CISC 327
Software Quality Assurance

Lecture ??
“Piece of Crap”
Everything is broken

I went back to the store
They gave me four more
The guy told me at the door
“It’s a piece of crap”

PIECE OF CRAP

—Neil Young
1. “Error: Success”

• Logic for error handling:

```c
if ((attempt_something()) == NULL) {
    ...
    // ← if errno was not set, or “...” resets errno, errno could be 0
    printf("Error: %s\n", strerror());
    // ...which might be printed as “Success”
}
```

2. “Dear 0 Dunfield:”

August 25, 2008

Joshua Dunfield
Montreal, QC CA

Dear 0 Dunfield,

Thank you for making your reservation at the YWCA HOTEL, VANCOUVER. We have made the following reservations for you as listed below:
3.

Tony Hoare - Wikipedia
https://en.wikipedia.org/wiki/Tony_Hoare
Sir Charles Antony Richard Hoare FRS FREng (born 11 January 1934), commonly known as ... I call it my billion-dollar mistake. It was the invention of the null ... Null pointer - Hoare logic - Occam

Null References: The Billion Dollar Mistake - InfoQ
https://www.infoq.com/.../Null-References-The-Billion-Dollar-Mistake-Tony-Hoare

25 Aug 2009 ... He talks about that decision considering it "my billion-dollar mistake". ... If the billion dollar mistake was the null pointer, the C gets function is a ...
3. Null Pointers

• Types include some things and not others
  – Integers do not include 3.14159
  – Booleans do not include “sorta-kind”
  – A flying cocktail shrimp is not a QBASIC Front End session, because a flying cocktail shrimp is completely unlike a QBASIC Front End session
  – Why should null (or NULL, or nil, or None) be considered a QBASIC Front End session?
3. Null Pointers

• Programming language theory:
  – Types have “inversion principles”, which say things like:
    • “If x is a bool, then either x == true or x == false.”
  – The inversion principle for a Session class that you want is:
    • “If s is a Session, then s implements the methods writeTransactionSummary() and ..., and has the instance variables ...”
3. Null Pointers

• Programming languages theory:
  – Types (in statically typed languages) can have “inversion principles”, which say things like:
    • “If x is a bool, then either x == true or x == false.”
  – The inversion principle for a Session class that you get in Java is:
    • “If s is a Session, then either (1) s implements the methods writeTransactionSummary() and ..., and has the instance variables ..., or (2) s == null, has no methods, and has no instance variables”
3. Null Pointers

- Programming in a language with null pointers is like having a hole in your (exo-)pocket
  - You are constantly at risk of your keys falling out
3. Null Pointers

• Sometimes null pointers are fine!
  – The inversion principle for trees looks like
    • If t is a tree, then **either**
      1. t is a branch node containing an integer key, a left subtree, and a right subtree, **or**
      2. t is an empty tree (a leaf) and contains no information
  – Null pointers happen to match this:
    • If t is a tree, then **either**
      1. t is a Node with an integer key, a left subtree, and a right subtree, **or**
      2. t == null, representing an empty tree (a leaf)
3. Null Pointers

• Sometimes null pointers are fine!
  – The inversion principle for **linked lists**:
    • If L is a list, then **either**
      1. L has a head and a tail, **or**
      2. L is the empty list and contains no information
  – Null pointers happen to match this:
    • If L is a list, then **either**
      1. L has a head and a tail, **or**
      2. L == null, representing the empty list

http://lambda-the-ultimate.org/node/3186
4. People’s Names

• http://www.kalzumeus.com/2010/06/17/falsehoods-programmers-believe-about-names/

• For example: a database with two fields, “firstname” and “lastname”, is tricky:
  – “lastname” is not necessarily a family name
  – both first and last names could contain spaces, numbers, apostrophes, accented characters, and characters not in the Latin alphabet
  – the first or last name could be empty
4. People’s Names

- [https://en.wikipedia.org/wiki/Indonesian_names](https://en.wikipedia.org/wiki/Indonesian_names)
  
  In general, Indonesian names fall into one of the following categories:
  
  - A single name, such as Sukarno and Suharto
  - Two (or more) names *without* a family name, such as Susilo Bambang Yudhoyono
  - Two (or more) names *with* a family name such as Abdul Haris Nasution or Mahyadi Panggabean
  - Two (or more) names *with* a patronymic, such as Megawati Sukarnoputri or Abdurrahman Wahid
5. Time

• http://infiniteundo.com/post/25326999628/falsehoods-programmers-believe-about-time
6. Gender

• https://medium.com/@malpinder/falsehoods-programmers-believe-about-gender-cf1a55085ab2
A general rule

• People are ignorant
• People don’t pay attention
• Programmers are people

• **Rule:** Anything that has to do with people is probably more complicated than you expect
• Listen to people who know more than you
7. Line Breaks

- Unix: line feed only (0x0A, ‘\n’, LF)
- Apple II, old Mac OS: carriage return only (0x0D, ‘\r’, CR)
- Windows, and the internet (“network line break”): carriage return followed by line feed (0x0D0A, ‘\r\n’, CR LF)
  - Billions of http requests have included these useless extra bytes
8a. Character Set Encodings

This is the UBC library’s checkout (“sign-out”?) receipt for a book whose proper title is

“Recherches sur la déduction logique (Untersuchungen über das logische Schließen) Traduction et commentaire par Robert Feys et Jean Ladrière.”
8a. Character Set Encodings

This ancient punch card has a much better approximation of the French é than the “modern” computer system.
8b. Unicode Flags

https://twitter.com/python_tip/status/1026354685891014656

Be careful when reversing #unicode strings. You may be surprised…

```python
>>> s = "Welcome in 🇬🇧"
>>> s[::-1]
'ɐW emocleW ni 🇧🇬'

(thanks @piskvor for the inspiration!)
```

The above is an image, because PowerPoint got very confused by the flags when I tried to paste the text.
8c. Manually Correcting Improperly Encoded Cyrillic

- Someone mailed a package to Russia
- Russian uses Cyrillic, which has various encoding systems
- The same string of bytes may look completely different depending on the OS/software encoding settings (like € becoming θ on the library receipt)
- The sender of the package didn’t have the right settings, so the Cyrillic address looked like a bunch of semi-random Latin characters with accents
8c. Manually Correcting Improperly Encoded Cyrillic

• The sender carefully hand-wrote the garbled name and address, but did write the country in French (RUSSIE) so the package made it out of France

• A Russian postal worker, apparently used to dealing with this, hand-translated the garbled address into Cyrillic by writing a tiny Cyrillic letter above each and every character

• The package arrived...
8c. Manually Correcting Improperly Encoded Cyrillic

8d. Millennials Killing Wingdings

- https://twitter.com/ow/status/1007265229183561728

“It’s short for <FONT FACE=WingDings>J</FONT>”
8d. Millennials Killing Wingdings

- “damn he is right”
  [link](https://twitter.com/andreasklinger/status/1007299455073202176)
Interlude: “Code comments.”

- https://twitter.com/amyengineer/status/1043541585911263232
Interlude: macOS filenames

• The original Mac OS supported
  \textit{VolumeName:FileName}

• The only “illegal” or “special” character was :, because it was used to separate the volume and file name

• When the Mac got directories, this became a general path separator:
  \textit{VolumeName:Dir:Subdir:FileName}

• A quirk was that unlike Unix, where you begin a path with / to mean “go up to the root”, on the old Mac you had to begin the path with : to mean “in the current directory”
Interlude: macOS Filenames

- When Apple shifted to OS X (now “macOS”), they switched to a file system based on Unix.
- Unix uses “/” as a path separator.
- For compatibility (back when Apple cared about that), if you used the Finder to rename a file to something with “/”, it would be stored as “:” instead (try `ls`).
- The Finder will not allow you to use “:” in filenames.
- All this, because of a decision Apple made around 1983.
9. The Unspeakable Filenames

- https://twitter.com/Foone/status/1058676834940776450
9. The Unspeakable Filenames


Do not use the following reserved names for the name of a file:

CON, PRN, AUX, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, and LPT9. Also avoid these names followed immediately by an extension; for example, NUL.txt is not recommended. For more information, see Namespaces.
Software and hardware

• Much more could be said about software, but the last three are about hardware
• A *Software* Quality Assurance course can mostly ignore hardware, but for *security*, hardware really can’t be ignored
10. Radio Emissions

- Melissa Elliott, DEFCON 2013
  https://www.youtube.com/watch?v=5N1C3WB8c0o

(as usual on YouTube, DO NOT READ THE COMMENTS)
11. Rowhammer

https://en.wikipedia.org/wiki/Row_hammer

“an unintended side effect in dynamic random-access memory (DRAM) that causes memory cells to leak their charges and interact electrically between themselves, possibly altering the contents of nearby memory rows that were not addressed in the original memory access.”
12. Using Software to Break Hardware

https://twitter.com/yoz/status/1006636464350695424

ferlatte 12 days ago
The Second Life updater just downloaded the updater.exe from the website and ran it with no validation. One day, that returned a 404.

Cool thing about Win32: if you try to run an EXE, Windows checks to see if it's a valid format (PE). If it's not, it assumes that it's a COM: 16 bit x86 instructions, no header, no validation.

The 404 page, when interpreted as x86 bytecode, effectively opened the LPT DOS device and wrote garbage into it.

Windows would map that into your actual printer driver in some cases if you had a printer connected directly to your computer. Cheap inkjet printers don't do any validation, so they would freak out, spew paper, and in one case, physically break.
PIECE

• OF
CRAP