

# Bugs, bugs everywhere

- *Pregled nekih zanimljivih bagova -*

Diana Šantavec  
[diana.santavec@gmail.com](mailto:diana.santavec@gmail.com)

Istraživačka stanica Petnica

07.04.2024.





# Literally everywhere

```
src > integration > inicio > --> behavior.test.js > ⚡ describe('Inicio-Desktop', callback) {
    import { desktopSizes, tabletSizes, mobileSizes, getSize } from '../../../../../tools/common.tools';
    import { axios, endpoint, tag, emailAddress, startTimestamp } from '../../../../../tools/testmailapp.tools';

    describe('Inicio-Desktop', () => {
        desktopSizes.forEach((size) => {
            it(` ${size} - Comprueba si funciona el carrusel hacia delante`, () => {
                getSize(size);
                cy.get('.next-btn > .fa').click();
                cy.get('.cliente09').should('be.visible');
            });
            it(` ${size} - Comprueba si funciona el carrusel hacia atrás`, () => {
                getSize(size);
                cy.get('.prev-btn > .fa').click();
                cy.get('[data-slick-index="10"] > .image > .cliente08').should('be.visible');
            });
            it(` ${size} - Comprueba el Carousel de opiniones`, () => {
                getSize(size);
                cy.get('.owl-pagination > :nth-child(3)').click();
                cy.scrollTo(0, 2000);
                cy.get('.owl-wrapper > :nth-child(5)').should('be.visible');
            });
            it(` ${size} - Comprueba si se envian los emails desde el formulario de la Landing`, () => {
                getSize(size);
                cy.get('#email').type(emailAddress).get('#aceptar').click().get('#ibenviar').click().wait(2000);
                cy.get('#incorrecto').should('be.visible');
            });
        });
    });
}
```

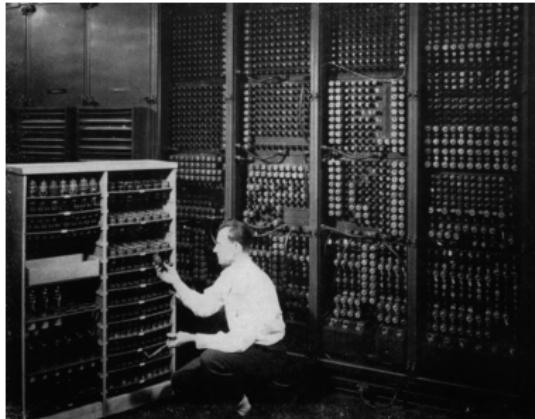
# Literally everywhere



# Literally everywhere



# Poreklo naziva



- Računari prve generacije (1940-1960)
- Vakuumske cevi

# Poreklo naziva

9/9

0800 Anton started  
1000 " stopped - anton ✓  
13°UC (03) MP-MC { 1.2700 9.037 847 025  
13°UC (03) MP-MC { 1.2700 9.037 846 995 corrupt  
023 PRO-2 2.130476415  
corrupt 2.130676415

Relays 6-2 in 033 failed special speed test  
In relay " 11.00 test .

Relay 2145  
Relay 3370

1100 Started Cosine Tape (Sine check)  
1525 Started Multi Adder Test.

1545



Relay #70 Panel F  
(Moth) in relay.

First actual case of bug being found.  
1600 Anton started.  
1700 closed down.

- Dr Grace Hopper (09.09.1947)

# printf ne radi?

- printf je funkcija za ispis teksta u C-u
- pritnf ("Hello\u017eworld");
- Prelazak u novi red je kontrolni karakter \n

# printf ne radi?

- **Situacija:** C program se pokreće u virtualnoj mašini i ispisuje poruku na terminal
- **Problem:** Tekst iz programa se nasumično ne ispisuje

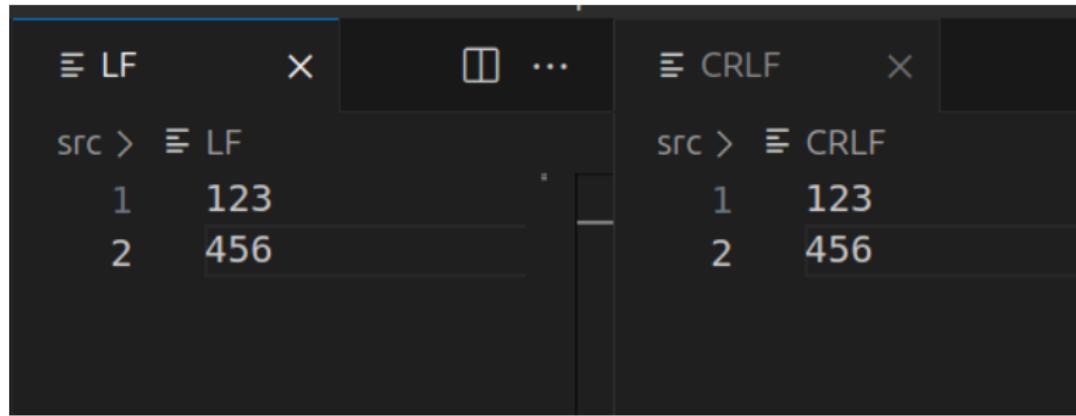
# printf ne radi?

- **Obrazloženje:** Linija terminala nije radila line wrap

```
dianas@dianas - ThinkPad ~>
dianas@dianas - ThinkPad ~>
dianas@dianas - ThinkPad ~> mkdir helloWorld
dianas@dianas - ThinkPad ~>
dianas@dianas - ThinkPad ~> █
```

- PS1 ili set horizontal-scroll-mode=off
- **Rešenja:**
  - Dodavanje nove linije na kraju ispisa
  - Ispravljanje vrednosti env varijabli

- **Situacija:** Kod pisan na Windows-u radi, ali kada se prebaci na Linux sistem i kompajlira, vraća grešku



- **Problem:** Različiti kraj linija
- **Obrazloženje:** na Windows-u se koristi CRLF a na Linux-u LF

- DOS/Windows: pratio mašine za pisanje
- Unix: izbacio CR

```
dianas@dianas-ThinkPad ~/P/P/b/src (master)>
dianas@dianas-ThinkPad ~/P/P/b/src (master)> hexdump -C LF
00000000  31 32 33 0a 34 35 36                                |123.456|
00000007
dianas@dianas-ThinkPad ~/P/P/b/src (master)> hexdump -C CRLF
00000000  31 32 33 0d 0a 34 35 36                                |123..456|
00000008
dianas@dianas-ThinkPad ~/P/P/b/src (master)>
dianas@dianas-ThinkPad ~/P/P/b/src (master)>
```

# Ali radi na mom računaru...

```
dianas@dianas-ThinkPad ~/P/P/b/src (master)> ascii -x
 00 NUL      10 DLE      20          30 0      40 @      50 P      60 `      70 p
 01 SOH      11 DC1      21 !      31 1      41 A      51 Q      61 a      71 q
 02 STX      12 DC2      22 "      32 2      42 B      52 R      62 b      72 r
 03 ETX      13 DC3      23 #      33 3      43 C      53 S      63 c      73 s
 04 EOT      14 DC4      24 $      34 4      44 D      54 T      64 d      74 t
 05 ENQ      15 NAK      25 %      35 5      45 E      55 U      65 e      75 u
 06 ACK      16 SYN      26 &      36 6      46 F      56 V      66 f      76 v
 07 BEL      17 ETB      27 '      37 7      47 G      57 W      67 g      77 w
 08 BS       18 CAN      28 (      38 8      48 H      58 X      68 h      78 x
 09 HT       19 EM       29 )      39 9      49 I      59 Y      69 i      79 y
 0A LF       1A SUB      2A *      3A :      4A J      5A Z      6A j      7A z
 0B VT       1B ESC      2B +      3B ;      4B K      5B [      6B k      7B {
 0C FF       1C FS       2C ,      3C <      4C L      5C \      6C l      7C |
 0D CR       1D GS       2D -      3D =      4D M      5D ]      6D m      7D }
 0E SO       1E RS       2E .      3E >      4E N      5E ^      6E n      7E ~
 0F SI       1F US       2F /      3F ?      4F O      5F _      6F o      7F DEL
```

```
dianas@dianas-ThinkPad ~/P/P/b/src (master)>
```

- **Situacija:** Iz logova se izvlači timestamp i poredi se da li je isti kao i očekivan
- Poređenje se radi sa *datetime* objekata, tako da se string pretvara u *datetime* objekat
- Kada se test pokrene na lokalnom računaru, prolazi, ali na serveru ne

- **Problem:** Različiti formati datuma na samom operativnom sistemu
- **Obrazloženje:** C# kada konvertuje string u datum uzima regionalna podešavanja operativnog sistema

# Weird filenames making weird behaviours

- Komanda se sastoji od naziva komande i liste parametara razdvojenih razmakom
- touch naziv1 naziv2 naziv3
- Nova linija označava kraj komande
- **Situacija:** Pokrećemo komandu sa listom fajlova i dobijamo grešku da ne postoji komanda "naziv fajla"

- **Problem:** Ime fajla je bilo nova linija
- **Obrazloženje:**
  - ① Linux dozvoljava da nazivi fajlova budu specijalni karakteri
  - ② Komanda može da čita listu parametara iz fajla

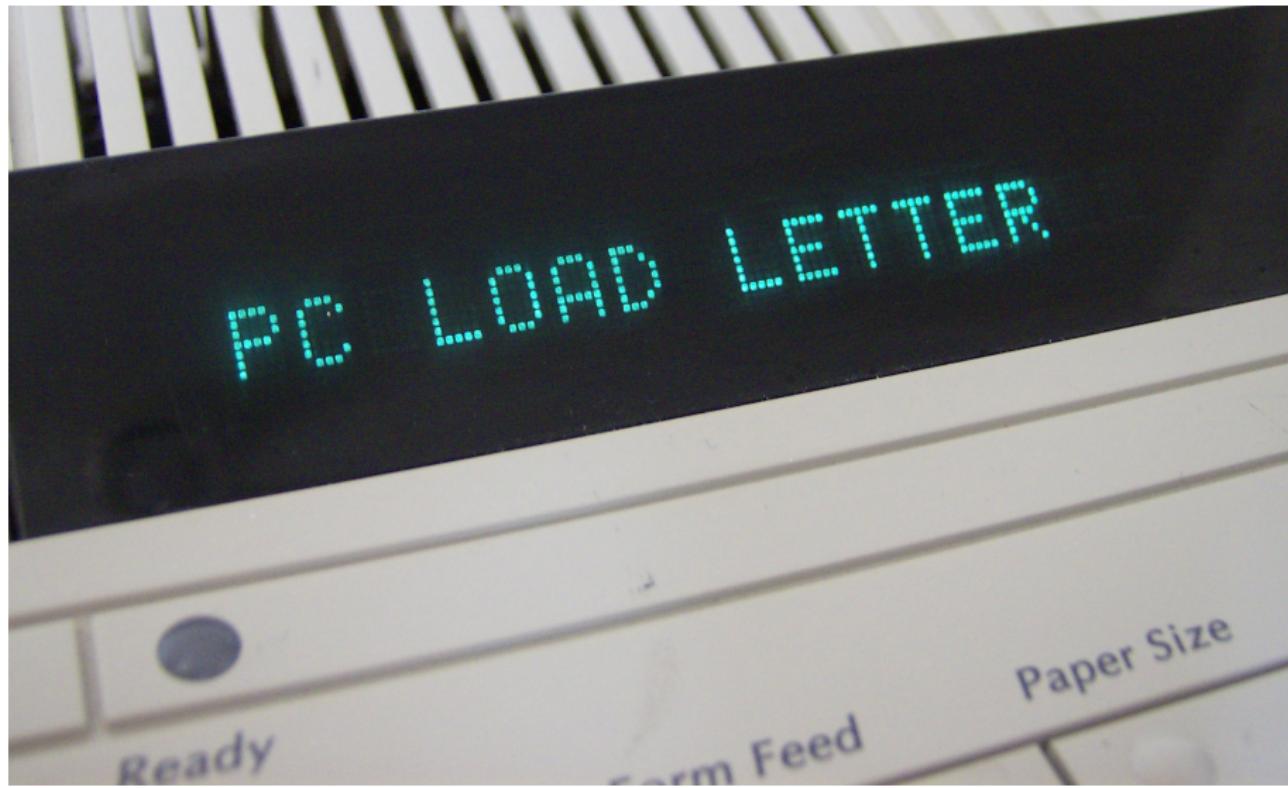
# Stari UNIX-ovi bagovi

- /etc/passwords
- lpr
- setuid proces koji ga pokrene ima sva prava
- prilikom nasilnog prekidanja pravi se file core u koji se upisuje poruka o grešci
- može se napraviti simbolički link na /etc/passwords

- **Situacija:** Ne može da se uloguje, login dugme stoji kao da je non stop pritisnuto, ali može da kuca druge stvari

- **Obrazloženje:** Postojali instalirani python2 i python3
- Kada se u terminalu ukuca python pokreće python2
- Pokušaj rešenja je bio da obriše python2 i napravi simbolički link na python kroz python3
- **Problem:** Sistem je koristio python2 za neke stvari
- **Rešenje:** Ući u live sistem, obrisati link i instalirati python2

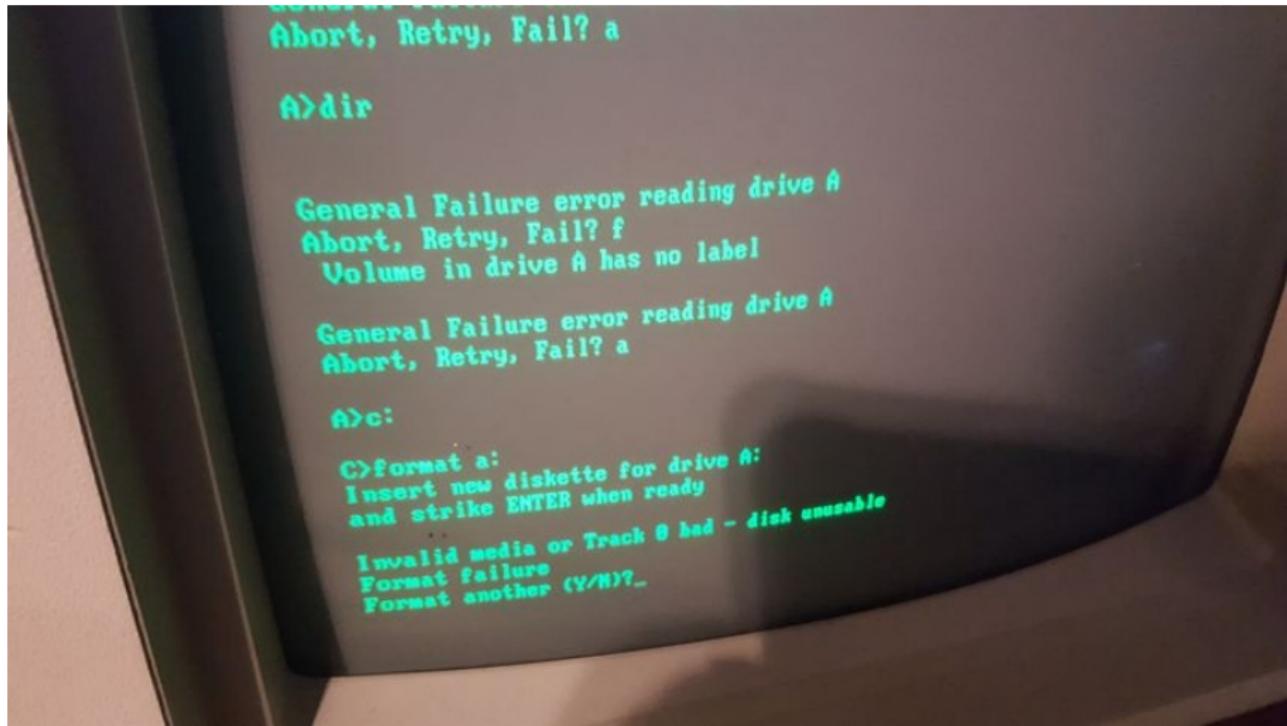
# Čudna poruka na ekranu



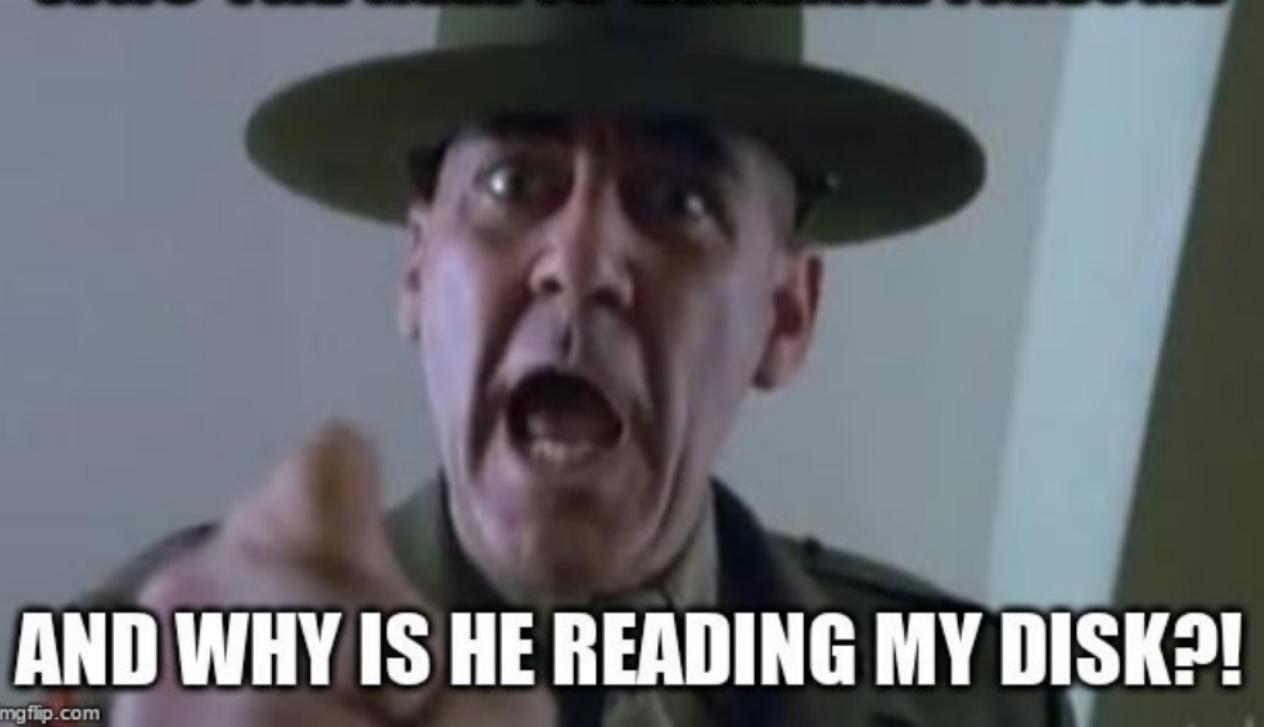
# Čudna poruka na ekranu

- HP LaserJet štampač
- Poruka o grešci i statusu iz legacy razloga može da ima samo 2 karaktera (PC - Paper Cassette)
- Instrukcija ('LOAD')
- Veličina papira (LETTER - US i Kanada)

# General Failure



**WHO THE HELL IS GENERAL FAILURE**



imgflip.com

- **Situacija:** Podešen je novi mail server i kada se šalje mail na univerzitet koji je udaljen više od oko 520 milja, mail ne biva poslat

## Zašto?

# The 500-mile email

- Konfiguracija je pisana na novijem SunOS sa Sendmail8, a koristio se stari
- Sendmail5 je imao predefinisanu vrednost vremena za čekanje od 0s i ukoliko u 0s ne dobije odgovor smatra je neuspešno slanje
- Postoji mali prozor vremena, koji ukoliko server koji prima mail nije pod velikim load-om
- Brzina svetlosti u optičkom kablu sa zakašnjenjem u ruteru i serveru daje oko 500 milja

# Ali i u Petnici...

- Na ruter je postavljena konfiguracija sa drugog rutera
- Postojala je razlika u verzijama sistema na ruterima
- Konfiguracija je bila za stariju verziju sistema i sve razlike u parametrima je sam dopunio
- Problem kada je ruter postavljen je što je deo mreže radio, a deo nije, jer je deo konfiguracije padao

# HTTP kodovi za greške

- 400 - Bad Request
- 403 - Forbidden
- 404 - Not Found
- **418 - ?**
- 451 - Unavailable For Legal Reasons
- 500 - Internal Server Error

# HTTP kodovi za greške

- 400 - Bad Request
- 403 - Forbidden
- 404 - Not Found
- **418 - I'm a teapot**
- 451 - Unavailable For Legal Reasons
- 500 - Internal Server Error

- HTCPPC: Protokol za kontrolu, monitoring i dijagnostifikovanje kuvala za kafu
- Prvoaprilska šala
- Emacs implementirao klijentsku stranu

# Još bagova sa okruženjem?

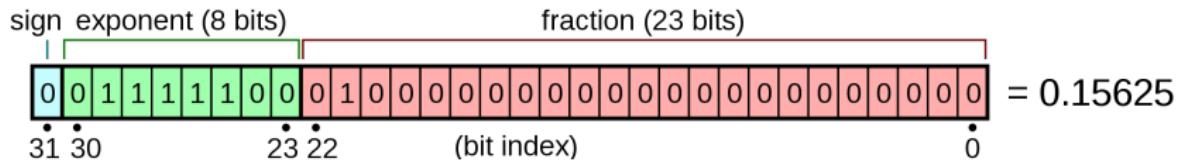
- Dirty cow
- PwnKit
- Y2K i Y2K38 problem
- log4j

# Bagovi sa tipovima

Tip	Veličina u bajtovima	Opseg vrednosti
bool	1 (8bit)	True / False
char	1 (8bit)	od -128 do 127
uint16_t	2 (16bit)	od 0 do 65535
int32_t	4 (32bit)	od -2,147483,468 do 2,147483,469

# Bagovi sa tipovima

- IEEE 754
- 32bit
  - znak 1 bit
  - eksponent 8 bitova
  - mantisa (frakcija) 23 bita
- 64bit
  - znak 1 bit
  - eksponent 11 bitova
  - mantisa (frakcija) 52 bita



# Greška "pas 38"

- **Situacija:** Imena pasa se upisuju u bazu, ali ako ima više pasa sa istim nazivom doda im se broj 1,2,...
- **Problem:** Kada u bazi postoji 37 pasa sa istim imenom, 38. ne može da se upiše
- 00100110 (8bit)

# Greška "pas 38"

- **Obrazloženje:** u bazi je polje char (6) a brojevi se zapisuju u formatu rimskih brojeva
- XXXVIII

# Švajcarski vozovi duhovi

- **Situacija:** Vozovi nestaju iz sistema
- **Problem:** Brojač osovina je 8bitni broj (do 256)
- **Obrazloženje:** Kada prođe voz sa tačno 256 osovina, desi se overflow i brojač se resetuje na 0, te se voz više ne vidi
- **Rešenje:** ?

- **Rešenje:** Promena regulativa, zabranjeni vozovi sa 256 osovina

## 3.7.4 Zugbildung

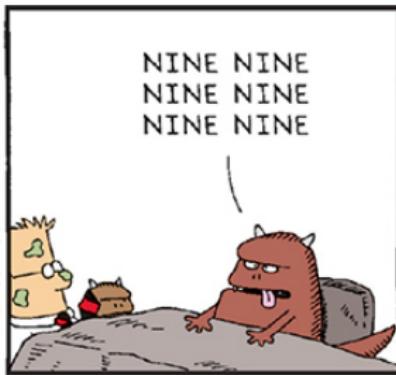
Um das ungewollte Freimelden von Streckenabschnitten durch das Rückstellen der Achszähler auf Null und dadurch Zugsgefährdungen zu vermeiden, darf die effektive Gesamtachszahl eines Zuges nicht 256 Achsen betragen.

"To avoid falsely signalling a section of track as clear by resetting the axle counter to zero, and thus to avoid [collisions], the total number of axles in a train must not equal 256."

## Random is not random



[www.dillbert.com](http://www.dillbert.com) [scootdams@aol.com](mailto:scootdams@aol.com)



10/25/00 © 2001 United Feature Syndicate, Inc.



# Random is not random

- Harverski random brojevi
- Pseudorandom brojevi
- Algoritam radi sa *seed-om*
-

# Lavarand (Silicon graphics)



## Press your luck



# Press your luck

- Vozač kamiona za sladoled Michael Larson - 110,237\$ (8 puta više od prosečnog igrača)
- Prvo se odgovara na trivija pitanja i tako se zarađuju "spinovi"
- Jako se kratko zadržava na slikama, te je odabir nasumičan

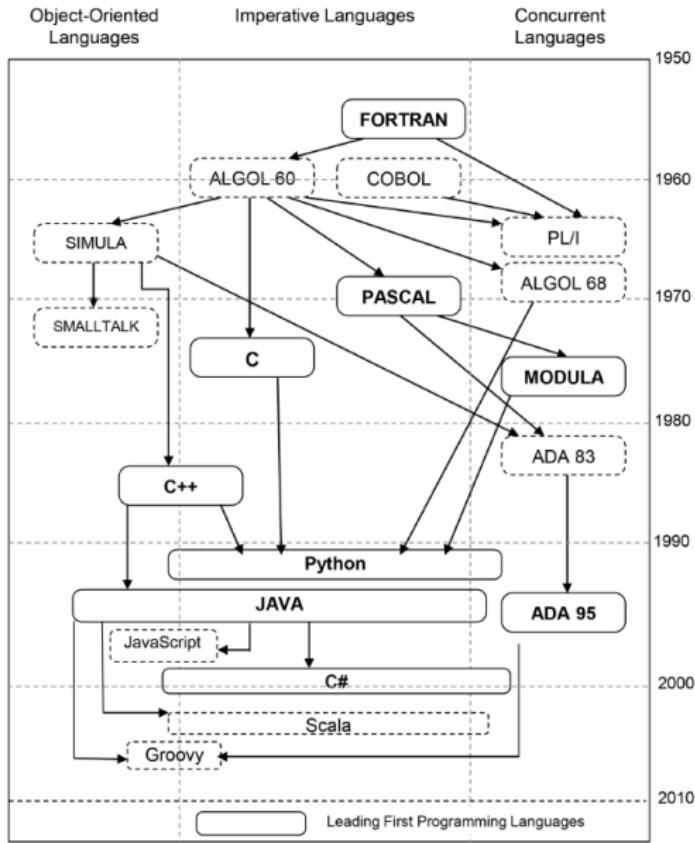
# Press your luck

- Zapravo je postojalo 5 predefinisanih krugova
- Snimao epizode i uočio i zapamtio sekvencu

# NULL - "billion-dollar mistake"

- null pointer exception
- Tony Hoare uvodi NULL u ALGOL W (1965)
- Naslednik ALGOL 60 (1960)
- Konferencija 2009.

# NULL - "billion-dollar mistake"



# NULL - "bilion-dollar mistake"

- **Situacija:**

- ALGOL W uvodi RECORD (class/struct)
- Potrebna referenca na stack-u na RECORD
- Uvodi se NULL, kada ne postoji podatak na heap-u

# NULL - "billion-dollar mistake"

```
RECORD PERSON (
    STRING(25) NAME;
    INTEGER AGE;
    REFERENCE (PERSON) FATHER, MOTHER
);
// pretpostavimo da postoji referencia R
// koja pokazuje na neku osobu
REFERENCE(PERSON)P, M;
P := FATHER(FATHER(R));
IF P = NULL THEN
    M := MOTHER(P)
ELSE
    P
```

- Link ka referenci

- HR unese zaposlenog i on nestane iz tabele
- Problem sa prezimenom

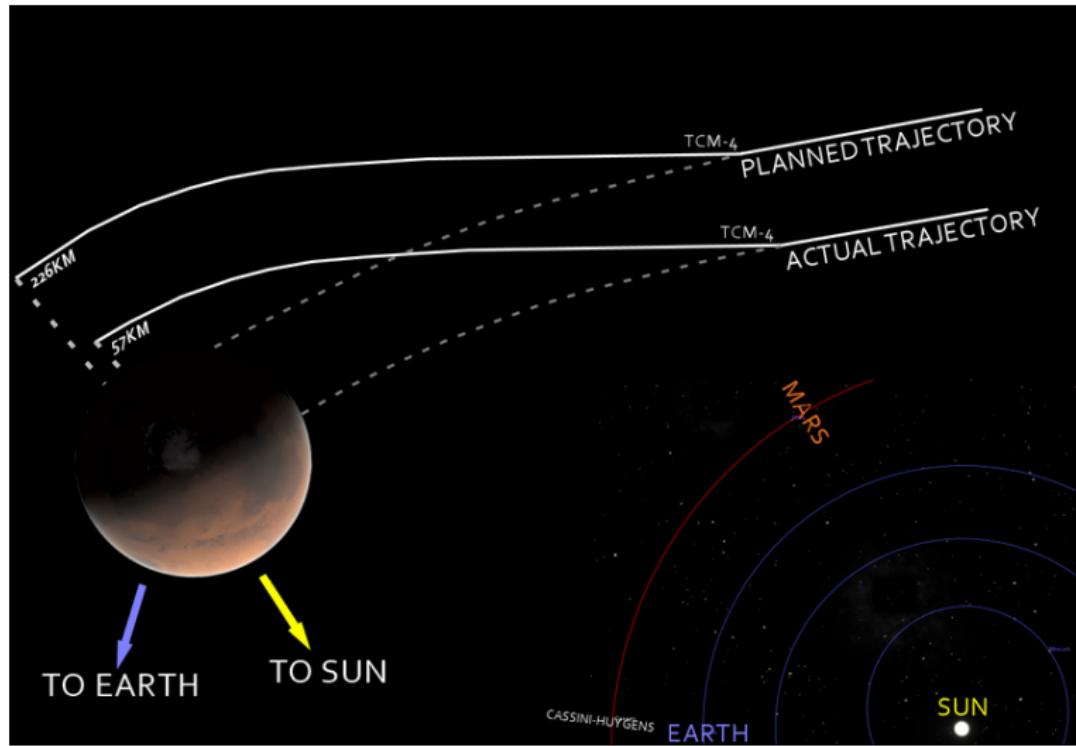
# Najskuplja '-'

- Mariner 1 - 1960thi NASA
- Matematičke formule se pretvarale u kod
- $\bar{R}$  "smooth over period of time"
- Ali greškom upisano  $R$
- 18.000.000\$

# Greška u orbiti Marsa

- Mars Climate Orbiter (1998)
- **Situacija:** Orbiter prilazi Marsu i odjednom pada
- **Problem:** Različite merne jedinice (mm i in)
- Lockheed Martin koristio inče
- 327.000.000\$

# Greška u orbiti Marsa

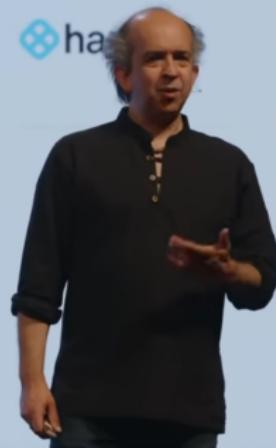


- European Space Agency (1996)
- Floating point bug - integer overflow
- **Situacija:** Raketa je nedugo nakon uzletanja skrenula i eksplodirala
- 500.000.000\$

- **Problem:** 64bitna floating-point vrednost je konvertovana u 16bitni označeni integer
- Broj koji predstavlja horizontalnu brzinu je bio veći od 32767
- Debugging podaci issecureli u memoriju za navigaciju
- Backup računar je imao isti kod
- Ili? Sistem za samouništenje se upalio

# Ariane 5

#FAIL • Kevlin Henney • GOTO 2022



```
1556
if L_M_DON_32 > 32767 then
    P_M_DERIVE(T_ALG.E_DON) := 16#7FFF#;
elsif L_M_DON_32 < -32768 then
    P_M_DERIVE(T_ALG.E_DON) := 16#8000#;
else
    P_M_DERIVE(T_ALG.E_DON) := UC_16S_EN_16NS(
        TDB.T_ENTIER_16S(L_M_DON_32));
end if;

P_M_DERIVE(T_ALG.E_DOE) := UC_16S_EN_16NS (TDB.T_ENTIER_16S
    ((1.0/C_M_LSB_DOE) *
     G_M_INFO_DERIVE(T_ALG.E_DOE))

L_M_BV_32 := TDB.T_ENTIER_32S ((1.0/C_M_LSB_BV) *
     G_M_INFO_DERIVE(T_ALG.E_BV));
if L_M_BV_32 > 32767 then
    P_M_DERIVE(T_ALG.E_BV) := 16#7FFF#;
elsif L_M_BV_32 < -32768 then
    P_M_DERIVE(T_ALG.E_BV) := 16#8000#;
else
    P_M_DERIVE(T_ALG.E_BV) := UC_16S_EN_16NS (TDB.T_ENTIER_16S(L_M_BV));
end if;

P_M_DERIVE(T_ALG.E_BH) := UC_16S_EN_16NS (TDB.T_ENTIER_16S
    ((1.0/C_M_LSB_BH) *
     G_M_INFO_DERIVE(T_ALG.E_BH)))
end LIRE_DERIVE;
--$finprocedure
```



38:33 / 1:03:45 • 101 things I learned in architecture school >

Scroll for details



## Slični bagovi

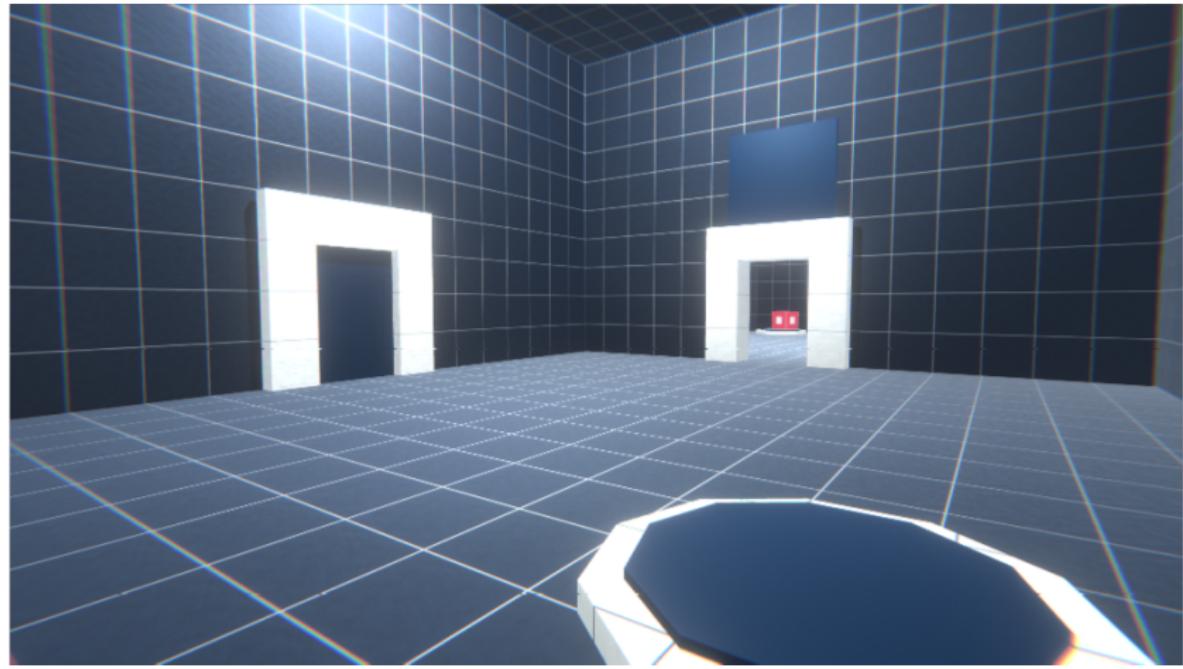
- Boeing 737 MAX
- Knight Capital
- Therac-25

# Bagovi u igricama

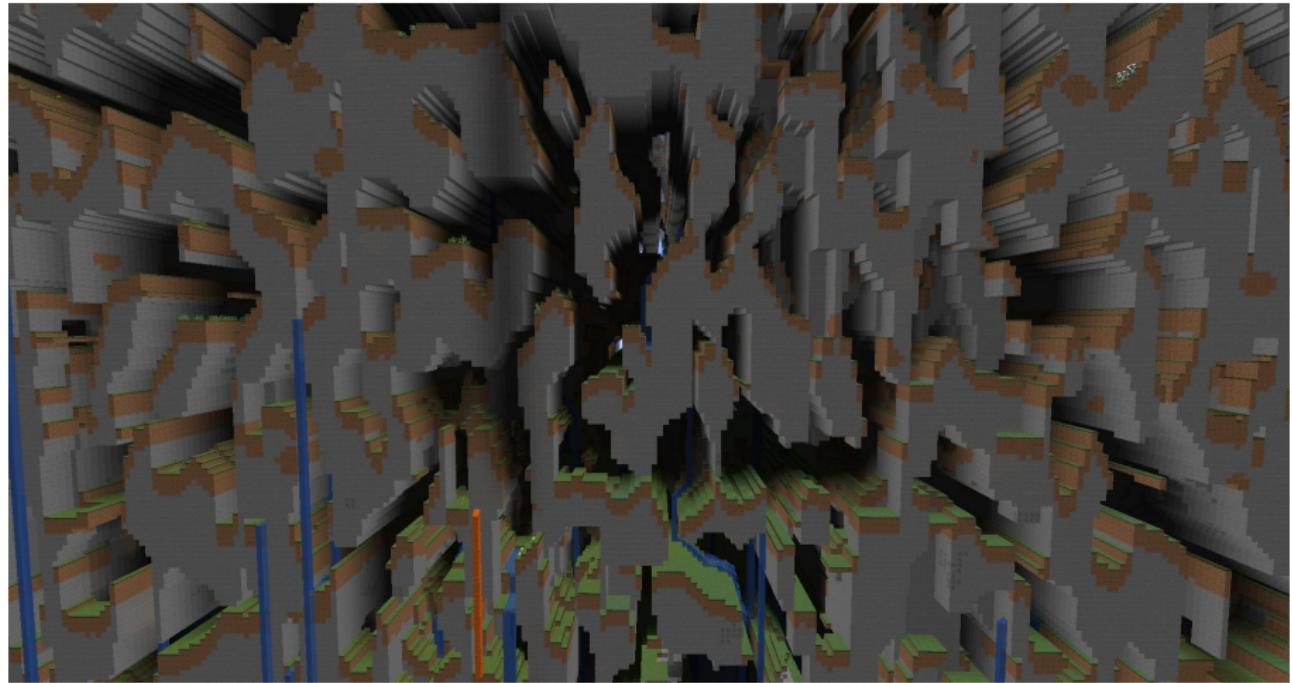
- Sa kakvim bagovima ste se susretali?

# Intentional bugs

- Grey-box testing



# Minecraft



# Minecraft

## 1024-bit Limit

$$>1.8 \times 10^{308}$$

### Maximum distance

#### 64-bit Limit

>9 223 372 036 854 775 807

Corner Farthest Lands	Edge Farthest Lands > 312 430 307 758 379 832					Corner Farthest Lands
Edge Farthest Lands	Corner Fartherer Lands	Edge Fartherer Lands 53 905 378 846 979 747-4 312 430 307 758 379 832			Corner Fartherer Lands	Edge Farthest Lands
Edge Fartherer Lands	Corner Farther Lands 1 004 065 811-53 905 378 846 979 747 32-bit Limit Super Landar > 312 430 307 758 379 832	Edge Farther Lands 2 147 483 647		Corner Farther Lands Clock Override > 312 430 307 758 379 832	Edge Fartherer Lands	Edge Fartherer Lands
Edge Fartherer Lands	Corner Far Lands > 312 430 307 758 379 832	Edge Far Lands 1 004 065 811 12 550 821	Corner Far Lands 12 550 821	Edge Far Lands 0-12 550 821	Edge Far Lands	Edge Fartherer Lands
Corner Fartherer Lands	Corner Far Lands	Edge Far Lands	Corner Far Lands	Corner Far Lands	Corner Far Lands	Corner Fartherer Lands
Corner Fartherer Lands	Edge Fartherer Lands				Corner Fartherer Lands	Corner Fartherer Lands
Corner Farthest Lands	Edge Farthest Lands					Corner Farthest Lands

# Minecraft

- Sky far lands
- Void far lands
- Far lands
- Vertex far lands

- 12.550.824
- Generisanje terena - Perlin noise
- Generisanje random brojeva, ali je teren "gladak"
- 16 octaves

- 171.103 pixela na mapi predstavljaju jedan blok
- $12.550.824 = 2^{31} / 171.103$
- integer overflow
- predmeti se drugačije ponašaju
- problem sa zvukom

# Wing Commander

Thank you for playing Wing Commander!  
C:\wc1>

# Wing Commander

Thank you for playing Wing Commander!

C:\wc1>

- Poruka greške pretvorena u pozdravnu poruku

- Kamera prestane da prati igrača
- Nasleđuje klasu PhysicalObject
- Trpi damage i biva "ubijena"

# Dodatni saveti

- Nazivi fajlova i poruke u programu
- Ne kopirati komande/kod bez razumevanja
- Debugger-i su prijatelji 😊

# Dodatni saveti

- Pisanje testova
- Rekurzija
- Endianness

# Reference

- Kolege ☺
- Programming's Greatest Mistakes - Mark Rendle - NDC Copenhagen 2022
- FAIL - Kevlin Henney - GOTO 2022
- Dirty programming, Aleksandar Beserminji
- I made a Game with Intentional Bugs
- Minecraft - Farlands

# Diskusija

- Kakve ste bagove sretali?

HVALA NA PAŽNJI!

Pitanja?