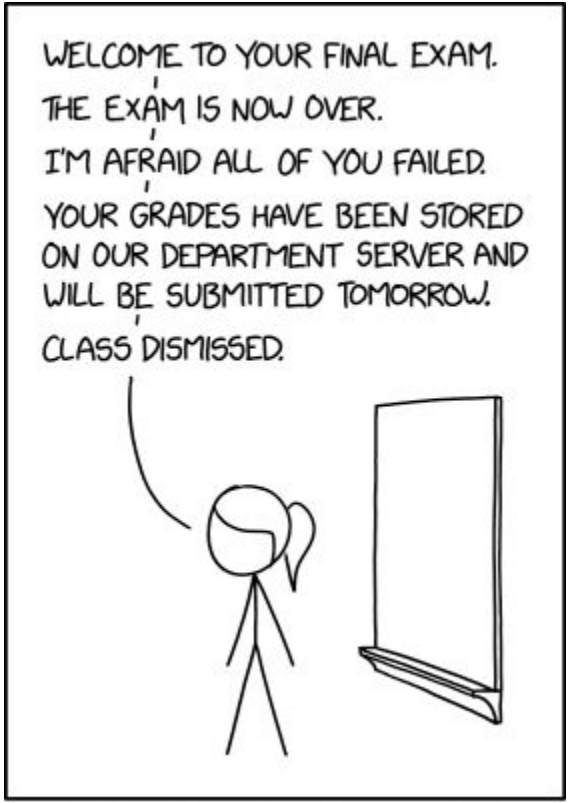
Security & ethics

iGCSE Computer Science

Security



CYBERSECURITY FINAL EXAMS


WIRED

Network security

Firewalls

Firewalls inspect the network traffic passing through it to determine whether or not to allow it to pass.

For example, you can create a firewall rule to allow no incoming traffic where the source address is “<insert address of person you don’t trust>”.

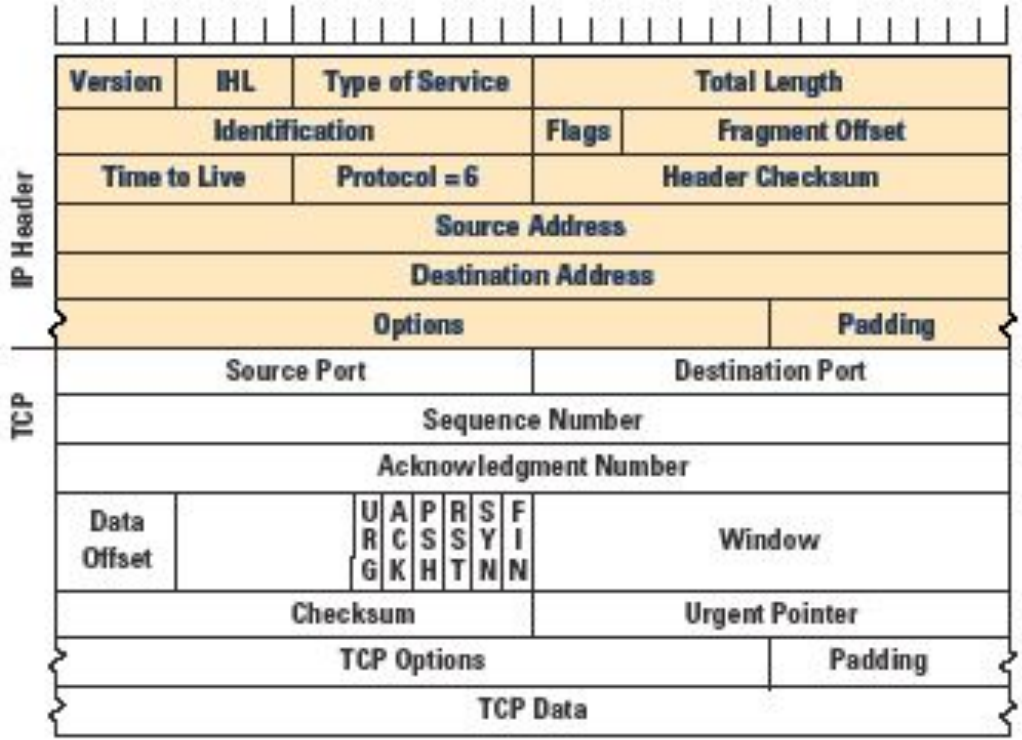
Most firewall rules focus on one or more of the following fields:

- Source address
- Destination address
- Source port
- Destination port

Firewall

A firewall is just software that inspects the bytes on the network. A firewall device will have (at least) two network cards: One for the internal network, and one for the external.

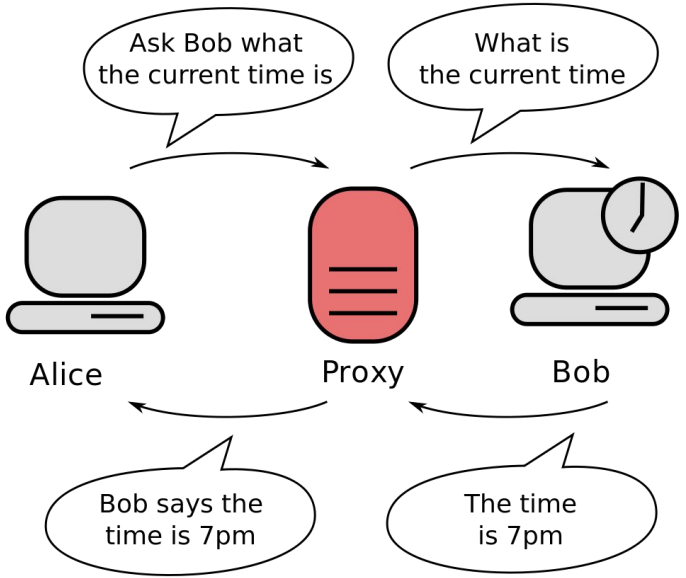
The firewall will inspect the data received on one card, and decided whether or not to then forward the packet to the other network.



Proxy servers

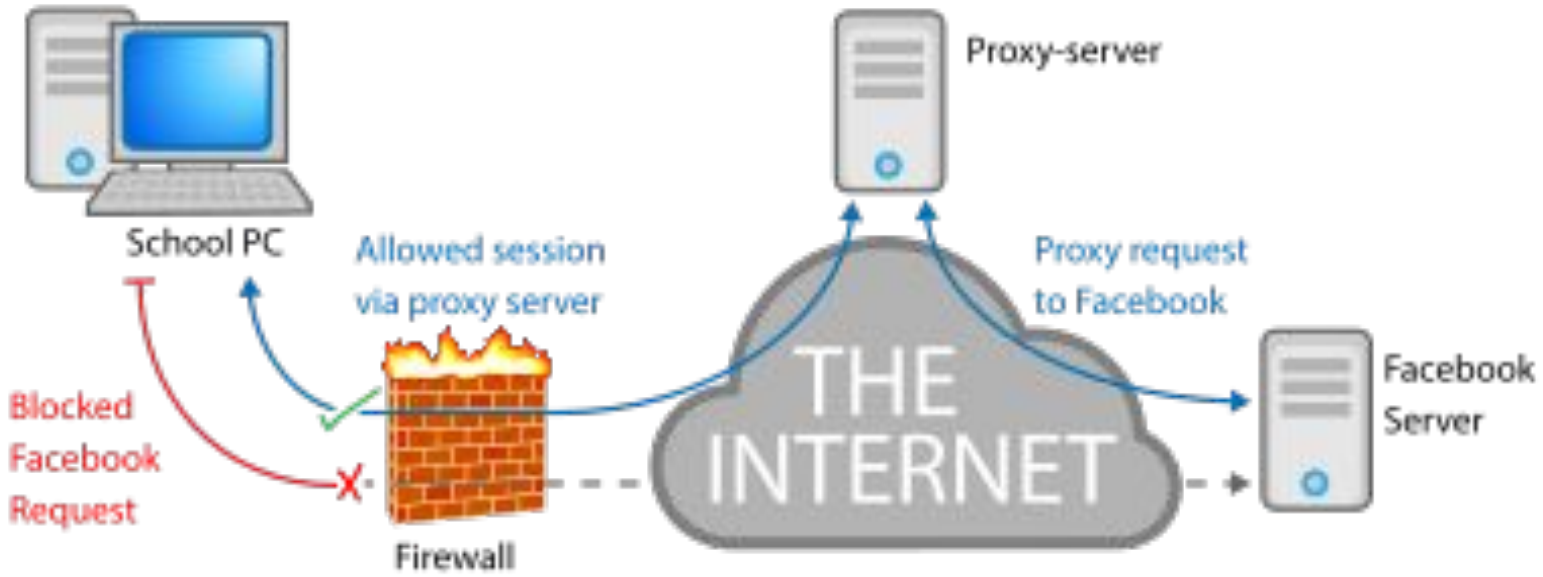
A proxy server is just a server (computer) that will receive requests, and forward those on to servers for their reply, before sending the reply to the computer that originally asked it.

Useful for switching between subnets such as from a private network to the public network. Your router at home would do this.



Proxy servers

Proxy's "other" use: To visit a "legitimate" server in order by bypass a firewall restriction.



Proxy servers

From a security perspective, be aware, because you are sending your traffic to a proxy, and it is receiving the replies on your behalf, it is able to see the content of the messages being exchanged between you and the ultimate destination. Yet another reason by using encrypted traffic is important.

Secure web browsing

Secure web browsing

Post video questions:

1. How are SSL and TLS related?
2. What is the role of a certificate?
3. Why must the issuer of certificates be trusted by both parties?
4. What version of TLS should you be using now?
5. How can you determine what protocol you are using on a given website (not in the article, google for instructions on how to check this with Chrome or your browser of choice)
6. What is the problem with self-signed certificates?
7. How is it possible for traffic to be encrypted but yet still subject to an attack

Proxy servers

Creating a basic proxy server in Python

https://www.geeksforgeeks.org/creating-a-proxy-webserver-in-python-set-1/

Encryption & hashing

What is encryption

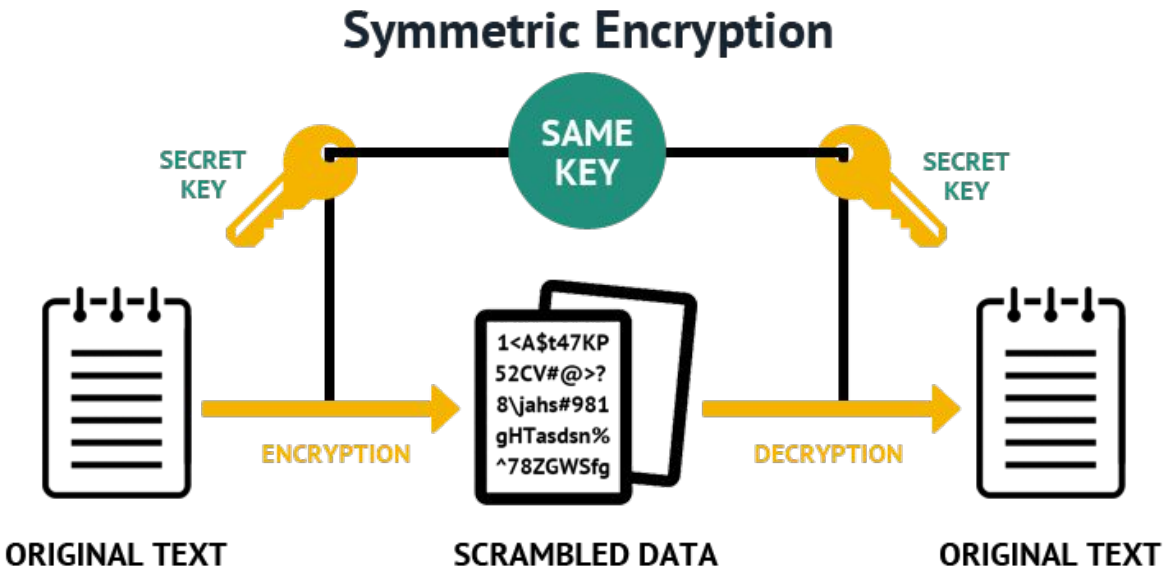
The process of converting information or data into a code, especially to prevent unauthorized access (Oxford dictionary).

Encryption as an idea has been around for a long time.

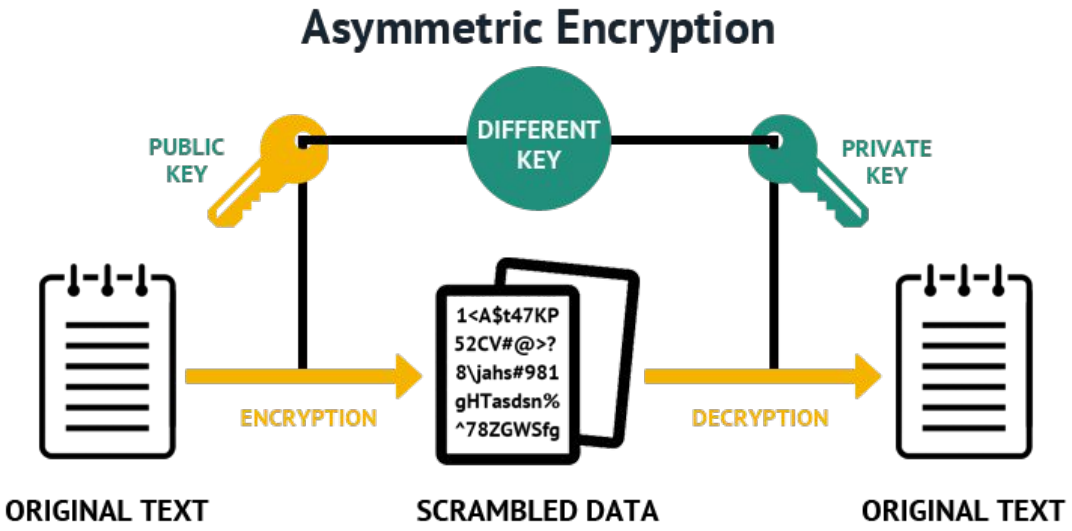
- The Caesar Shift Cipher Was Used By the Roman Army in 1st century BC
- Scytale was used by the Spartans in 7th century BC.

Modern encryption using computer algorithms come in two forms: Symmetric and asymmetric.

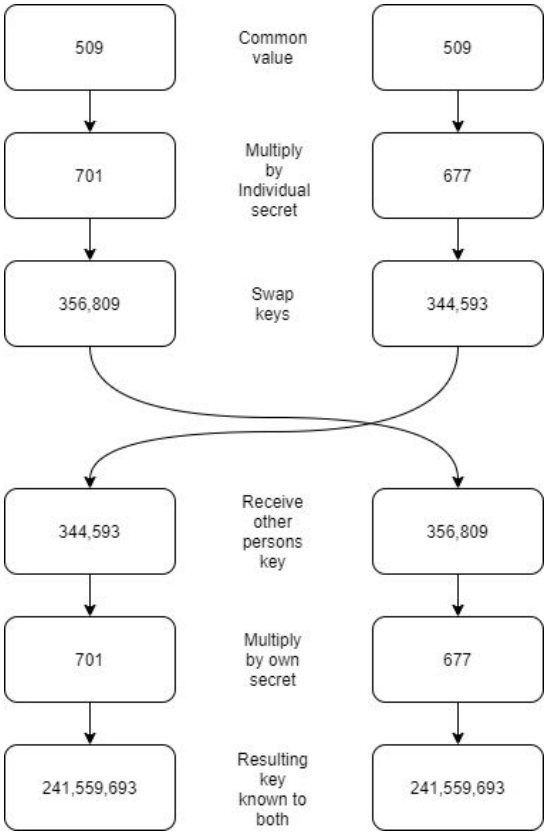
Symmetric encryption



Asymmetric encryption



Diffie Hellman key exchange



Symmetric encryption protocols

AES-256 (Advanced Encryption Standard) used by the US government. Keys are up to 256 bits. It considered impervious to any attack except brute force.. It is the default standard.

Blowfish. Keys are 32 bits to 448 bits, and so far the encryption has never been defeated. Popular as it is open source freeware.

RSA (Rivest-Sharmir-Adleman)
RSA keys are 1024 to 2048 bits long. However, the 2048-bit keys are recommended by the government and IT industry.

Triple DES (Data Encryption Standard).
3 x 56 bit keys, though due to a vulnerability so only effectively 112 bit. It is being phased out.

What is a hashing algorithm

Algorithm that operates one-way to produce a unique sequence of numbers that (in theory) can only be produced by the source data that created it. It can be used to verify that two blocks of data match.

Uses of hash algorithms

- Verifying content integrity

  Hashing Algorithms and Security - Computerphile (Tom Scott)
  https://www.youtube.com/watch?v=b4b8ktEV4Bg

- Cryptocurrency
- Password matching
- Law enforcement (DCMA copyright protection, CP detection recent Apple update)

Common hash algorithms

The phrase "Hello world!" in several hashing algorithms:

MD5	0d7a9db5a3bed4ae5738ee6d1909649c
SHA1	d3486ae9136e7856bc42212385ea797094475802
SHA256	c0535e4be2b79ffd93291305436bf889314e4a3faec05ecffcbb7df31ad9e51a
SHA3-256	d6ea8f9a1f22e1298e5a9506bd066f23cc56001f5d36582344a628649df53ae8

Status of each

- MD5 - broken
- SHA1 - broken
- SHA2 - partially broken
- SHA3 - safe

To see just how broken MD5 and SHA1 are, try the following website:
https://project-rainbowcrack.com/table.htm

Hashing passwords

Techniques

- Salting - what is it, why use it
- Different salts per password - why
- PBKDF2 - Hash algorithm designed specifically for passwords
    - Requires a salt as part of the algorithm
    - Runs 1000s of times
    - Try it at https://asecuritysite.com/encryption/PBKDF2y

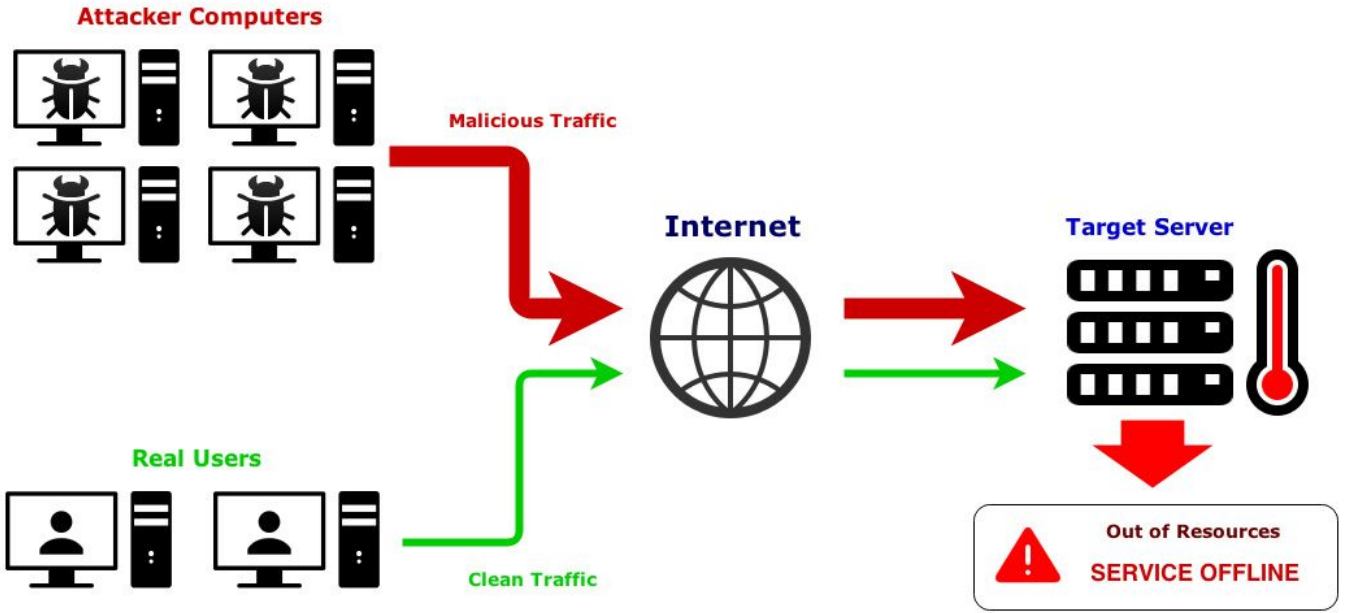
Hashing in Python

```
import hashlib

original = input("Message: ")

# Convert string to array of bytes
byte_array = original.encode('utf-8')

# Hashing the byte array
md5 = hashlib.md5(byte_array).digest()
sha1 = hashlib.sha1(byte_array).digest()
sha3_256 = hashlib.sha256(byte_array).digest()

# Printing
print("md5 =      "+md5.hex())
print("sha1 =     "+sha1.hex())
print("sha3_256 = "+sha3_256.hex())
```

Threats & mitigation

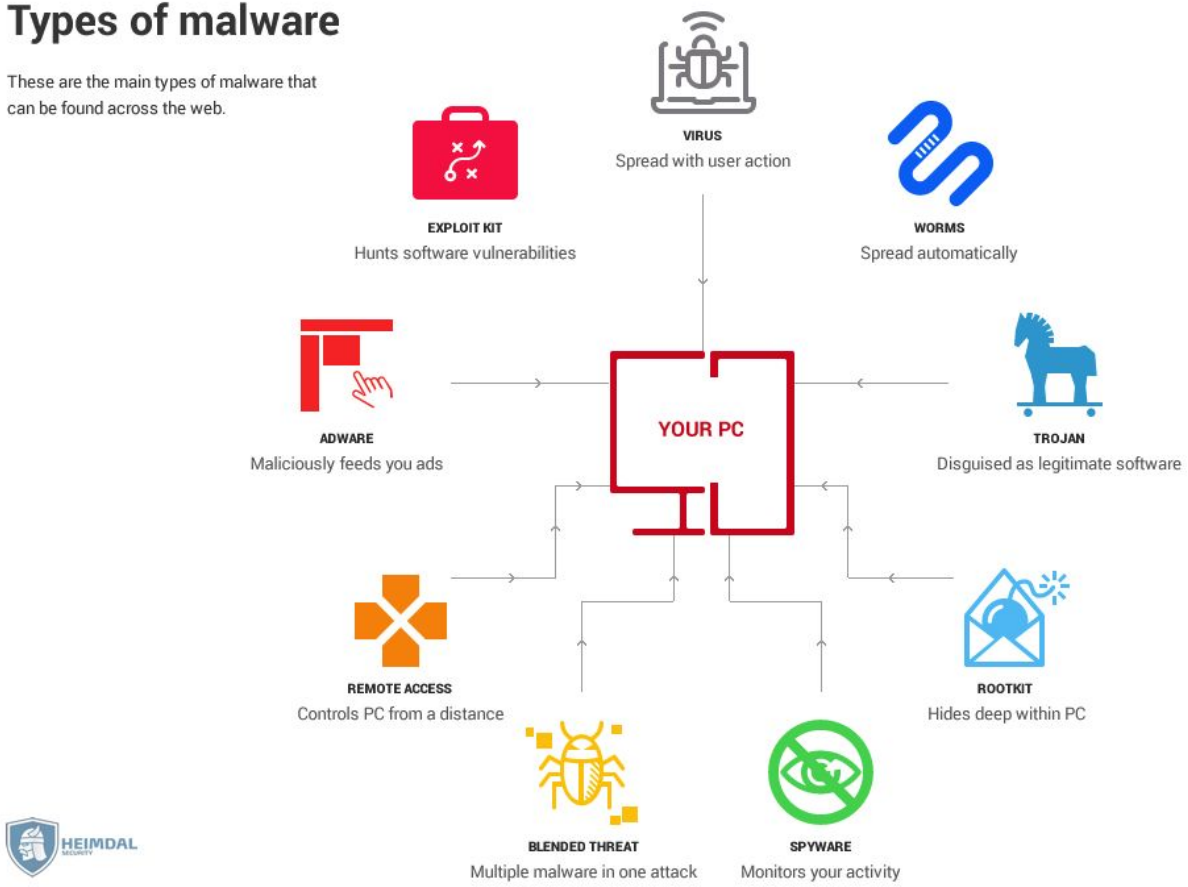
DoS: Denial of service

- What is denial of service?
- What is distributed denial of service?



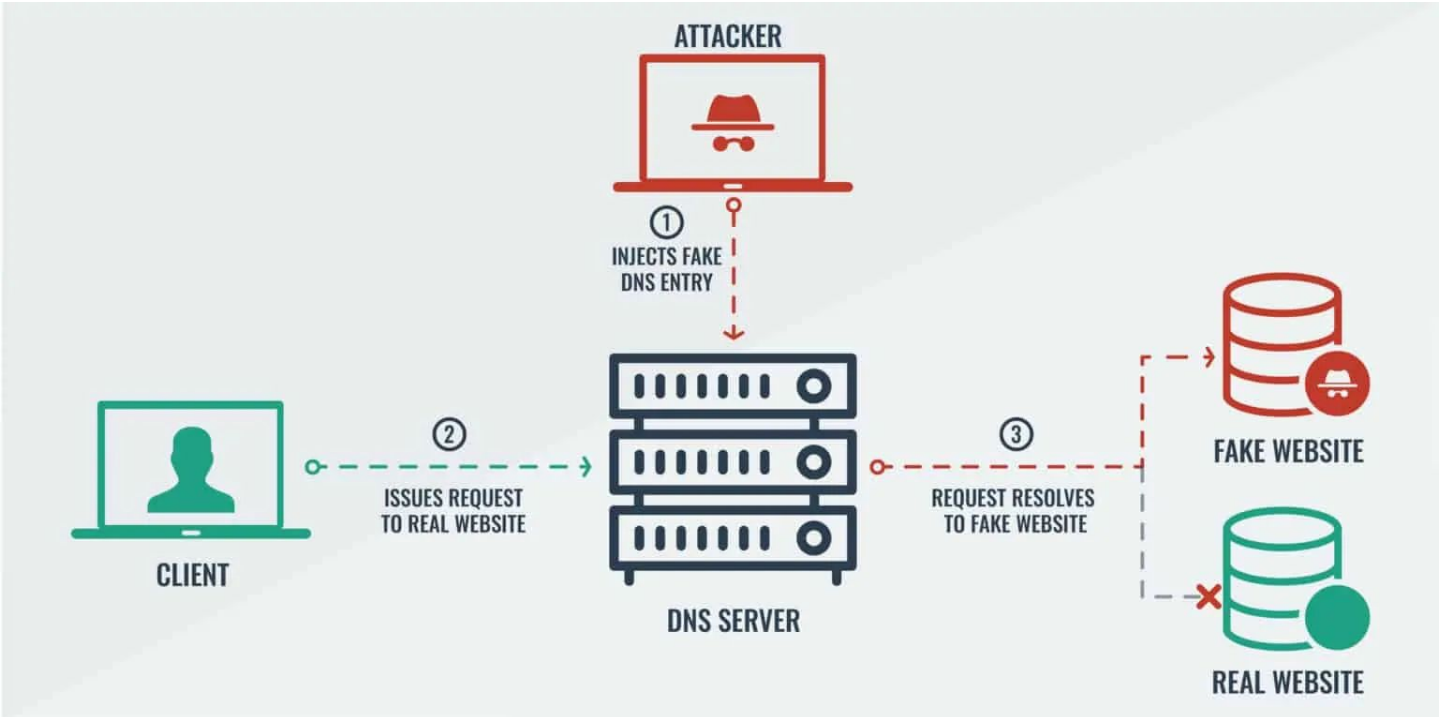
Malware

- Viruses and spyware are just the tip of the iceberg.



Social engineering

- Phishing
- Pharming



Phishing v pharming

	Phishing	Malware-based pharming	DNS server poisoning
URL	Different URL to real site	URL in address bar is same as real site	URL in address bar is same as real site
Attack vector	A link in an email that takes you to a malicious site*	An email attachment or link that installs malware on your device (then visiting a legitimate URL takes you to the fake site)	DNS server is attacked so no user action is required (visiting a legitimate URL takes you to the fake site)
Complexity	Simple for anyone to set up but fairly easy to spot	More difficult to execute and harder to identify	Requires advanced techniques and difficult to spot
Frequency and scope	One-time attack on a single user (each instance requires user action, although many victims can be targeted simultaneously with a mass email)	Repeated attack on a single user (once the malware is installed on the device, no further user action is required)	Repeated attack on multiple users (once the DNS server is poisoned, anyone trying to visit the legitimate site is affected)

Accidental damage

including corruption and human errors

Accidental damage

including corruption and human errors

Malicious attack

- Hacking, cracking
- Other forms of social engineering

Brute forcing passwords

Brute forcing is the method of trying every password, from 0000000 to ZZZZZZZ until you find a match.

There are tricks to speeding up a brute force. Dictionary matches. Common patterns (dictionary word + 1 number)

Hashcat is a program designed to brute force hashes against a file of target passwords.
https://hashcat.net/hashcat/

Compare the time it takes to brute force the same passwords when hashed with:
MD4, MD5, SHA1, SHA256.

Threats & mitigation

Validate your inputs

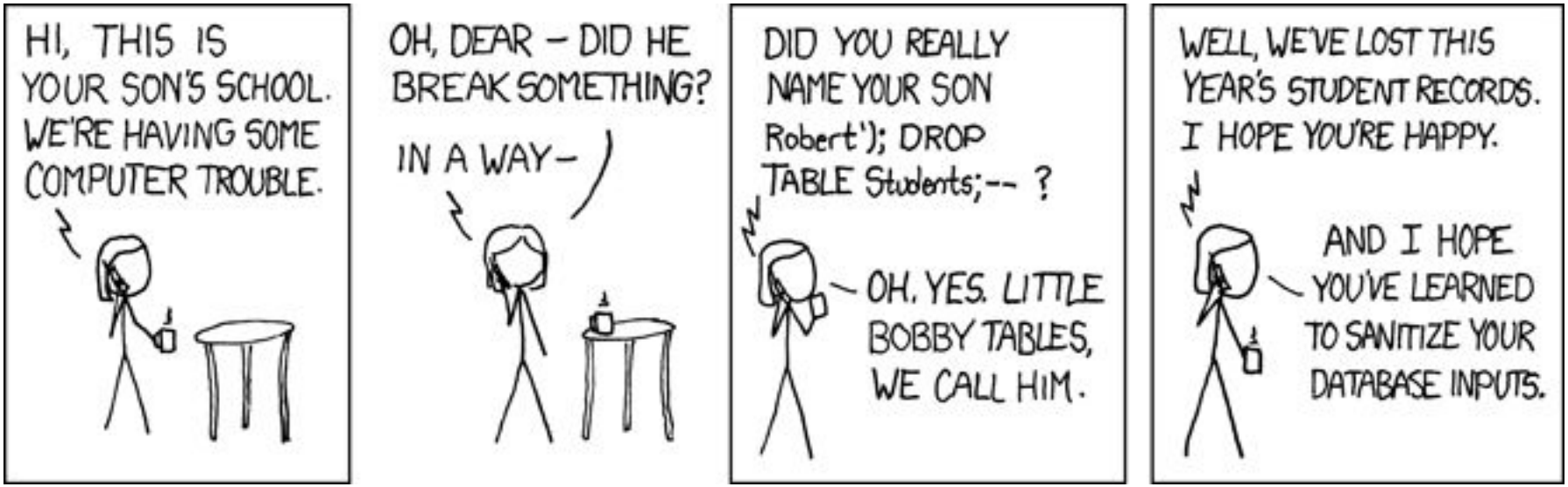
Consider the **heartbleed attack**.

Randall Munroe's excellent illustration of how the bug works here: https://www.explainxkcd.com/wiki/index.php/1354:_Heartbleed_Explanation

For details on the different real-world ways the vulnerability could expose information, read here: http://www.pabr.org/heartbleedtax/heartbleedtax.en.html

The bug is a great illustration of why input validation is such a critical part of security programming!

Validate your inputs, part 2



Validate your inputs, part 2

Consider this Python code...

```
sql = "INSERT INTO Students VALUES ('" + first_name + "', '" + family_name + "')";
```

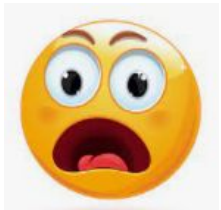
Set first_name to: `Robert'); DROP TABLE Students; --`

Substituted this becomes

```
sql = "INSERT INTO Students VALUES ('Robert'); DROP TABLE Students; --', 'Doe')"
```

SQL allows multiple commands in one string when separated by semicolons, so this actually turns into three commands!

1. `INSERT INTO Students VALUES ('Robert');`
2. `DROP TABLE Students;`
3. `--', 'Doe')`



Never trust the user! Always validate your inputs!

Don't use untrusted USB devices

University of Illinois study. 48% of drives dropped around campus were picked up and plugged into a device then had files opened. https://foundersec.substack.com/p/usb-keys-will-end-you

Malware protection tools

Antivirus software scans a file, program, or an application and compares a specific set of code with information stored in its database. If it finds code that is identical or similar to a piece of known malware in the database, that code is considered malware and is quarantined or removed

Backup, backup, and again I say back up!

When was the last time you backed up your files?!

Secure programming

Don't make passwords worse

If a password is properly hashed, it won't matter how long it is. If you are ever told by a system the password has a maximum length, chances are it means they are storing it unhashed clear text! Run, run far away!

Modern password policy

A truly excellent article that is well worth your time to read.
https://www.troyhunt.com/passwords-evolved-authentication-guidance-for-the-modern-era/

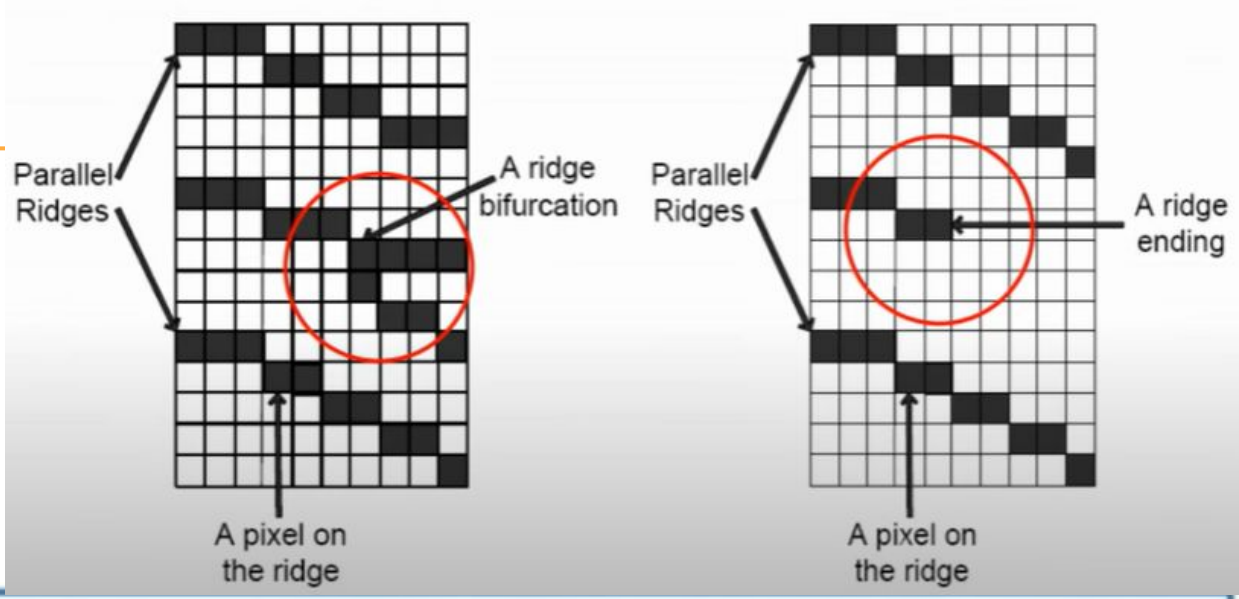
One time passwords

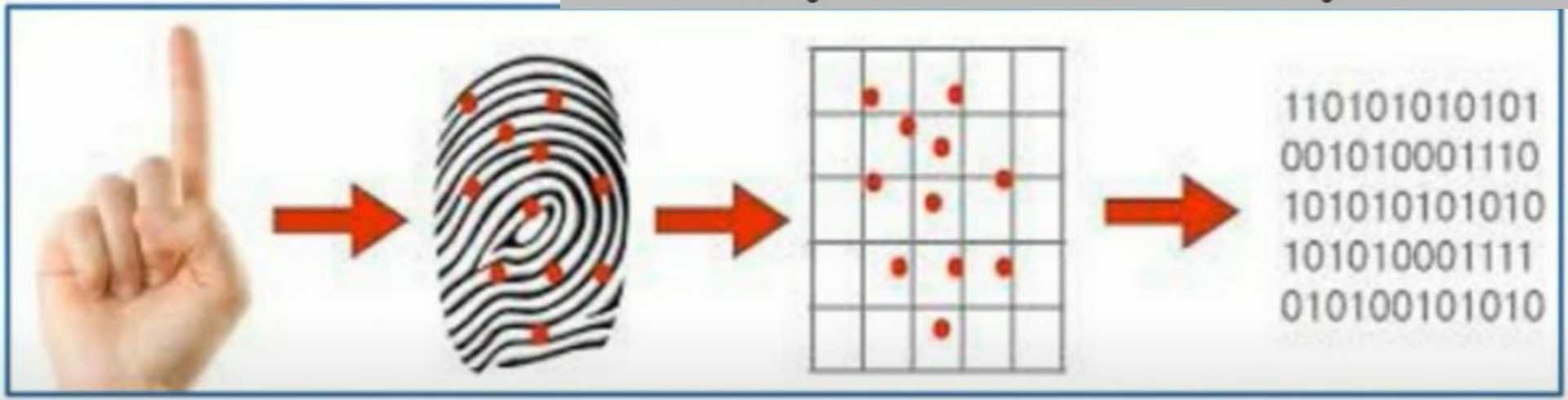
As a developer, if you care about your users security, you should enable one time passwords.

- PyOTP - The Python One-Time Password Library makes it easy. https://github.com/pyauth/pyotp

As a consumer, if you care about your security, you should enable 2 factor authentication on as many services as possible and use an app such as Authy.

Biometrics


Parallel Ridges
A ridge bifurcation
A pixel on the ridge
Parallel Ridges
A ridge ending
A pixel on the ridge


110101010101
001010001110
101010101010
101010001111
010100101010

Responsible programming

Guarding your user information

- You have an ethical obligation to treat your user's data with respect. Secure it as you would want your own data secured. Eg:
- Encrypt the database
- Firewall well managed and up to date
- Limit which members of the developer team have access to the customer data
- Log all access to customer data
- How much data do you legitimately need to be collecting?
- Be aware of any data protection laws, privacy laws that you may have to comply with.

Don't tempt the troll

- Anonymity issues
- People behave differently online when they think they are anonymous. Eg: Trolling.
- If you are going to develop software that allows for anonymous interaction between users, you need to consider what safeguards to put in place.

Be inclusive

Mallory Yu @mallory_yu · Jan 5

Replying to @mallory_yu

I added a space to the end of my name and that seems to have been a "workaround" because I now have an account, but REALLY?!?!

There are millions of people with my last name alone! How are they still "not valid" or recognized?! In 2021!!!

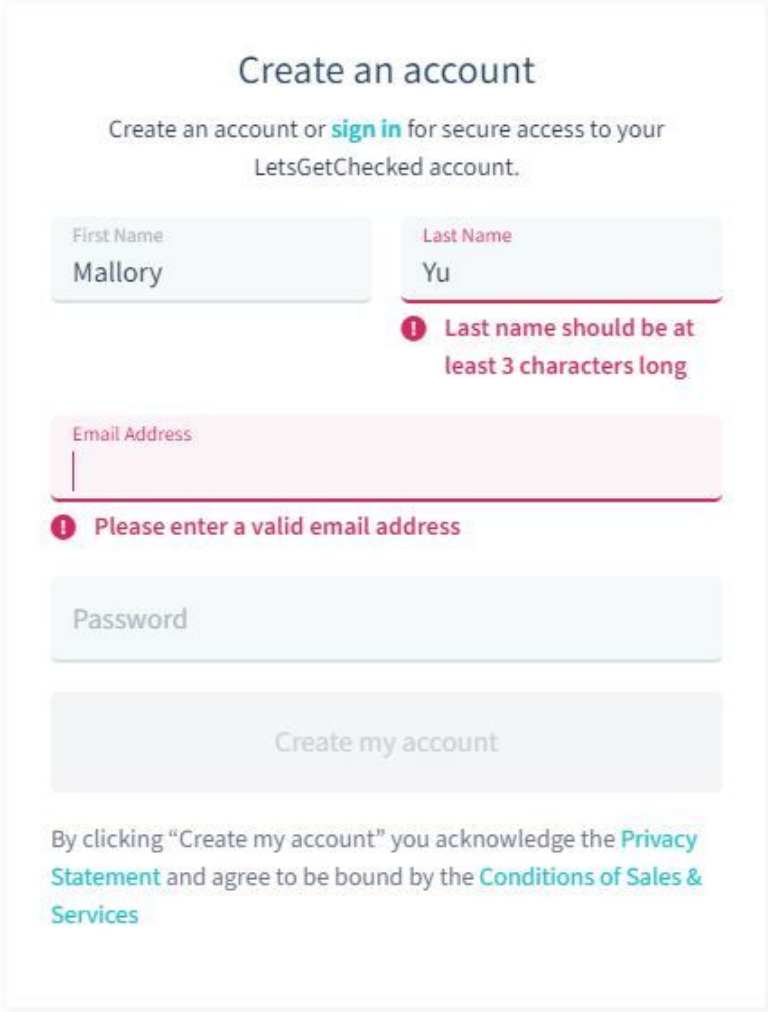
77 490 24.2K

Mallory Yu @mallory_yu · Jan 5

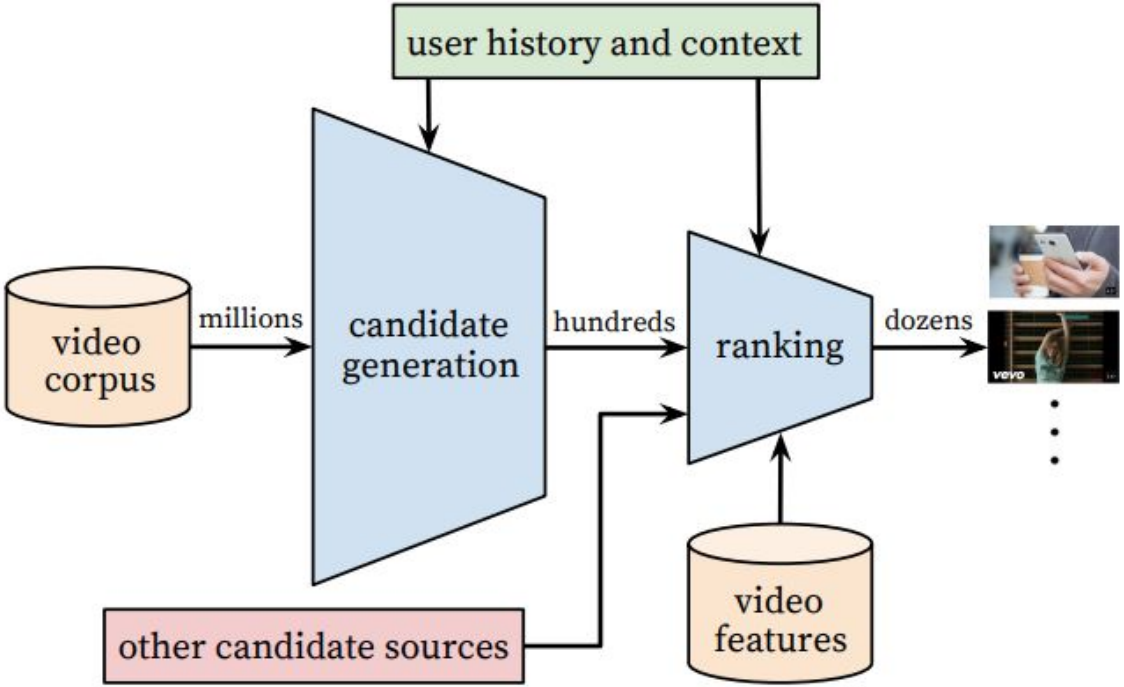
A few people have responded something like "this isn't racism because it's unintentional!"

So let me say: The original code was racist by not recognizing valid names, many of which are non-Western. Given our global interconnectedness, that's unacceptably racist.

231 992 25.5K



Recommendation engines



Is The YouTube Algorithm Radicalizing You? It's Complicated.

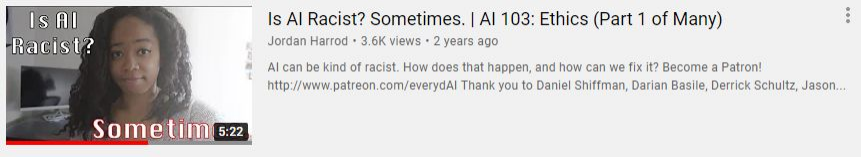
Jordan Harrod • 2.1K views • 1 year ago

In the past several years, there's been increasing concern that the YouTube algorithm contributes to alt-right user radicalization. Recently, researchers have tried to test this hypothesis,...

Recommendation engines

Software designed to maximise time/engagement on the platform doesn't know or care about the nature of the content. Its goal is to keep you on the site.

AI is not benign



AI is not benign

Want to see a half-naked woman? Well, you're in luck! The internet is full of pictures of scantily clad women. There are so many of these pictures online, in fact, that artificial intelligence (AI) now seems to assume that women just don't like wearing clothes.

Researches fed an image generation AI images of people cropped at the neck for it to auto-complete.

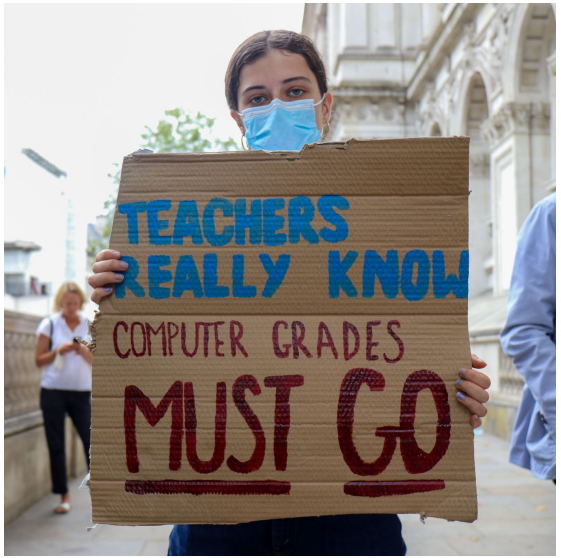
- For men: 43% were dressed in a suit
- For women: 53%!! were dressed in low cut tops or bikinis.

The reason? *Garbage in means garbage out: the AI "learned" what a typical woman looked like by consuming an online dataset which contained lots of pictures of half-naked women*

https://www.technologyreview.com/2021/01/29/1017065/ai-image-generation-is-racist-sexist/

Software deciding what university offers you get?

https://www.youtube.com/watch?v=BkTFqu8jyj0

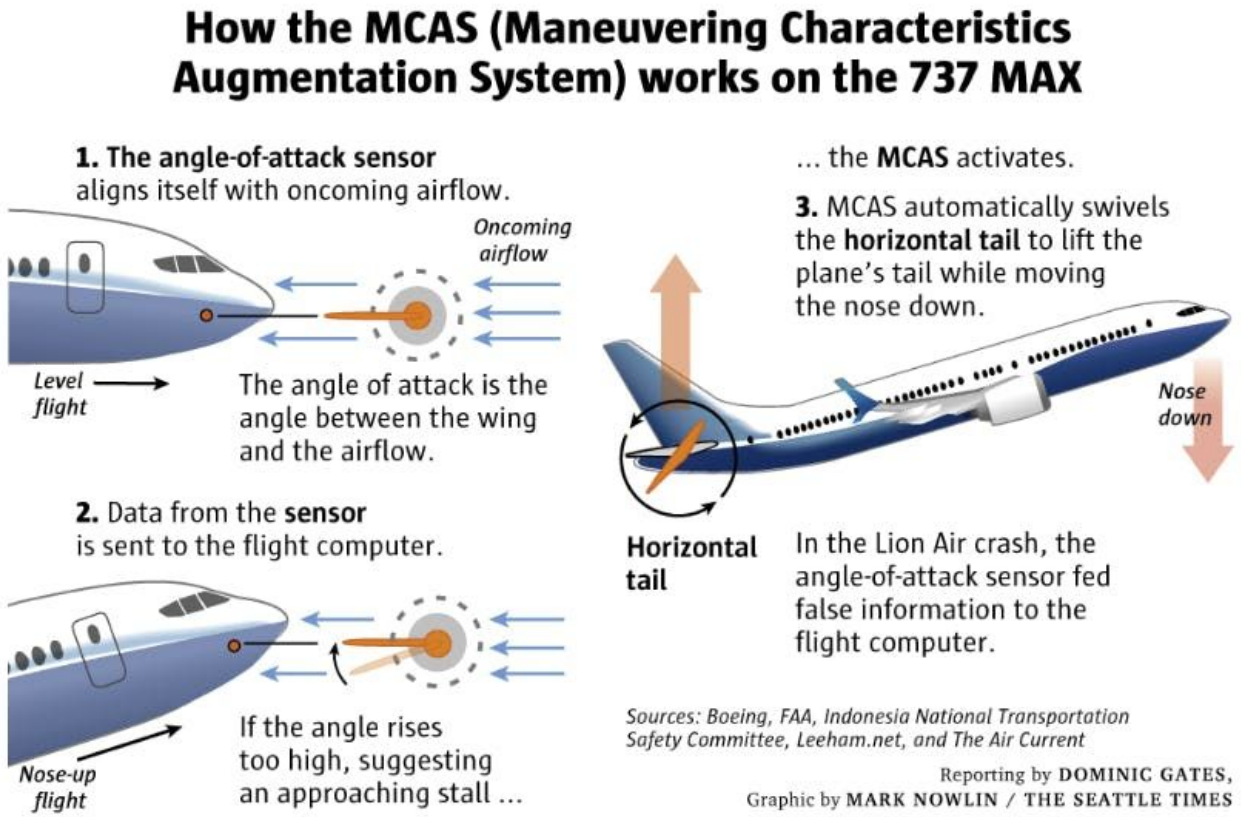


This AI Determines Your Grades | A-Levels + IB Scores 2020

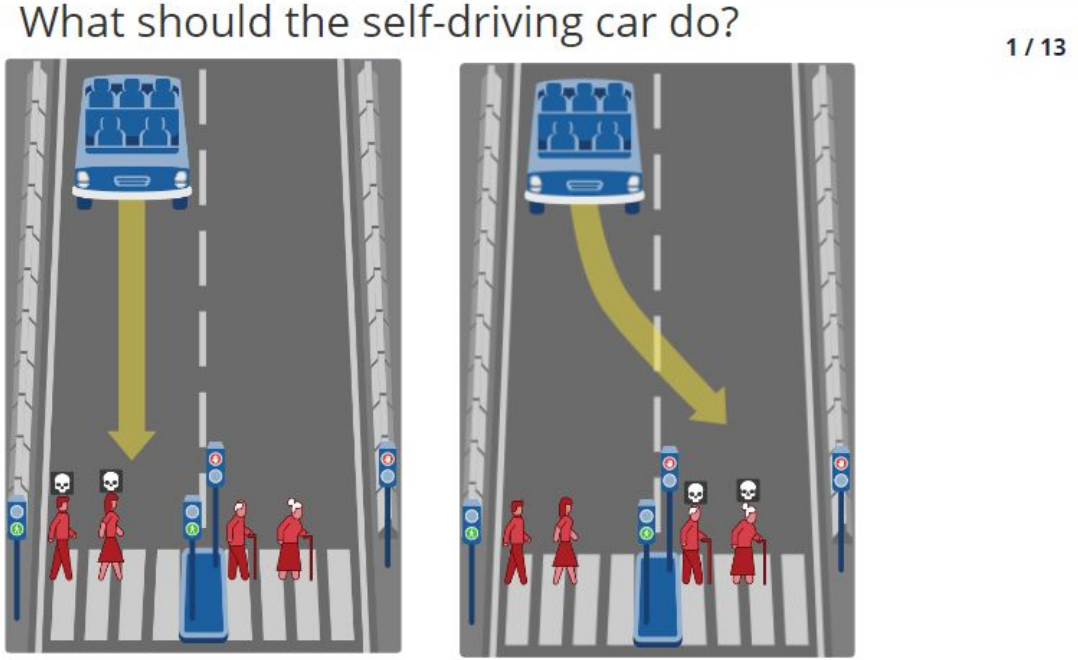
Jordan Harrod • 1.9K views • 9 months ago

Had your final exams cancelled because of COVID? Don't worry, this algorithm will just predict your final grades instead. If you'd like to take a class or learn something new without having...

Software in control of life and death?



Should software be tasked with "moral" choices?



Spend some time exploring the moral machine. What do you "train" the AI to do?

https://www.moralmachine.net/

Software licenses

Software licenses

Distinguish between:

- Commercial
- Freeware
- Shareware
- Open source

“free as in beer vs free as in speech”

Tasker

Discuss these Tasker project elements

flask_login
settings
class User()
load_user() function
@login_manager decorators
flask_login.current_user object

Review

Past paper questions