

Exploiting and Defense

Dobin Rutishauser
December 2016

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Intro - Technical

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

What is a picture?





What is a picture? In an hex editor



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ÿà..JFIF.....
00000010	00	01	00	00	FF	DB	00	84	00	05	03	04	09	09	09	08ÿÛ.....
00000020	08	08	08	06	08	08	08	06	07	07	07	08	07	07	07	07
00000030	07	07	07	07	07	07	07	07	07	07	07	07	0A	10	0B	07
00000040	08	0E	09	07	07	0C	15	0C	0E	11	11	13	13	13	07	0B
00000050	16	18	16	12	18	10	12	13	12	01	05	05	05	08	07	08
00000060	0C	07	07	0C	12	08	07	08	12	12	12	12	12	12	12	12
00000070	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
00000080	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
00000090	12	12	12	1E	12	12	12	1E	12	12	FF	C0	00	11	08	04ÿÀ....
000000A0	B0	06	40	03	01	22	00	02	11	01	03	11	01	FF	C4	00	°.@.."......ÿÄ.
000000B0	1D	00	00	02	03	01	01	01	01	01	00	00	00	00	00	00
000000C0	00	00	02	03	00	01	04	05	06	07	08	09	FF	C4	00	43ÿÄ.C
000000D0	10	00	02	02	01	03	02	05	03	03	03	03	03	03	02	02
000000E0	0B	01	02	00	03	11	04	12	21	05	31	06	13	22	32	41!.1.."2A
000000F0	42	51	52	07	14	62	23	61	72	15	33	82	43	71	92	16	BQR..b#ar.3,Cq'.
00000100	24	53	08	81	A2	34	B2	C2	44	63	91	17	25	73	83	E2	\$S..c4*ÂDc'.%sfâ
00000110	54	FF	C4	00	1B	01	00	03	01	01	01	01	01	00	00	00	TÿÄ.....
00000120	00	00	00	00	00	00	00	01	02	03	04	05	06	07	FF	C4ÿÄ
00000130	00	29	11	01	01	00	02	02	03	01	00	02	03	01	01	00	.).....
00000140	02	03	00	00	01	02	11	03	12	13	21	31	04	14	41	05!.1..A.
00000150	22	51	61	32	71	91	06	52	62	FF	DA	00	0C	03	01	00	"Qa2q`.RbÿÛ.....
00000160	02	11	03	11	00	3F	00	FC	73	17	19	17	05	24	9F	12?.üs....\$ÿ.
00000170	49	F1	00	A9	72	A5	FC	40	AA	49	24	90	24	92	49	20	Iñ.@rÿü@*I\$. \$'I
00000180	12	49	24	80	4F	89	52	FE	25	40	21	92	43	24	02	47	.I\$€O%Rp%@!'C\$.G

JFIF file structure		
Segment	Code	Description
SOI	FF D8	Start of Image
JFIF-APP0	FF E0 s1 s2 4A 46 49 46 00 ...	see below
JFXX-APP0	FF E0 s1 s2 4	
... additional marker segments (for example SOF, DHT, COM)		
SOS	FF DA	
	compressed image	
EOI	FF D9	

JFIF APP0 marker segment [\[edit\]](#)

In the mandatory JFIF APP0 marker segment the parameters of the image are specified. Optionally an uncompressed

JFIF APP0 marker segment		
Field	Size (bytes)	Description
APP0 marker	2	FF E0
Length	2	Length of segment excluding APP0 marker
Identifier	5	4A 46 49 46 00 = "JFIF" in ASCII, terminated by a null byte
JFIF version	2	First byte for major version, second byte for minor version (01 02 for 1.02)
Density units	1	Units for the following pixel density fields <ul style="list-style-type: none"> 00 : No units; width:height pixel aspect ratio = Xdensity:Ydensity 01 : Pixels per inch (2.54 cm) 02 : Pixels per centimeter
Xdensity	2	Horizontal pixel density. Must not be zero.
Ydensity	2	Vertical pixel density. Must not be zero.
Xthumbnail	1	Horizontal pixel count of the following embedded RGB thumbnail. May be zero.
Ythumbnail	1	Vertical pixel count of the following embedded RGB thumbnail. May be zero.



```

maxresdefault.jpg - JPEGsnoop
File Edit View Tools Options Help
[Icons]
Filesize: [136356] Bytes

Start Offset: 0x00000000
*** Marker: SOI (xFFD8) ***
  OFFSET: 0x00000000

*** Marker: APP0 (xFFE0) ***
  OFFSET: 0x00000002
  Length      = 16
  Identifier   = [JFIF]
  version     = [1.1]
  density     = 1 x 1 (aspect ratio)
  thumbnail   = 0 x 0

*** Marker: DQT (xFFDB) ***
  Define a Quantization Table.
  OFFSET: 0x00000014
  Table length = 132
  ----
  Precision=8 bits
  Destination ID=0 (Luminance)
  DQT, Row #0:  5   3   9   8   6   7   7   7
  DQT, Row #1:  4   9   8   8   7   7   7   7
  DQT, Row #2:  9   8   8   7   7   7   9   7
  DQT, Row #3:  8   8   8   7   7  14  12   7
  DQT, Row #4:  6   7   7   7   8  21  19  11
  DQT, Row #5:  7   7   7   7  12  19  22  16
  DQT, Row #6:  7   7  11  14  19  24  24  18
  
```

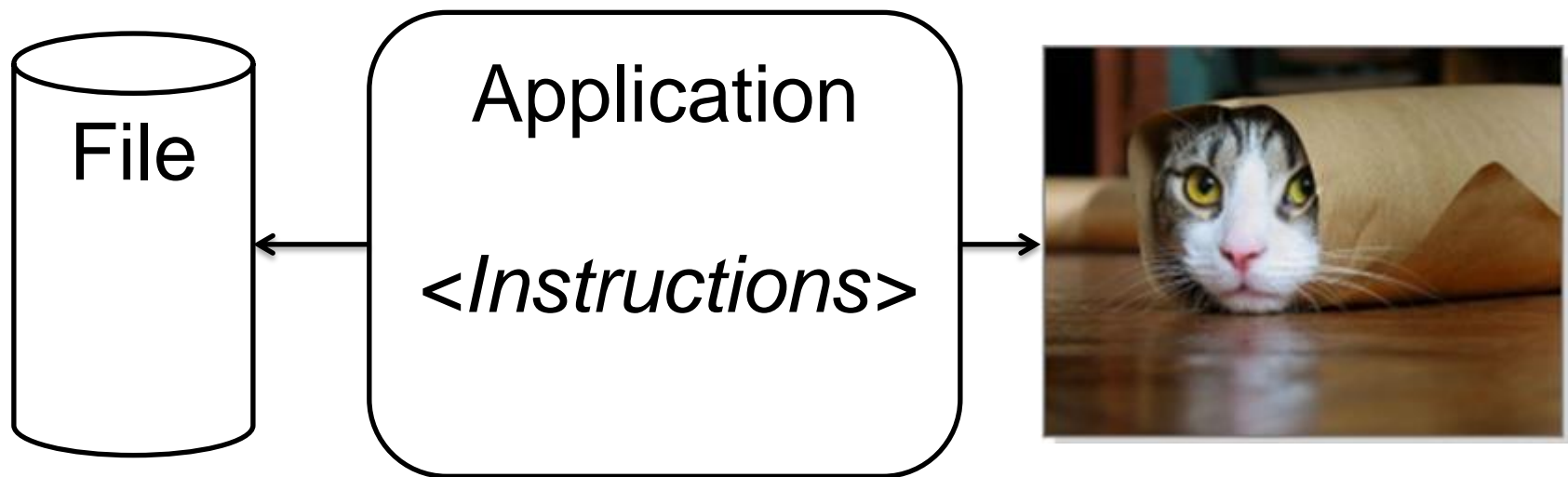
Image (RGB, DC) @ 12.5% (1/8)



What is a picture?



- ★ Data for the computer
- ★ When interpreted correctly, displays a cat (via GPU)
- ★ When interpreted wrongly, displays garbage / crashes
- ★ When interpreted wrongly in the right way, lets us hack a computer



What is a picture?



Which one is data and which is instructions?

```
0004 8384 0084 c7c8 00c8 4748 0048 e8e9
00e9 6a69 0069 a8a9 00a9 2828 0028 fdfe
00fc 1819 0019 9898 0098 d9d8 00d8 5857
0057 7b7a 007a bab9 00b9 3a3c 003c 8888
8888 8888 8888 8888 288e be88 8888 8888
3b83 5788 8888 8888 7667 778e 8888 8888
d61f 7abd 8818 8888
8b06 e8f7 88aa 8388
8a18 880c e841 c988
```

how the computer
sees instructions

how the computer
sees data

```
f0 32 7d 60 95 48 d0 62 08 80 4b 67 b4 4a 21 dc
80 3f 6c dd 4a f5 a3 d4 ce 32 8d e4 21 d7 a5 5a
92 93 4b f1 ca 0a ce 3c b9 14 20 a5 00 a4 4a 3e
bd 4b 8c b4 d1 90 2b 25 a9 c8 f4 c8 10 85 fb d6
fc 2a 1f c6 8a 7f 25 e7 47 f4 95 01 e2 d7 82 fe
22 95 fa 8e 49 e4 50 98 d3 84 95 a7 97 1d 97 92
25 32 9f 90 0c a9 07 73 c2 2b 49 06 4c 1a 26 69
b2 75 3e 20 db 65 bf 22 68 cf 29 1b 8a 65 8d 54
91 ba 33 f3 05 59 07 39 cd 43 96 6f 5d 88 bb 7a
55 50 d7 04 b1 c6 33 75 8c 60 f7 c7 70 73 af 66
```

What is a picture?



Is it possible to create an image which executes code?

Yes

If this is intentional, it's a feature

If this is not intentional, the picture is an exploit

What is an exploit?

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Simple Definition of EXPLOIT

- ✦ to get value or use from (something)
- ✦ to use (someone or something) in a way that helps you unfairly

Full Definition of EXPLOIT

- ✦ to make productive use of : UTILIZE <exploiting your talents> <exploit your opponent's weakness>
- ✦ to make use of meanly or unfairly for one's own advantage <exploiting migrant farm workers>

<http://www.merriam-webster.com/dictionary/exploit>

What is an exploit?

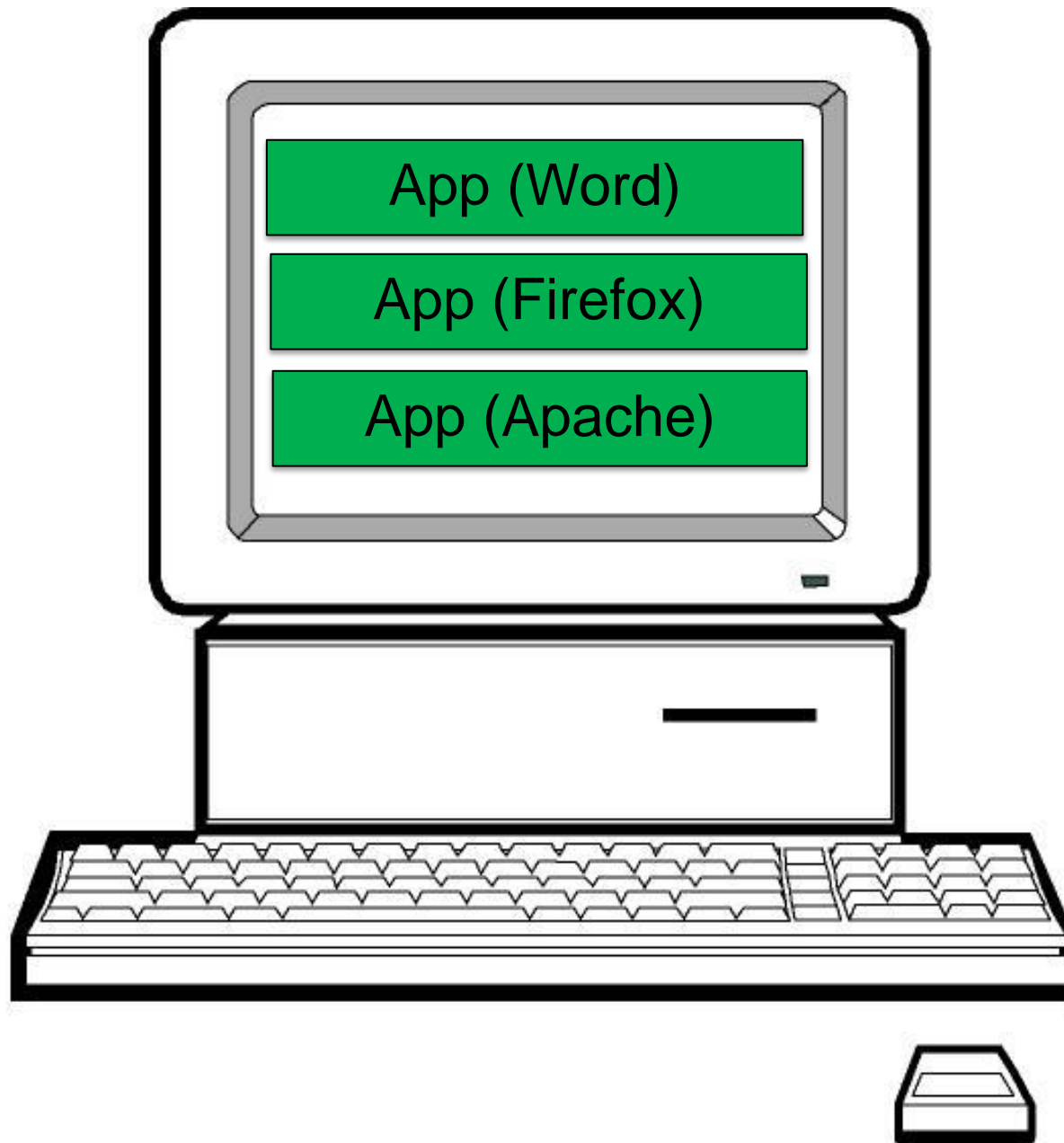


Exploit (v): To take advantage of a vulnerability so that the target system reacts in a manner other than which the designer intended.

Exploit (n): The tool, set of instructions, or code that is used to take advantage of a vulnerability.

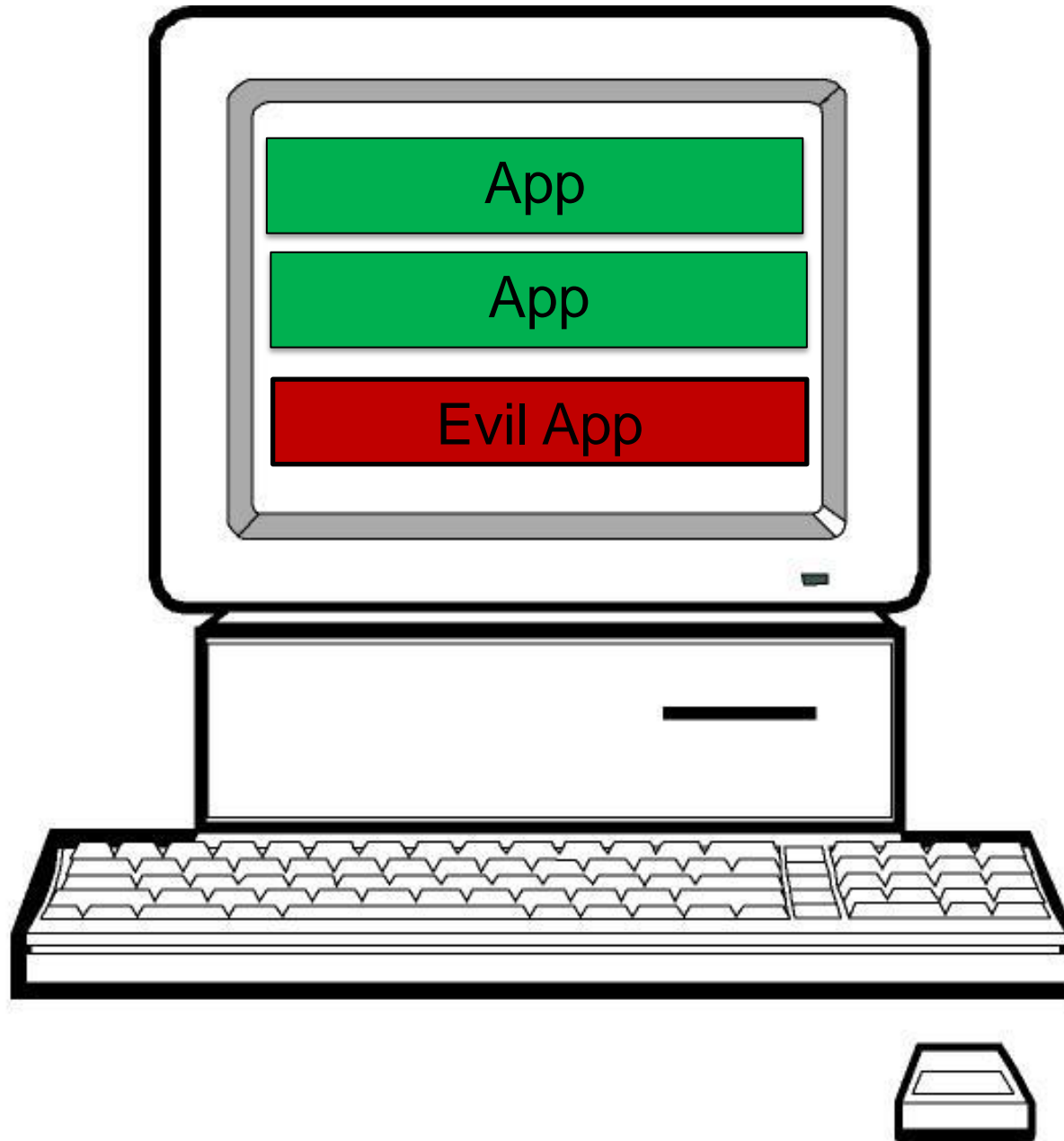
(The Shellcoders Handbook, 2nd Edition, p4)

What is an exploit?



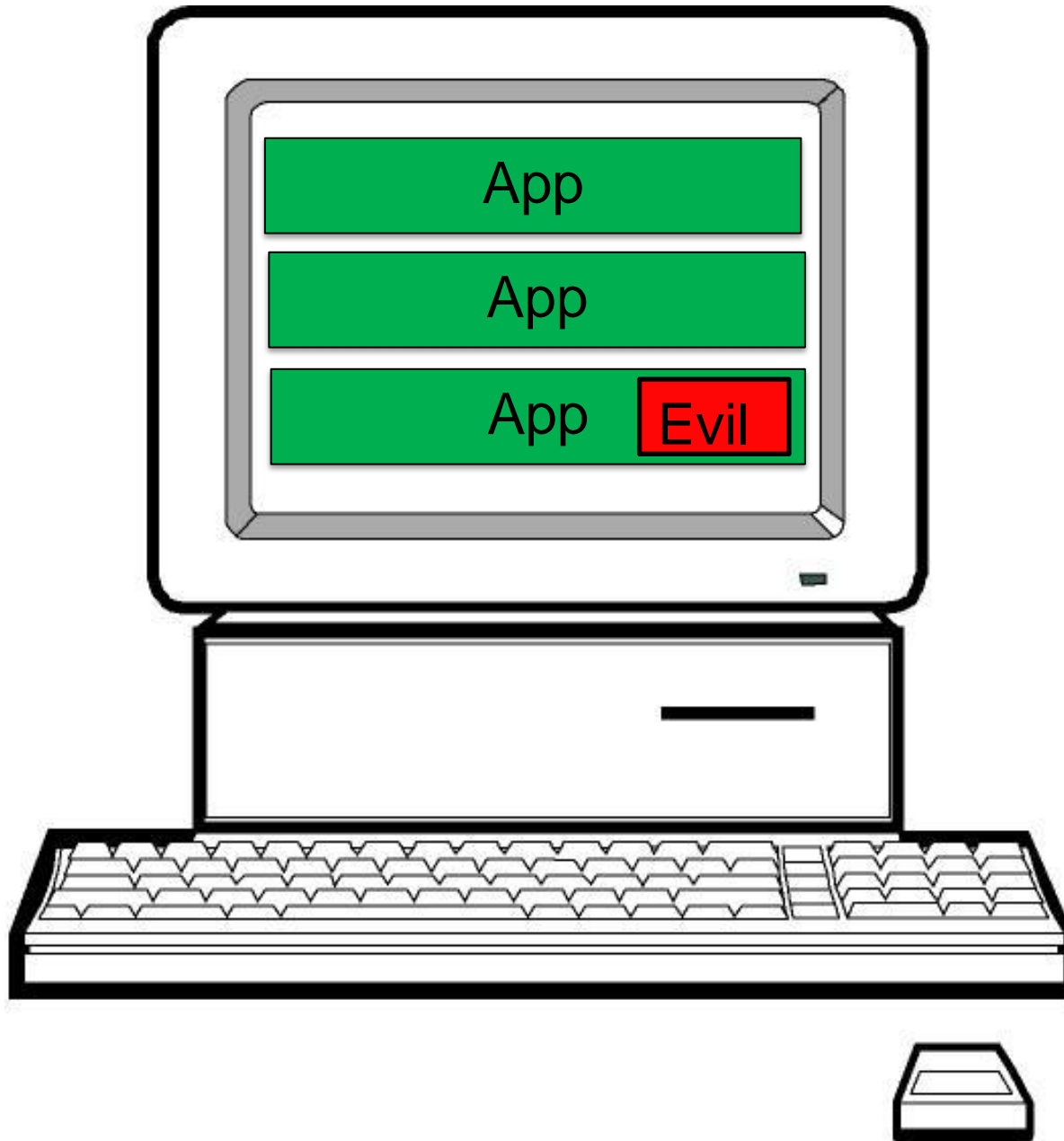
Only trusted
apps (code)
running
Computer
fully secure

What is an exploit?



Virus /
Backdoor /
Trojan /
Malware
Is NOT
Exploit

What is an exploit?



Introduce
new code
into running
software

Types of exploits

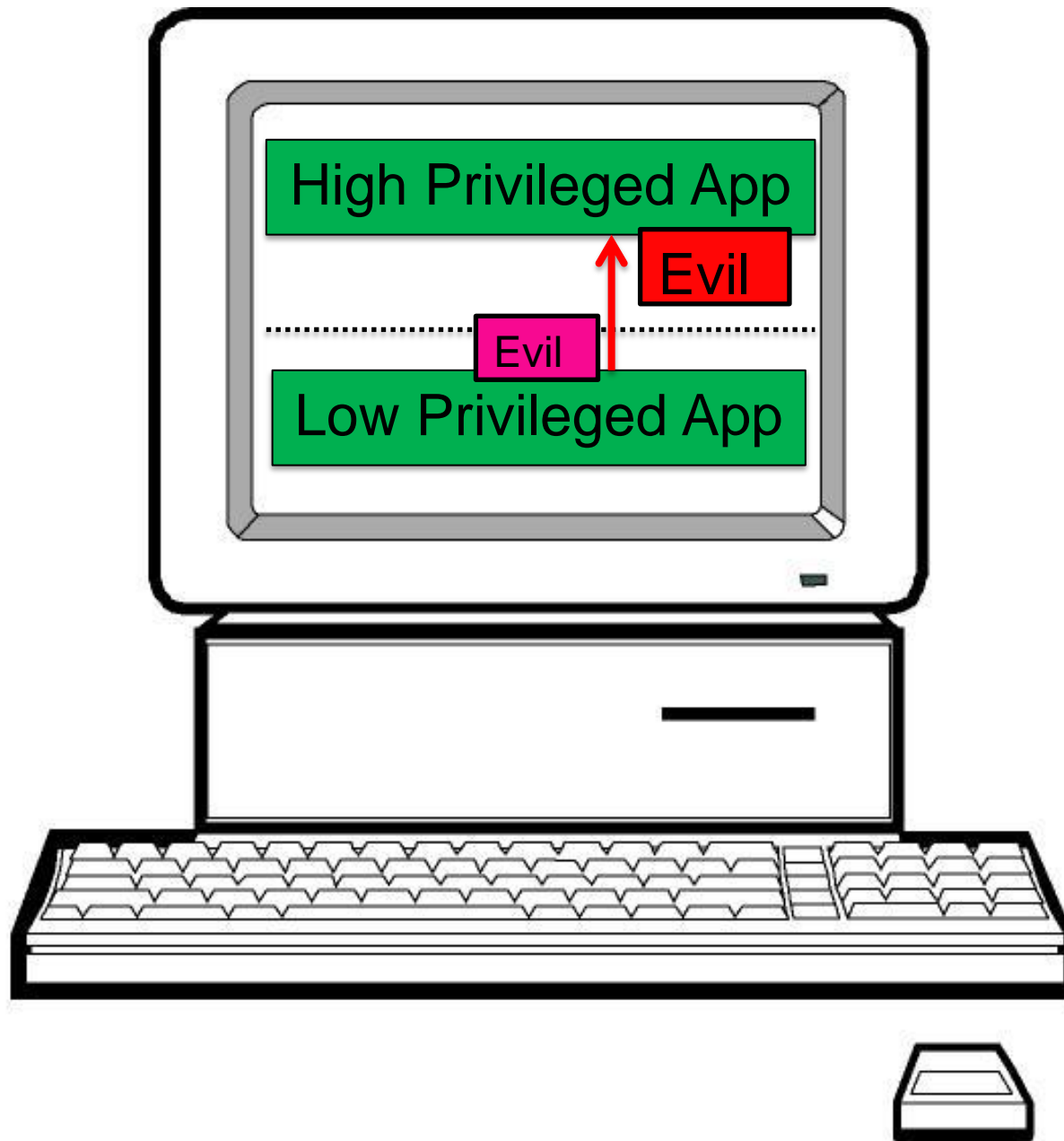


Local

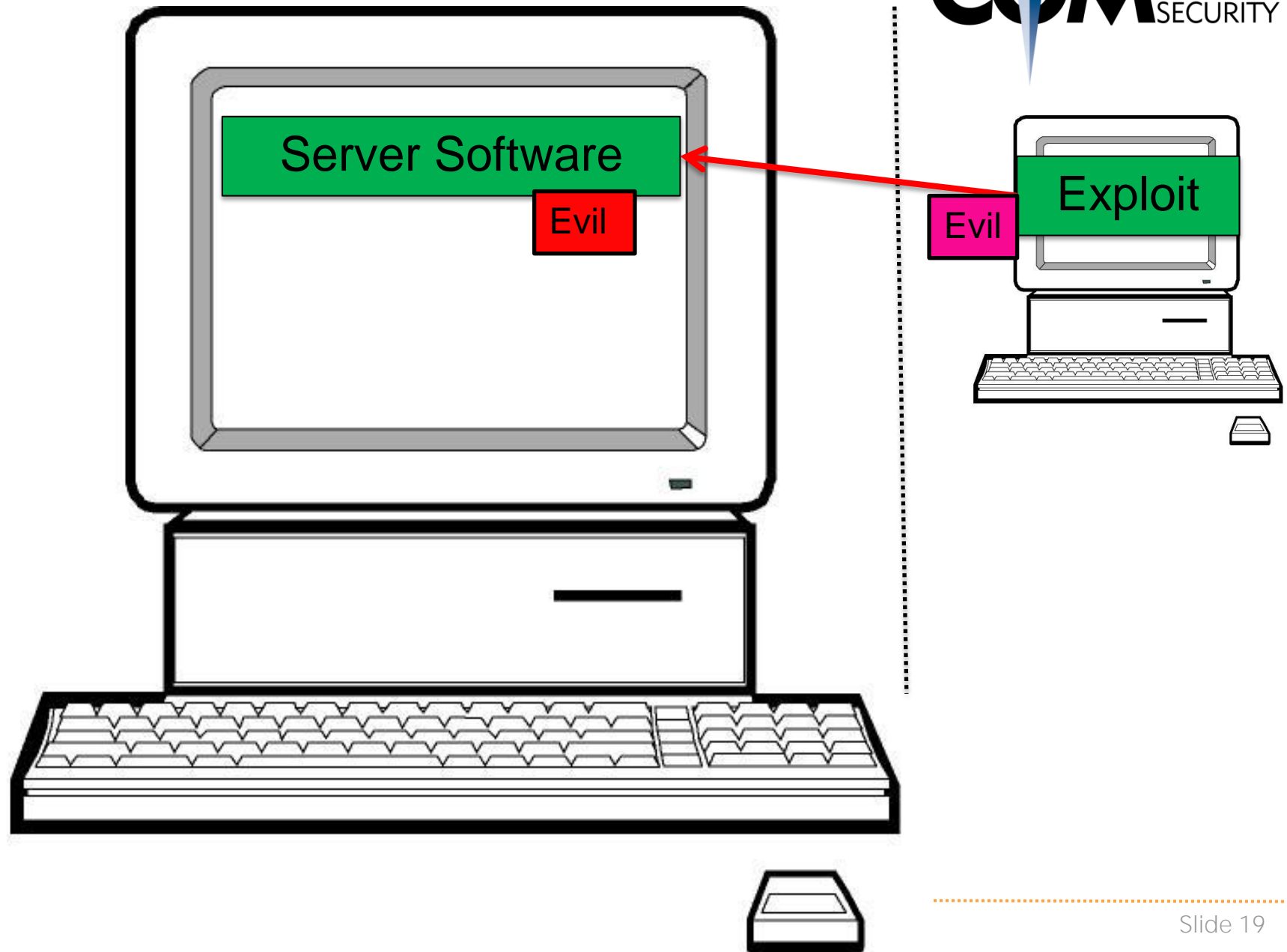
Server-side

Client-side

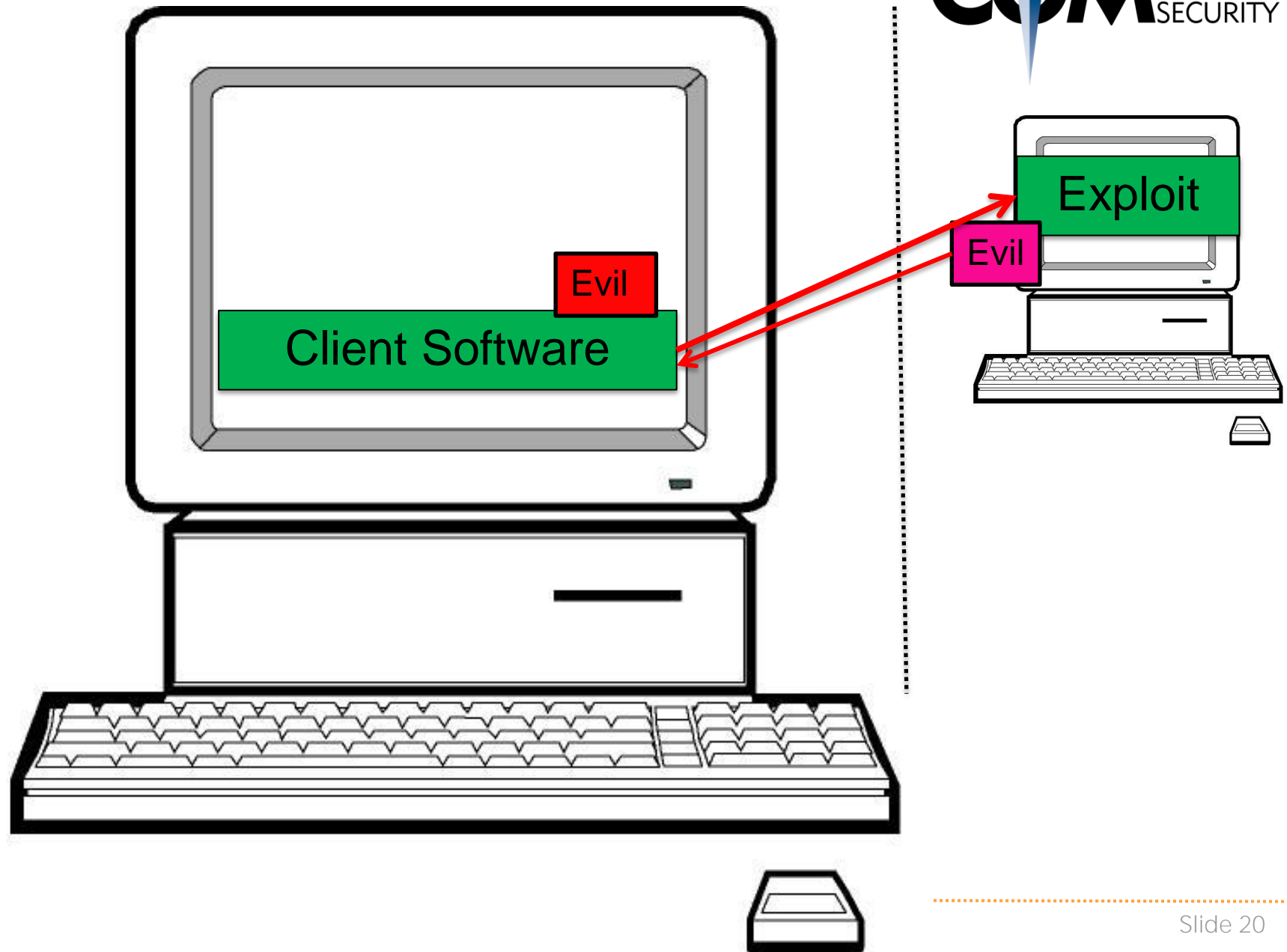
Types of exploits - Local exploit



Types of exploits - Server-side exploit



Types of exploits - Client-side exploit



Local Exploit:

- ✦ Attacker is already on a host
- ✦ Wants to execute his code with higher privileges
- ✦ "Privilege Escalation"

Linux:

- ✦ SUID Programs
- ✦ www-data -> root

Windows:

- ✦ User -> Local Admin (->System)

Remote Exploit:

- ✦ Attacker can directly talk with a server software on a host
- ✦ Wants to execute his code on the remote host

Server Examples

- ✦ FTP Server (proftp, wuftp)
- ✦ DNS Server (bind)
- ✦ Web Server (IIS, Apache)

Client Exploit:

- ✦ Attacker can influence data which a client receives
- ✦ Wants to execute his code on the client host

Examples:

- ✦ Browser
 - ✦ Flash
 - ✦ Java
 - ✦ Image Viewer
- ✦ Word
- ✦ Putty
- ✦ Git

Is exploit writing hacking?

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Is exploit writing hacking?



Hack

1. to cut, notch, slice, chop, or sever (something) with or as with heavy, irregular blows (often followed by *up* or *down*):
to hack meat; to hack down trees.

Is exploit writing hacking?



An aspect of hack value is performing feats for the sake of showing that they can be done, even if others think it is difficult. **Using things in a unique way outside their intended purpose** is often perceived as having hack value.

Examples:

- ✦ using a dot matrix impact printer to produce musical notes
- ✦ using an optical mouse as barcode reader.
- ✦ making soup with your coffee machine

https://en.wikipedia.org/wiki/Hacker_culture

Is exploit writing hacking?



hack: *Computers.*

to modify (a computer program or electronic device) or write (a program) in a skillful or clever way:

Developers have hacked the app.

I hacked my tablet to do some very cool things.

to circumvent security and break into (a network, computer, file, etc.), usually with malicious intent:

Criminals hacked the bank's servers yesterday.

Our team systematically hacks our network to find vulnerabilities.

<http://www.dictionary.com/browse/hacking>

Is exploit writing hacking?



Hackerethik:

Freier Zugriff auf Computer

Freier Zugriff auf Wissen

Misstrauen gegenüber Autoritäten und Bevorzugung von Dezentralisierung.

Hacker sollten nur nach ihrer Fähigkeit beurteilt werden.

Du kannst Kunst und Schönheit mittels Computer erzeugen

Verbesserung der Welt durch das Verbreiten von Technologien

<https://de.wikipedia.org/wiki/Hackerethik>

A vertical strip on the left side of the slide shows a close-up of a computer keyboard. A magnifying glass is positioned over a key, and a yellow padlock is resting on the keyboard, symbolizing security and vulnerability.

Vulnerability types

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Vulnerability types

- ✦ **Memory corruption**
- ✦ Authentication
- ✦ Authorization
- ✦ Configuration error
- ✦ Input validation
- ✦ Logic error
- ✦ Sensitive data protection
- ✦ Session management
- ✦ Encoding Error
- ✦ Cryptographic Errors
- ✦ Permission Problems
- ✦ ...

Memory corruption occurs in a computer program when the **contents of a memory location are unintentionally modified** due to programming errors; this is termed violating memory safety. When the corrupted memory contents are used later in that program, it leads either to program crash or to strange and **bizarre program behavior**

Modern programming languages like C and C++ have **powerful features of explicit memory management and pointer arithmetic**. These features are designed for developing efficient applications and system software.

https://en.wikipedia.org/wiki/Memory_corruption

What is vulnerable against memory corruption?

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

What is vulnerable?



What software is affected?

Software developed in unsafe programming languages

- ✦ (ASM)
- ✦ C
- ✦ C++
- ✦ Fortran (lol)

What is vulnerable?



What software is affected?

Software developed in unsafe programming languages

- ✦ (ASM)
- ✦ C
- ✦ C++
- ✦ Fortran (lol)

Who writes software in C/C++, anyway?

- ✦ IE, Chrome, Firefox
- ✦ Apache / IIS
- ✦ Postfix, Sendmail
- ✦ BIND
- ✦ MS Office / LibreOffice
- ✦ Antivirus
- ✦ Other "Security" Software

What is vulnerable?



Not affected:

Software written in interpreted languages

- ✦ PHP
- ✦ Perl
- ✦ Ruby
- ✦ Bash
- ✦ Python
- ✦ JavaScript

Software with strict bound checking

- ✦ Rust
- ✦ C#
- ✦ Java

Exception: Native calls

What is vulnerable?



Special case: Interpreter itself

What language is PHP, Java, JavaScript, ... written-in?

✦ C / C++

Some memory corruption vuln's

From 2015

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

What is vulnerable?



Vulnerability Details : [CVE-2015-8617](#)

Format string vulnerability in the zend_throw_or_error function in Zend/zend_execute_API.c in PHP 7.x before 7.0.1 allows remote attackers to execute arbitrary code via format string specifiers in a string that is misused as a class name, leading to incorrect error handling.

Publish Date : 2016-01-19 Last Update Date : 2016-01-21

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#)

▼ [Scroll To](#)

▼ [Comments](#)

▼ [External Links](#)

[Search Twitter](#) [Search YouTube](#) [Search Google](#)

– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	134

CVE-2015-6094

- ✦ Microsoft Office is prone to a remote memory-corruption vulnerability because it fails to properly handle objects in memory.
- ✦ Excel 2010, 2013, 2016

CVE-2015-6068

- ✦ Microsoft Internet Explorer is prone to a remote memory-corruption vulnerability. Attackers can exploit this issue by enticing an unsuspecting user to view a specially crafted webpage.
- ✦ IE11

CVE-2015-5122

- ✦ Use-after-free vulnerability in the DisplayObject class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.302 on Windows and OS X, 14.x through 18.0.0.203 on Windows and OS X, 11.x through 11.2.202.481 on Linux, and 12.x through 18.0.0.204 on Linux Chrome installations allows remote attackers to execute arbitrary code
- ✦ Flash 11, 12, 13, 14

CVE-2015-0287

- ✦ ASN.1 structure reuse memory corruption. Reusing a structure in ASN.1 parsing may allow an attacker to cause memory corruption via an invalid write.
- ✦ **OpenSSL 0.9.8-1.0.2**

CVE-2015-7852

- ✦ A potential off by one vulnerability exists in the cookedprint functionality of ntpq. A specially crafted buffer could cause a buffer overflow potentially resulting in null byte being written out of bounds.
- ✦ **NTP 4.2.8p2**

CVE-2015-1538 (Stagefright)

- ✦ Integer overflow in the SampleTable::setSampleToChunkParams function in SampleTable.cpp in libstagefright in Android before 5.1.1 LMY48I allows remote attackers to execute arbitrary code via crafted atoms in MP4 data that trigger an unchecked multiplication
- ✦ **Android 1.5 - 5.1**

Some memory corruption bugs



Android:

Overview ▾

Bulletins ▲

Advisories ▾

April 2016

March 2016

February 2016

January 2016

December 2015

November 2015

October 2015

September 2015

August 2015

Authentication ▾

Keystore ▾

Elevation of Privilege Vulnerability in Telecom Component	CVE-2016-0847	High
Elevation of Privilege Vulnerability in Download Manager	CVE-2016-0848	High
Elevation of Privilege Vulnerability in Recovery Procedure	CVE-2016-0849	High
Elevation of Privilege Vulnerability in Bluetooth	CVE-2016-0850	High
Elevation of Privilege Vulnerability in Texas Instruments Haptic Driver	CVE-2016-2409	High
Elevation of Privilege Vulnerability in a Video Kernel Driver	CVE-2016-2410	High
Elevation of Privilege Vulnerability in Qualcomm Power Management Component	CVE-2016-2411	High
Elevation of Privilege Vulnerability in System_server	CVE-2016-2412	High
Elevation of Privilege Vulnerability in Mediaserver	CVE-2016-2413	High
Denial of Service Vulnerability in Minikin	CVE-2016-2414	High
Information Disclosure Vulnerability in Exchange ActiveSync	CVE-2016-2415	High
Information Disclosure Vulnerability in Mediaserver	CVE-2016-2416 CVE-2016-2417 CVE-2016-2418 CVE-2016-2419	High
Elevation of Privilege Vulnerability in Debuggerd Component	CVE-2016-2420	Moderate
Elevation of Privilege Vulnerability in Setup Wizard	CVE-2016-2421	Moderate
Elevation of Privilege Vulnerability in Wi-Fi	CVE-2016-2422	Moderate
Elevation of Privilege Vulnerability in Telephony	CVE-2016-2423	Moderate
Denial of Service Vulnerability in SyncStorageEngine	CVE-2016-2424	Moderate
Information Disclosure Vulnerability in AOSP Mail	CVE-2016-2425	Moderate
Information Disclosure Vulnerability in Framework	CVE-2016-2426	Moderate
Information Disclosure Vulnerability in BouncyCastle	CVE-2016-2427	Moderate

Some memory corruption bugs



Firefox:

Fixed in Firefox 45

- 2016-38** Out-of-bounds write with malicious font in Graphite 2
- 2016-27** Use-after-free during XML transformations
- 2016-26** Memory corruption when modifying a file being read by FileReader
- 2016-19** Linux video memory DOS with Intel drivers
- 2016-18** CSP reports fail to strip location information for embedded iframe pages
- 2016-17** Local file overwriting and potential privilege escalation through CSP reports
- 2016-16** Miscellaneous memory safety hazards (rv:45.0 / rv:38.7)

Some I

IE11

Internet Explorer 11



Bulletins 1-15 of 30

Date ▼	Bulletin Number	K		Internet Explorer 11 (3139929)	Remote Code Execution	Critical	
3/8/2016	MS16-023	3	Windows 7 for 32-bit Systems Service Pack 1	Internet Explorer 11 (3139929)	Remote Code Execution	Critical	
2/9/2016	MS16-009	3	Windows 7 for x64-based Systems Service Pack 1	Internet Explorer 11 (3139929)	Remote Code Execution	Critical	
1/12/2016	MS16-001	3	Windows 8.1 for 32-bit Systems	Internet Explorer 11 (3139929)	Remote Code Execution	Critical	
12/8/2015	MS15-124	3	Windows 8.1 for x64-based Systems	Internet Explorer 11 (3139929)	Remote Code Execution	Critical	ing
11/10/2015	MS15-112	3	Windows Server 2008 R2 for x64-based Systems Service Pack 1	Internet Explorer 11 [1] (3139929)	Remote Code Execution	Moderate	
10/13/2015	MS15-106	3	Windows Server 2012 R2	Internet Explorer 11 (3139929)	Remote Code Execution	Moderate	
9/8/2015	MS15-094	3	Windows RT 8.1	Internet Explorer 11 [1] [2] (3139929)	Remote Code Execution	Critical	
8/18/2015	MS15-093	3	Windows 10 for 32-bit Systems [3] (3140745)	Internet Explorer 11	Remote Code Execution	Critical	
8/11/2015	MS15-079	3	Windows 10 for x64-based Systems [3] (3140745)	Internet Explorer 11	Remote Code Execution	Critical	
7/14/2015	MS15-065	3	Windows 10 Version 1511 for 32-bit Systems [3] (3140768)	Internet Explorer 11	Remote Code Execution	Critical	
6/9/2015	MS15-056	3	Windows 10 Version 1511 for x64-based Systems [3]	Internet Explorer 11	Remote Code Execution	Critical	
5/12/2015	MS15-043	3	Windows 10 Version 1511 for x64-based Systems [3]	Internet Explorer 11	Remote Code Execution	Critical	de 43

Some memory corruption bugs



Conclusion:

- ✦ Important software is written in C/C++
- ✦ Memory corruption bugs are very prevalent

Recap:

- ✦ We are concerned with **memory corruption vulnerabilities**
- ✦ A program which misuses a memory corruption vulnerability is called an **exploit**
- ✦ There can be local-, server- and client exploits
- ✦ A exploit injects **additional code** into a trusted app and executes it

Programs and Data

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Definition of a "program":

"A program is a set of instructions
which modify data"

Definition of a "program":

"A program is a set of instructions
~~which modify data~~
which is controlled by data"

Definition of a "program":

"A program is a set of instructions
~~which modify data~~
which is controlled by data"

Or in other words:

Data is manipulating the
instruction flow of a program,
not the other way round

Weird machine:

In computer security, the weird machine is a computational artifact where additional code execution can happen outside the original specification of the program.

It is closely related to the concept of weird instructions, which are the building blocks of an exploit based on crafted input data

Programming of "Weird Machines"

Gain very detailed understanding of:

- ✦ Program logic
- ✦ Implementation of "hidden mechanics"
 - ✦ Stack, Heap etc.
- ✦ Error conditions

Leads from from:

- ✦ "This bugs randomly crashes my program!"

To:

- ✦ "This bugs lets me reliably execute arbitrary code"

Obligatory history lesson...

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Morris worm

- ✦ 02.11.1988
- ✦ Written by graduate student Robert Morris, MIT
- ✦ He wanted to count the number of computers on the internet
- ✦ Worm had a bug, re-infected already infected computers, killed the Internet
- ✦ Attacked fingerd and sendmail (and some more things)



fingerd bug in BSD4 on VAX machines:

The bug exploited to break fingerd involved **overrunning the buffer the daemon used for input**. The standard C library has a few routines that read input without checking for bounds on the buffer involved. In particular, the **gets** call takes input to a buffer without doing any bounds checking; this was the call exploited by the Worm.

The Internet Worm Program: An Analysis (2004)

★ <http://spaf.cerias.purdue.edu/tech-reps/823.pdf>

