

# Bugs, bugs everywhere

- *Pregled nekih zanimljivih bagova* -

Diana Šantavec  
diana.santavec@gmail.com

Istraživačka stanica Petnica

23.04.2023.





# printf ne radi?

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

- **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@archhostname ~ >  
dianas@archhostname ~ >  
dianas@archhostname ~ >  
dianas@archhostname ~ >  
dianas@archhostname ~ > mkdir helloWorld  
dianas@archhostname ~ > █
```

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

# Ali radi na mom računar...

- **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

# Ali radi na mom računar...

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

```
dianas@archhostname ~/P/b/bin > hexdump -C CRLF
00000000  31 32 33 0d 0a 34 35 36                |123..456|
00000008
dianas@archhostname ~/P/b/bin > hexdump -C LF
00000000  31 32 33 0a 34 35 36                |123.456|
00000007
dianas@archhostname ~/P/b/bin > □
```

# Ali radi na mom računar...

```
dianas@archhostname ~ > 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@archhostname ~ > □
```



# 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"

# Wierd filemanes making weird behaviours

- **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

# 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



- **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)

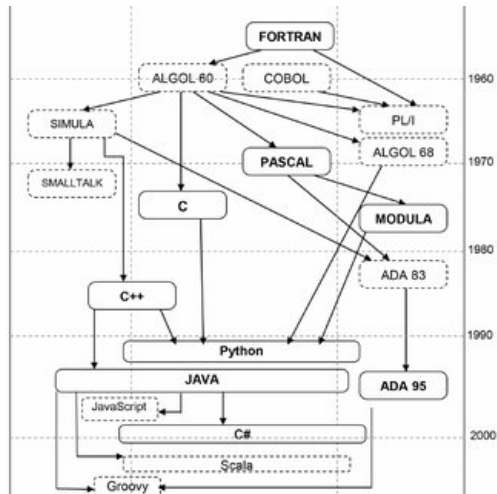
- **Obrazložjenje:** u bazi je polje char (6) a brojevi se zapisuju u formatu rimskih brojeva
- XXXVIII



# 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"



- **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"

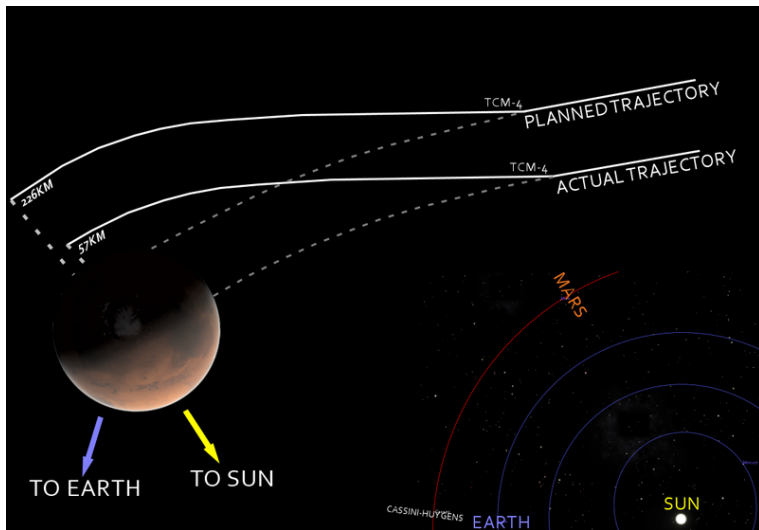
```
RECORD PERSON (  
    STRING(25) NAME;  
    INTEGER AGE;  
    REFERENCE (PERSON) FATHER, MOTHER  
);  
// pretpostavimo da postoji referenca R  
// koja pokazuje na neku osobu  
REFERENCE(PERSON)P, M;  
P := FATHER(FATHER(R));  
IF P = NULL THEN  
    M := MOTHER(P)  
ELSE  
    P
```

- *Link ka referenci*

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

- Mars Climate Orbiter
- **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
- 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 iscurili u memoriju za navigaciju
- Backup računar je imao isti kod
- Ili? Sistem za samouništenje se upalio

goto;



1555

```
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
    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
```

5.1

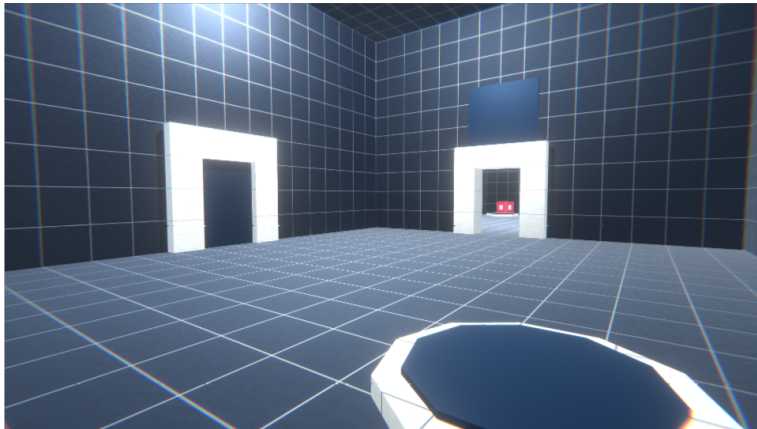
58:22 / 1:00:45 - 1st things learned in architecture school >

- Boeing 737 MAX
- Knight Capital

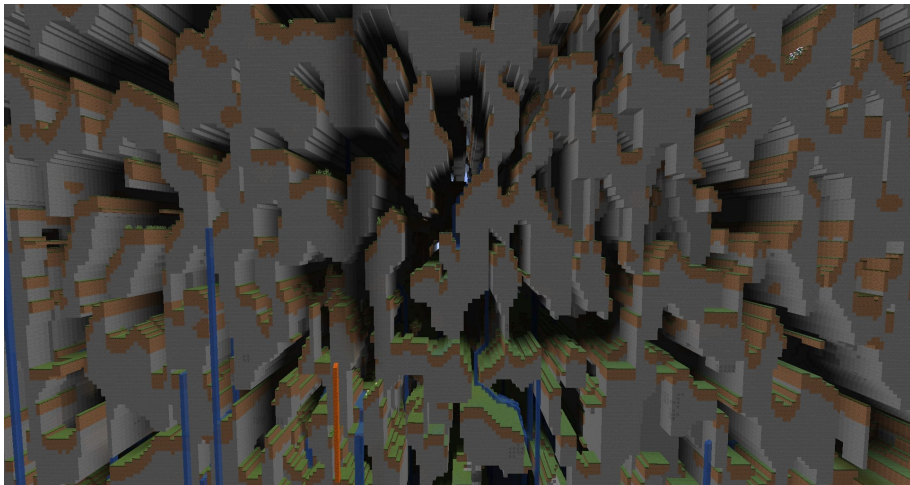
- Sa kakvim bagovima ste se susretali?

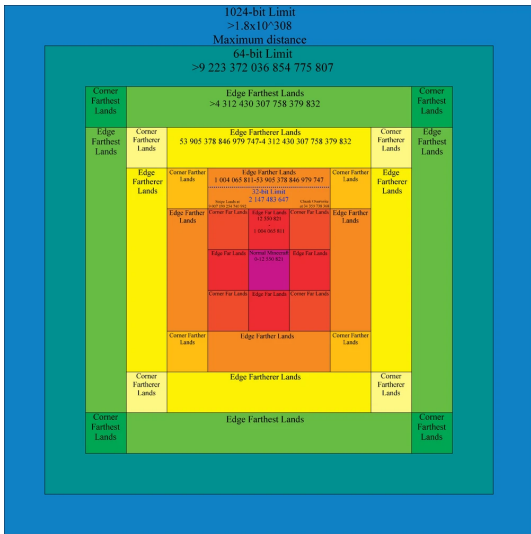
# Intentional bugs

- Grey-box testing



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

```
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"

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

- Pisanje testova
- Rekurzija
- Endianness

- 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

- Kakve ste bagove sretali?



Pitanja?