Bad Stories

Michele LORETI
Università di Camerino

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Goal

- In this lecture we two well known bad stories will be presented to show how vulnerabilities may have a deep impact on systems.

Prerequisites

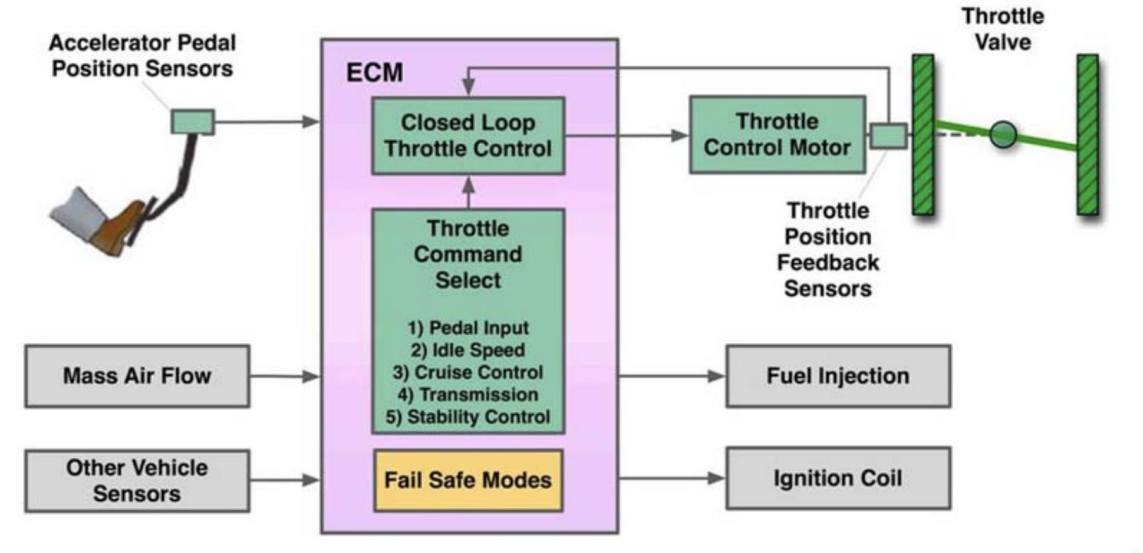
- Lecture:
  - Basic knowledge of C

Bad stories…

- Bugs in memory allocation can be the source of serious software vulnerabilities.
- Two well known examples are:
  - Toyota unintended acceleration (UA) cases
  - Heartbleed bug in OpenSSL

Unintentionally Acceleration

- NASA team investigates UA (2010-2011)



Technical Support to the National Highway Traffic Safety Administration (NHTSA) on the Reported Toyota Motor Corporation (TMC) Unintended Acceleration (UA) Investigation

Unintentionally Acceleration

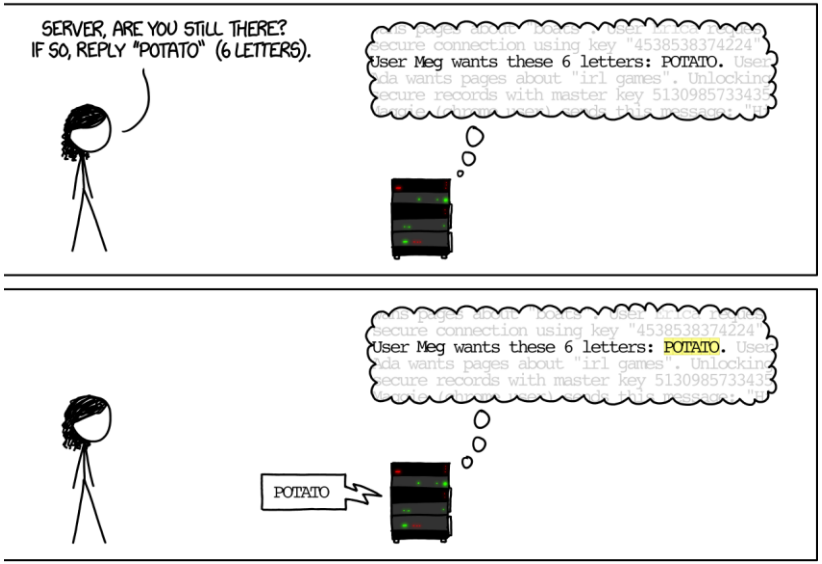
- The bug originated from a stack overflow that may corrupt critical variables of the Operating System
  - This is due to the use of (uncontrolled) recursion
  - Stack size exceeds the reserved space overriding controlling variables on the *heap*

Heartbleed bug

- The heartbeat functionality in SSL can be used to check if a connection is still alive
- Malformed input can be provided to OpenSSL to let it print a large part of the stack (possibly containing private keys)
- The same problem effects some TLS implementations (see CVE-2016-9244)

Heartbleed bug

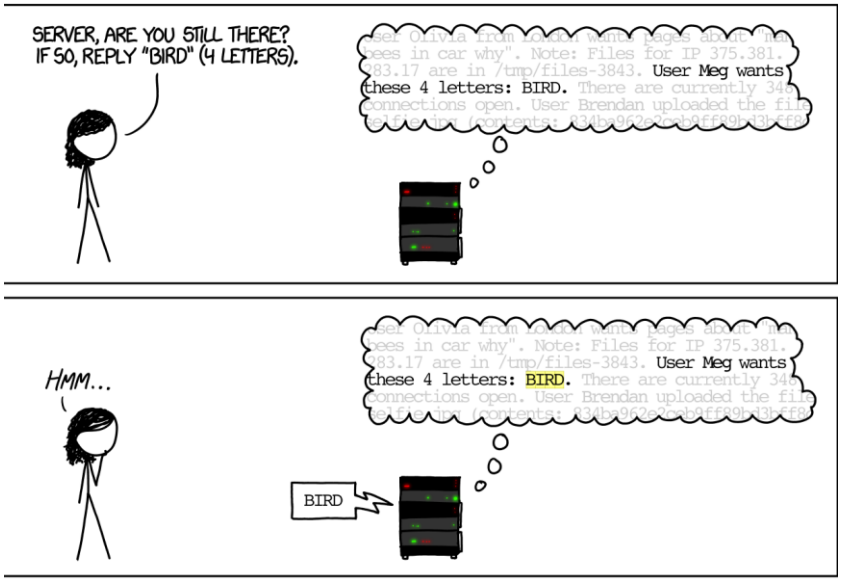
- Xkcd provides a nice explanation how the bug works:



https://xkcd.com/1354

Heartbleed bug

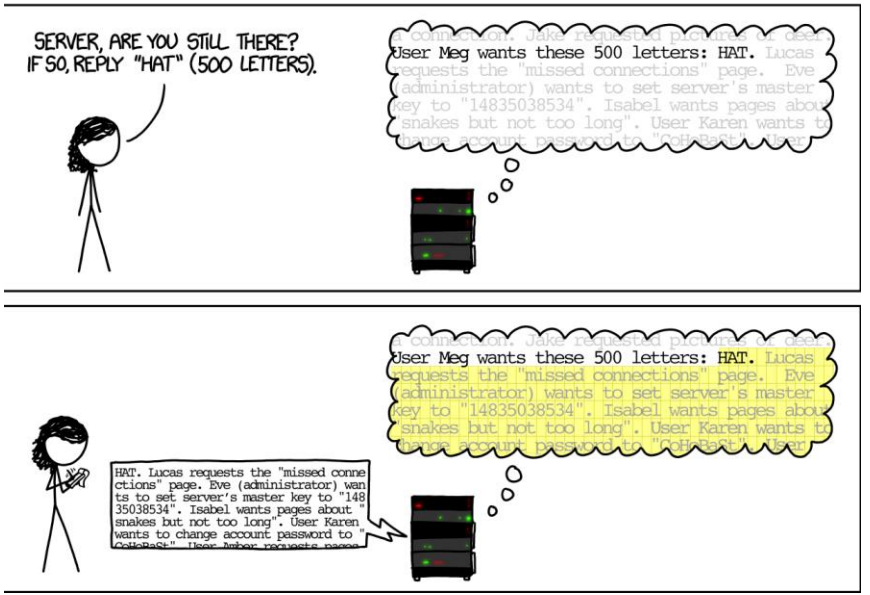
- Xkcd provides a nice explanation how the bug works:



https://xkcd.com/1354

Heartbleed bug

- Xkcd provides a nice explanation how the bug works:



https://xkcd.com/1354

Bad Stories

Michele LORETI
Università di Camerino

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it