Introduction to Binary exploitation

Sahana C
csahana95@gmail.com
https://www.linkedin.com/in/sahana-c-69a77576

Introduction

- What is a binary?

- Why do we care about native security?

- Memory management in C/C++ -> Developer's responsibility

- Memory corruption bugs

Apr 2019	Apr 2018	Programming Language	Ratings	Change
1	1	Java	15.035%	-0.74%
2	2	C	14.076%	+0.49%
3	3	C++	8.838%	+1.62%
4	4	Python	8.166%	+2.36%
5	6	Visual Basic .NET	5.795%	+0.85%
6	5	C#	3.515%	-1.75%
7	8	JavaScript	2.507%	-0.99%
8	9	SQL	2.272%	-0.38%
9	7	PHP	2.239%	-1.98%
10	14	Assembly language	1.710%	+0.05%

Source:
https://www.zdnet.com/article/programming-language-popularity-c-bounces-back-at-pythons-expense/


mozilla
Firefox


Adobe


Windows

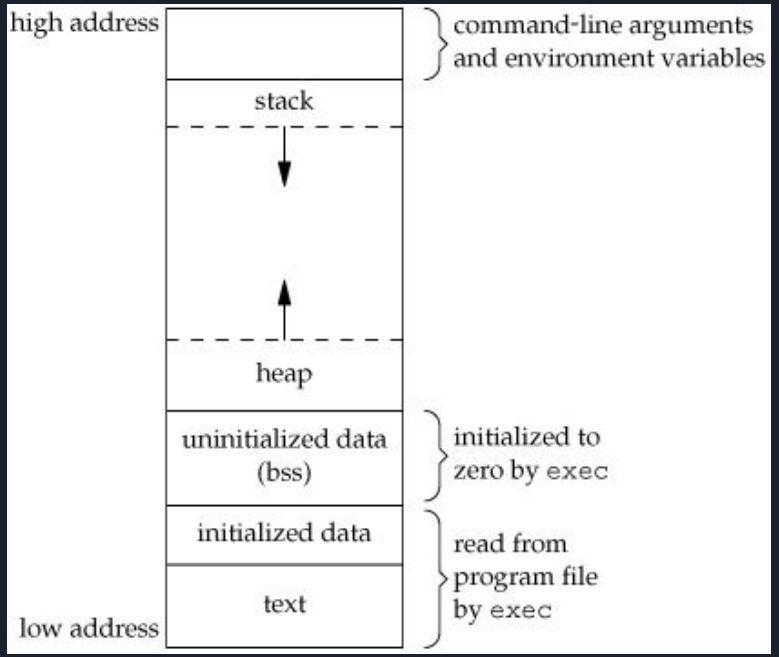
What could be the impact if things go wrong?

- Eternal Blue(MS)

Source:
https://nakedsecurity.sophos.com/

Let's hack a binary to get admin access!

Memory organization

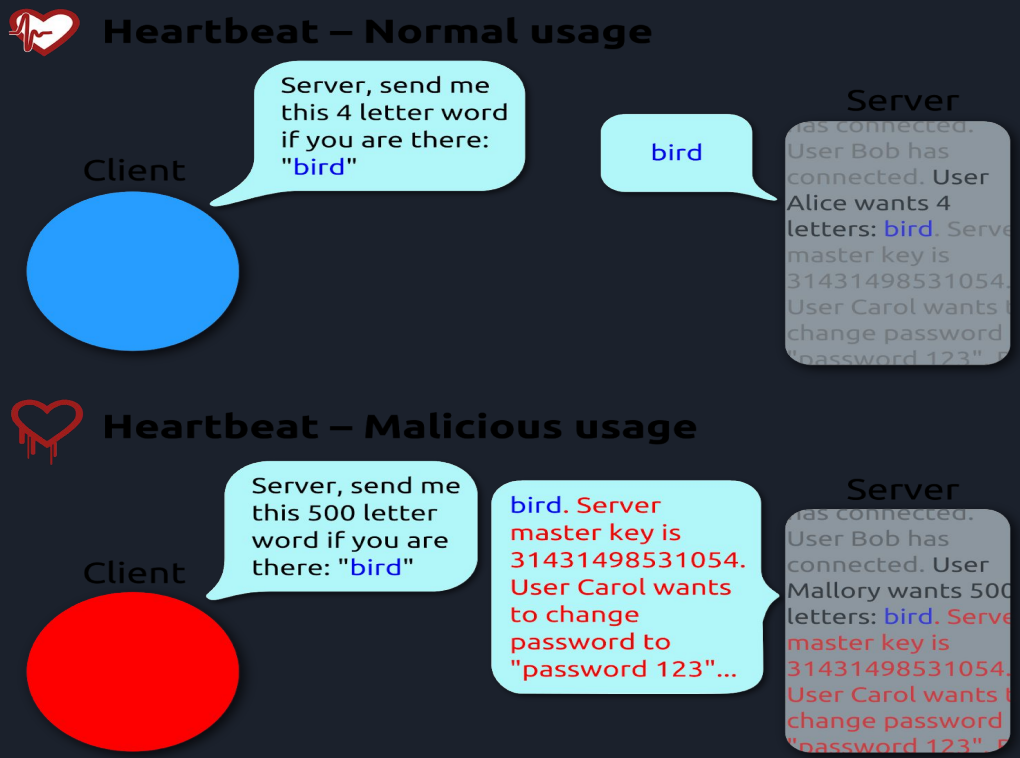


Source: https://i.stack.imgur.com/1Yz9K.gif

What are the vulnerabilities?

How to patch the binary?

Another real world example



Heartbleed vulnerability (CVE-2014-0160)

```
memcpy(bp, pl,
payload);
```

```
if (1 + 2 + payload
+ 16 >
s->s3->rrec.length)
return 0;
```

Source: Malwarebytes blog

How to get started?

- https://www.youtube.com/playlist?list=PLhixgUqwRTjxglIswKp9mpkfPNfHkzyeN

- https://ctf101.org/

- https://dhavalkapil.com/blogs/Buffer-Overflow-Exploit/

- https://pwnable.xyz/

Tools

-Debbuger - pwndbg https://github.com/pwndbg/pwndbg

- Participate in CTFs

Security of Voice Controlled Systems

Agenda

- Why security of VCS is important?

-Introduce different types of attacks targeted on Voice controlled systems

- Defence mechanisms proposed.

- Future of VCS security.

Voice is the new trend

Juniper estimates 3.25 billion voice assistants in use - 2019

Speech is the natural way of communication

Future trend

What if Voice assistant becomes your nightmare?

- Take control of household equipments.

- Shopping

- Banking

Various attacks

- VoiceEmployer - Bypassing android permissions using voice

- ShouldEndSession

- Skill squatting attack

- Smear skill squatting attack

- Voice morphing attacks

- Hidden command

- Inaudible command - exploiting hardware non-linearity loophole.

Minimizing the risk

- Notifying user

- Challenge response protocol

- Customizing the trigger word

- Communication protocol

Do users intrinsically trust IoT devices more than online websites?

References

- https://www.usenix.org/conference/nsdi18/presentation/roy

- https://nicholas.carlini.com/papers/2016_usenix_hiddenvoicecommands.pdf

- https://www.usenix.org/sites/default/files/conference/protected-files/security18_slides_kumar.pdf

Questions?