University of Applied Sciences and Arts Northwestern Switzerland
School of Business

Module D4 – Local Session 1
Instructions for the students

Task 1 – Secure Web-browser

Objectives and Preparation:

1. You have Firefox installed on your computer
2. You can connect to a Tor address and learn about its performance
3. You can send a (manually) encrypted email

Relevant resources:

- □ Personal Security Script part 2 + 3
- □ Personal notebook/computer
- □ Have internet access

Suggestion – Read the missing "Personal Security" slides part 2 [time estimate: 20']

If you did not already, please have a look at part 2 of the slides from last week. *https://mslscommunitycentre.ch/pluginfile.php/19842/course/section/2061/D4_S1%20Personal%20Security%20p.2.pdf*

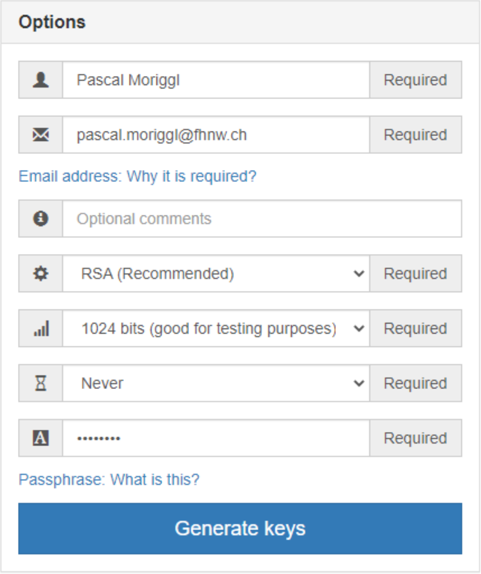
The slides introduce naming terminology, an example of a security model (slide 18), and some comments about MS Office Macros.

Exercise 1 – "Install Firefox and install Tor" [time estimate: 10']

1. If you don't have it already, install the Firefox web browser. Other web browsers will work with Tor, but you will have to configure the "proxy servers" manually. Under Windows, at least, this will be performed automatically if you have Firefox.
2. Go to http://tor.eff.org/ and download, install and run Tor
3. Start Tor and press connect. If it does not work, restart the Tor browser once more.
4. Visit https://www.guardian2zotagl6tmjucg3lrhxdk4dw3lhbqnkvvkywawy3oqfoprid.onion/international
5. Take and save a screenshot of the site (screenshot on windows: press windows+shift+s / Shift, Command, and 3 on mac)

Exercise 2 – "**Encrypt a message using PGP**" [time estimate: 20']

1. Go to https://pgptool.org/
2. Generate your PGP keys using your credentials, and essential: note down your passphrase somewhere!



Options

Pascal Moriggl — Required

pascal.moriggl@fhnw.ch — Required

Email address: Why it is required?

Optional comments

RSA (Recommended) — Required

1024 bits (good for testing purposes) — Required

Never — Required

•••••••• — Required

Passphrase: What is this?

a.

3. Download both key files (public and private). (pub) is the public key, (sec) the private. Both files can be opened using a normal text editor (right-click, open with, editor). The public key file is your address that you can share with anyone, basically like your public post box. But your key file must stay hidden and secure, do not share this with anyone in reality (if it is not an exercise like here).

4. Now go on the same tool page https://pgptool.org/ to the section Encrypt (+sign)

Use my public key to send a message to me using my public key as file:

0x8C98D8DD-pub.asc download here from moodle:

Or as raw PGP code:

xo0EYzHmcwEEAL6axSvAIeMFxrdFdl/d3Sv+9EKqP/noQGQK9LbBWR1WfTn1R89gwQsZmTl4S1
3s1/2dbWP/s962m9nPbno2mG6YLwyp46GYqJ9KDI1bJgpAydE17jIND7OJG1Bs9gINt3pox2xQFAjI
SXRe1pzHu9+4072eH27KB+0Iqx1pbUoVABEBAAHNJ1Bhc2NhbCBNb3JpZ2dsIDxwYXNjYWwub
W9yaWdnbEBmaG53LmNoPsK6BBMBCgAkBQJjMeZzAhsvAwsJBwMVCggCHgECF4ADFgIBAhk
BBQkAAAAAAAoJEFyy7N6MmNjd/I4EAJjoOGGefba2Ls/rcs4d7SYhKMqimM/fblQsd4B1lfGcF1BkE
Htnowwfln+XgA3GNDzwmqpe8f93QdkWlbBgp6YvJITgmStZj+sOjFBXJE0/EIlNVSMbVIeK9ja++ice
CsCGEr4fkbD19oqLJr+OU8btNPrvF1cwUxThUtDHU3wlzo0EYzHmcwEEAM4FWLlBYO7QJcZLxI9
YyJOFPwpz7DrB0fMnUR9eBR9ZCB+5i/YeavmJSmrAX+2Wrh4mLR7/utgNdy+gPCM1gzXMTUGp
UuW2KA1+7Ap2cczAkJXPBR+nblFHfaNJgccG9wKhtwWsdGDDYLjyXDZcxsizbLXvSerSswKVoMX
wSkujABEBAAHCwIMEGAEKAA8FAmMx5nMFCQAAAAACGy4AqAkQXLLs3oyY2N2dIAQZAQoA
BgUCYzHmcwAKCRC1bUBwH2fXXzj9A/48QMIDtDnPIodJmbv4dIDrBudJsO5PZBIzv6ihQfRKQ3x+
WxKxIRHVFJtg1hCmmt5NwYaDwCHYVWDh5UZb2IfNeW+d7p3+vtqtXuB9CnIgMSkqP2cVhoTTS
XTwLQvCRYPZ/x/GunCy0ww/qjXyc8pK5uQTBv//myABVRP2c0zT/u26A/wLxxhjAm3/uuPGLwmvN
1/Trj5LIGVfb4P4Sgt6cyBqApD2scEsbWydoxWKGebKtxbmT0JD/3lBzF/u+lpzi+DhOL8kq/SMv/D80n
waBxEqxGXKJV8aQryjHw9RIOfiRNkAPunGzVOygJZKSmiCw3iv6+C6o3TtDUwaj2++sJokCc6NBG
Mx5nMBBACo9YHSmHlpgePQc2SW5jl71mCrXopjlX16iiTClhChe3Y8aq3qT9MRmuv91u1yxB8rMq
XiaJnIs/6k7PxmOwXvx3ifkdtIu1n8I6mFBZs9+c5iGF/Nj/Zwg7vuuVzvrtR8hrO5Xj7NZ/O6lBzc62rUKz
k2r/doJ9FTXgYlYQ9QUQARAQABwsCDBBgBCgAPBQJjMeZzBQkAAAAAhsuAKgJEFyy7N6Mm
NjdnSAEGQEKAAYFAmMx5nMACgkQAkjg4o/xthsvhgQAmUob5Pg4544ceckzGDCLwiw/Pr5wya+e
WQpFqYWoKDg0e0gRCpiEovM6Db1I9jqi14Lz7jN9veV30ThML1wjUtz4eWX3OFL0txUuOTIDV5F0
RI5fu7b6xGEKTvfV7TNpXIrvq4WpIkhgeMNW/UbaUky6A+C7LbuQikC+dDtqvisCkwP/fGATFY+YE
X2Q0SveRROzVYdZjSEjlG98bpmso70swbo3KGMBs2aVvffmMMXvp7VAQ7FAUlvvWft2e4nysjvVF
MRf21k7VKQDvo43NBlZugpWyUVxDYJoep18/jooPvxQtLRjNGcvn+p3AS0T+Z1zeAJulHepVnXQd
uXifPHzwHI==FNVJ

5. Choose your private key file (which you have saved locally), and add your passphrase to proof that this is you.
6. Write a message, state in the message what is the apparent disadvantage of the Tor browser
7. Add the previous Tor screenshot as an attachment
8. Press “Encrypt the message.”
9. Download encrypted message
10. Send both the message file and your public key file in an email to me at pascal.moriggl@fhnw.ch, and only I will be able to decrypt your message and attachmend since I am the holder of the private key to the public key you have used when writing your message.

Task 2 – Add some plugins to your Firefox browser

Objectives and Preparation:

- □ You understand what an Addon (or browser-plugin) for a web browser is, and how to install one
- □ You know about the impact an Addon can have on your browser experience

Relevant resources:

- □ Personal Security Script part 3
- □ Have Firefox web browser installed on your computer
- □ Have internet access

Exercise 3 [time estimate: 10 min']

1. *If you do not have any Addons on Firefox yet, open Firefox, go to youtube, and test any video and enjoy the annoying adds for a second.*
2. *Install "uBlock Origin" first, close Firefox, open it again and go to the same youtube video. The adds should be gone now.*
3. *Install any Addon that was suggested in the slides part 3. Recommended are privacybadger, decentraleyes, duckduckgo privacy essentials, https everywhere. They are available here: https://addons.mozilla.org/de/firefox/*
4. *Many software services you may use regularly are also available as an Addon (e.g., Grammarly, Bitwarden, some Video downloaders, …)*

Task 3 – Download KeyPass 2, create and store a very secure password

Objectives and Preparation:

- □ You understand how a password manager can improve your security settings
- □ You know keypass 2 and how to perform basic manipulations with it

Relevant resources:

- □ Personal Security Script part 3
- □ Have internet access

Exercise 4 [time estimate: 10 min']

KeyPass 2 is not the most convenient password manager, but it allows for a rudimentary and secure showcase of a working password manager. For convenience and regular use (private), I can recommend Bitwarden (paid version).

1. *Download KeyPass 2 from here: https://keepass.info/download.html (or https://macpassapp.org/ for Mac users)*
2. *Follow the guide (Keypass2 / Macpassapp) to*
   a. *Start the program on your computer*
   b. *Create a first database (where your passwords will be safely stored)*
   c. *Either store an existing username/password / URL entry or create one*
   d. *Test it by retrieving it / login*

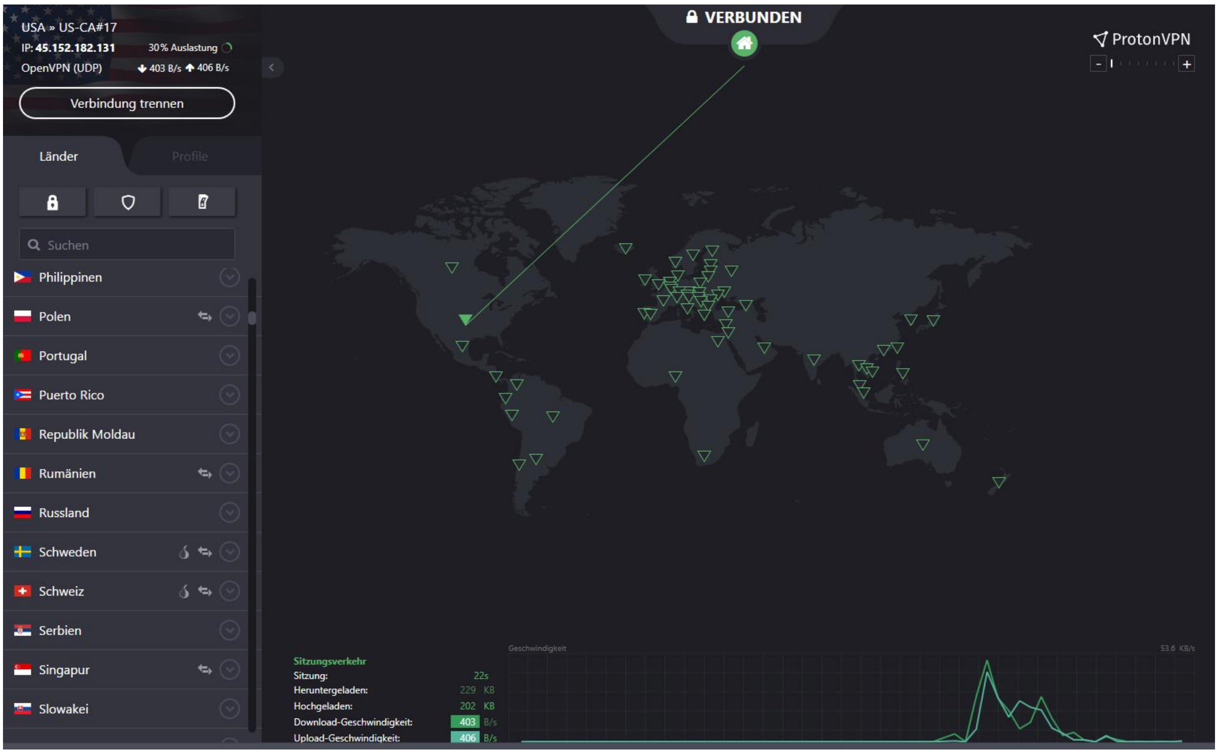
Suggested additional exercises [time estimate: 20 min']

Please feel free to try out and test additional software if you already know the ones above or are simply curious.

e.g. install Dangerzone (and Docker – careful it is large) – and open this PDF:

pascalmoriggl.salaryAug22.exe.pdf download here from moodle

e.g. install ProtonVPN and change your IP address. First see your current one (most likely university network location): https://nordvpn.com/de/what-is-my-ip/. Now install ProtonVPN and connect to any free server of a country of your choice (e.g. US). Check again the link above, it should display you know as a user from that country.



USA » US-CA#17
IP: **45.152.182.131** 30% Auslastung
OpenVPN (UDP) 403 B/s 406 B/s

Sitzungsverkehr
Sitzung: 22s
Heruntergeladen: 229 KB
Hochgeladen: 202 KB
Download-Geschwindigkeit: 403 B/s
Upload-Geschwindigkeit: 406 B/s

Please do not forget to uninstall and/or remove software that you do not wish to use any longer. If you have followed all the exercices, this would be the list to consider for uninstall if not having a future use for:

- □ Firefox Browser
- □ Tor Browser
- □ KeyPass 2 / Macpassapp
- □ Dangerzone
- □ Docker
- □ ProtonVPN