Digital security basics
Sessions

- Digital security basics
- Protection from malware
- Browser security & privacy
- Online anonymity & censorship circumvention
Session 1:
Digital security basics
So what am I even protecting?
Threat models

- **What** do you want to protect?
- **Who** do you want to protect it from?
- How likely is it that you will need to protect it?
- How bad are the **consequences** if you fail?
- How much trouble are you willing to go through in order to try to prevent those?
Evaluating your tools: Key questions

1. Is it open source or is it proprietary?
2. What is the business model of the company which owns the service?
3. What are the terms of service?
4. Has the tool been securely audited?
5. Who carried out the security audit?
Features

Enjoy the simplicity of Ubuntu’s intuitive interface. Fast, secure and with thousands of apps to choose from — for everything you want to do, Ubuntu has what you need.

Download Ubuntu

Take the tour ›
And remember to always update your software!
Encryption

SAMPLE ENCRYPTION AND DECRYPTION PROCESS

Encryption

Plain Text

Algorithm

Cipher Text

Decryption

Cipher Text

Algorithm

Plain Text
Three concepts to understand in encryption

1. Private and public keys

2. Security certificates

3. Key Fingerprints (e.g. 342e 2309 bd20 0912 ff10 6c63 2192 1928)
So if I encrypt my stuff, I'm TOTALLY safe right?!

Er... no.

How did Hacking Team get hacked?

They used passwords like *Passw0rd*. 
KeePassX: Secure Password Manager

- Save all your passwords in one encrypted database
- Copy & paste passwords so you don't need to memorize them
- Generate completely random (& secure) passwords
Install KeePassX
Resources

- Passwords: https://securityinabox.org/en/guide/passwords
- Encryption: https://ssd.eff.org/en/module/what-encryption
Session 2: Protection from malware
How much of a threat is malware?
Kaspersky Labs Interactive Map

GERMANY
#3 MOST-ATTACKED COUNTRY

- 1104174 OAS
- 294485 005
- 229139 WAV

- 9082 MAV
- 20026 IDS
- 12784 VUL

- 95578 KAS

Detections discovered since 00:00 GMT

Share data
How do I get infected?
How to become Wonder Woman in just a couple of easy clicks - just follow the link!

http://www.wikihow.com/Make-a-Wonder-Woman-Costume
----- Forwarded Message -----  
From: Melissa Chan <melissa.aljazeera@gmail.com>  
To:  
Sent: Tuesday, 8 May 2012, 8:52  

Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.

Please check the attached detailed report along with torture images.
VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.
By Catherine Stupp
APRIL 13, 2015
1010 WORDS

In late February, the German newspaper Die Tageszeitung, known by its shortened name ‘taz’, published a chronology on its website detailing the discovery of a keylogger that was used to steal data from newsroom computers. Keyloggers record every keystroke entered on a keyboard, which means recording passwords and communication before they can be protected through most encryption techniques. Since the...
Publications

Reports and Research Briefs

Bill Marczak (Lead), Nicholas Weaver (Lead), Jakub Dalek, Roya Ensaifi, David Fifield, Sarah McKune, Arna Rey, John Scott-Railton, Ronald Deibert, Vern Paxson, “China’s Great Cannon,” Citizen Lab Research Brief No. 52, April 2015. [Download PDF]

Katie Kleemola, Masashi Crete-Nishihata, and John Scott-Railton, “Tibetan Uprising Day Malware Attacks,” Citizen Lab Research Brief No. 51, March 2015. [Download PDF]


John Scott-Railton and Seth Hardy, “Malware Attack Targeting Syrian ISIS Critics,” Citizen Lab Research Brief No. 49, December 2014. [Download PDF]


Citizen Lab, “Asia Chats: LINE keyword filtering upgraded to include regular expressions,” Citizen Lab Research Brief No. 47, October 2014. [Download PDF]

Morgan Marquis-Boire, “Schrödinger’s Cat Video and the Death of Clear-Text,” Citizen Lab Research Brief No. 46, August 2014. [Download PDF]

Citizen Lab, “Iraq Information Controls Update: Analyzing Internet Filtering and Mobile Apps,” Citizen Lab Research Brief No. 45, July 2014. [Download PDF]

How can I protect myself?
Defending against malware

Tools:

- Anti-Malware scanner - Malwarebytes
- Anti-virus programs - Avast, Avira
- Anti-Spyware – Spybot, Detekt
Defending against malware

Tips:

- Activate your firewall
- Watch out for suspicious links
- Don't forget about physical security
Session 3:
Browser security & privacy
Choosing your browser

- Is it open source or proprietary?
- What is the business model of the company which owns the browser?
- Can I enhance my privacy & security?
Change your default privacy settings

- Limit online tracking (Do Not Track)
- Remove cookies
- Clear history
- Incognito mode
Alternative search engines

- DuckDuckGo
- Searx
- StartPage
- Ixquick
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>131</td>
<td>46.503857</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>HTTP</td>
<td>POST /admin/do_login.php HTTP/1.1 (application/x-www-form-urlencoded)</td>
</tr>
<tr>
<td>133</td>
<td>46.796971</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>HTTP</td>
<td>POST /admin/index.php HTTP/1.1</td>
</tr>
<tr>
<td>135</td>
<td>46.935024</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>HTTP</td>
<td>GET /admin/index.php HTTP/1.1</td>
</tr>
<tr>
<td>230</td>
<td>48.877844</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>HTTP</td>
<td>GET /admin/do_login.php HTTP/1.1</td>
</tr>
<tr>
<td>268</td>
<td>49.850529</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>HTTP</td>
<td>GET /javascript/JSCookMenu/ThemeOffice/theme.css HTTP/1.1</td>
</tr>
<tr>
<td>275</td>
<td>50.010766</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>HTTP</td>
<td>GET /css/big3.gif HTTP/1.1</td>
</tr>
<tr>
<td>282</td>
<td>50.488101</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>HTTP</td>
<td>GET /css/sign_big3.gif HTTP/1.1</td>
</tr>
<tr>
<td>287</td>
<td>50.613311</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>HTTP</td>
<td>200 OK (GIF89a)</td>
</tr>
<tr>
<td>312</td>
<td>50.954657</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>HTTP</td>
<td>200 OK (GIF89a)</td>
</tr>
<tr>
<td>328</td>
<td>51.070983</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>HTTP</td>
<td>200 OK (GIF89a)</td>
</tr>
<tr>
<td>329</td>
<td>51.073215</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>HTTP</td>
<td>200 OK (GIF89a)</td>
</tr>
<tr>
<td>350</td>
<td>51.292112</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>HTTP</td>
<td>200 OK (PNG)</td>
</tr>
<tr>
<td>126</td>
<td>46.339425</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>TCP</td>
<td>hb-engine &gt; http [SYN] Seq=0 Win=65535 Len=0 MSS=1400</td>
</tr>
<tr>
<td>127</td>
<td>46.381720</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>TCP</td>
<td>http &gt; hb-engine [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0</td>
</tr>
<tr>
<td>128</td>
<td>46.382226</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>TCP</td>
<td>hb-engine &gt; http [ACK] Seq=1 Ack=1 Win=65535 Len=0</td>
</tr>
<tr>
<td>129</td>
<td>46.382611</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>130</td>
<td>46.503694</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>TCP</td>
<td>http &gt; hb-engine [ACK] Seq=1 Ack=594 Win=6523 Len=0</td>
</tr>
<tr>
<td>132</td>
<td>46.555285</td>
<td>192.168.1.11</td>
<td>euroradio.fm</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
</tbody>
</table>

Follow TCP Stream

Stream Content

```plaintext
Accept-Charset: ISO-8859-1, utf-8; q=0.7,*; q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://euroradio.fm/admin/login.php
Cookie: PHPSESSID=48e3ed080d2e50510271cca2131f7334
Content-Type: application/x-www-form-urlencoded
Content-Length: 170

f_is_encrypted=1&f_user_name=dmvit&f_password=KyFzt8fofkgGeeU0fc&f_login_language=en&Login=Login&f_xkoery=f134314bf4d4a1bc
302 Found
Date: Mon, 14 Jul 2008 08:04:59 GMT
Server: Apache/2.0.55 (Ubuntu) PHP/5.1.2
X-Powered-By: PHP/5.1.2
Set-Cookie: PHPSESSID=48e3ed080d2e50510271cca2131f7334; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

Find Save As Print Entire conversation (103685 bytes)
HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. **Encrypt the web: Install HTTPS Everywhere today.**

**Install in Firefox**

- **Install in Firefox for Android**
- **Install in Chrome**
- **Install in Opera**
Privacy Badger blocks spying ads and invisible trackers.
Click & Clean
Resources

- https://myshadow.org/increase-your-privacy
- https://myshadow.org/resources
Session 4:
Online anonymity & censorship circumvention
How Tor Works: 1

Alice

Dave

[1] [2] [3]

Jane

Bob
https://www.eff.org/pages/tor-and-https
• Tor Browser
• Tor hidden services ("onion services")
• Tor relays
• Orbot (Android)
• Orfox (Android)
• Onion Browser (iOS)
• Tails
Install Tor Browser
Install Orbot & Orfox (Android) or Onion Browser (iOS)
Privacy for anyone anywhere

Tails is a live operating system, that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity, and helps you to:

- use the Internet anonymously and circumvent censorship;
- all connections to the Internet are forced to go through the Tor network;
- leave no trace on the computer you are using unless you ask it explicitly;
- use state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging.

Learn more about Tails.

News

Tails 1.5.1 is out
Posted Fri 28 Aug 2015 12:34:56 PM

Security

Numerous security holes in Tails 1.5
Posted Wed 26 Aug 2015 01:02:03 AM
Digital Hygiene: Top Tips to Keep it Clean!

- Use strong passwords.
- Watch out for suspicious links & attachments (malware).
- Secure your devices with full-disk encryption.
- Encrypt your files, emails, and communications.
- Connect securely with HTTPS Everywhere.
- Anonymize your connections using Tor Browser.
- Use secure software alternatives.
Resources

- https://www.eff.org/torchallenge/what-is-tor.html
- https://www.torproject.org/
- https://tails.boum.org/install/linux/usb/overview/index.en.html