ROMHACK

SAFE: Self Attentive Function Embedding for Binary Similarity

Luca Massarelli

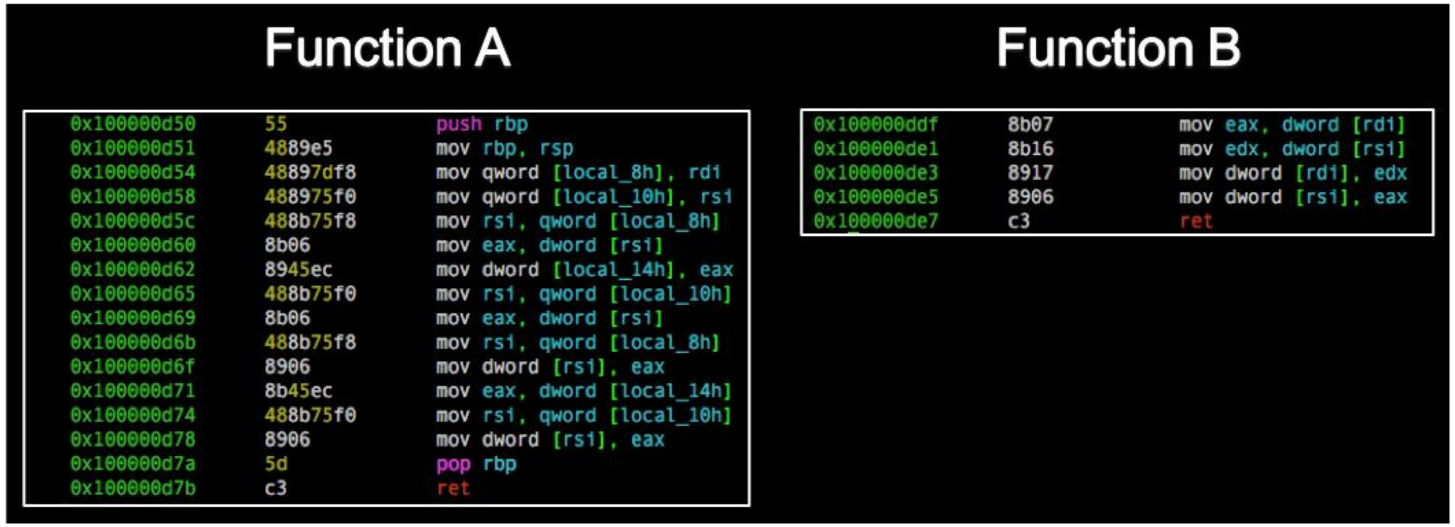
Who am I?

PhD Student @ Sapienza University of Rome

Exploring how to leverage Artificial Intelligence to improve security!

Reverse Engineering is painful…

Image Credit: G. A. Di Luna



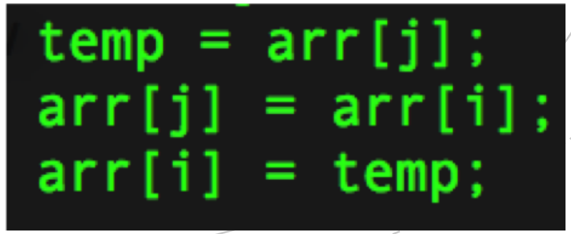
Function A

```
0x100000d50   55          push rbp
0x100000d51   4889e5      mov rbp, rsp
0x100000d54   48897df8    mov qword [local_8h], rdi
0x100000d58   488975f0    mov qword [local_10h], rsi
0x100000d5c   488b75f8    mov rsi, qword [local_8h]
0x100000d60   8b06        mov eax, dword [rsi]
0x100000d62   8945ec      mov dword [local_14h], eax
0x100000d65   488b75f0    mov rsi, qword [local_10h]
0x100000d69   8b06        mov eax, dword [rsi]
0x100000d6b   488b75f8    mov rsi, qword [local_8h]
0x100000d6f   8906        mov dword [rsi], eax
0x100000d71   8b45ec      mov eax, dword [local_14h]
0x100000d74   488b75f0    mov rsi, qword [local_10h]
0x100000d78   8906        mov dword [rsi], eax
0x100000d7a   5d          pop rbp
0x100000d7b   c3          ret
```

Function B

```
0x100000ddf   8b07        mov eax, dword [rdi]
0x100000de1   8b16        mov edx, dword [rsi]
0x100000de3   8917        mov dword [rdi], edx
0x100000de5   8906        mov dword [rsi], eax
0x100000de7   c3          ret
```

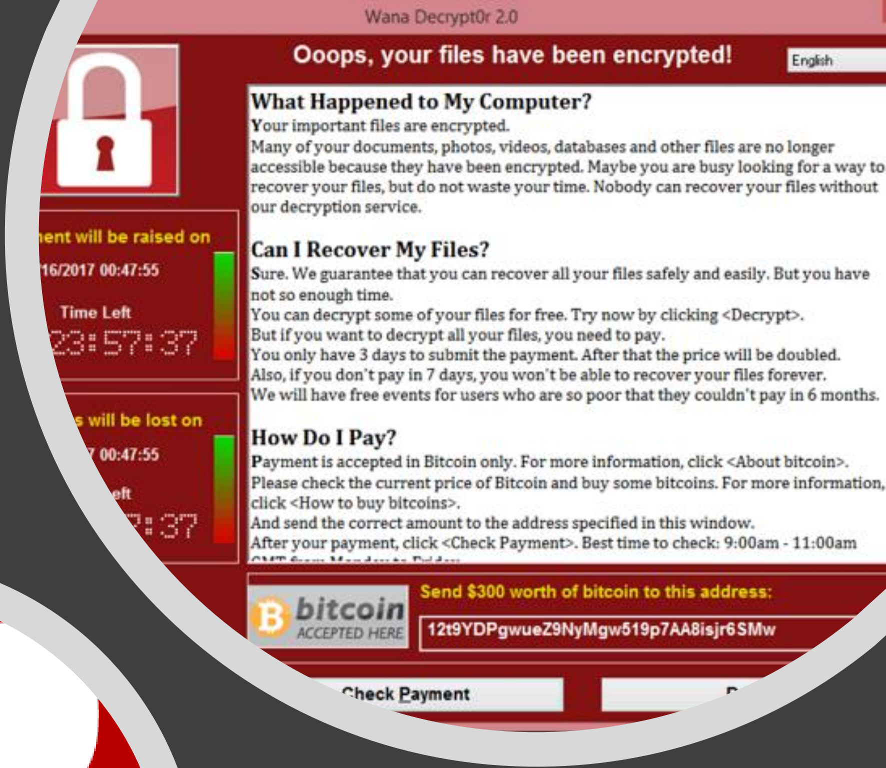
Binary Similarity Problem



```
temp = arr[j];
arr[j] = arr[i];
arr[i] = temp;
```

Applications

- **Vulnerability Detection**
- **Library Function Identification**
- **Malware Hunting**



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

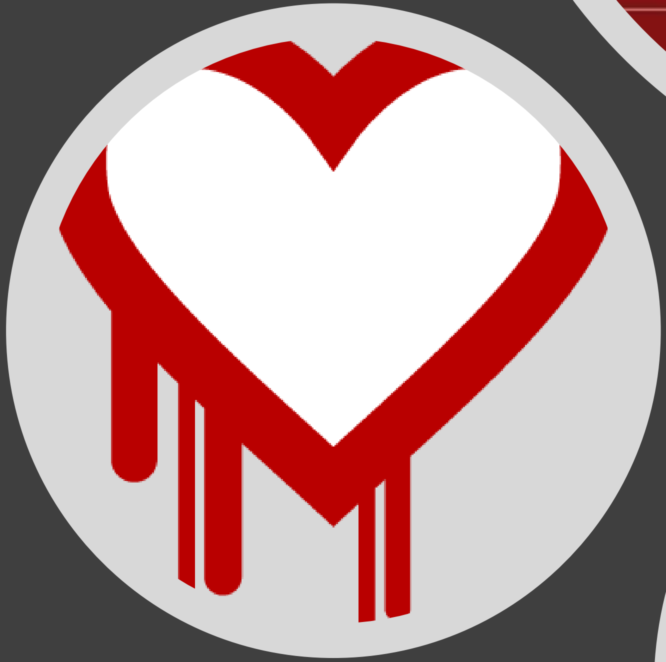
ment will be raised on
16/2017 00:47:55
Time Left
23:57:37

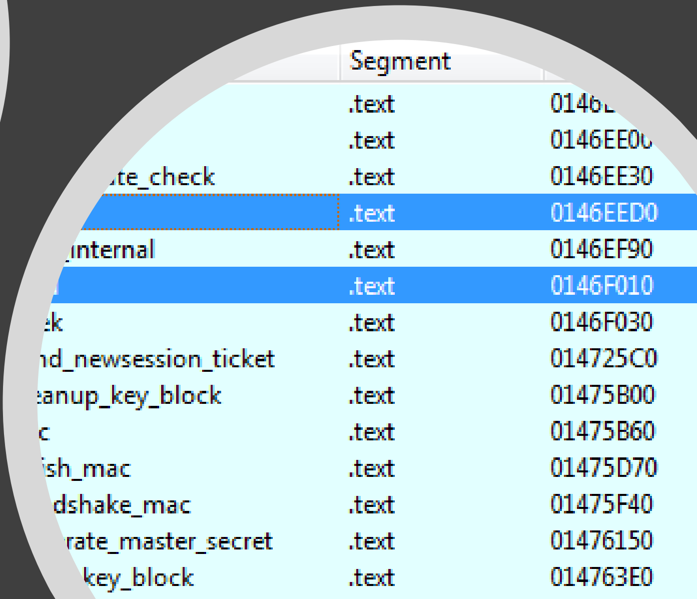
s will be lost on
7 00:47:55
eft
7:37

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

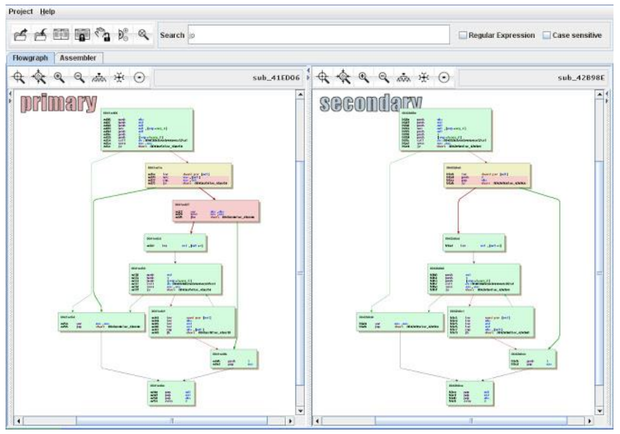
Check Payment



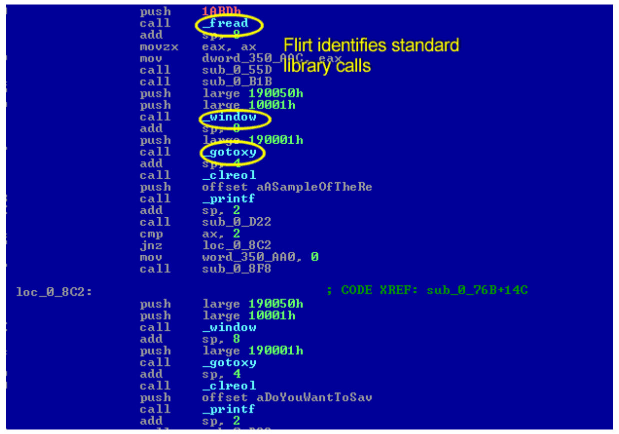


	Segment	
	.text	0146
	.text	0146EE0
te_check	.text	0146EE30
	.text	0146EED0
internal	.text	0146EF90
	.text	0146F010
k	.text	0146F030
d_newsession_ticket	.text	014725C0
anup_key_block	.text	01475B00
c	.text	01475B60
sh_mac	.text	01475D70
dshake_mac	.text	01475F40
rate_master_secret	.text	01476150
key_block	.text	014763E0

Existing Commercial Solutions

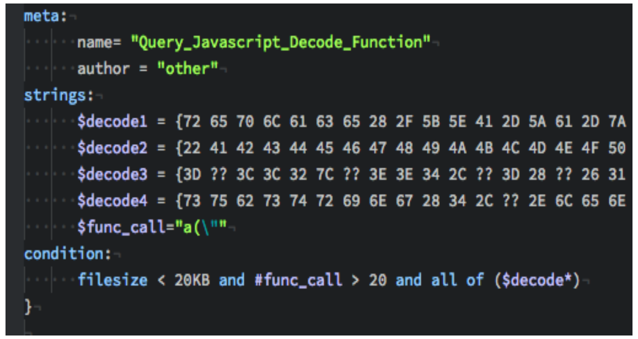


BinDiff



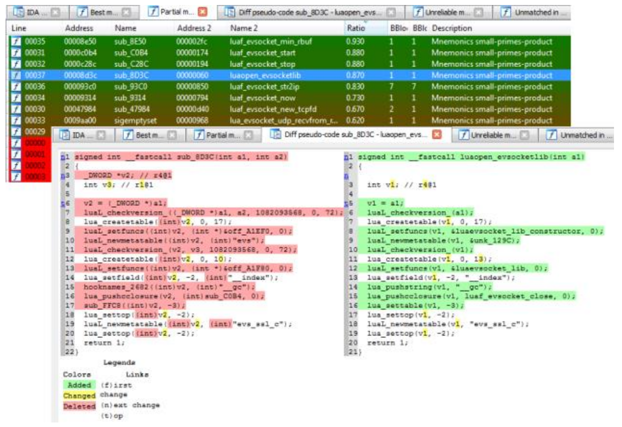
```
            push    1ABDh
            call    _fread
            add     sp, 8
            movzx   eax, ax
            mov     dword_350_AAC, eax
            call    sub_0_55D
            call    sub_0_B1B
            push    large 190050h
            push    large 10001h
            call    _window
            add     sp, 8
            push    large 190001h
            call    _gotoxy
            add     sp, 4
            call    _clreol
            push    offset aASampleOfTheRe
            call    _printf
            add     sp, 2
            call    sub_0_D22
            cmp     ax, 2
            jnz     loc_0_8C2
            mov     word_350_AA0, 0
            call    sub_0_8F8

loc_0_8C2:                              ; CODE XREF: sub_0_76B+14C
            push    large 190050h
            push    large 10001h
            call    _window
            add     sp, 8
            push    large 190001h
            call    _gotoxy
            add     sp, 4
            call    _clreol
            push    offset aDoYouWantToSav
            call    _printf
            add     sp, 2
```

IDA F.L.I.R.T.



```
meta:
    name= "Query_Javascript_Decode_Function"
    author = "other"
strings:
    $decode1 = {72 65 70 6C 61 63 65 28 2F 5B 5E 41 2D 5A 61 2D 7A
    $decode2 = {22 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50
    $decode3 = {3D ?? 3C 3C 32 7C ?? 3E 3E 34 2C ?? 3D 28 ?? 26 31
    $decode4 = {73 75 62 73 74 72 69 6E 67 28 34 2C ?? 2E 6C 65 6E
    $func_call="a(\""
condition:
    filesize < 20KB and #func_call > 20 and all of ($decode*)
}
```

yara



Line	Address	Name	Address 2	Name 2	Ratio	BBlo	BBlc	Description
00035	00008e50	sub_8E50	000002fc	luaf_evsocket_min_rbuf	0.930	1	1	Mnemonics small-primes-product
00031	0000c0b4	sub_C0B4	00000174	luaf_evsocket_start	0.880	1	1	Mnemonics small-primes-product
00032	0000c28c	sub_C28C	00000194	luaf_evsocket_stop	0.880	1	1	Mnemonics small-primes-product
00037	00008d3c	sub_8D3C	00000060	luaopen_evsocketlib	0.870	1	1	Mnemonics small-primes-product
00036	000093c0	sub_93C0	00000850	luaf_evsocket_str2ip	0.830	7	7	Mnemonics small-primes-product
00034	00009314	sub_9314	00000794	luaf_evsocket_now	0.730	1	1	Mnemonics small-primes-product
00030	00047984	sub_47984	00000d40	luaf_evsocket_new_tcpfd	0.670	2	1	Mnemonics small-primes-product
00033	0009aa00	sigemptyset	00000968	lua_evsocket_udp_recvfrom_r...	0.620	1	1	Mnemonics small-primes-product
00029								
00000								
00001								
00002								
00003								

```
signed int __fastcall sub_8D3C(int a1, int a2)
{
  _DWORD *v2; // r4@1
  int v3; // r1@1

  v2 = (_DWORD *)a1;
  luaL_checkversion_((_DWORD *)a1, a2, 1082093568, 0, 72);
  lua_createtable((int)v2, 0, 17);
  luaL_setfuncs((int)v2, (int *)&off_A1EF0, 0);
  luaL_newmetatable((int)v2, (int)"evs");
  luaL_checkversion_(v2, v3, 1082093568, 0, 72);
  lua_createtable((int)v2, 0, 10);
  luaL_setfuncs((int)v2, (int *)&off_A1F80, 0);
  lua_setfield((int)v2, -2, (int)"__index");
  hooknames_2682((int)v2, (int)"__gc");
  lua_pushcclosure(v2, (int)sub_C0B4, 0);
  sub_FFC8((int)v2, -3);
  lua_settop((int)v2, -2);
  luaL_newmetatable((int)v2, (int)"evs_ssl_c");
  lua_settop((int)v2, -2);
  return 1;
}
```

```
signed int __fastcall luaopen_evsocketlib(int a1)
{

  int v1; // r4@1

  v1 = a1;
  luaL_checkversion_(a1);
  lua_createtable(v1, 0, 17);
  luaL_setfuncs(v1, &luaevsocket_lib_constructor, 0);
  luaL_newmetatable(v1, &unk_129C);
  luaL_checkversion_(v1);
  lua_createtable(v1, 0, 13);
  luaL_setfuncs(v1, &luaevsocket_lib, 0);
  lua_setfield(v1, -2, "__index");
  lua_pushstring(v1, "__gc");
  lua_pushcclosure(v1, luaf_evsocket_close, 0);
  lua_settable(v1, -3);
  lua_settop(v1, -2);
  luaL_newmetatable(v1, "evs_ssl_c");
  lua_settop(v1, -2);
  return 1;
}
```

Legends

Colors	Links
Added	(f)irst
Changed	change
Deleted	(n)ext change
	(t)op

DIAPHORA

Not Scalable (BinDiff - Diaphora)

Require an extact copy of the function (IDA F.L.I.R.T. - YARA)

Analyst have to write rule (YARA)

Main Limitations

A few word about recompilation

Easy to do!

Effective

How to create new efficient and effective solutions?

WORD2VEC
ALL THE THINGS!
memegenerator.net

EMBEDDINGS!!

IDEA BORROWED FROM
Natural Language Processing

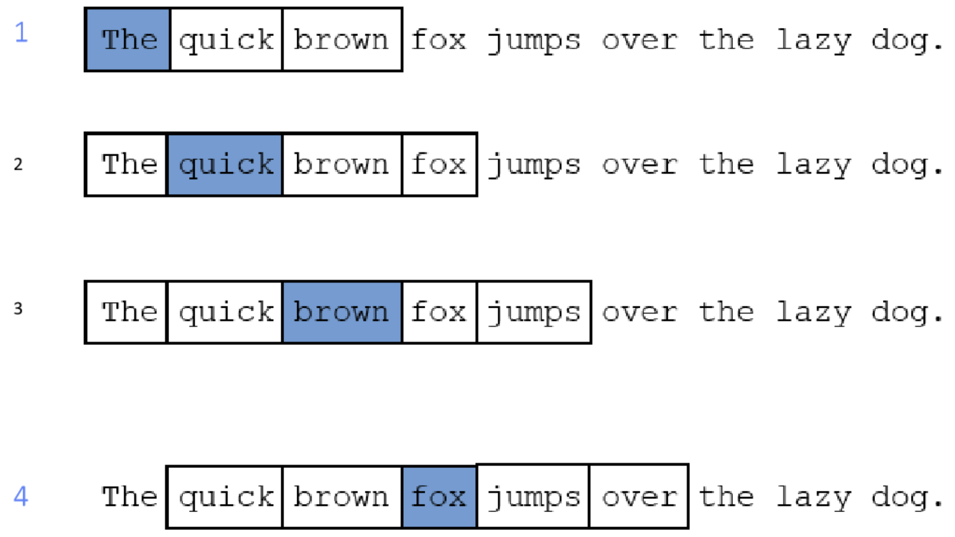
Representation of words, sentences or documents using vector!

$$BINARY = v1 = [\,0.17\,, 0.19\,, \ldots, 0.21]$$

$$BINARIES = v2 = [\,0.16\,, 0.23\,, \ldots, 0.20]$$

$$\downarrow$$

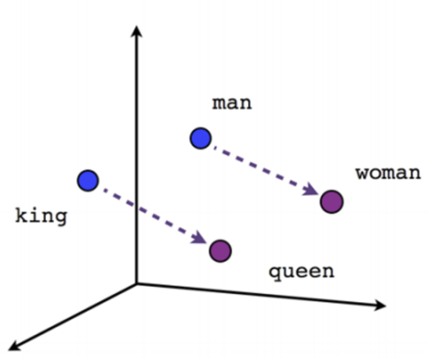
$$SIM(BINARY, BINARIES) = < v1, v2 > = 0.9$$


1 The quick brown fox jumps over the lazy dog.
2 The quick brown fox jumps over the lazy dog.
3 The quick brown fox jumps over the lazy dog.
4 The quick brown fox jumps over the lazy dog.

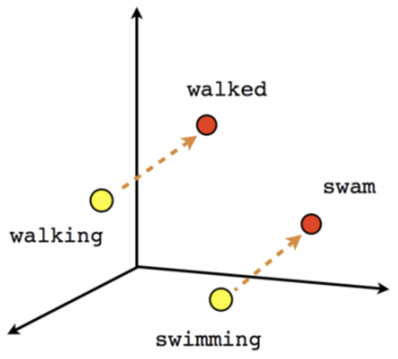
Unsupervised !

Word2Vec Model

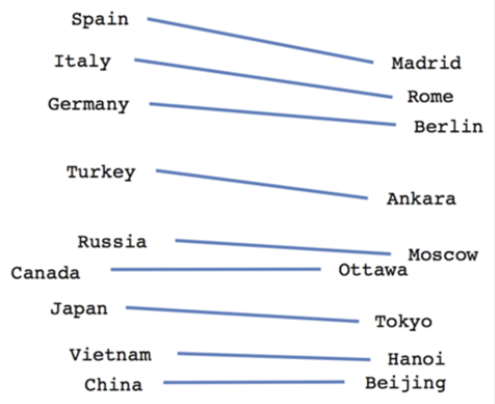
- The embedding of each word is computed with an unsupervised algorithm that consider the context in od the word.



Male-Female



Verb tense



Country-Capital

Word2Vec Model

- Words relationship can be retrieved from the embeddings:

$$man : women = king : ???$$

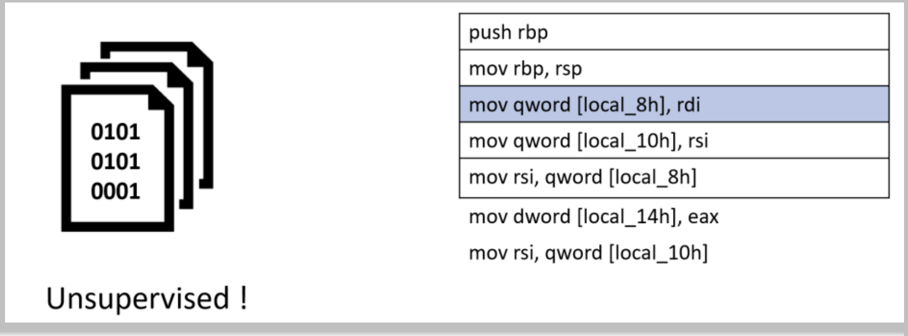
$$v2w(man) - v2w(king) + v2w(women) = w2v(queen)$$

Word2Vec Model For ASM

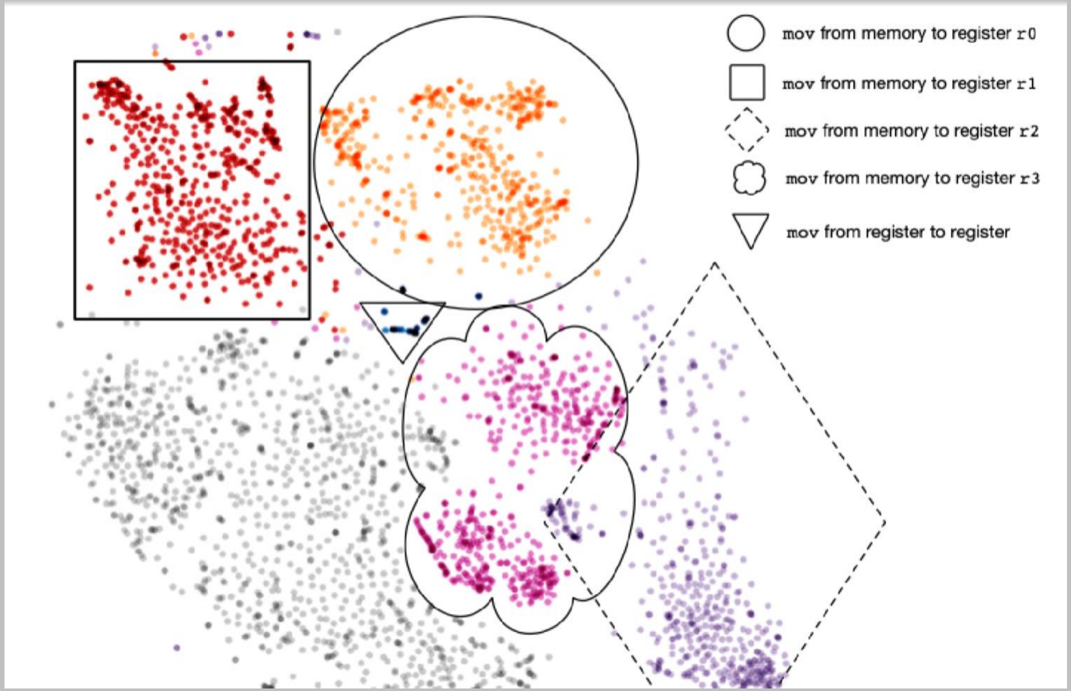
We can do the same with assembly code!

$push\ rbp : pop\ rbp = \ \ push\ rax : ???$

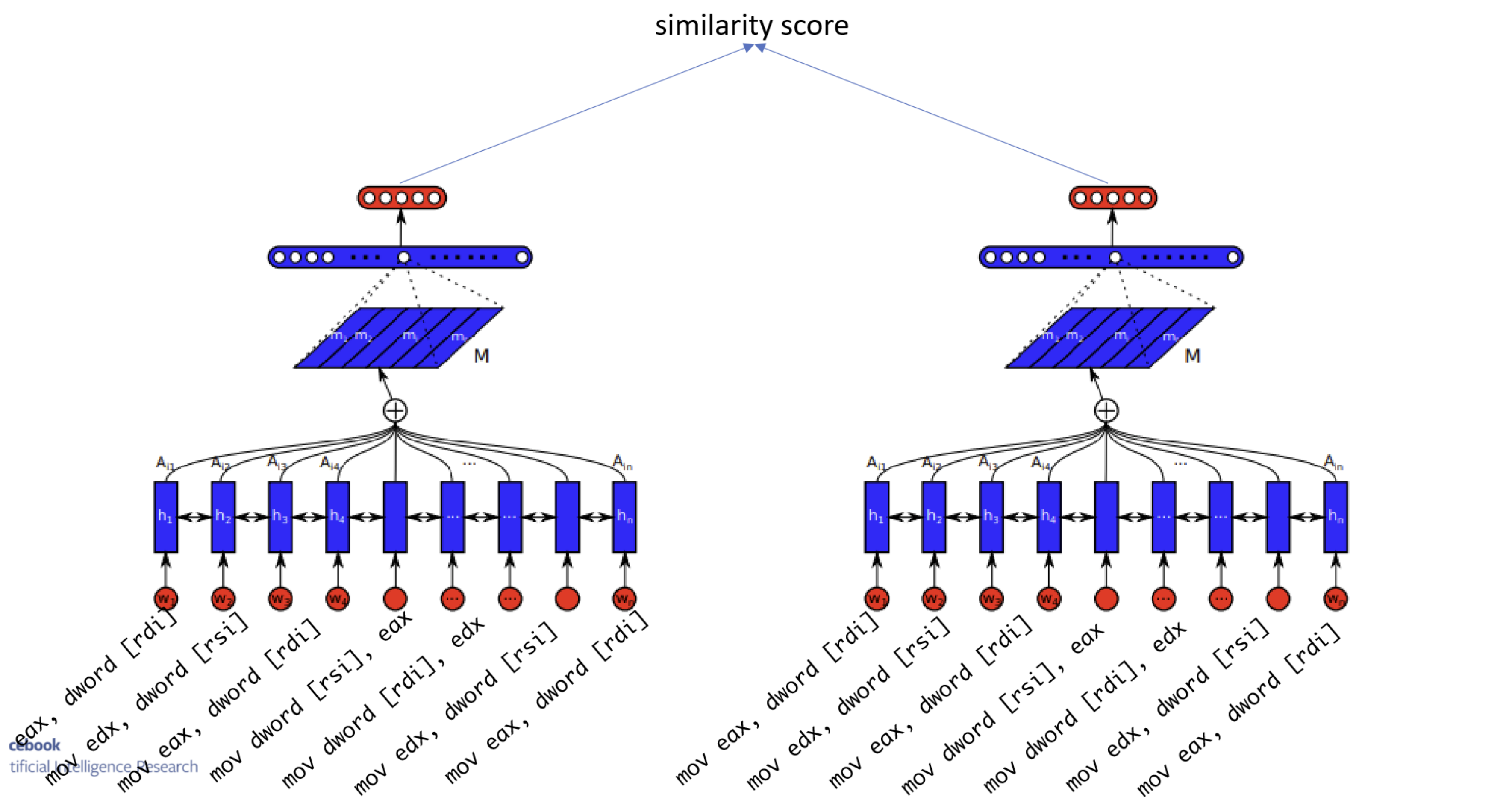
pop rax



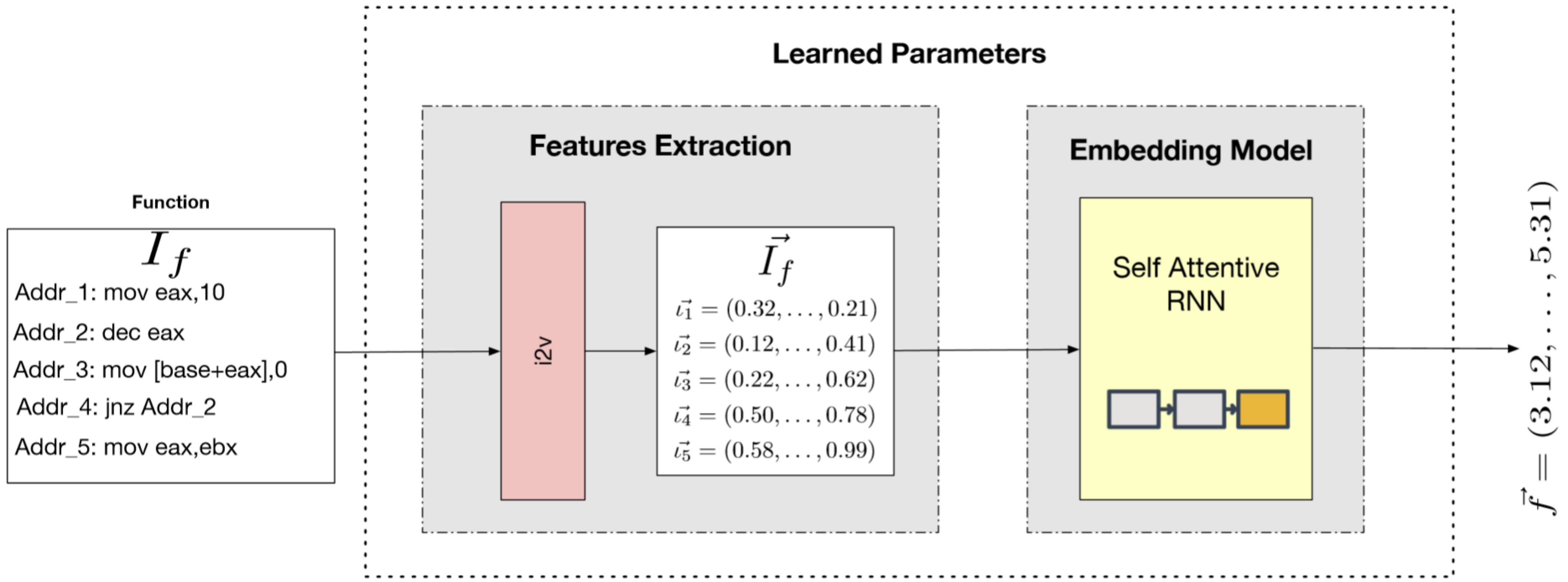
```
push rbp
mov rbp, rsp
mov qword [local_8h], rdi
mov qword [local_10h], rsi
mov rsi, qword [local_8h]
mov dword [local_14h], eax
mov rsi, qword [local_10h]
```



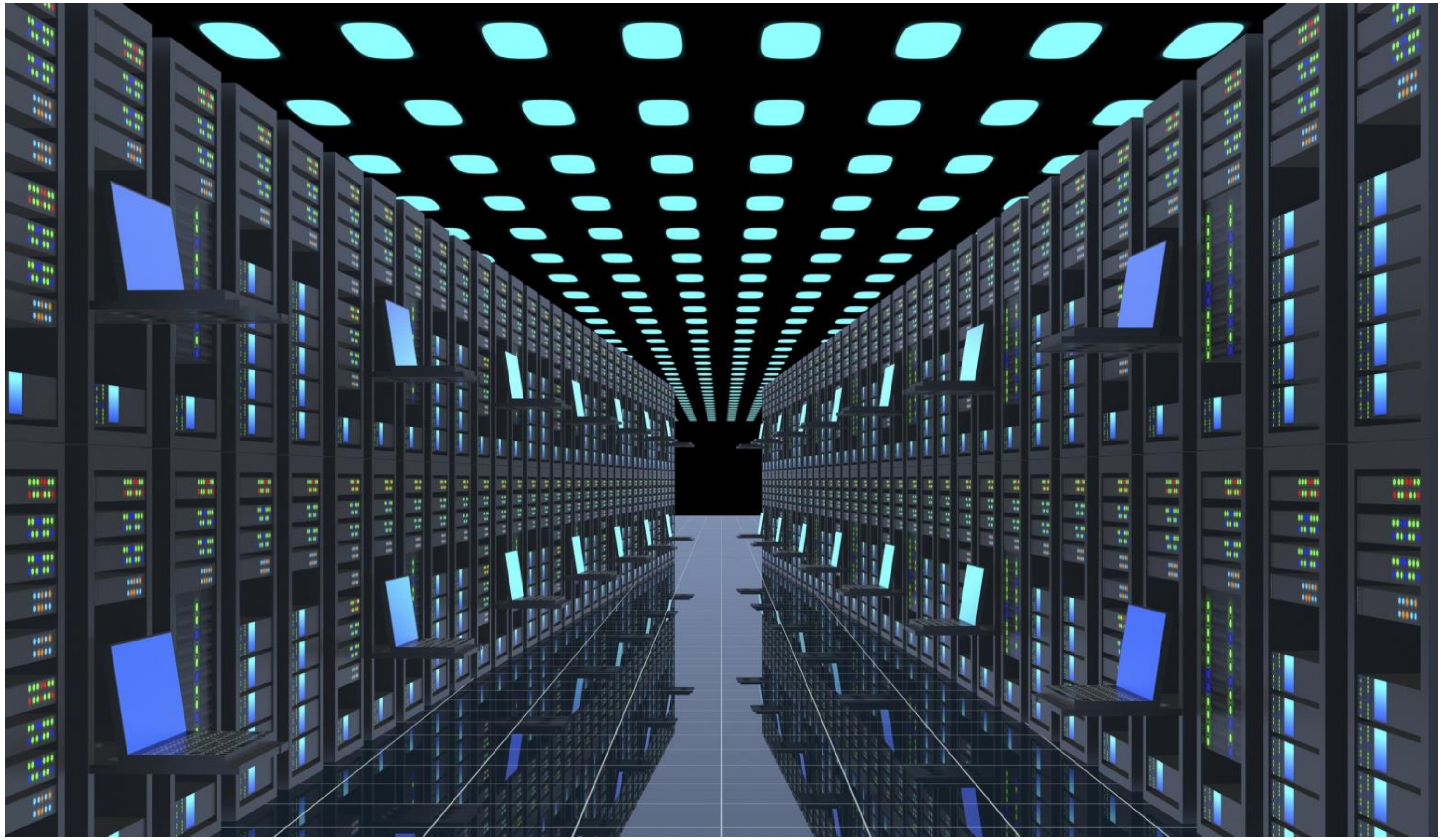
How we **aggregate** instruction embeddings to function embeddings?



Structured Self Attentive Model


Learned Parameters
Features Extraction
Embedding Model
Function
I_f
Addr_1: mov eax,10
Addr_2: dec eax
Addr_3: mov [base+eax],0
Addr_4: jnz Addr_2
Addr_5: mov eax,ebx
i2v
$\vec{I_f}$
$\vec{\iota_1} = (0.32, \dots, 0.21)$
$\vec{\iota_2} = (0.12, \dots, 0.41)$
$\vec{\iota_3} = (0.22, \dots, 0.62)$
$\vec{\iota_4} = (0.50, \dots, 0.78)$
$\vec{\iota_5} = (0.58, \dots, 0.99)$
Self Attentive RNN
$\vec{f} = (3.12, \dots, 5.31)$

The Full Pipeline

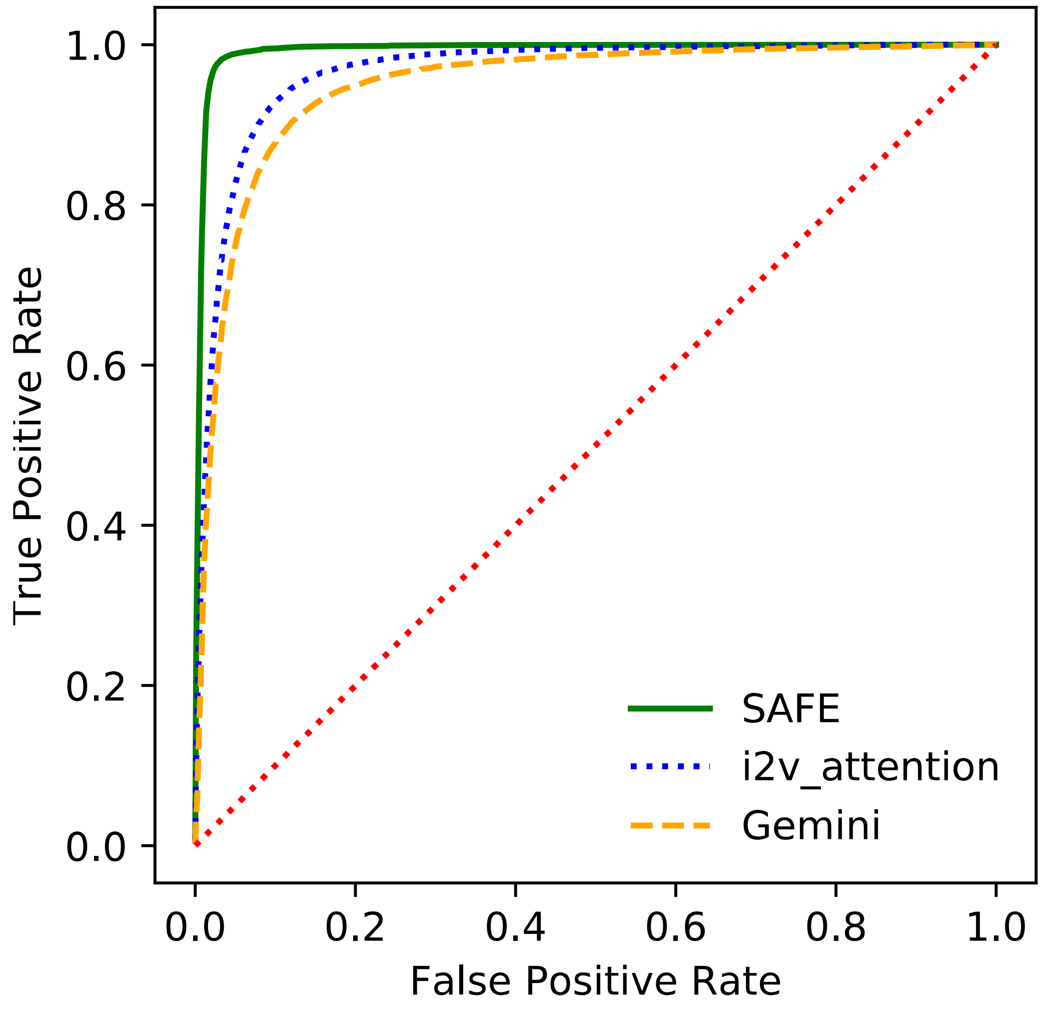


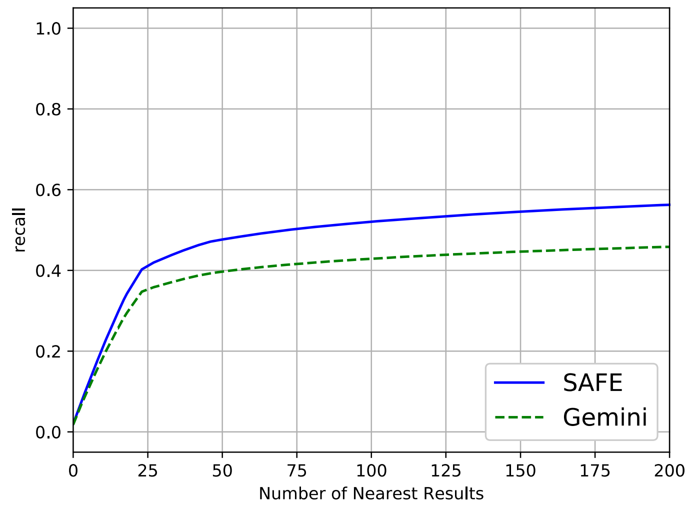
Creating the dataset

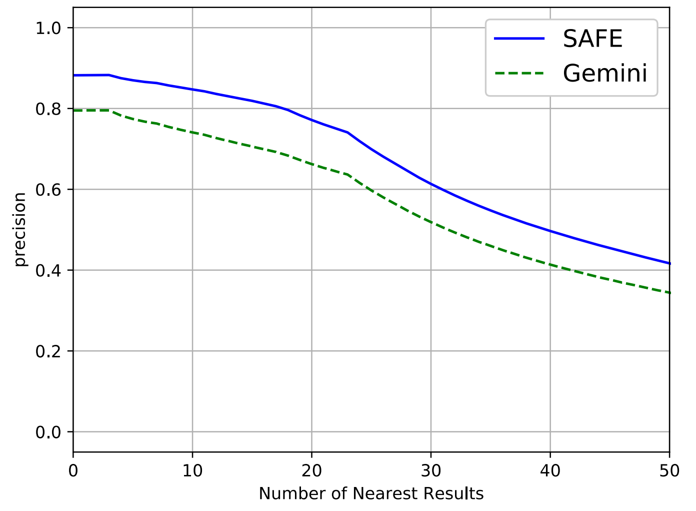
- This is easy!!!
- We compile 11 different projects with different compilers and optimization!
- … and we disassemble everithing!

It works!!

- AUC:
  - SAFE: 0.99
  - I2v_attention: 0.96
  - Gemini (MFE): 0.95
- We tested SAFE on different task!





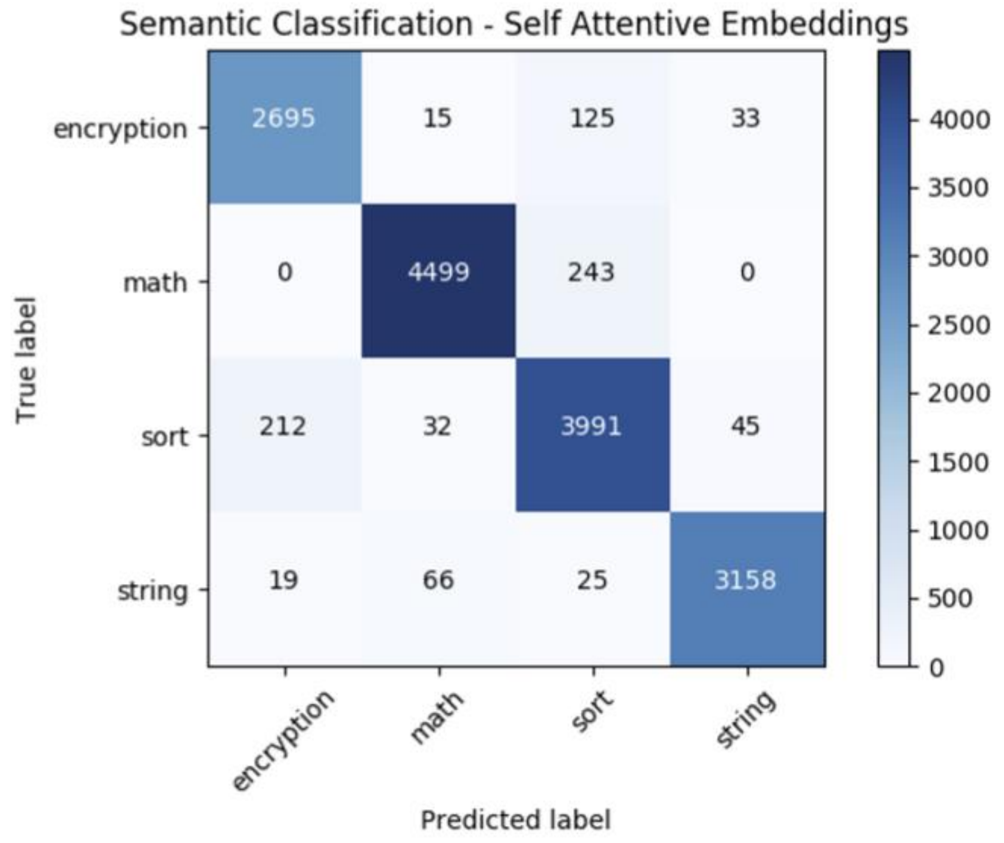


Function Search Engine!

- We tested SAFE as a function search engine!
- We try to retrieve from a knowledge base similar function to the query!

Semantic Classification

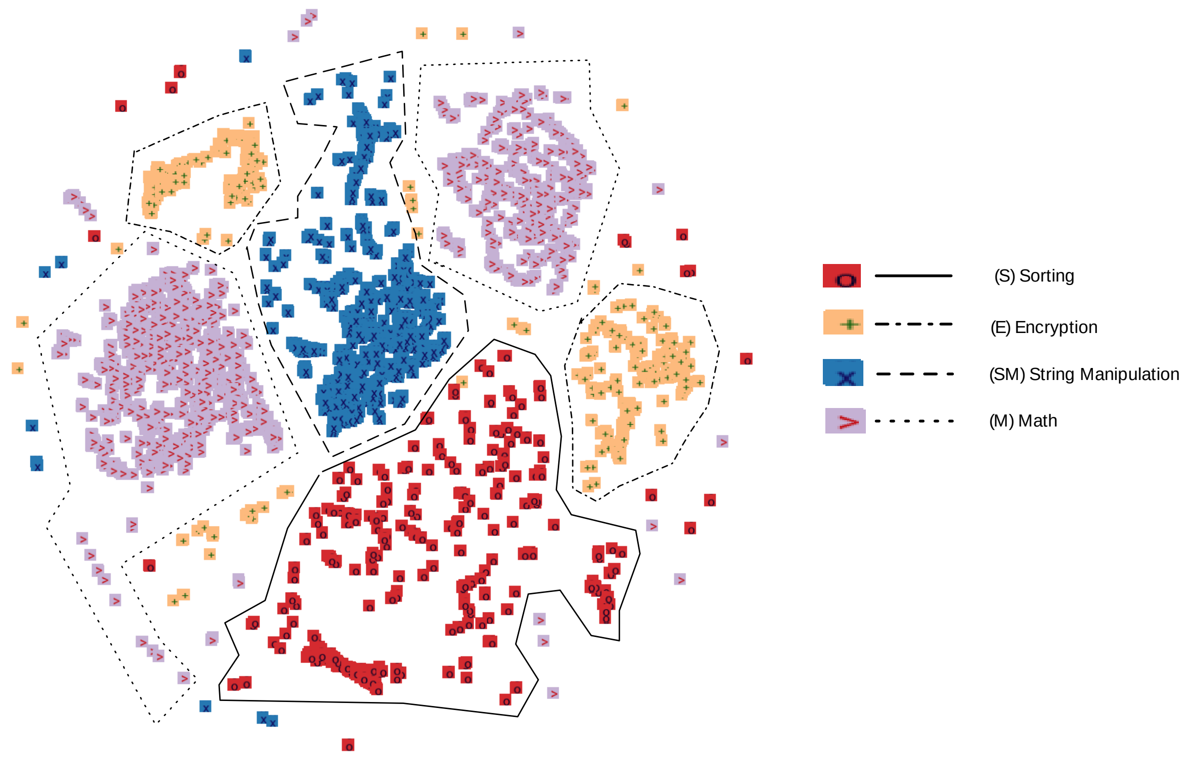
- We try to classify functions to 4 different semantic classes using embeddings!
  - Math
  - String
  - Encryption
  - Sorting



True label \ Predicted label	encryption	math	sort	string
encryption	2695	15	125	33
math	0	4499	243	0
sort	212	32	3991	45
string	19	66	25	3158

Semantic Classification Visualization

Embeddings are clustered in the space according to their semantic!



Applications

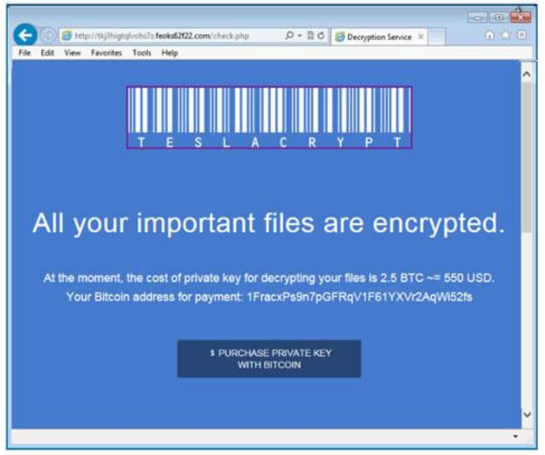
IDENTIFICATION OF AN ENCRYPTION FUNCTION INSIDE A MALWARE!

IDENTIFICATION OF A VULNERABLE FUNCTIONS INSIDE A FIRMWARE!

YARASAFE – USING SAFE INSIDE YARA

TeslaCrypt Ransomware

- We disassemble the sample with IDA and we used our semantic classifier to analyze every function!
- The Classifier founds seven functions that has encryption semantic!
- 6 of them were effectively performing encryption!!


http://tkj3higtqlvohs7z.feoks62f22.com/check.php
Decryption Service
File Edit View Favorites Tools Help
T E S L A C R Y P T
$ PURCHASE PRIVATE KEY WITH BITCOIN

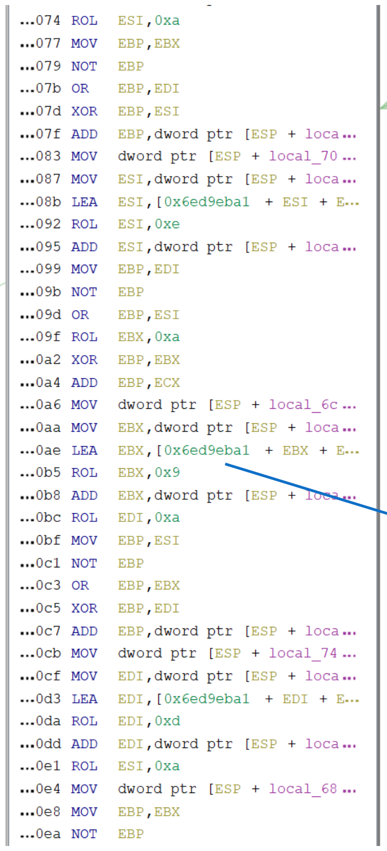
All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC ~= 550 USD.
Your Bitcoin address for payment: 1FracxPs9n7pGFRqV1F61YXVr2AqWi52fs

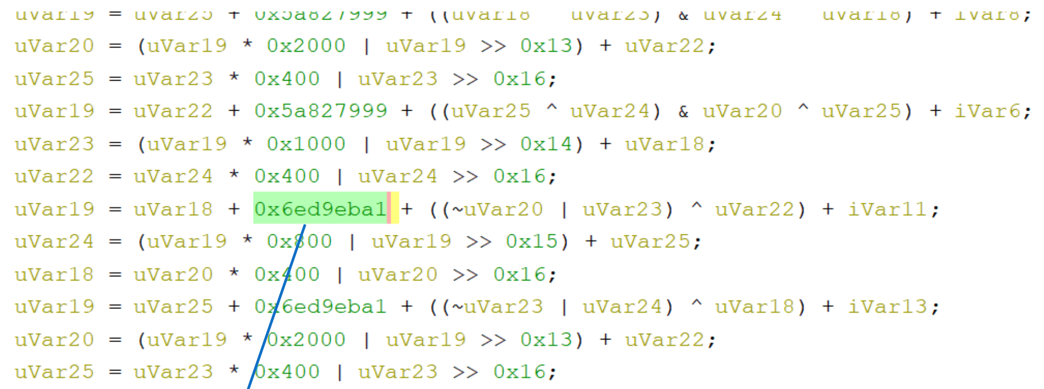
Sample:3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370

Detected Functions: 0x41e900, 0x420ec0, 0x4210a0,0x4212c0, 0x421665,0x421900, 0x4219c0

Function Detected At 0x41E900

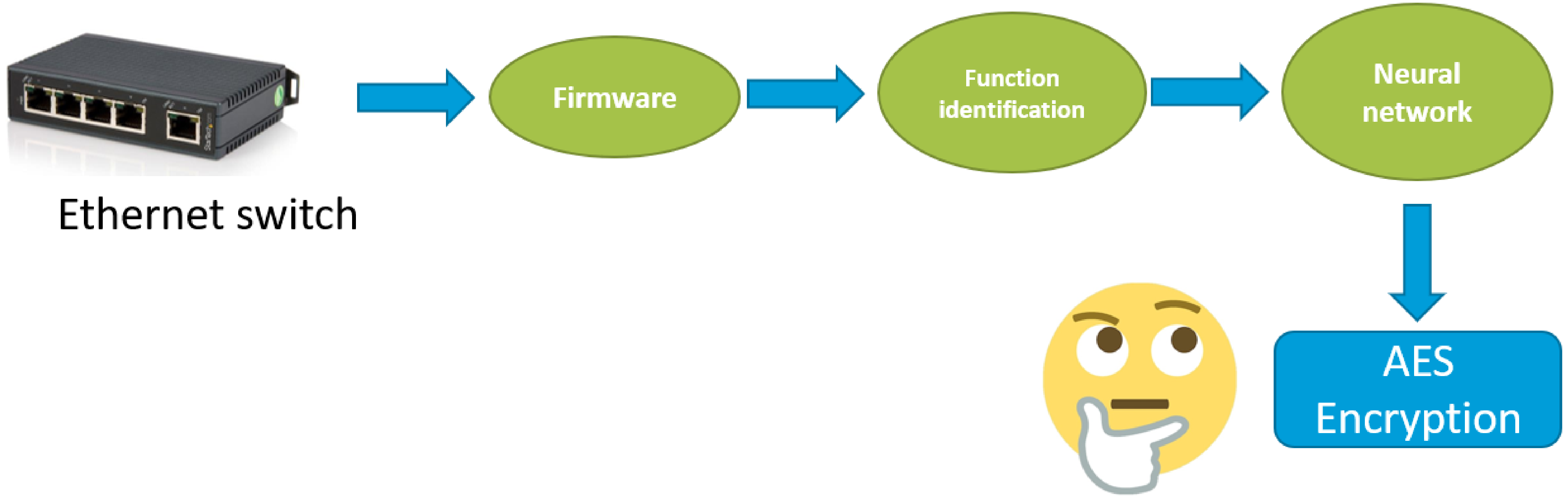


```
...074 ROL  ESI,0xa
...077 MOV  EBP,EBX
...079 NOT  EBP
...07b OR   EBP,EDI
...07d XOR  EBP,ESI
...07f ADD  EBP,dword ptr [ESP + loca...
...083 MOV  dword ptr [ESP + local_70 ...
...087 MOV  ESI,dword ptr [ESP + loca...
...08b LEA  ESI,[0x6ed9eba1  + ESI + E...
...092 ROL  ESI,0xe
...095 ADD  ESI,dword ptr [ESP + loca...
...099 MOV  EBP,EDI
...09b NOT  EBP
...09d OR   EBP,ESI
...09f ROL  EBX,0xa
...0a2 XOR  EBP,EBX
...0a4 ADD  EBP,ECX
...0a6 MOV  dword ptr [ESP + local_6c ...
...0aa MOV  EBX,dword ptr [ESP + loca...
...0ae LEA  EBX,[0x6ed9eba1  + EBX + E...
...0b5 ROL  EBX,0x9
...0b8 ADD  EBX,dword ptr [ESP + loca...
...0bc ROL  EDI,0xa
...0bf MOV  EBP,ESI
...0c1 NOT  EBP
...0c3 OR   EBP,EBX
...0c5 XOR  EBP,EDI
...0c7 ADD  EBP,dword ptr [ESP + loca...
...0cb MOV  dword ptr [ESP + local_74 ...
...0cf MOV  EDI,dword ptr [ESP + loca...
...0d3 LEA  EDI,[0x6ed9eba1  + EDI + E...
...0da ROL  EDI,0xd
...0dd ADD  EDI,dword ptr [ESP + loca...
...0e1 ROL  ESI,0xa
...0e4 MOV  dword ptr [ESP + local_68 ...
...0e8 MOV  EBP,EBX
...0ea NOT  EBP
```

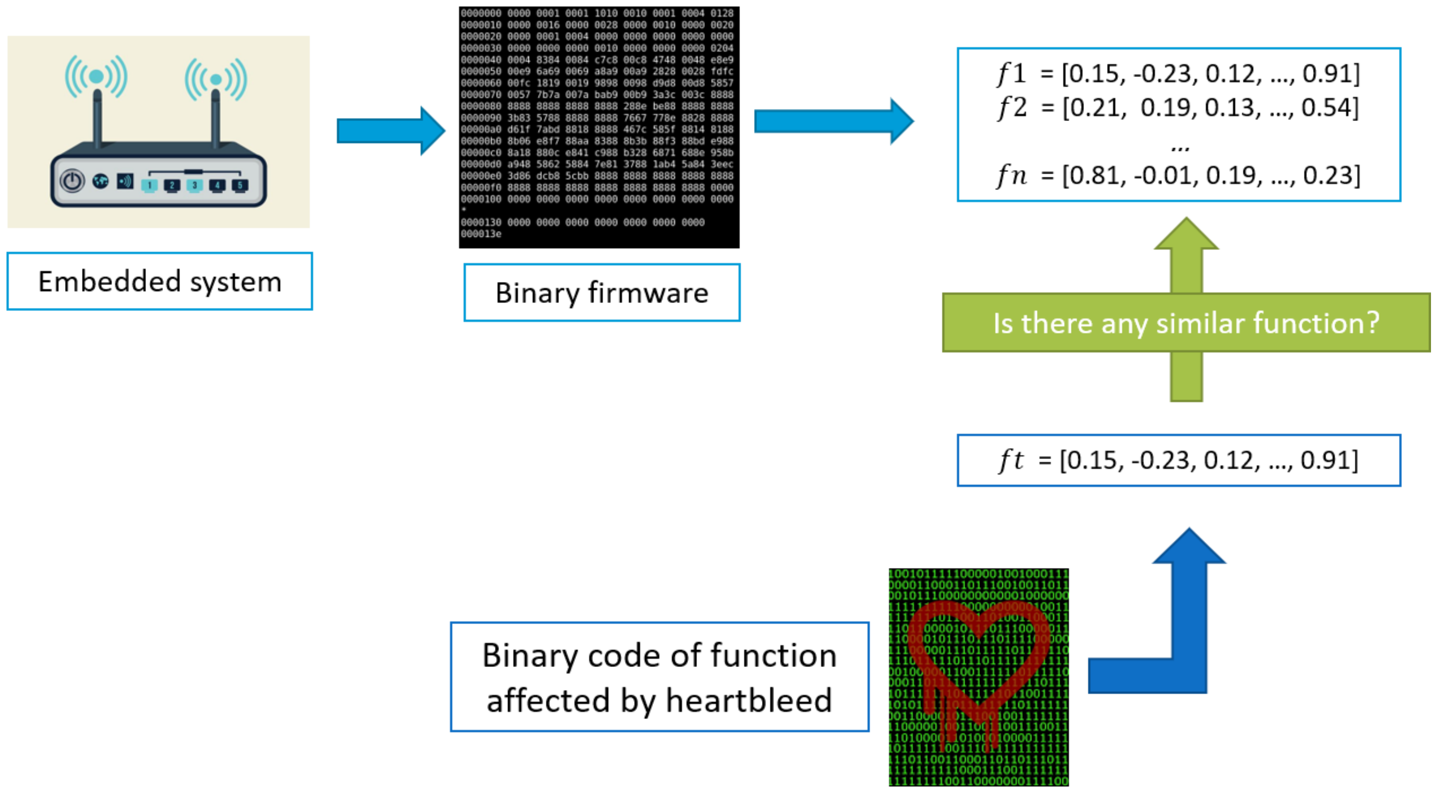


```
uVar19 = uVar25 + 0x5a827999 + ((uVar18   uVar23) & uVar24   uVar18) + iVar8;
uVar20 = (uVar19 * 0x2000 | uVar19 >> 0x13) + uVar22;
uVar25 = uVar23 * 0x400 | uVar23 >> 0x16;
uVar19 = uVar22 + 0x5a827999 + ((uVar25 ^ uVar24) & uVar20 ^ uVar25) + iVar6;
uVar23 = (uVar19 * 0x1000 | uVar19 >> 0x14) + uVar18;
uVar22 = uVar24 * 0x400 | uVar24 >> 0x16;
uVar19 = uVar18 + 0x6ed9eba1 + ((~uVar20 | uVar23) ^ uVar22) + iVar11;
uVar24 = (uVar19 * 0x800 | uVar19 >> 0x15) + uVar25;
uVar18 = uVar20 * 0x400 | uVar20 >> 0x16;
uVar19 = uVar25 + 0x6ed9eba1 + ((~uVar23 | uVar24) ^ uVar18) + iVar13;
uVar20 = (uVar19 * 0x2000 | uVar19 >> 0x13) + uVar22;
uVar25 = uVar23 * 0x400 | uVar23 >> 0x16;
```

SHA1 Constant

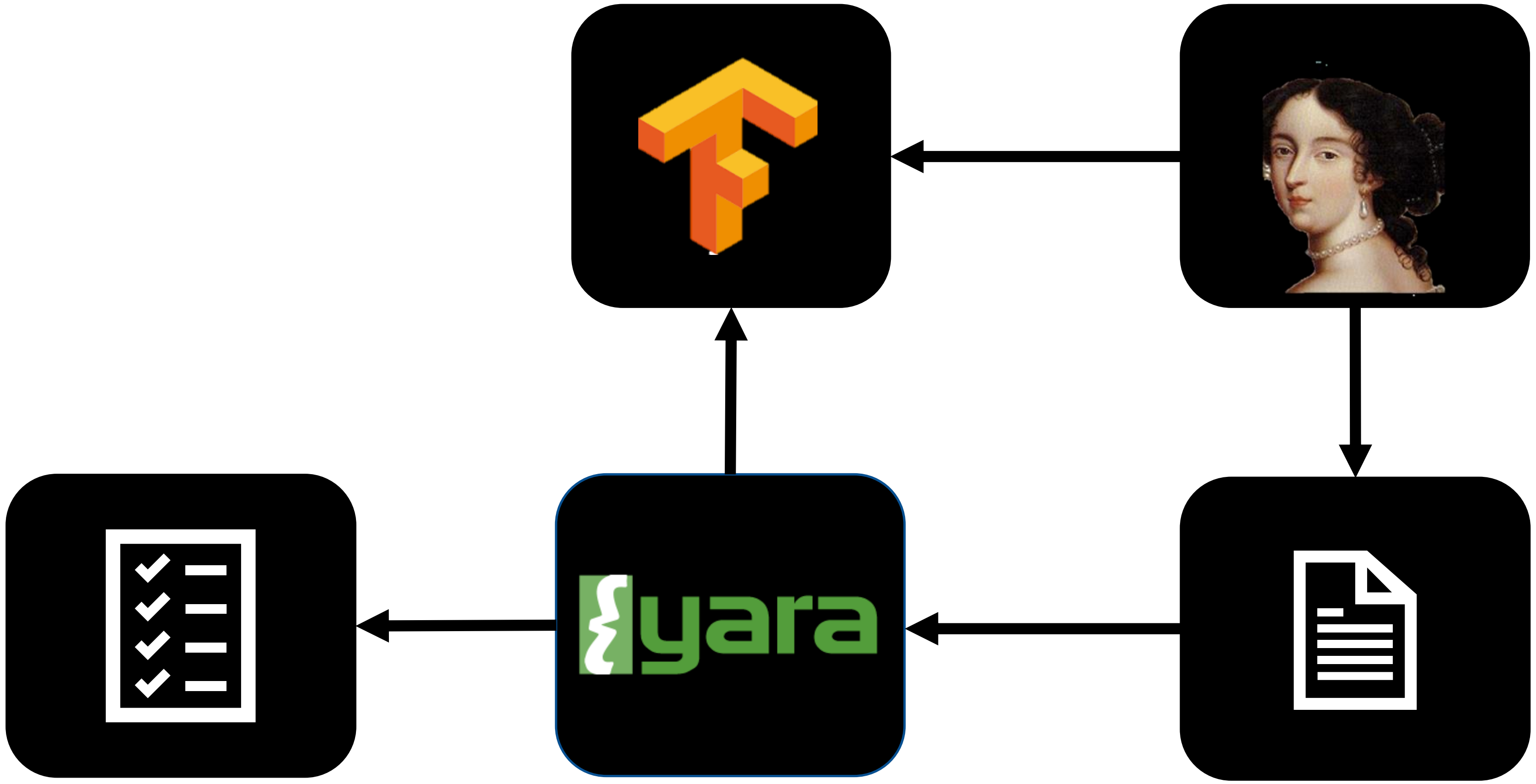


Possible improvent: Detecting Suspicious functionality inside a firmware


Embedded system
Binary firmware
$f1$ = [0.15, -0.23, 0.12, ..., 0.91]
$f2$ = [0.21, 0.19, 0.13, ..., 0.54]
...
fn = [0.81, -0.01, 0.19, ..., 0.23]
Is there any similar function?
ft = [0.15, -0.23, 0.12, ..., 0.91]
Binary code of function affected by heartbleed

- We develop a tool: YARASAFE, to simplify this process!

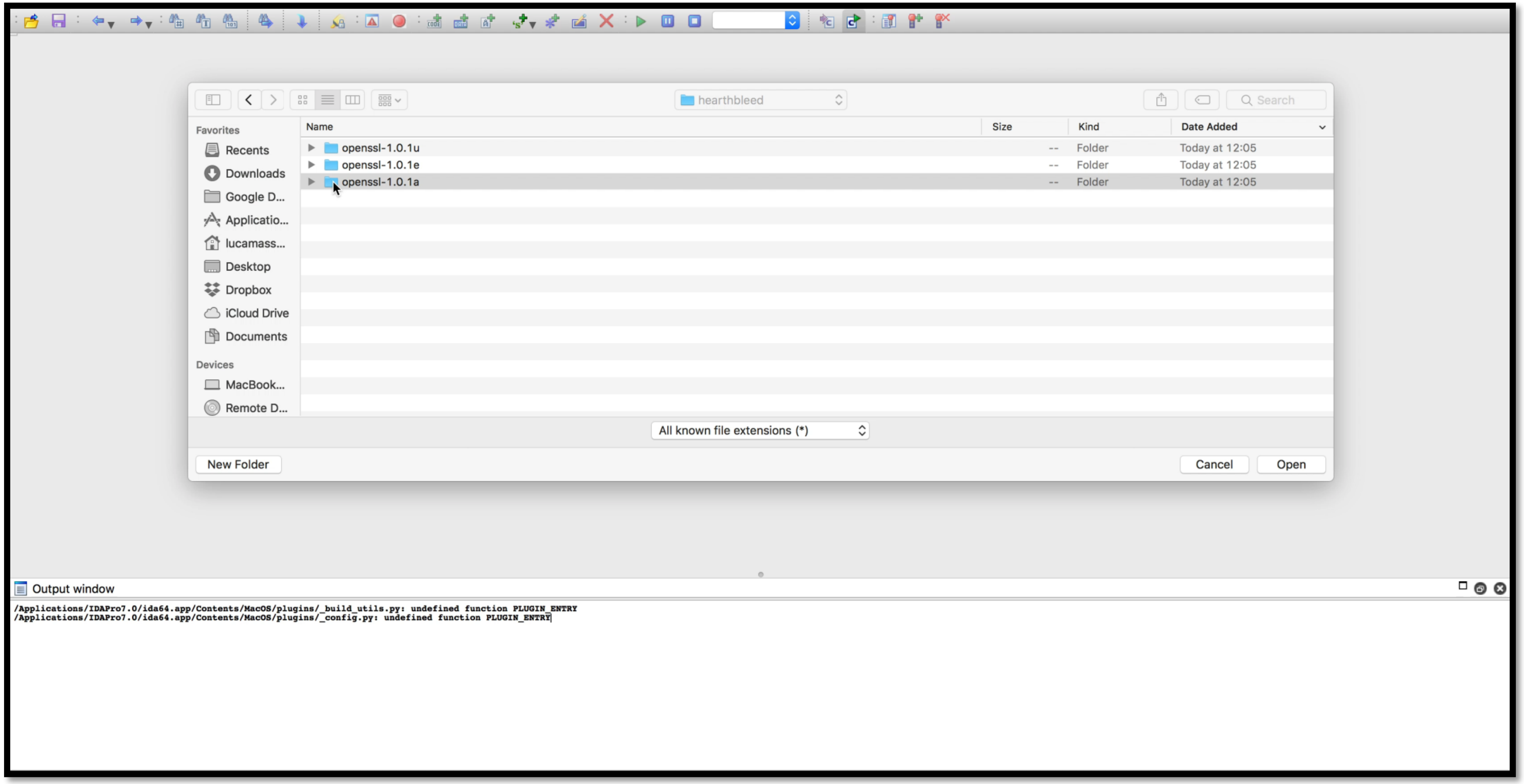
Spotting Vulnerability in COTS software



YARA-SAFE

```
import "safe"

rule Heartbleed
{
    condition:
         safe.similarity("[0.094,  …. , 0.0597]") > 0.97
}
```

YARA-SAFE Rule



Name	Size	Kind	Date Added
openssl-1.0.1u	--	Folder	Today at 12:05
openssl-1.0.1e	--	Folder	Today at 12:05
openssl-1.0.1a	--	Folder	Today at 12:05

```
/Applications/IDAPro7.0/ida64.app/Contents/MacOS/plugins/_build_utils.py: undefined function PLUGIN_ENTRY
/Applications/IDAPro7.0/ida64.app/Contents/MacOS/plugins/_config.py: undefined function PLUGIN_ENTRY
```

Rule - Creation

DEMO!!

Github

Paper