BU551X - Financial Crime and Cybersecurity
Lecture Notes

Rodrigo Miguel

February 6, 2023

Contents

Chapter 1

Introduction

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.
On another hand, you can also help yourself by taking some safety measures like:

- Turning off your mobile phone;
- Using another computer to hide your real location (RDP connection);
- Social behaviour is your demise.

Chapter 2

Tor and Hidden Services

2.1 Tor

2.1.1 Why use Tor?

As previously seen, it is very easy to track and identify users online. Tor (The Onion Router) is an open-source program that focuses on anonymous web surfing. It works by directing traffic through an overlay network, by using nodes. The user connects to an entry node and then traffic is directed to other nodes until it gets to the exit node and arrive at the targeted server. Tor was developed by the US Naval Research Laboratory in the 1990s. While it is very good at hiding your identity, the program still has its weaknesses, like the traffic between the exit node and the target server can still be monitored. Other techniques can also be used to augment security, for example, by using a VPN to encrypt the connection from the user to the entry point (or bridge). These combined give authorities a much harder job of tracking and identifying the user, but don't make it impossible.

2.1.2 Installation and Verification

The browser can be easily downloaded in most countries, but it is recommended to use GnuPG to check for the installation's integrity as a precaution measure. Before using it, it might also be necessary to use a bridge to connect to the network (check documentation online).

2.1.3 Optimize Tor settings

- Never use TOR in full screen mode! - This will identify your screen size and lead it to you;
- Always use the most up-to-date version of the browser;
- Change settings carefully, e.g. firewall ports;

- Never remember history;
- Tracking protection should be on "always";
- Block pop-up windows, warn when websites try to install add-ons;
- Check "Deceptive Content and Dangerous Software Protection".

2.2 Hidden Services

2.2.1 Search Engines

- DuckDuckGo;
- NotEvil;
- torch;
- ahmia;
- r/privacy;
- r/deepweb.

Chapter 3

The Dark Web and TAILS

3.1 Warning

3.1.1 Limits of TOR

- TOR is not completely safe as your operating system still communicates with the clear web - crashing logs, reports, etc.;
- To eliminate this, we need more secure operating systems to explore the dark web;
- Never use direct links on the dark web as attacks are very common - this stresses the importance of using safer operating systems;
- TOR can be very slow - consider using a bridge.

3.1.2 Posting Comments

- Never post comments directly on a website - keystrokes can be identifiable - they are like a fingerprint.
- A simple work-around on this is to type it on an off-line in text editor and then copying and pasting your message onto the website;

3.2 E-mail

3.2.1 E-mail services

- Fake ID Generator;
- Temporary e-mail providers;
- Other providers source;
- Permanent e-mail provider, focusing on privacy;

- Check updated links to hidden services.

3.3 Messaging

3.3.1 Instant Messaging

- XMPP/Jabber is a free and open-source protocol not owned by any company;
- Pidgin is pre-installed on TAILS - you can register here to get your own account.
  - Add XMPP account with your username and password - domain refers to dismail.de;
  - Note: The XMPP server is on the clearnet - better to use it with hidden services;
  - To do this, you need to modify Pidgin - use the onion service shown in list for dismail.de - This will ensure that traffic stays within the TOR network;
  - Use off-the-record end-to-end encryption - this way, the server cannot read the message;
  - Verification of contact: click on verify and select question/answer - fingerprint can also be set as an alternative form of communication.

3.4 TAILS

3.4.1 Operating Systems

- Your OS such as Windows or macOS collects information - even when using TOR correctly;
- Programs connect to the Internet directly without using a browser;
- Instead, you should use TAILS, which is a Linux based operating system;
- This is a 'live' OS which is usually installed on a USB stick;
- Anything will go through TOR network without leaks;
- TAILS runs on RAM and leaves no trace on the computer used;
- By switching off the computer after using TAILS, the information is deleted.

3.4.2 Whonix: an alternative to TAILS

- Whonix is a Linux based operating system which can run in a virtual machine;
- All traffic goes through the Tor network;
- Note: Whonix is not amnesic, providing more convenience but less security than TAILS;
- In VirtualBox import Whonix Gateway and Workstation - always start Gateway first;

Chapter 4

Cryptocurrencies

Chapter 5

Kali Linux

Chapter 6

Networks

Chapter 7

Scanning and First Attack

Chapter 8

Python for Networking and Automation

Chapter 9

Defence