Information Security – attacks and defence

Hannah Dee
hmd1@aber.ac.uk

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

Outline

1. Intro
2. Technical attacks
3. Social engineering
4. The future of hacking

More of our lives are lived online

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

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

Information security: CIA

The predominant conceptual framework in information security is CIA

- 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

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
- You might not consider things like address, phone number and so on to be sensitive
- PII (personal identifying information) is worth protecting

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

What other systems are there?

Multi-factor authentication (MFA / 2FA)

- 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)

Hackers, crackers, and con artists

Outline

1. Intro
2. Technical attacks
3. Social engineering
4. The future of hacking

Why's it important?

Outline

1. Intro
2. Technical attacks
3. Social engineering
4. The future of hacking

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”

Pretexting

A family of attack types (could be a phishing attack, or an in-person attack) where the attacker tries to establish a rapport

- Might dress as an engineer from a particular company
- Might know details that make them appear more trustworthy
- Generates a *pretext* which makes them seem plausible

Baiting

Enticing people to install something that's not quite what it seems

- CD-ROMS through the post
- USB sticks left in public places
- Free downloads that have a malicious aspect

Quid-pro-quo

Similar to baiting, however you are getting a service.

- Visa application sites which will carry out things for a (hefty) fee
- Passport application checkers which charge hundreds of pounds
- . . .

If it's free, there's a chance the price you'll pay is data.

Some argue that social media is a quid-pro-quo attack on a grand scale . . .

Tailgating

This is very much a physical attack – and one which organisations have to defend against, more frequently than individuals.

This refers to sneaking through door behind a legitimate employee.

Hacker accounts feature lots of “hanging around in smoking areas”

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

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

Outline

1. Intro
2. Technical attacks
3. Social engineering
4. The future of hacking

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?

Any questions?