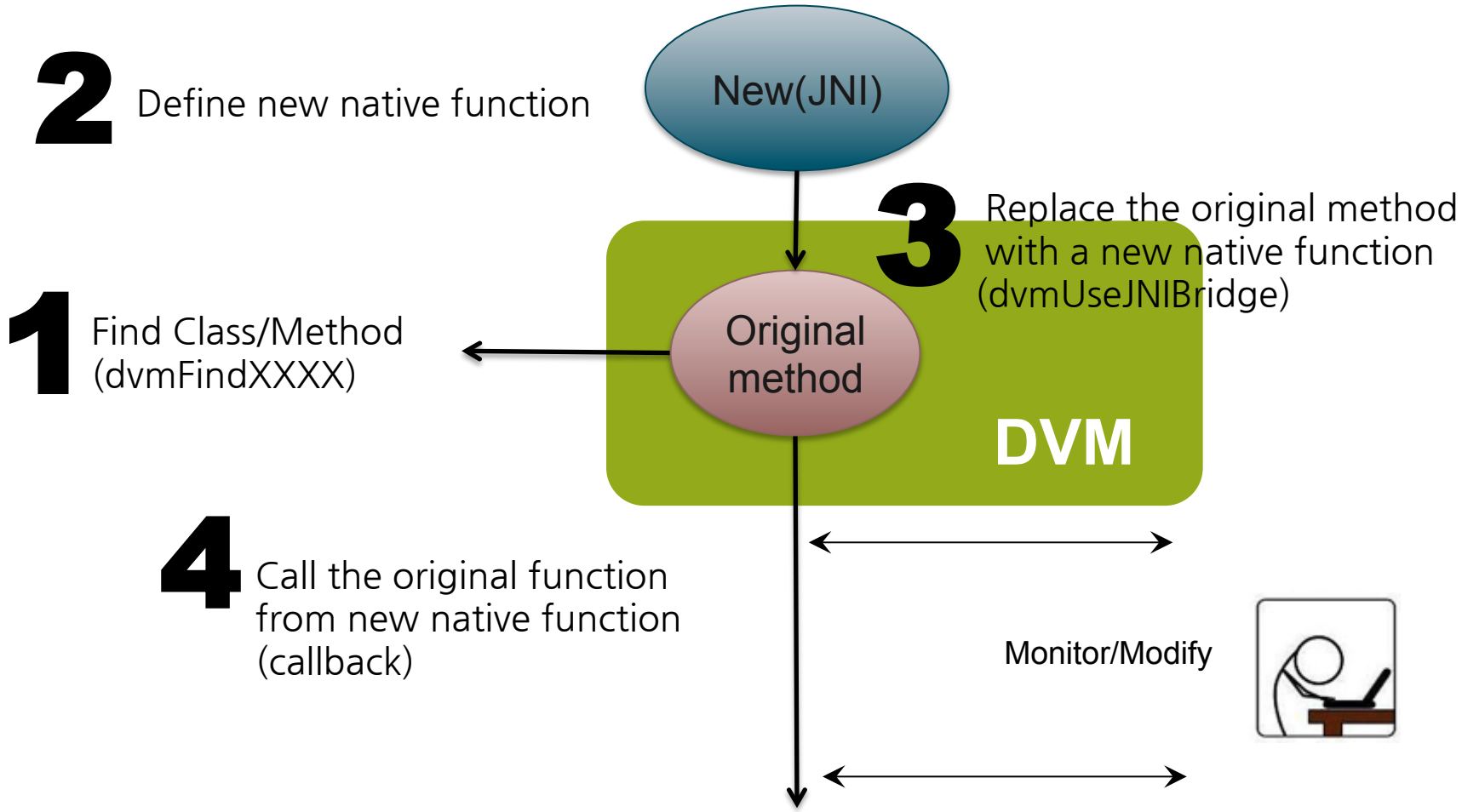
How to implement Android Client

Implemented using **JNI(Java Native Interface)**

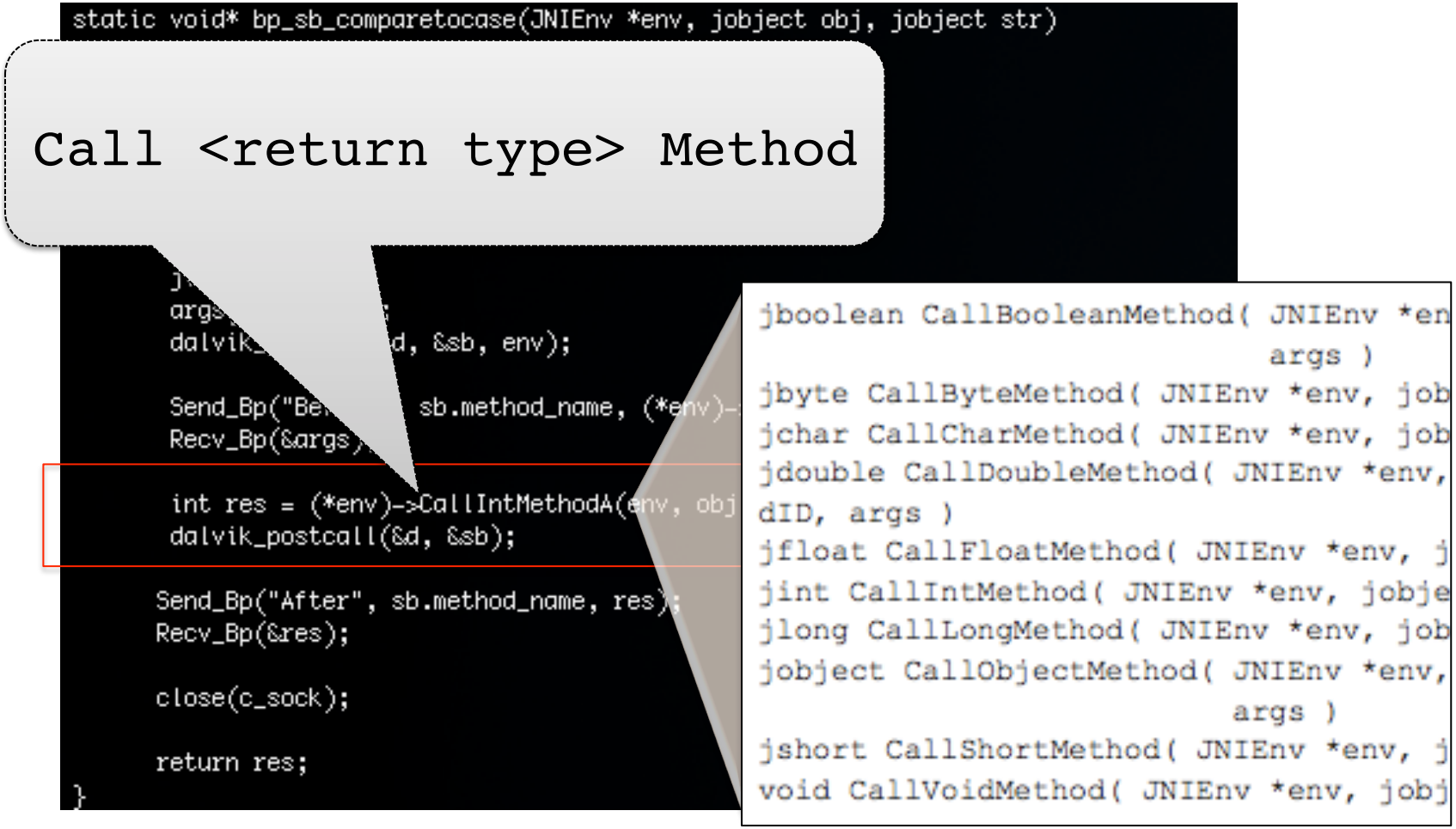


- Get the method Information loaded
- Define/Prototype new function(native) for target function(method)
- Call Original Method from new function.
- Monitor/Modify a argument/return value

How to implement … (Cont'd)



How to implement .. (Cont'd)



DEMO - PoC for Android App

DEMO

DEMO

Let's Crack

Password-Protection

: Modify RETURN

Let's Crack Application

: Monitor ARG. & RETURN

How to make?

Ways of build iOS client & PoC

Key Requirements - How To hook ..

- We can use for hooking in iOS:
  a. Cydia Substrate for iOS
  b. fishhook
  c. Mach-O-Hook

How to implement iOS client

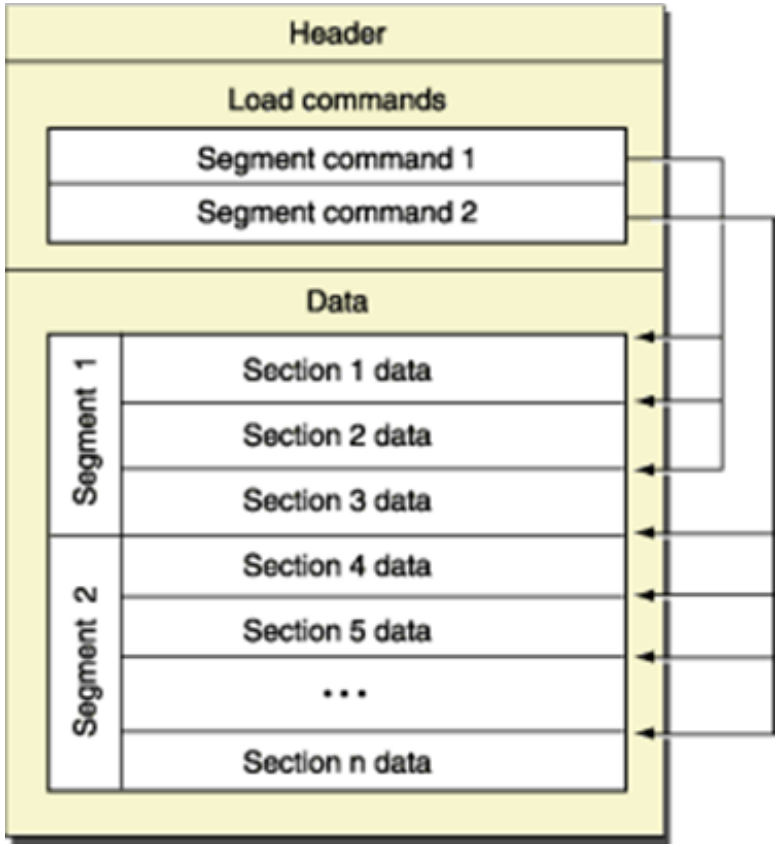
- Use a CydiaSubstrate
  a. Why CydiaSubstrate?
     -> verified stability

- Most of Apps in Cydia are use a CydiaSubstrate!

- Component of CydiaSubstrate
  a. MobileHooker
  b. MobileLoader
  c. Safe Mode

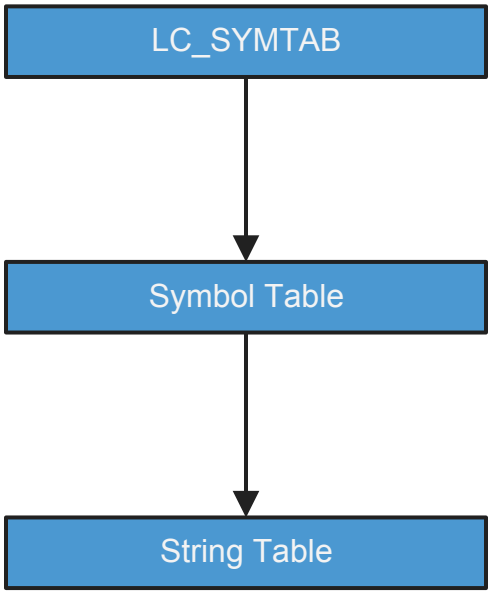
Key Requirements - What & How extract...

- Mach-O File Format



Key Requirements - What & How extract...

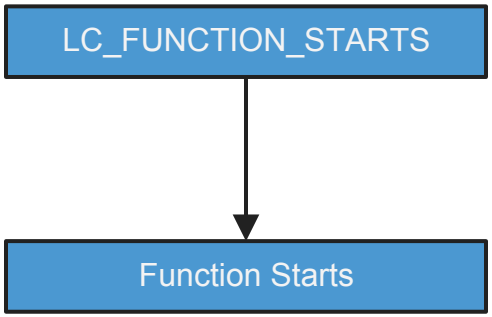
- API



Offset	Data	Description	Value
0000CDCC	00000CA7	String Table Index	_socket
0000CDD0	01	Type	
		00	N_UNDF
		01	N_EXT
0000CDD1	00	Section Index	NO_SECT
0000CDD2	0500	Description	
		0	REFERENCE_FLAG_UNDEFINED_NON_LAZY
		Library Ordinal	5 (libSystem.B.dylib)
0000CDD4	00000000	Value	0
0000CDD8	00000CAF	String Table Index	_strcmp
0000CDDC	01	Type	
		00	N_UNDF
		01	N_EXT
0000CDDD	00	Section Index	NO_SECT
0000CDDE	0500	Description	
		0	REFERENCE_FLAG_UNDEFINED_NON_LAZY
		Library Ordinal	5 (libSystem.B.dylib)
0000CDE0	00000000	Value	0

Key Requirements - What & How extract...

- Objective-C and User Function Address



Offset	Data	Description	Value
0000C4EC	95D301	uleb128	0xA995
0000C4EF	BC03	uleb128	0xAB51
0000C4F1	44	uleb128	0xAB95
0000C4F2	44	uleb128	0xABD9
0000C4F3	74	uleb128	0xAC4D
0000C4F4	D403	uleb128	0xAE21
0000C4F6	28	uleb128	0xAE49
0000C4F7	30	uleb128	0xAE79
0000C4F8	28	uleb128	0xAEA1
0000C4F9	30	uleb128	0xAED1
0000C4FA	3C	uleb128	0xAF0D
0000C4FB	60	uleb128	0xAF6D
0000C4FC	30	uleb128	0xAF9D
0000C4FD	30	uleb128	0xAFCD
0000C4FE	30	uleb128	0xAFFD
0000C4FF	30	uleb128	0xB02D
0000C500	30	uleb128	0xB05D
0000C501	1C	uleb128	0xB079
0000C502	2C	uleb128	0xB0A5
0000C503	2C	uleb128	0xB0D1
0000C504	9001	uleb128	0xB161

_SendLoginCheck	...	0000A994
-[ViewController viewDidLoad]	...	0000AB50
-[ViewController didReceiveMemo...	...	0000AB94
-[ViewController textFieldShouldR...	...	0000ABD8
-[ViewController LoginButton:]	...	0000AC4C
-[ViewController loginPassword]	...	0000AE20
-[ViewController setLoginPassword:]	...	0000AE48
-[ViewController infoMsg]	...	0000AE78
-[ViewController setInfoMsg:]	...	0000AEA0
-[ViewController .cxx_destruct]	...	0000AED0
-[AppDelegate application:didFini...	...	0000AF0C
-[AppDelegate applicationWillResi...	...	0000AF6C
-[AppDelegate applicationDidEnte...	...	0000AF9C
-[AppDelegate applicationWillEnte...	...	0000AFCC
-[AppDelegate applicationDidBec...	...	0000AFFC
-[AppDelegate applicationWillTer...	...	0000B02C
-[AppDelegate window]	...	0000B05C
-[AppDelegate setWindow:]	...	0000B078
-[AppDelegate .cxx_destruct]	...	0000B0A4
_main	...	0000B0D0
_objc_autoreleaseReturnValue$shim	...	0000B160

How to implement iOS client

- Target API and method selection
  a. Extracting Objective C classes & methods
  b. Extracting API lists
  c. Finding out user-defined function's args and types

- Monitoring an entire method and API by using hooking (Logging?) (Logging?)

DEMO - PoC for iOS App

DEMO


화면 공유
연결
편집
보기
윈도우
도움말
목 오전 3:13
데스크탑 — Python — 50×22
iksui-Mac:Desktop iks$ python SampleApp_server.py
('Server Port : ', 8888)
데스크탑 — bash — 50×22
iksui-Mac:Desktop iks$
iksui-iPhone
서비스 안 됨
오전 3:13
기타
음성 메모
FaceTime
뉴스 가판대
Activator
Cydia
SampleApp
SBSettings
전화
Mail
Safari
음악
SampleApp_server.py
01.server
Test_App
bak
binproxy_server.py
html
burpsuite_free_v1.6.jar

Anything else?

Future Works

Implementation Methods

- How to obtain a target application's function list and detail informations of the function
- How to utilize database information to distinct functions

Additional Functions

- arbitrary function execution
- arbitrary code execution
- memory scan and patch
- function control based on script languages
- disassemble and decompilation

And…

- Performance Improvement
- Additional OS Support

谢谢

Any Other Questions or Comments?

email : binproxy@0-day.me