Information Security – attacks and defence

Hannah Dee
hmd1@aber.ac.uk

U3A Aberystwyth, April 2023
Aberystwyth University, Department of Computer Science

Outline

More of our lives are lived online than ever before

It seems like (some) people now use the internet for pretty much everything

- Banking
- Shopping
- Socialising
- Filling in tax returns
- Watching TV and films
- Romance (?!)

The Internet solves a lot of problems

It also lets us make more mistakes, more quickly, than ever before.

It exposes us to the mistakes of others on a wider scale than ever before.

And it opens us up to more scammers, from a wider range of places, than ever before.

Information security: CIA

Information security uses the CIA framework:

- Confidentiality: we want things to be visible only to those people allowed to see them
- Integrity: we want things to be changeable only by those people allowed to change them
- Availability: we want things to be accessible when we need to access them

Thinking about our activity online in these terms can clarify lots of things

Cyberattacks

- Confidentiality - they want to find out something they shouldn't know, like stealing state secrets
- Integrity - they want to change something, like your bank balance
- Availability - they want to stop something working, for example by taking down a website they don't like

Outline

Identity

You can't have CIA without being able to determine the identity of people who are interacting with your systems.

- We all have multiple intersecting identities
  - NI number, UTR, bank account number, passport number, email address, facebook id ...
- We can prove or validate these identities in a host of different ways
  - Documents, passports, bank cards, PINs, and probably, several hundred passwords...

Your data is valuable

- Your identity is valuable, so things which you might use to prove your identity are also valuable
- PII (personal identifying information) is worth protecting

If threat actors can assume your identity, you've got a problem.

Passwords and other authenticators

How many passwords do you have?

How do you choose them?

How do you remember them?

Passwords and other authenticators

Passwords are a flawed system

- We are poor at remembering them
- We are bad at choosing them
- We manage them badly
- They are sometimes leaked in hacking events or through incompetence

Don't make it easy for attackers

If a site is compromised, attackers might steal:

- Name, address
- Payment data
- Usernames
- Passwords

If you've re-used the password, any hacker has an easy job.

You can see if you've been in a breach at
`https://haveibeenpwned.com/`

Recommendation 1

Use a password manager so you don't have to recall 100s of passwords, and you don't re-use passwords.

`https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers`

Multi-factor authentication (MFA / 2FA)

What other systems are there?

- Inherence: things you are (face, fingerprint, voice, other biometrics)
- Posession: things you have (smartphone, telephone, tokens, badges and cards)
- Knowledge: things you remember ('cognitive passwords', pin numbers)

Recommendation 2

Turn on multi-factor authentication for anything important.

Email, definitely (it's the gateway to everything else)

`https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email`

Internet and computer systems are under constant attack

- Software applications are investigated by not only by "threat actors" but also by "bug hunters"
- When security holes are found, they're reported to the companies in question
- This means that often, software is *patched* before any holes are *exploited*

You can't take advantage of these fixes if you're running old versions

Recommendation 3

Install software updates.

`https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates`

(This also applies to "smart devices" - watches, Alexa-type things, etc.)

Outline

Social Engineering

Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data.
Human beings are essentially social creatures.

- We like to help one another.
- We generally defer to people higher up in the hierarchy than we are.
- We tend to trust that other people are honest, mean what they say, and are who they say they are

Types of Social Engineering attack

- Phishing
- Pretexting
- Baiting
- Quid Pro Quo
- Tailgating

Lots of these are as old as time, and aren't so much cyberattacks as con-artistry.

Phishing

- An email, phonecall or SMS attack
- Usually bulk (thousands are sent out - the scammer only needs one or two people to fall for it)
- “You have a delivery” or maybe “You have won a prize”

An exercise!

Look at the handout, and consider one of the examples

1. What's the scammer exploiting? (Fear? Greed? Desire to help others? Sense of urgency?)
2. What makes the message suspicious?
3. What do you think would happen if you fell for it?

What happens when you follow it up?

- Might be a site that looks genuine
- Might be a site that smells fishy
- Might engage you in conversation trying to get you to give over details
- Might ask you to pay for something

from: prof. chris price <cjp.aberac.uk@gmail.com>
sent: 25 october 2018 11:28:09
to: hannah dee [hmd1]
subject: are you on campus?

are you available?
sent from my iphone

```
-----------------------------------------------------------------
prifysgol aberystwyth www.aber.ac.uk
prifysgol y flwyddyn ar gyfer ansawdd dysgu - the times & the su

aberystwyth university www.aber.ac.uk
university of the year for teaching quality - the times & the su

--
personal chair
contact details
• email: cjp@aber.ac.uk
• office: e48, llandinam building
• phone: +44 (0) 1970 622444
• Personal Website: http://users.aber.ac.uk/cjp
```

On Thu, 25 Oct 2018 at 12:04 PM, Hannah Dee [hmd1]
<hmd1@aber.ac.uk> wrote:

nope not today, i'm at home. could be in in 15 if needed?

--
Dr Hannah Dee, Senior Lecturer,
Computer Science,
Aberystwyth University,
http://users.aber.ac.uk/hmd1

I'm in a meeting right now and that's why I'm contacting you through here. I should have called you but phone is not allowed to be used during the meeting. I don't know when the meeting will be rounding off and I want you to help me out on something very important right away.

what would you like me to do?

I need you to help me get iTunes Gift cards from the store, I will reimburse you back when I get back to the office. I need to send it to someone and it is very important. I'm still in a meeting and I need to get it sent right away. It's for a programming setup on apple gadgets. The amount I need you to get right now is £600 I will be reimbursing back to you. I need physical cards which you are going to get from the store. When you get them, scratch it and take pictures of the cards and attach it to this email then send it to me here ok.

sure i can do that. where should i go to get the physical cards? do they sell them in IBERS Bach?

No, go to other stores.

Which stores would you recommend? I haven't got much time

Walmart.

Walmart is a bit challenging - i'm not sure I can get there and back in time. Might they sell them in Harrods?

Yes, I think you should get them there.

Great I'll just pop to Harrods. Should be back in about 20 mins. Remind me what you want me to do with these cards?

I need you to scratch the cards and attach them to this email.

ok i'm back from harrods with the cards and i have scratched them but i am not sure how to attach the cards to this email.

Take pictures of the cards and send to this email.

oh, you want pictures of them?

i have to wait for my camera to charge.

You can write codes out and send here.

```
you want me to write you some code?

what language?
```

Other variants of basically the same scam . . .

- "Hi Mum" my phone's been stolen so I'm borrowing a friends, can I get some money to get a new phone?
- I need to get a ticket home, can you . . .
- I need amazon vouchers . . .

MFA scam

- "My whatsapp (or some other system) has been hacked they'll send out a code but my phone's not working can you let me know the code?"
- You get a reset code from the service in question
- You send the code to the scammer
- That scammer now has your login to the service in question

Consumer level phone scam

Phone calls from people who claim to be technicians calling from a 'Support Team'.

- They might even spoof the caller ID (so it looks genuine)
- "Your computer has a problem"

To 'prove it' they might:

- Show you 'error messages' often on fake websites.
- Or full screening your browser with popup messages that won't go away – locking up the browser ('so computer not work, sir').
- Or by a opening console app and viewing system logs where there are usually a lot of 'warnings' and 'errors' and crash logs.

What do they actually want to do?

Social engineering creates a blended attack

What are they trying to (get you to) do?

- Install a remote control program
- Install a keylogger
- Install other **spyware**
- Give away a password
- Give away data
- Hand over money (either for a service, or through pretending to be a person in need)

Rarely (but not never) will you do damage by simply downloading a thing from the Internet.

Recommendation 4

If an email or a call feels suspicious, it probably is.

1. Check independently - can you ask for an official number to call them back on?
2. Don't let yourself be rushed into anything
3. Report scam emails

`https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-email`

Outline

On a positive note...

On a positive note...

Only kidding.

This is not a positive talk.

I see three future trends which will make all this worse

IoT

IoT means "Internet of Things"

- Internet connected devices aren't just computers
  - speaker
  - thermostat
  - doorbell
  - smoke alarm
  - watch
  - lightbulbs
  - car
  - toaster
- This gives a much bigger "attack surface"

AI

How could AI language models create realistic emails?

- AI language models can create realistic emails by using natural language generation algorithms that are trained on large data sets of real emails. These models can analyze patterns in the language and style of real emails, and then generate new emails that are similar in structure and content to the real ones.
- Additionally, AI language models can be programmed to personalize emails based on information that is gathered about the target recipient. This information can include the recipient's name, location, job title, or other details that make the email seem more targeted and legitimate.
- However, it is important to note that the use of AI to create convincing phishing emails is unethical and illegal. AI should be used in a responsible manner and not for illicit purposes such as cybercrime.

Deepfakes

- We've already seen (last year, in the USA) voice-based scans which used AI to mimic the vocal patterns of a trusted person.
- Scammers can take a video of someone you know, and from that generate a video of that person saying absolutely anything.
- In a few years, expect realistic video, real-time.

The voice on the phone may sound like someone you know, or the face in the zoom call might look like someone you know...

But are they?

My recommendations again:

1. Use a password manager.
2. Turn on multi-factor authentication for anything important.
3. Install software updates.
4. If a message feels suspicious, it probably is. Leave it or report it, don't answer or follow links.

Any questions?