BU551X - Financial Crime and Cybersecurity
Lecture Notes

Rodrigo Miguel

January 29, 2023

Contents

Chapter 1

Lecture 1

1.1 Cybercrime

1.1.1 What is cybercrime?

- Virus, malware and spyware;
- Denial-of-Service attacks;
- Hacking of personal computers;
- Hacking of social media and e-mail;
- Hacking combined with extortion, e.g. Sextortion.
- DDoS or denial-of-service attacks;
- PBX (Private Branch Exchanges) - where hackers target telephone systems of companies to make expensive calls.

1.1.2 The scale of the problem

- The "Nature of fraud and computer misuse in England and Wales" is the only dataset available from the Office for National Statistics. Action Fraud reported 31 322 cases in 2020/2021 with $\frac{1}{3}$ being social media and e-mail hacking. This summed up for losses of £9.6 million.
- More than $\frac{1}{3}$ of Internet users reported a "negative online incident" - but most cases, including virus attacks, were not recorded as crimes.
- Research focused on alleged increase in online crime during the COVID-19 pandemic, argues that the changes in online retail habits have contributed for a higher exposure to cybercrime.

These activities however, are underreported, being it from companies that do not want to disclose attacks or simply not knowing, to people that are embarrassed of admitting to be attacked.

1.2 Leaks

1.2.1 Checking for Leaks

It is important to check online for leaks of your e-mails, mobile phones and passwords. There are a couple of websites that can help you do this:

- Have I Been Pwned - Checks your e-mails, mobile phones and passwords against any leaks including in the dark web;

Lastly, as a good practice measure, you can also use password managers for all your internet accounts:

- Bitwarden - Recommended due to its open-source and free nature.

1.2.2 Hacking your home network

There are four sources of vulnerabilities for small office/home office networks:

- Internet;
- Devices on the network;
- Wireless;
- Connection to your business.

It has a public IP address, which can be easily identified. If you want to test for vulnerabilities in your network, this tool, can scan your network with your public IP address.

1.3 Identity Theft

1.3.1 Why is it a major issue in the UK?

The UK, unlike other many other countries in the world, has no identity card system. This lack of system, creates a problem of identity theft.

- Lack of system for registration.
- Proof of address is used more times than needed, creating loopholes and fakes;
- Lack of photo IDs;
- Lack of checks, lead to fraud;

To fight against it, you should check your credit reports regularly. These checks also include dark web searches.

1.4 VPN

1.4.1 Can you be identified online?

You can test your browser security with Cover Your Tracks. Part of this information can also be spoofed using VPNs and the TOR browser.

1.4.2 What does a VPN do?

There are many VPN providers available to the end user, however, private providers, like ZSVPN, will not sell/store your information to other companies. Put simply, a VPN works by:

- Sending data from your computer to the VPN computer with the use of encryption;
- However, traffic going from the VPN computer to other websites is not encrypted;
- To remediate this, you can create a secure tunnel using a VPN and then connecting to the TOR network.
- As previously mentioned, you shouldn't rely on free providers and make sure you use HTTPS (Hypertext Transfer Protocol Secure) (TLS encryption) with every connection.
- Another good measure, is to check how much information your VPN provider has of you. e.g. name, address, phone number, etc.

1.4.3 Is a VPN sufficient for your security?

Simply put, "No!". Your metadata is sufficient evidence to trace back to you. For example, your ISP (Internet Service Provider) knows when you access YouTube, but they don't know which videos you are watching. VPN providers work the same way, they still have access to your data and store your transaction info, e.g. your credit card.

Chapter 2

Lecture 2