# Fork bomb

In <u>computing</u>, a **fork bomb** (also called **rabbit virus** or **wabbit** $^{[1]}$ ) is a <u>denial-of-service attack</u> wherein a process continually replicates itself to deplete available system resources, slowing down or crashing the system due to resource starvation.

#### **Contents**

**History** 

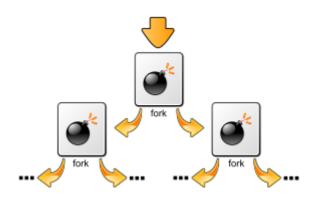
**Implementation** 

**Prevention** 

See also

References

**External links** 



The concept behind a fork bomb — the processes continually replicate themselves, potentially causing a denial of service

# History

Around 1978, an early variant of a fork bomb called wabbit was reported to run on a <u>System/360</u>. It may have descended from a similar attack called **RABBITS** reported from 1969 on a <u>Burroughs 5500</u> at the <u>University</u> of Washington. [1]

# **Implementation**

Fork bombs operate both by consuming CPU time in the process of <u>forking</u>, and by saturating the <u>operating</u> <u>system</u>'s process table. [2][3] A basic implementation of a fork bomb is an <u>infinite loop</u> that repeatedly launches new copies of itself.

In <u>Unix</u>-like operating systems, fork bombs are generally written to use the fork <u>system call</u>. As forked processes are also copies of the first program, once they resume execution from the next address at the <u>frame pointer</u>, they continue forking endlessly within their own copy of the same infinite loop; this has the effect of causing an <u>exponential growth</u> in processes. As modern Unix systems generally use a <u>copy-on-write</u> resource management technique when forking new processes, a fork bomb generally will not saturate such a system's memory.

<u>Microsoft Windows</u> operating systems do not have an equivalent functionality to the Unix fork system call; a fork bomb on such an operating system must therefore create a new process instead of forking from an existing one.

A classic example of a fork bomb is the  $\underline{\text{Unix shell}}$  one :() { :|:& };:, which can be more easily understood as:

```
fork() {
fork | fork &
}
fork
```

In it, a function is defined (fork()) as calling itself (fork), then <u>piping</u> (|) its result to a background <u>job</u> of itself (&).

The Windows equivalent, given the limitations in system calls, could be written as such in batch:

```
@echo off
start
copy c:\fork{
pause
goto start
```

An even shorter version of this can be achieved by using anonymous functions:

```
%0|%0
```

#### **Prevention**

As a fork bomb's mode of operation is entirely encapsulated by creating new processes, one way of preventing a fork bomb from severely affecting the entire system is to limit the maximum number of processes that a single user may own. On Linux, this can be achieved by using the *ulimit* utility; for example, the command ulimit - u 30 would limit the affected user to a maximum of thirty owned processes. [6] On PAM-enabled systems, this limit can also be set in /etc/security/limits.conf, and on FreeBSD, the system administrator can put limits in /etc/login.conf. [8] Modern Linux systems also allow finer-grained fork bomb prevention through cgroups and process number (PID) controller. [9]

### See also

- Deadlock
- Logic bomb
- Time bomb (software)

### References

- 1. Raymond, Eric S. (October 1, 2004). "wabbit" (http://catb.org/~esr/jargon/html/W/wabbit.html). The Jargon Lexicon. Retrieved October 15, 2013.
- 2. Ye, Nong (2008). Secure Computer and Network Systems: Modeling, Analysis and Design. p. 16. ISBN 0470023244.
- 3. Jielin, Dong (2007). Network Dictionary. p. 200. ISBN 1602670005.
- 4. Dhamdhere, Dhananjay M. (2006). Operating Systems: A Concept-based Approach. p. 285. ISBN 0-07-061194-7.
- 5. Hammond, Mark (2000). *Python Programming On Win32: Help for Windows Programmers*. p. 35. ISBN 1565926218.
- 6. Cooper, Mendel (2005). Advanced Bash Scripting Guide. pp. 305-306. ISBN 1430319305.

- 7. Soyinka, Wale (2012). Linux Administration: A Beginners Guide. pp. 364–365. ISBN 0071767592.
- 8. Lucas, Michael W. (2007). *Absolute FreeBSD: The Complete Guide to FreeBSD*. pp. 198–199. ISBN 1593271514.
- 9. "Process Number Controller in Documentation/ as appeared in Linux kernel 5.3" (https://www.kernel.org/doc/html/latest/admin-guide/cgroup-v1/pids.html). October 8, 2019.

### **External links**

Examples of fork bombs in many languages (https://github.com/aaronryank/fork-bomb)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Fork bomb&oldid=1007808459"

This page was last edited on 20 February 2021, at 01:20 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.