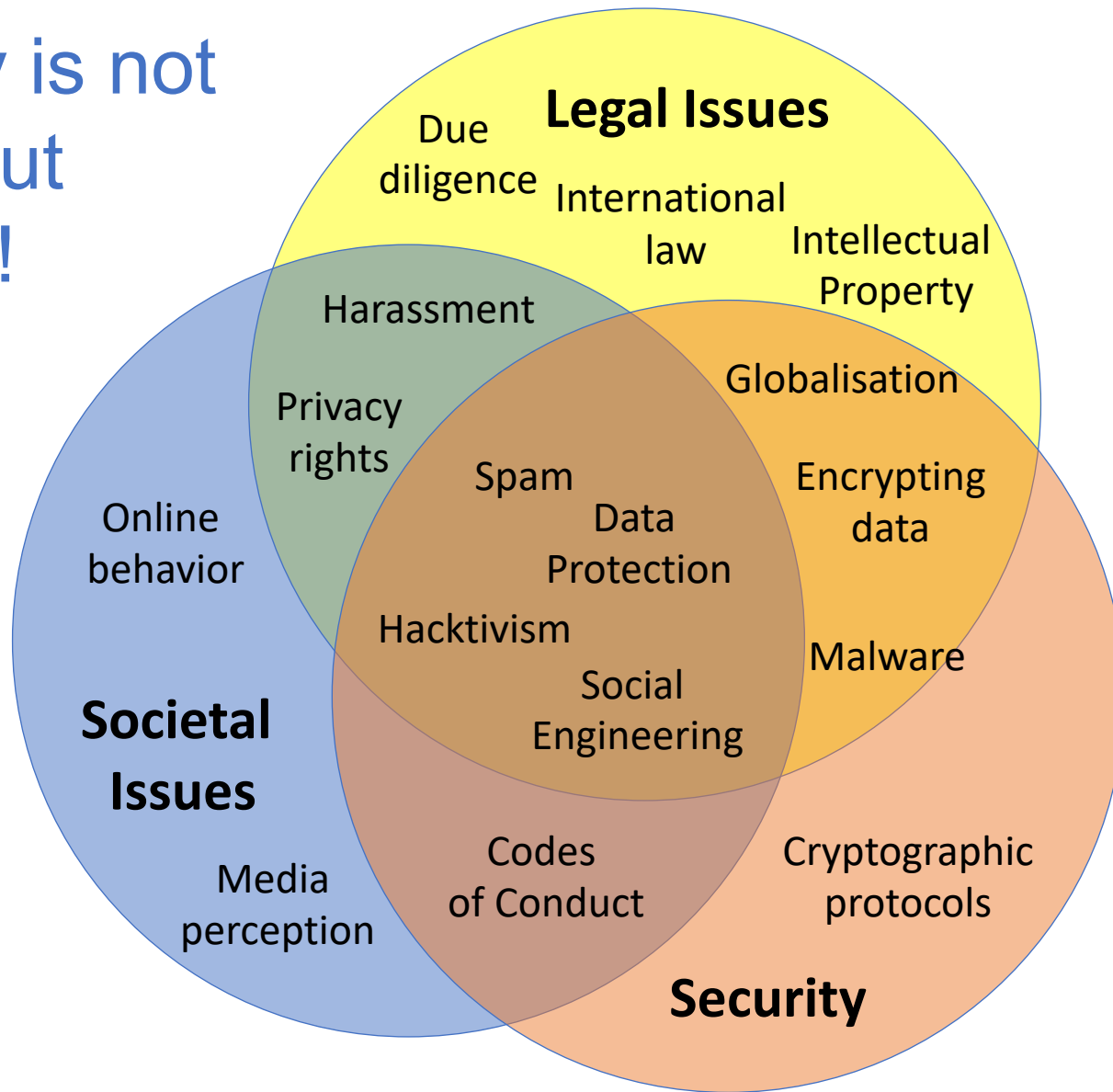


Security is not
just about
security!



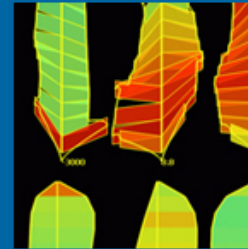
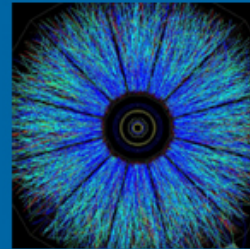
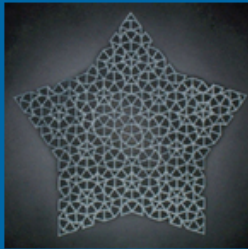


Swansea University
Prifysgol Abertawe

CS-130 Professional Issues

Computer Security Basics:

Malware



Lecture Learning Goals

Who are hackers?

What are the key terms we use in Computer Security?

What assumption do we make when we talk about securing a computer most of the time?

Why do we have passwords?

How do we store passwords?

Key Terms in Computer Security

Authorised users: The people who are meant to have access to a system

Hackers: People who attempt to gain access to a computer system in a way not intended by the systems owner

MalWare: Malicious software created or used by hackers that does something the owner of a system doesn't want to happen

Severity: The seriousness of a crime either from the perspective of the victim *or* from the perspective of judges and sentencing

Secure Systems: Secure against known threats and reasonable, theoretical ones – maybe!

Who are Computer Hackers?

White hat hackers – Security professionals brought in and paid specifically to test the security of a system

Grey hat hackers – People who gain access to a system without permission but not do anything malicious with the data

- Often only aim to make the company or users aware of vulnerabilities
- The escalation process if a company refuses to act is ethically challenging

Black hat hackers – People who will gain access to a system without permission and steal or alter data

- Not always for personal profit, sometimes it's an act of civil disobedience

Hacking In: Reading, writing, or worse?

Technically, there are two levels of seriousness in regards to computer crime: **Accessing** systems to view them or **Writing** to change systems and data

- Think *read-write-execute* permissions when you are familiar with Linux
- Sometimes this can make a difference in the eyes of judges

In reality, severity usually judged stems from the connection to further crimes (including creating holes for further computer crime)

- Either type can carry potentially very long criminal sentences or large fines
- International law and computer crime complicates things:
- Recently a UK based hacker was extradited to the US

Why is it hard to protect a computer if a hacker has physical access to it?

What steps can you authorised users take to protect it in this case?

Why don't users take this step?

The Key Assumption in Computer Security

Physical Security of End-Points: An important assumption in all of this is that malicious people don't have physical access to your computer

- We can simply pull data directly from a hard drive by plugging it into another computer
- **Shoulder surfing** attacks are also possible (next lecture discusses attacks more)
- Put a password on a file? You can just delete that part of the hard drive (you can't do this remotely so passwords do work online)
- Encrypting the Hard Drive is the only answer, but it makes it slow to use the system and may still be vulnerable if someone leaves their computer unattended

Basic Malicious Software or Malware

There are a range of different types of Software coded to deliberately sabotage a computer

- Note that many of these terms are not mutually exclusive as we go through them!

Computer Viruses – unwanted, self-replicating embedded code with a debilitating effect

- Different to a “bug” as it is deliberate
- Come in a wide variety of flavours
- Virus detection relies on recognising the code in viruses

Basic Malicious Software or Malware

Trojan Horses – software that masquerades as something else that does something malicious when executed

- Typically delivered in a download from a website or email
- PDFs, .doc files, .xls, .jpeg – all can act as a Trojan

Worms – a network propagated virus, meaning it spreads from computer to computer

Zombies – a software program that is used to control your computer remotely without your knowledge or a computer controlled in such a way

Technically advanced Malware

Rootkits - hide software's presence from users by gaining /root access to a system

- When the computers Operating System asks what software is running, a root kit lies to it and hides the software
- Can only be removed by re-installing the OS unless you know exactly what type of root kit is involved

BIOS RootKits – the evolution of the root kit

- Can only be removed by “flashing” (reformatting) the BIOS
- Considered to be theoretical only until (Check? Cambridge demo? 2015)

Key loggers – software that sits on a computer and logs the keys you press

- Installed with a *Trojan Horse*, hidden with *RootKits*

Password Protecting Systems

Passwords authenticate you as an **authorised user** based upon a **shared secret** between you and the system

Passwords are stored in a single, **hashed and salted** file typically called a **password file**

- Every website you enter a password on has a file like this as does your computer
- Access to it should, in theory, be tightly controlled so not even the company owning the website can see your password

Ever had your password sent to you in an email after you set it?

- Bad news because if it's lost and someone can link it to you they can use the password on that site and elsewhere...

Hashing

So we need to store passwords to check that you are giving the right one but we also must not store them?

- **Hashing** – a mathematical process (a bit similar to encryption) that takes data of an arbitrary size and **maps** it to a fixed size hash-value
- **Collision resistant hashing**– makes it really hard (mathematically speaking) to find data that maps to the same hash value
- Salting

Brute force attacks – hash and compare random phrases to the stored passwords but it can take a long time (years, decades, millennia)

Password cracking

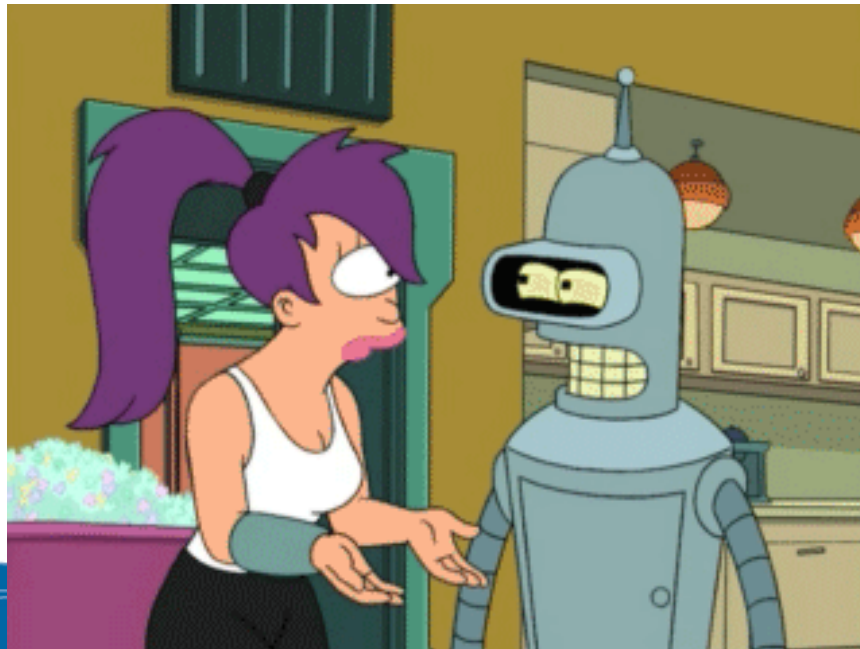
Dictionary attacks – encrypt non-random phrases like a dictionary (or list of common passwords!)

Rainbow table attacks – the smartest attack of all - store pre-computed, encrypted passwords and run the same attacks

Rainbow table attacks lead to the practice of **salting** in which websites add an arbitrary string to all passwords to drastically increase the time this type of attack takes if the password is complex

What about biometrics?

What about biometrics?



[illegible]

The 24 most common passwords of 2014

- | | |
|-------------------------|-----------------------|
| 1. 123456 (Unchanged) | 13. monkey (New) |
| 2. Password (Unchanged) | 14. login (Down 3) |
| 3. 12345678 (Up 1) | 15. abc123 (Down 1) |
| 4. qwerty (Up 2) | 16. starwars (New) |
| 5. 12345 (Down 2) | 17. 123123 (New) |
| 6. 123456789 (New) | 18. dragon (Up 1) |
| 7. letmein (New) | 19. passw0rd (Down 1) |
| 8. 1234567 (Unchanged) | 20. master (Up 1) |
| 9. football (Down 4) | 21. hello (New) |
| 10. iloveyou (New) | 22. freedom (New) |
| 11. admin (Up 4) | 23. whatever (New) |
| 12. welcome (Unchanged) | 24. qazwsx (New) |
| | 25. trustno1 (New) |

How can we relate the issues in computer security to Lessig's four modalities?

How can we relate the issues in computer security to Lessig's four modalities?

Law – the applicable Laws that relate to a piece of technology

Markets – the commercial factors that influence a piece of technology

Social norms – the ways that people interact with each other and technology, unwritten rules that govern how we behave

Architecture – any complex or designed physical structure

Lecture Learning Goals

Who are hackers?

What are the key terms we use in Computer Security?

What assumption do we make when we talk about securing a computer most of the time?

Why do we have passwords?

How do we store passwords?

Lecture Learning Goals

Who are hackers?

White, Grey and Black hat

What are the key terms we use in Computer Security?

Authorised Users, MalWare, RootKits, more!

What assumption do we make when we talk about securing a computer most of the time?

Physical security – without it we can't do much!

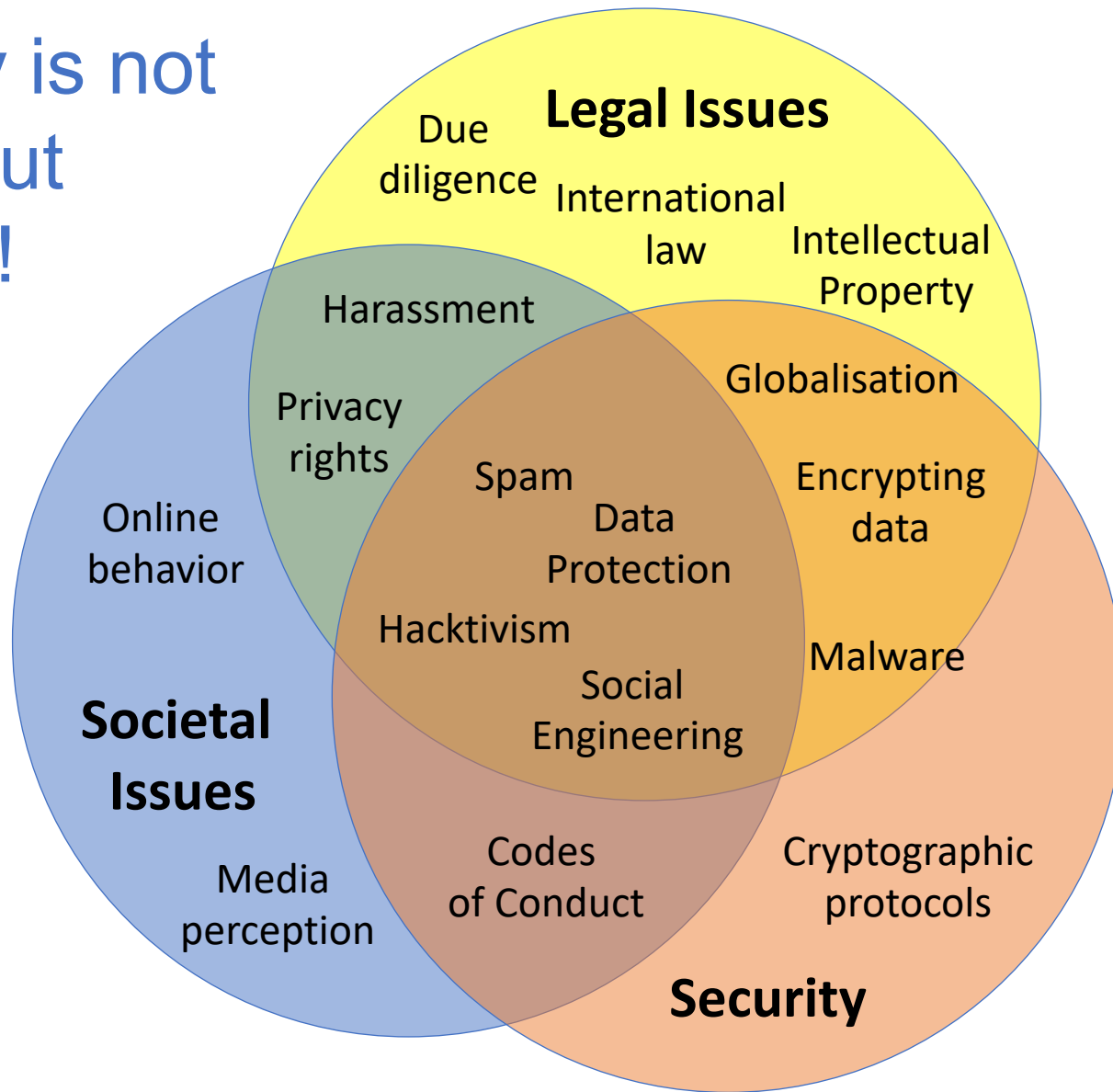
Why do we have passwords?

They act as a Shared Secret so we know who is an authorised user

How do we store passwords?

In an Encrypted, Salted Password file

Security is not
just about
security!



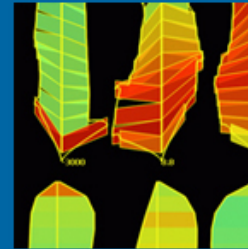
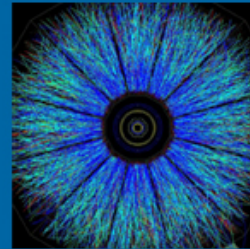
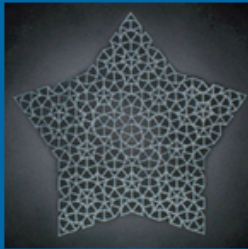


Swansea University
Prifysgol Abertawe

CS-130 Professional Issues

Computer Security Basics:

Malware



Lecture Learning Goals

Who are hackers?

What are the key terms we use in Computer Security?

What assumption do we make when we talk about securing a computer most of the time?

Why do we have passwords?

How do we store passwords?

Key Terms in Computer Security

Authorised users: The people who are meant to have access to a system

Hackers: People who attempt to gain access to a computer system in a way not intended by the systems owner

MalWare: Malicious software created or used by hackers that does something the owner of a system doesn't want to happen

Severity: The seriousness of a crime either from the perspective of the victim *or* from the perspective of judges and sentencing

Secure Systems: Secure against known threats and reasonable, theoretical ones – maybe!

Who are Computer Hackers?

White hat hackers – Security professionals brought in and paid specifically to test the security of a system

Grey hat hackers – People who gain access to a system without permission but not do anything malicious with the data

- Often only aim to make the company or users aware of vulnerabilities
- The escalation process if a company refuses to act is ethically challenging

Black hat hackers – People who will gain access to a system without permission and steal or alter data

- Not always for personal profit, sometimes it's an act of civil disobedience

Hacking In: Reading, writing, or worse?

Technically, there are two levels of seriousness in regards to computer crime: **Accessing** systems to view them or **Writing** to change systems and data

- Think *read-write-execute* permissions when you are familiar with Linux
- Sometimes this can make a difference in the eyes of judges

In reality, severity usually judged stems from the connection to further crimes (including creating holes for further computer crime)

- Either type can carry potentially very long criminal sentences or large fines
- International law and computer crime complicates things:
- Recently a UK based hacker was extradited to the US

Why is it hard to protect a computer if a hacker has physical access to it?

What steps can you authorised users take to protect it in this case?

Why don't users take this step?

The Key Assumption in Computer Security

Physical Security of End-Points: An important assumption in all of this is that malicious people don't have physical access to your computer

- We can simply pull data directly from a hard drive by plugging it into another computer
- **Shoulder surfing** attacks are also possible (next lecture discusses attacks more)
- Put a password on a file? You can just delete that part of the hard drive (you can't do this remotely so passwords do work online)
- Encrypting the Hard Drive is the only answer, but it makes it slow to use the system and may still be vulnerable if someone leaves their computer unattended

Basic Malicious Software or Malware

There are a range of different types of Software coded to deliberately sabotage a computer

- Note that many of these terms are not mutually exclusive as we go through them!

Computer Viruses – unwanted, self-replicating embedded code with a debilitating effect

- Different to a “bug” as it is deliberate
- Come in a wide variety of flavours
- Virus detection relies on recognising the code in viruses

Basic Malicious Software or Malware

Trojan Horses – software that masquerades as something else that does something malicious when executed

- Typically delivered in a download from a website or email
- PDFs, .doc files, .xls, .jpeg – all can act as a Trojan

Worms – a network propagated virus, meaning it spreads from computer to computer

Zombies – a software program that is used to control your computer remotely without your knowledge or a computer controlled in such a way

Technically advanced Malware

Rootkits - hide software's presence from users by gaining /root access to a system

- When the computer's Operating System asks what software is running, a root kit lies to it and hides the software
- Can only be removed by re-installing the OS unless you know exactly what type of root kit is involved

BIOS RootKits – the evolution of the root kit

- Can only be removed by “flashing” (reformatting) the BIOS
- Considered to be theoretical only until (Check? Cambridge demo? 2015)

Key loggers – software that sits on a computer and logs the keys you press

- Installed with a *Trojan Horse*, hidden with *RootKits*

W News ▸ UK News

Users warned over 15 apps which need to be deleted from your phone

The programs will hide themselves in your device in a bid to avoid detection or deletion

SHARE     

By Neil Shaw
07:58, 14 OCT 2019

NEWS


► Enter your postcode for local news and info

Enter your postcode

Go

In   YourArea

THE APPS INFECTED HAVE BEEN DOWNLOADED SINCE **OCTOBER 2017** BUT ARE **NO LONGER AVAILABLE TO PURCHASE ON THE PLAY STORE**

 Click for Sound

UP NEXT:

Change org petition to get Piers Morgan sacked from



RECOMMENDED



Tuna sandwich row sees boy pulled out of school



Popular burger and chicken meals could be banned in UK



Money Saving Expert on whether you should leave your heating on



Saddest ever episode of Grand Designs sees project stall for years

Password Protecting Systems

Passwords authenticate you as an **authorised user** based upon a **shared secret** between you and the system

Passwords are stored in a single, **hashed and salted** file typically called a **password file**

- Every website you enter a password on has a file like this as does your computer
- Access to it should, in theory, be tightly controlled so not even the company owning the website can see your password

Ever had your password sent to you in an email after you set it?

- Bad news because if it's lost and someone can link it to you they can use the password on that site and elsewhere...

Hashing

So we need to store passwords to check that you are giving the right one but we also must not store them?

- **Hashing** – a mathematical process (a bit similar to encryption) that takes data of an arbitrary size and **maps** it to a fixed size hash-value
- **Collision resistant hashing**– makes it really hard (mathematically speaking) to find data that maps to the same hash value
- Salting

Brute force attacks – hash and compare random phrases to the stored passwords but it can take a long time (years, decades, millennia)

Password cracking

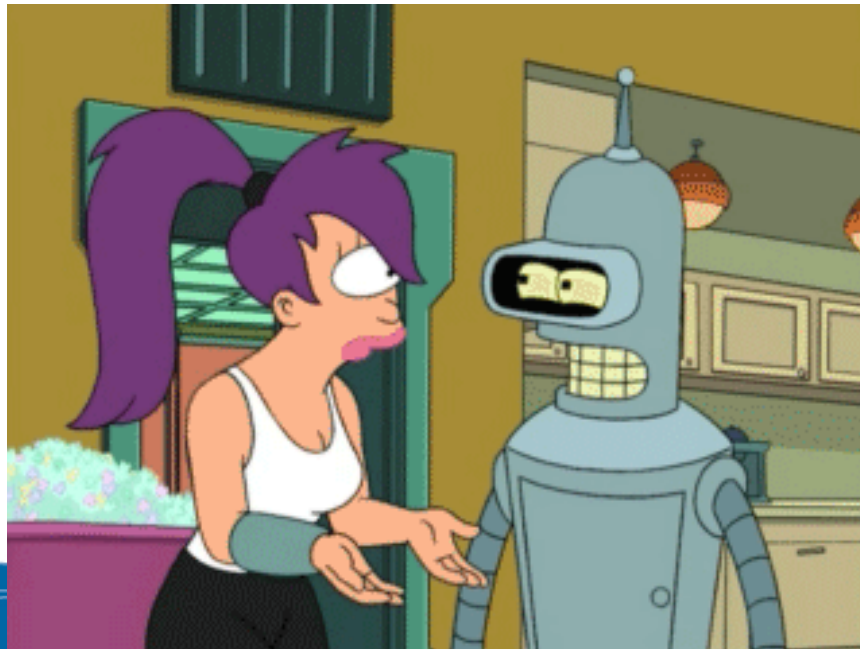
Dictionary attacks – encrypt non-random phrases like a dictionary (or list of common passwords!)

Rainbow table attacks – the smartest attack of all - store pre-computed, encrypted passwords and run the same attacks

Rainbow table attacks lead to the practice of **salting** in which websites add an arbitrary string to all passwords to drastically increase the time this type of attack takes if the password is complex

What about biometrics?

What about biometrics?



[illegible]

The 24 most common passwords of 2014

- | | |
|-------------------------|-----------------------|
| 1. 123456 (Unchanged) | 13. monkey (New) |
| 2. Password (Unchanged) | 14. login (Down 3) |
| 3. 12345678 (Up 1) | 15. abc123 (Down 1) |
| 4. qwerty (Up 2) | 16. starwars (New) |
| 5. 12345 (Down 2) | 17. 123123 (New) |
| 6. 123456789 (New) | 18. dragon (Up 1) |
| 7. letmein (New) | 19. passw0rd (Down 1) |
| 8. 1234567 (Unchanged) | 20. master (Up 1) |
| 9. football (Down 4) | 21. hello (New) |
| 10. iloveyou (New) | 22. freedom (New) |
| 11. admin (Up 4) | 23. whatever (New) |
| 12. welcome (Unchanged) | 24. qazwsx (New) |
| | 25. trustno1 (New) |

How can we relate the issues in computer security to Lessig's four modalities?

How can we relate the issues in computer security to Lessig's four modalities?

Law – the applicable Laws that relate to a piece of technology

Markets – the commercial factors that influence a piece of technology

Social norms – the ways that people interact with each other and technology, unwritten rules that govern how we behave

Architecture – any complex or designed physical structure

Lecture Learning Goals

Who are hackers?

What are the key terms we use in Computer Security?

What assumption do we make when we talk about securing a computer most of the time?

Why do we have passwords?

How do we store passwords?

Lecture Learning Goals

Who are hackers?

White, Grey and Black hat

What are the key terms we use in Computer Security?

Authorised Users, MalWare, RootKits, more!

What assumption do we make when we talk about securing a computer most of the time?

Physical security – without it we can't do much!

Why do we have passwords?

They act as a Shared Secret so we know who is an authorised user

How do we store passwords?

In an Encrypted, Salted Password file

Wider Reading

YouTube: Hacker Breaks Down 26 Hacking Scenes From Movies & TV

- Required viewing

Podcast: Reply All Episode130: The Snapchat Thief (Warning: Mature content)

- An insight into how and why hackers steal people's social media accounts including discussion of the problems with 2FA

Podcast Series: The Privacy, Security and OSINT Show

- A wide-reaching guide to the problems of keeping yourself secure online

TV Series: Mr Robot (Warning: Mature content)

- Streaming on Amazon Prime, despite the odd premise, the security attacks shown are grounded in real attacks we will discuss