Attack and Defense in the Cyber-Physical World

Ning Zhang

https://cybersecurity.seas.wustl.edu

Why should you care? It doesn't speed up your PC for sure!

Tremendous societal impacts of cybersecurity around the globe

"WannaCry" ransomware attack losses could reach $4 billion

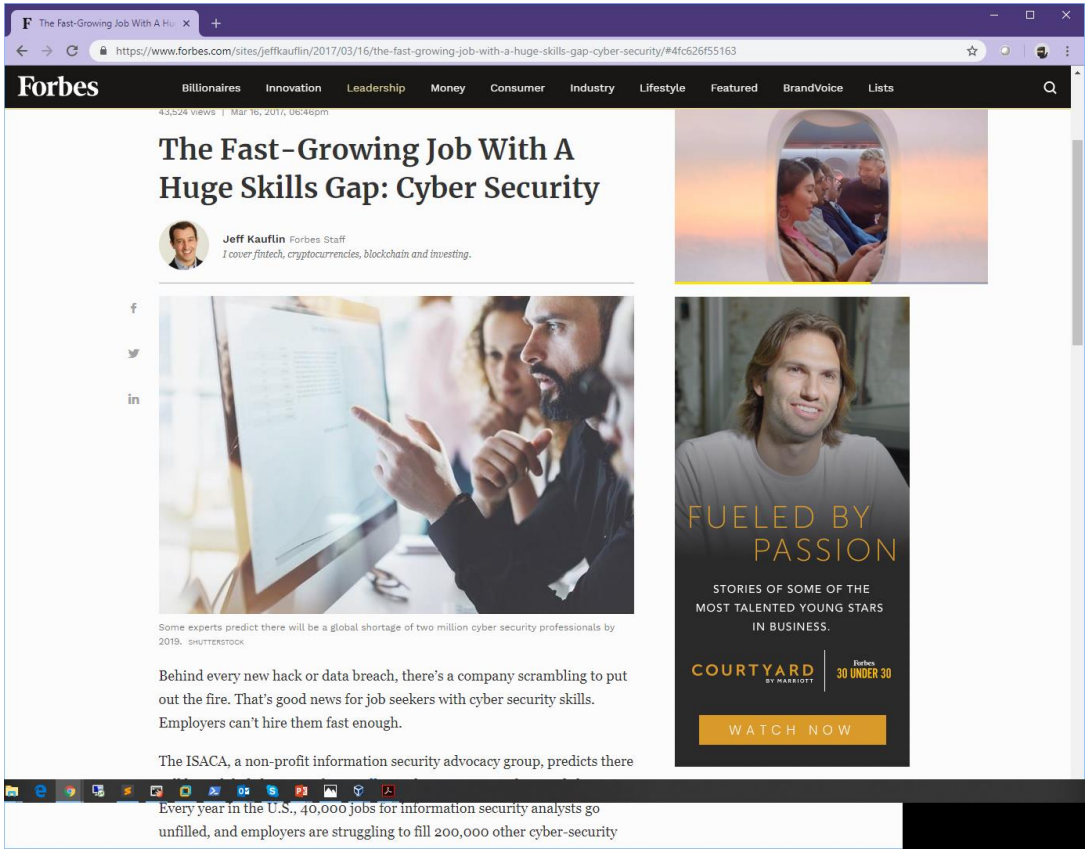
HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Russian Hacking and Influence in the U.S. Election

Complete coverage of Russia's campaign to disrupt the 2016 presidential election.

https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
https://www.nytimes.com/news-event/russian-election-hacking

There is a demand for people in this field



What is cyber security to you?

What do you think we do?

Security is a method of analyzing system

Is this piece of code secure ?

```
bool authenticate(const char * password)
{
        if(strncmp(password, “hello”, strlen(“hello”)==0)
                return true;
        else
                return false;
}
```

Security and Privacy (my best effort categorization)

Computer Security 101

Achieve some ***goal*** against some ***adversary***

System Goal / Security Service / Policy

Threat models

Mechanism

Common goals include:

Confidentiality – nobody can see my stuff except myself

Integrity – nobody can malicious modify my stuff

Availability – I should have access to my things when I need to

Today's discussion

Three of my on-going research

- Software Security
- Confidential Computing
- Architecture Security

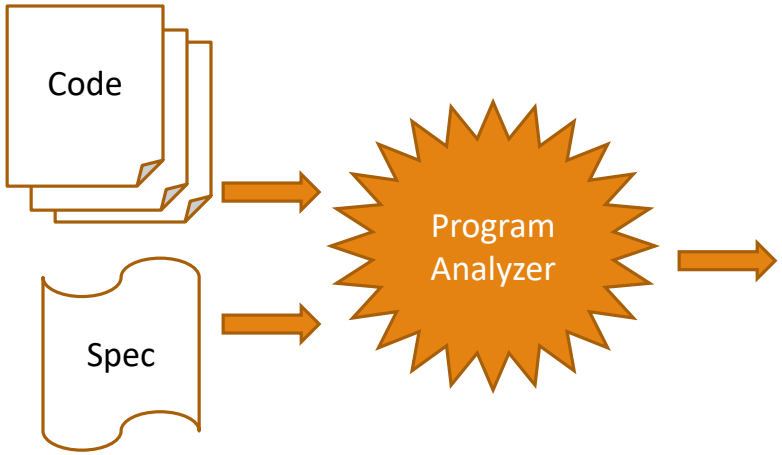
Software Security

Cyber Security

Capture the flag

How do we automatically find vulnerabilities?

Program Analyzers



Report	Type	Line
1	mem leak	324
2	buffer oflow	4,353,245
3	sql injection	23,212
4	stack oflow	86,923
5	dang ptr	8,491
…	…	…
10,502	info leak	10,921

Slide credit: John Mitchell

Two options

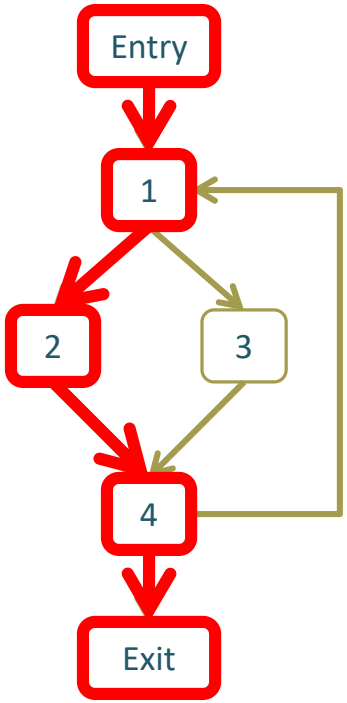
Static analysis

- Automated methods to find errors or check their absence
  - Consider all possible inputs (in summary form)
  - Find bugs and vulnerabilities
  - Can prove absence of bugs, in some cases

Dynamic analysis

- Run instrumented code to find problems
  - Need to choose sample test input
  - Can find vulnerabilities but cannot prove their absence

Slide credit: John Mitchell



Software

1 → 2 → 4

1 → 3 → 4

1 → 2 → 4 → 1 → 2 → 4

1 → 2 → 4 → 1 → 3 → 4

1 → 2 → 3 → 1 → 2 → 4 → 1 → 3 → 4

1 → 2 → 4 → 1 → 2 → 3 → 1 → 3 → 4

1 → 2 → 3 → 1 → 2 → 3 → 1 → 3 → 4

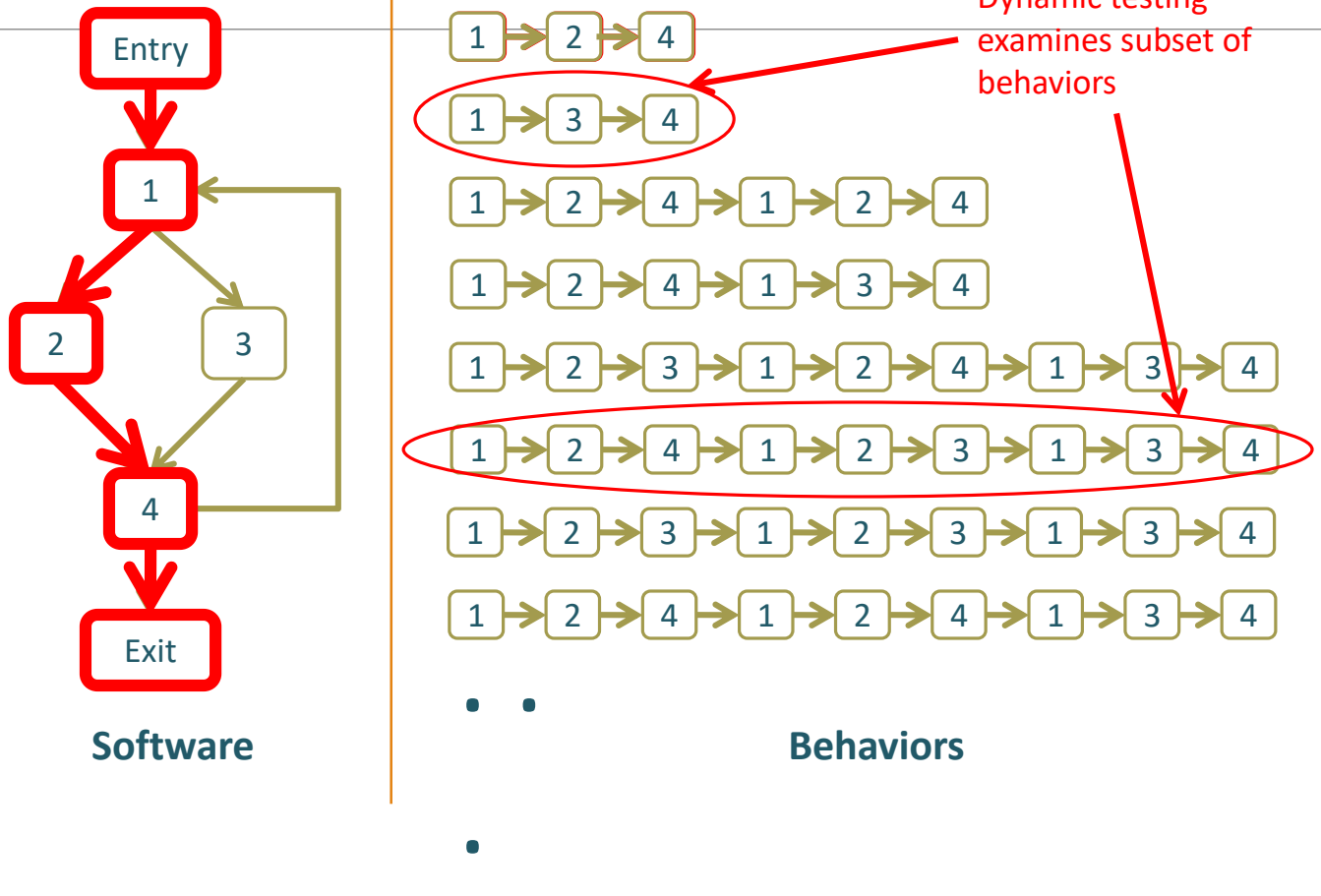
1 → 2 → 4 → 1 → 2 → 4 → 1 → 3 → 4

• •

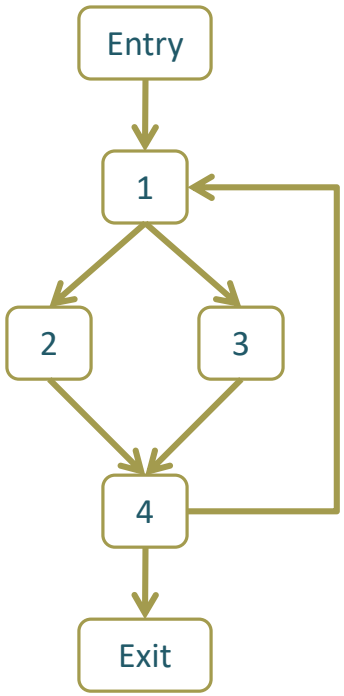
•

Behaviors

Slide credit: John Mitchell



Slide credit: John Mitchell



Software

Static testing uses abstraction to consider all behaviors

1 → 2 → 4

1 → 3 → 4

1 → 2 → 4 → 1 → 2 → 4

1 → 2 → 4 → 1 → 3 → 4

1 → 2 → 3 → 1 → 2 → 4 → 1 → 3 → 4

1 → 2 → 4 → 1 → 2 → 3 → 1 → 3 → 4

1 → 2 → 3 → 1 → 2 → 3 → 1 → 3 → 4

1 → 2 → 4 → 1 → 2 → 4 → 1 → 3 → 4

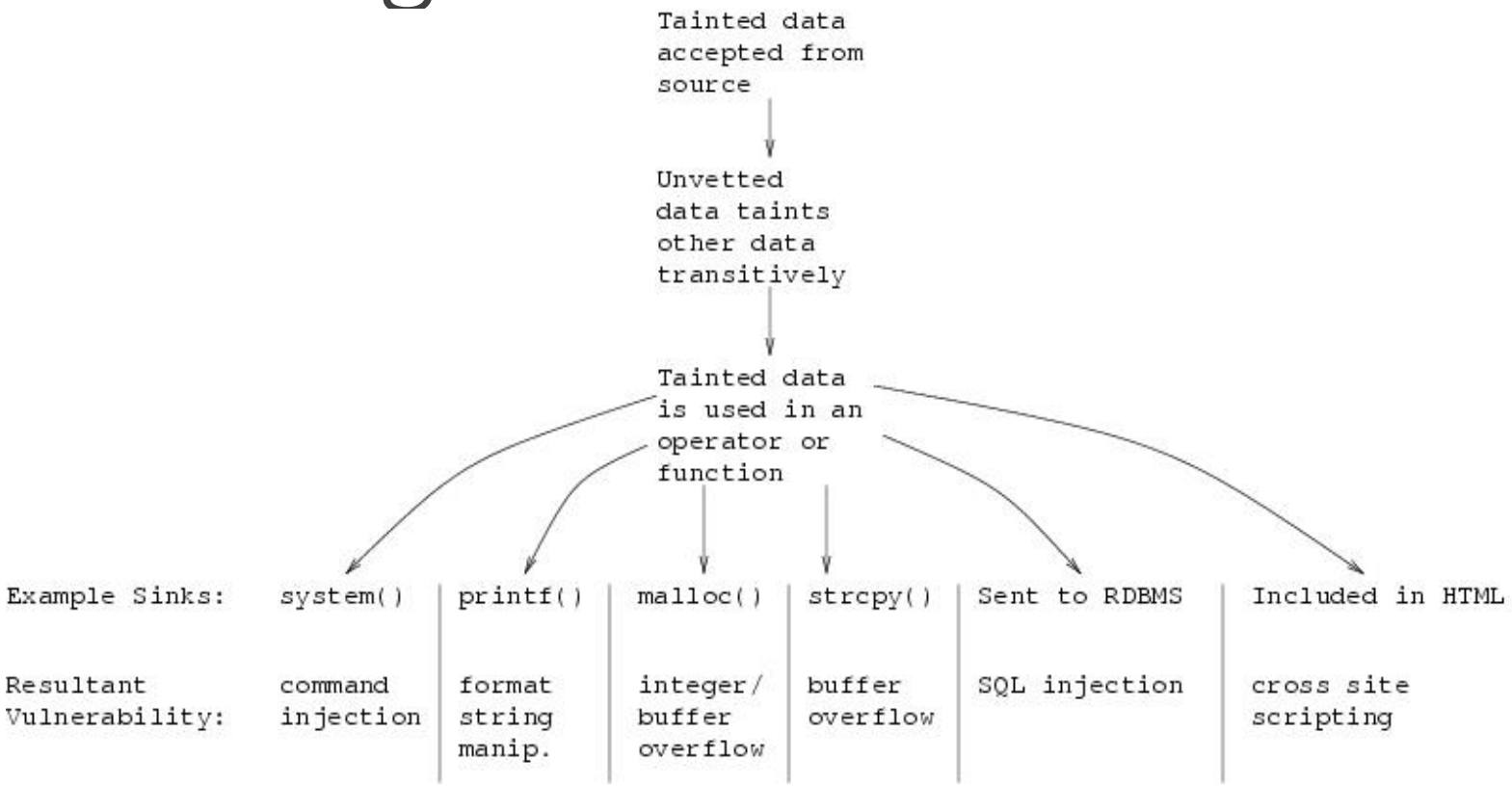
. .

Behaviors

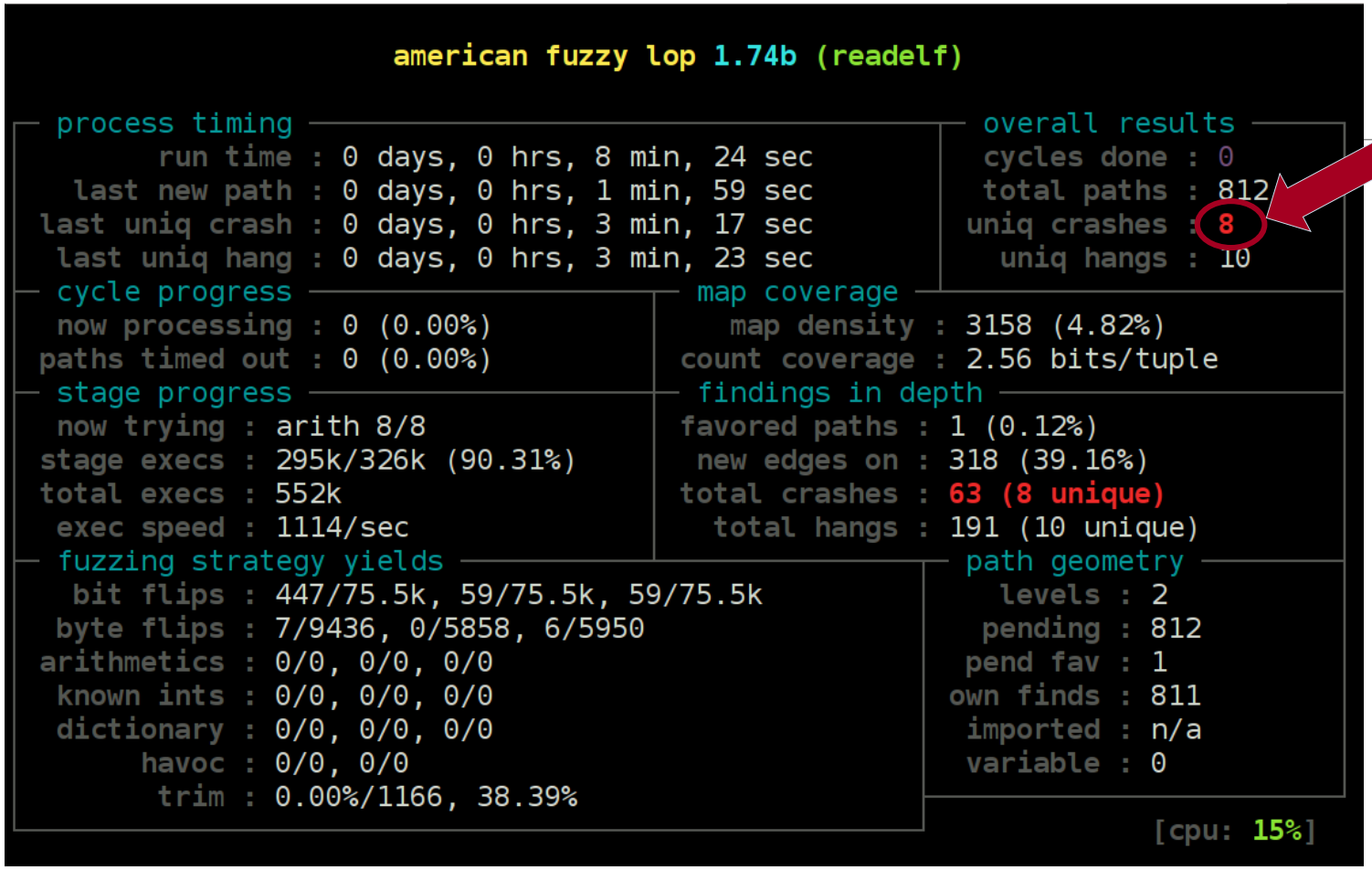
Slide credit: John Mitchell

.

Tainting checkers



Slide credit: John Mitchell



Slide credit: John Mitchell

Bugs to Detect

- Crash Causing Defects
- Null pointer dereference
- Use after free
- Double free
- Array indexing errors
- Mismatched array new/delete
- Potential stack overrun
- Potential heap overrun
- Return pointers to local variables
- Logically inconsistent code
- Uninitialized variables
- Invalid use of negative values
- Passing large parameters by value
- Underallocations of dynamic data
- Memory leaks
- File handle leaks
- Network resource leaks
- Unused values
- Unhandled return codes
- Use of invalid iterators

Slide credit: Andy Chou

Confidential Computing Data Privacy

Internet of Things with Intelligence

Imgsrc:readitquik.com

Data Privacy

Who can access my data?

Access Control (System or Cryptographically)

How can they use my data?

User Agreement

Google

google_privacy_policy_en.pdf 1 / 27

GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.

Effective May 25, 2018

Archived versions

Medical data privacy

Widespread availability of data

We are at the dawn of the age of data (Misused?)

TIME

SUBSCRIBE

U.S. • FACEBOOK

Facebook Is Telling People Their Data Was Misused by Cambridge Analytica and They're Furious

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia

Facebook–Cambridge Analytica data scandal

From Wikipedia, the free encyclopedia

The **Facebook–Cambridge Analytica data scandal** involves the collection of personally identifiable information of 87 million Facebook users[1] and reportedly a much greater number more[2] that Cambridge Analytica began collecting in 2014. The data was allegedly used to attempt to influence voter opinion on behalf of politicians who hired them. Following the discovery, Facebook apologized amid public outcry and risen stock prices. The way that Cambridge Analytica collected the data was called "inappropriate".[3]

An ideal world for data privacy

Confidentiality Protection of User Data

- Data shall always be encrypted with user controlled keys

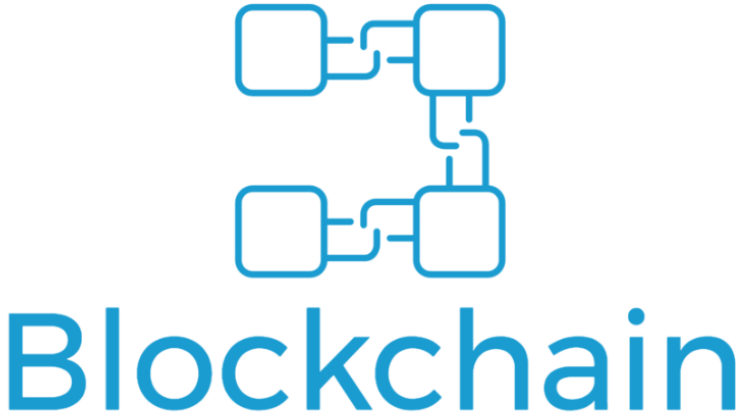
Verifiable user-controlled fine-grained utilization of data

- Access control: User can add terms and conditions as *who* can access *what data* for *which purpose* during *what time* under *what condition*
- Usage enforcement: Data can only be used for approved purposes

Non-repudiable recording of data use

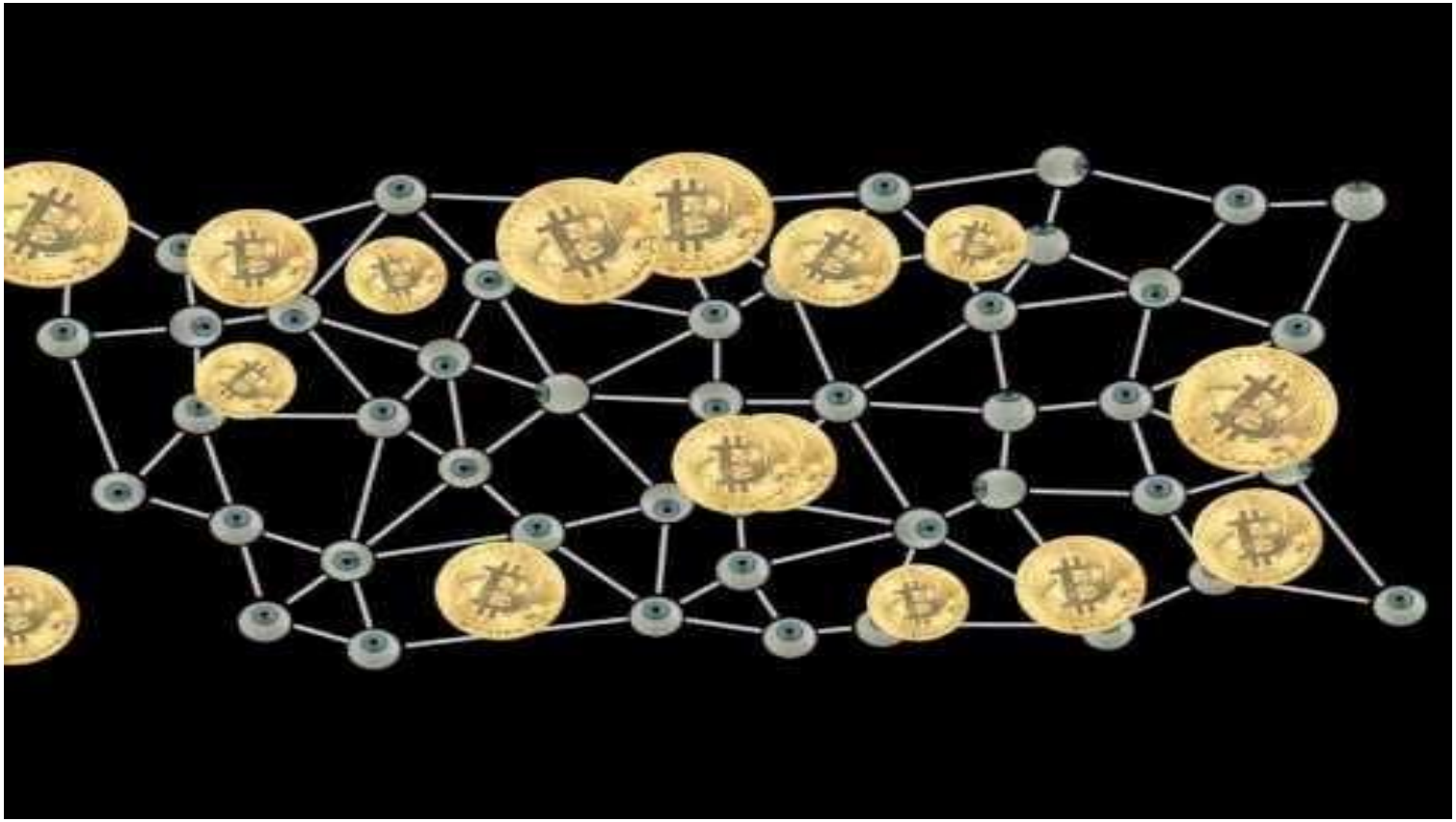
- When data is used, there will be *irreversible proof* of *how* it was used by *whom*

Trustworthy Non-repudiable recording ?



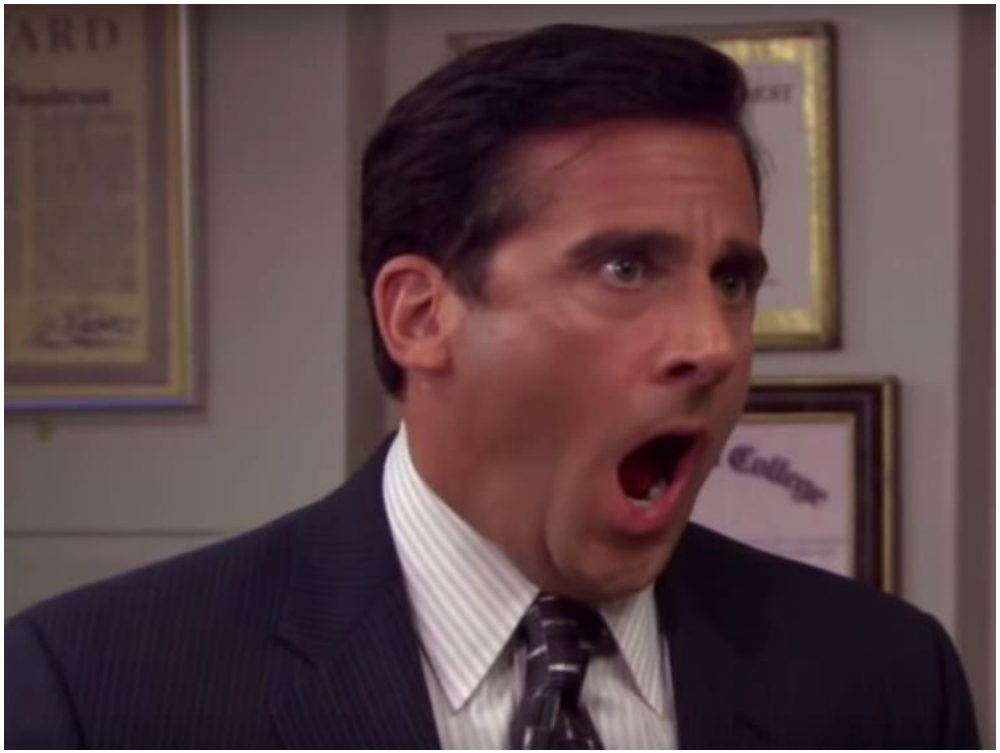
Imgsrc:www.kinesense-vca.com

What is blockchain ?

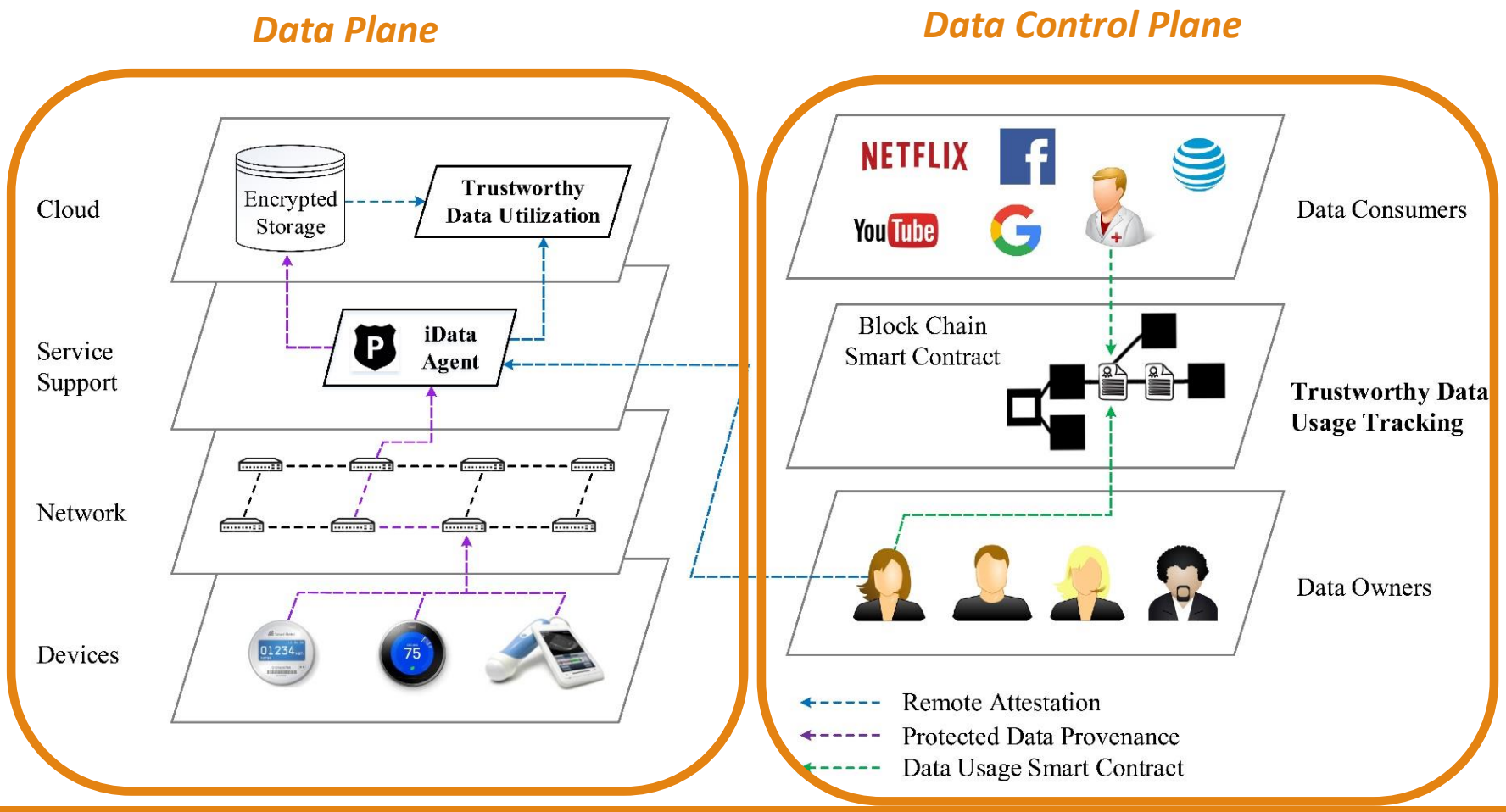


We are done ?

Unfortunately, it is never that easy!

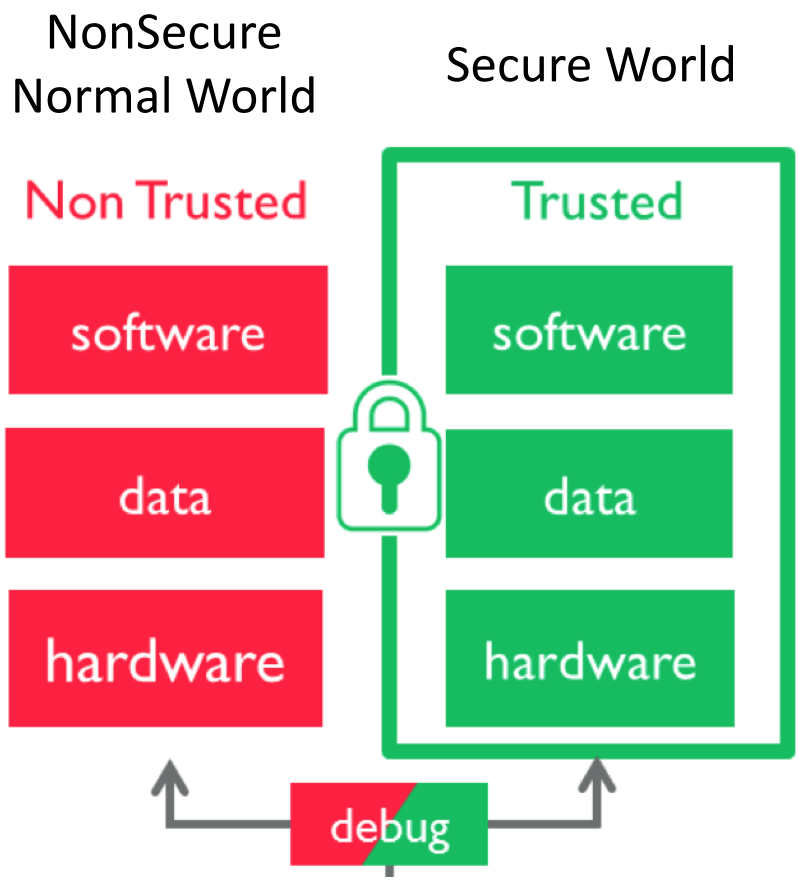


PrivacyGuard Framework



Architecture Security

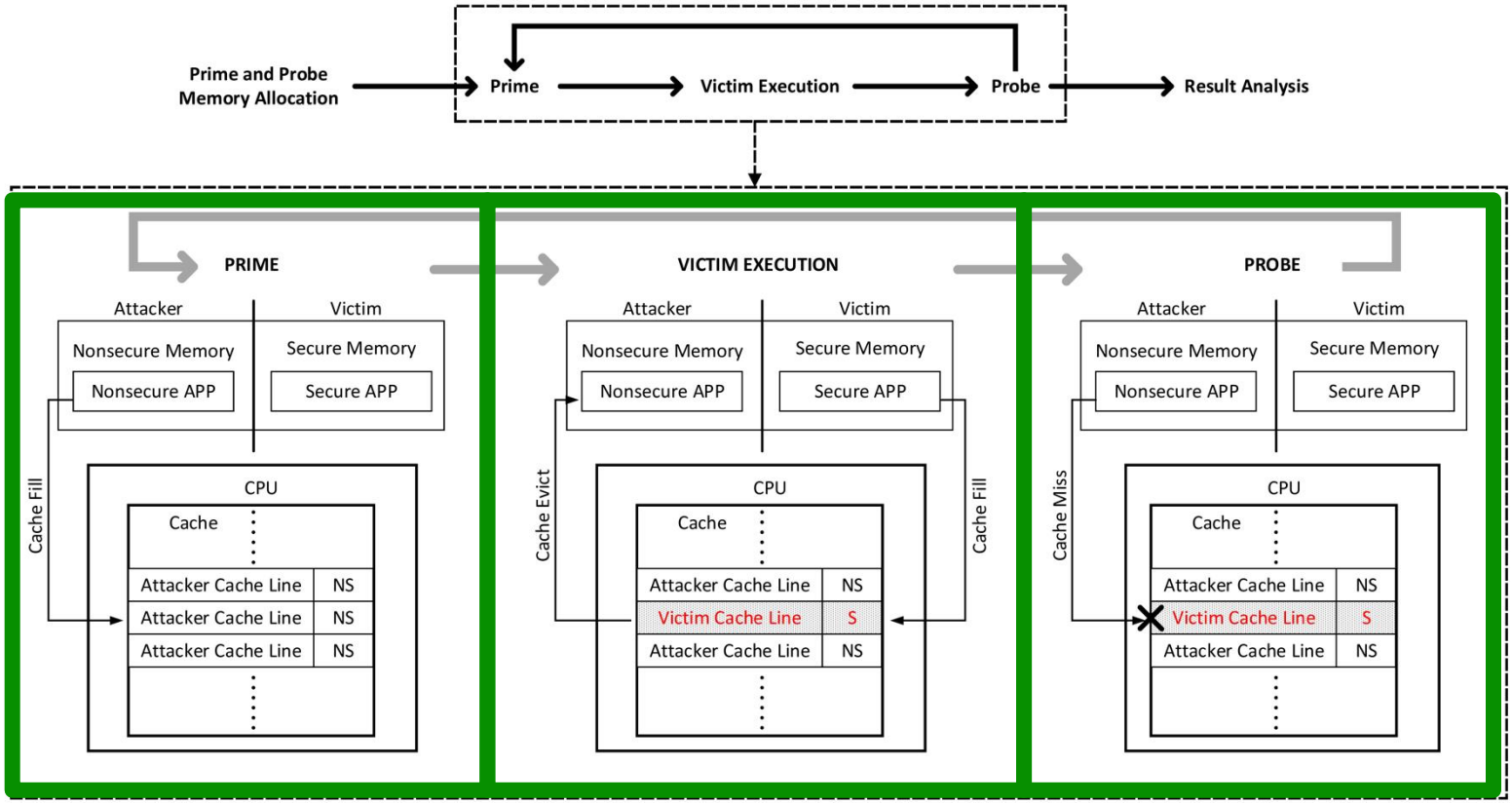
ARM TrustZone – resources are divided into two worlds



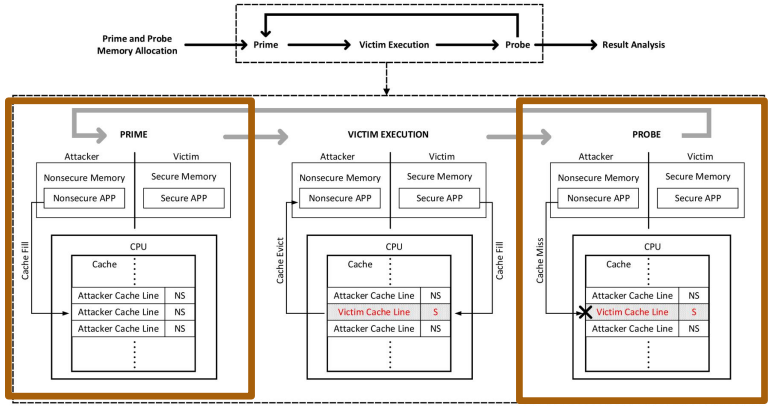
More than processor extension, TrustZone is system-wide security extension.

NonSecure(NS) bit is added to resource and bus

Attack overview – prime and probe



Two challenges



Prime - Triggering the cache contention

– Allocation of attack memory that will map the same cache sets of the victim process inside TrustZone.

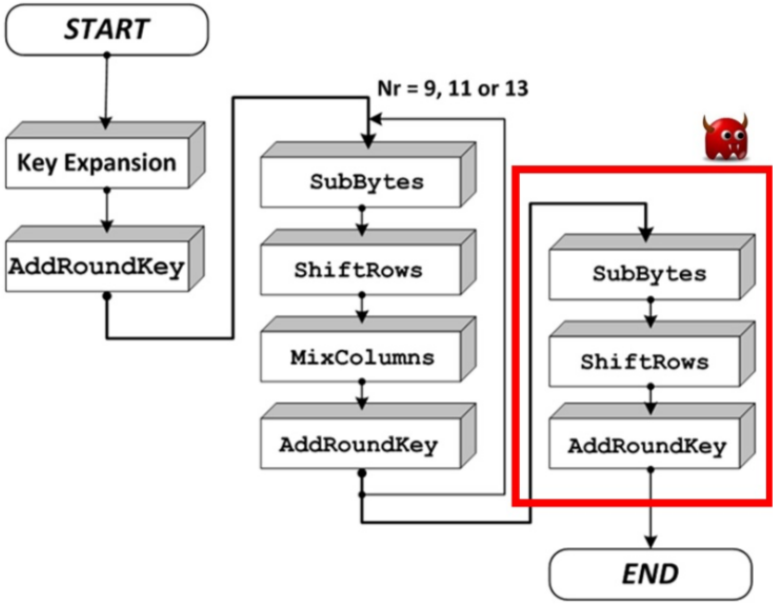
- Lack of virtual-to-physical address mapping

Probe - Detection of the cache contention

– Detect changes in the cache state as a result of the resource contention.

- Lack of high accuracy timer
- Lack of ability for fine grained cache manipulation

The magic of cache access to leakage of cryptographic keys



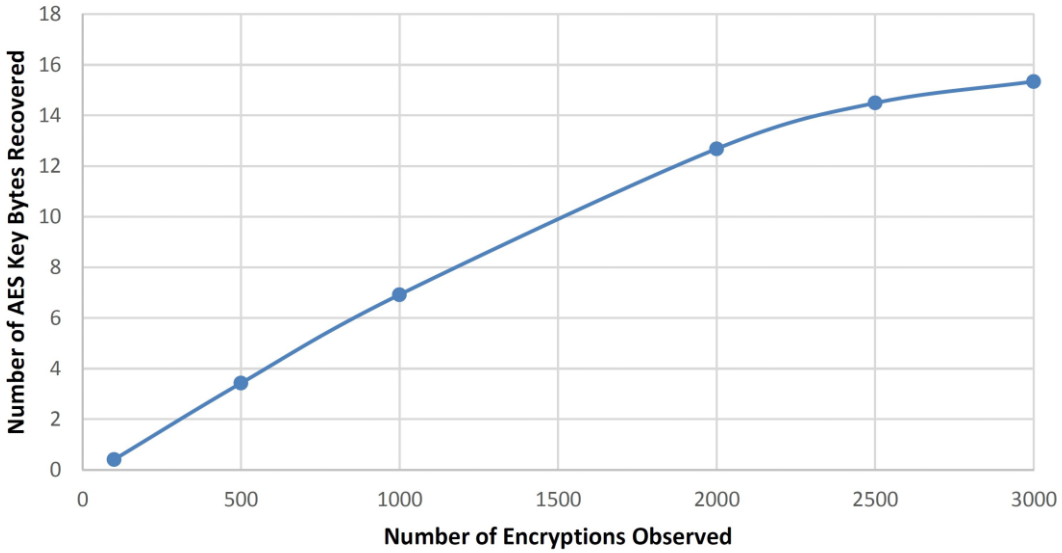
To speed up GF operations, precomputed tables are used instead, T_0 to T_4, 4KB size

$$C[j] = T_l[X_{i_{max}}] \otimes K_{i_{max}}[j]$$

$$X_i + 1 \begin{cases} X_i \otimes K_i & i = 0 \\ MC(SR(SB(X_i))) \otimes K_i & 0 < i < i_{max} \\ SR(SB(X_i))) \otimes K_i & i_{max} \end{cases}$$

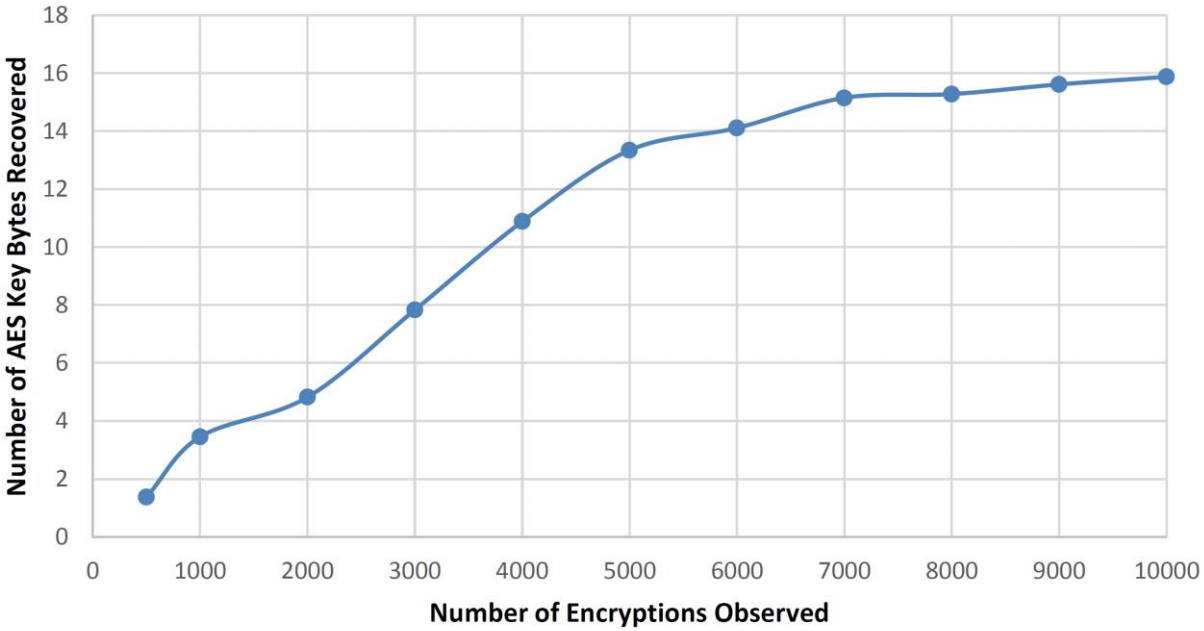
Key extraction from the normal world OS

Completes key extraction in 2.5 seconds

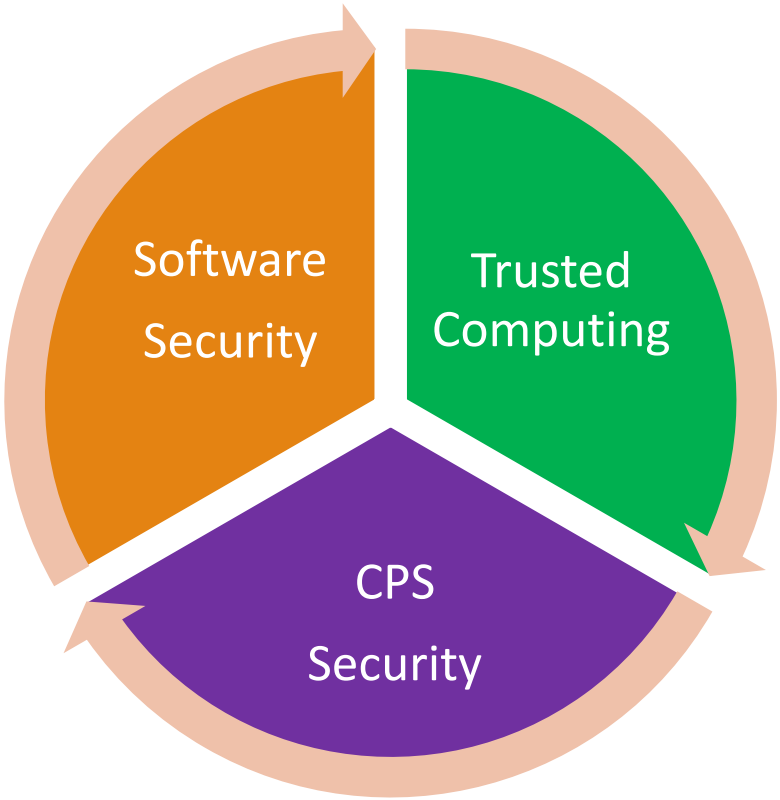


Key extraction from the normal world unprivileged app

Completes key extraction in 15 mins



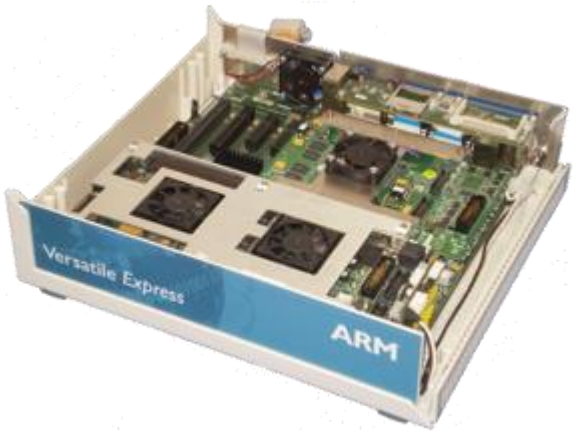
Broad Direction



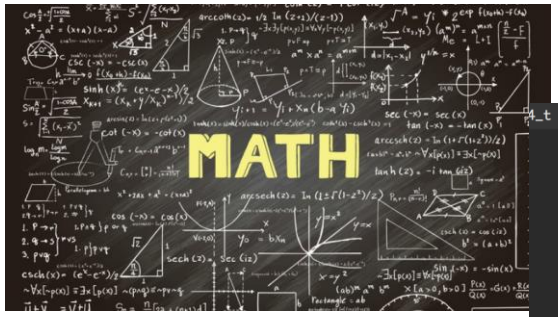
New Attacks that interleave the cyber and physical world

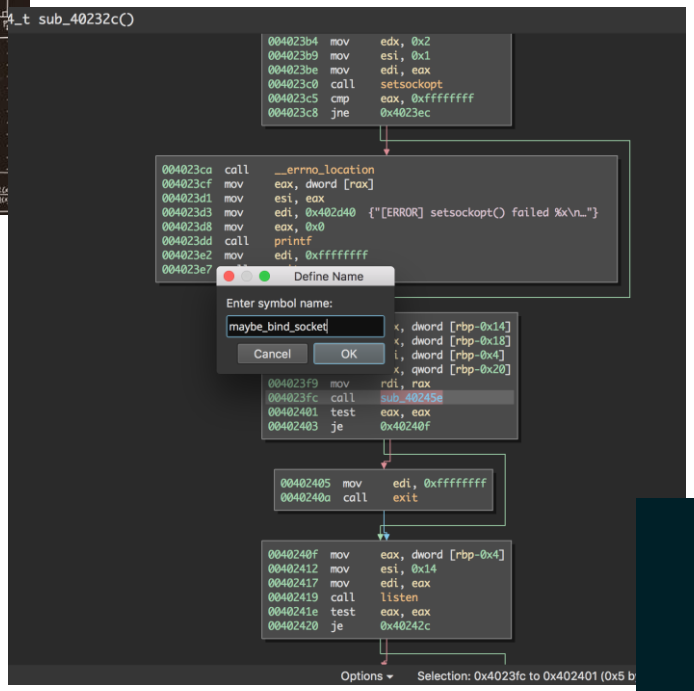
What can you expect when you get out of my lab ?

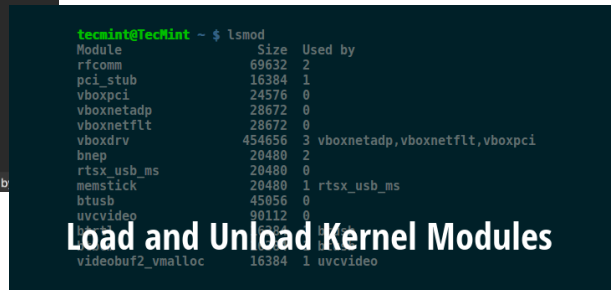
But what your life would be like while in my lab - problems



You will …


MATH


sub_40232c()
004023b4 mov edx, 0x2
004023b9 mov esi, 0x1
004023be mov edi, eax
004023c0 call setsockopt
004023c5 cmp eax, 0xffffffff
004023c8 jne 0x4023ec
004023ca call __errno_location
004023cf mov eax, dword [rax]
004023d1 mov esi, eax
004023d3 mov edi, 0x402d40 {"[ERROR] setsockopt() failed %x\n…"}
004023d8 mov eax, 0x0
004023dd call printf
004023e2 mov edi, 0xffffffff
Define Name
Enter symbol name:
maybe_bind_socket
Cancel
OK
004023f9 mov rdi, rax
004023fc call sub_40245e
00402401 test eax, eax
00402403 je 0x40240f
00402405 mov edi, 0xffffffff
0040240a call exit
0040240f mov eax, dword [rbp-0x4]
00402412 mov esi, 0x14
00402417 mov edi, eax
00402419 call listen
0040241e test eax, eax
00402420 je 0x40242c
Options
Selection: 0x4023fc to 0x402401 (0x5 b


tecmint@TecMint ~ $ lsmod
Module Size Used by
rfcomm 69632 2
pci_stub 16384 1
vboxpci 24576 0
vboxnetadp 28672 0
vboxnetflt 28672 0
vboxdrv 454656 3 vboxnetadp,vboxnetflt,vboxpci
bnep 20480 2
rtsx_usb_ms 20480 0
memstick 20480 1 rtsx_usb_ms
btusb 45056 0
uvcvideo 90112 0
videobuf2_vmalloc 16384 1 uvcvideo
Load and Unload Kernel Modules

What your life would be like while in my lab – Solution space

Sys Sec	Sw Sec	CPS Sec
• Applied cryptography • Operating system • Assembly language • Computer organization and architecture	• Program analysis • Static analysis • Dynamic analysis • Virtualization • Fuzzing • Symbolic execution • Compiler module	• Real-time system • Embedded System • Analog system • Digital Communication • Wireless Communication • Physics • Chemistry • Biology