

Crypto and privacy

A way-too-short introduction

EAL Hackaton

EAL

May 2016

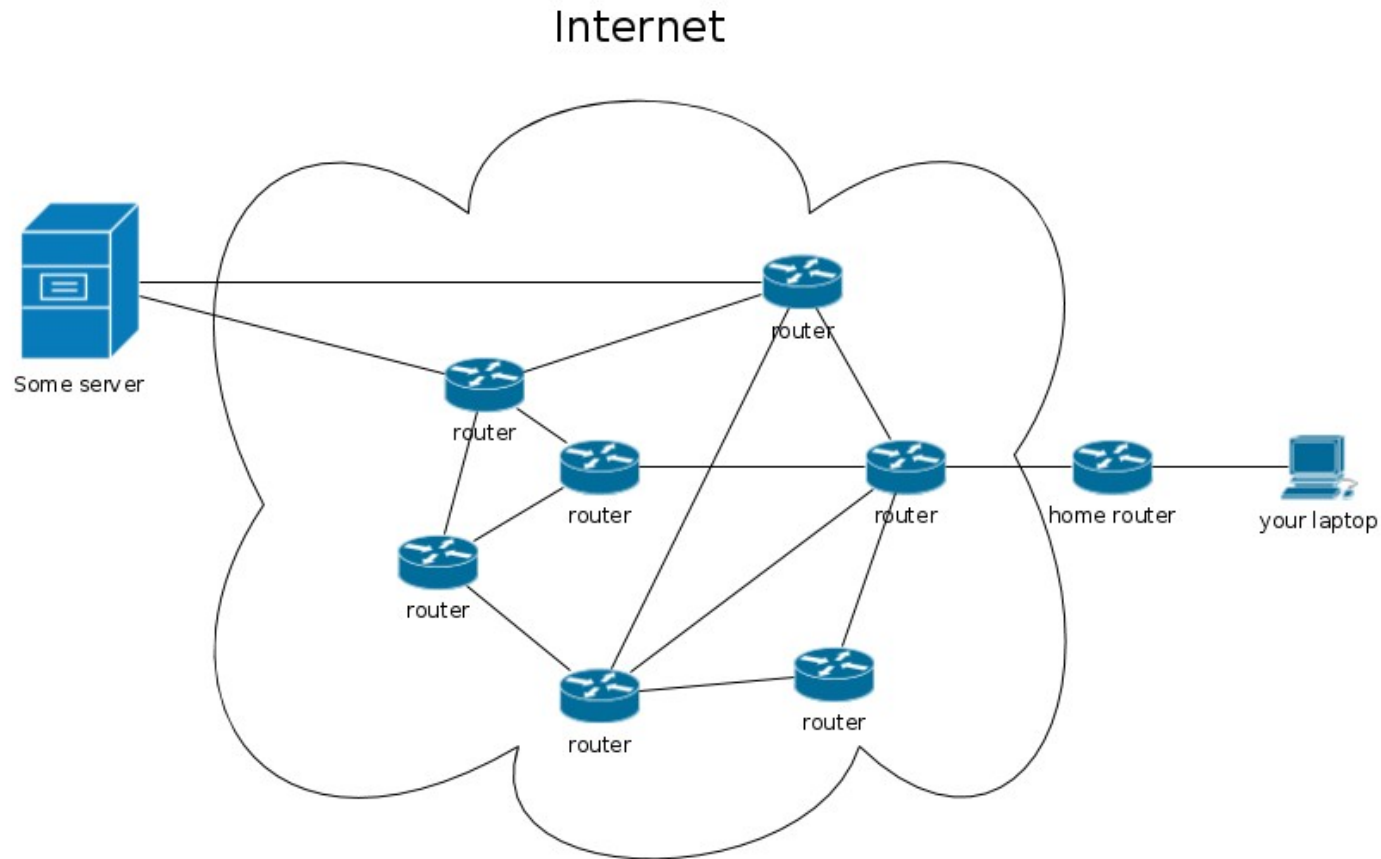


30 minutes on security and privacy

- Techie stuff
 - internet, protocols, sniffing and encryption
- What is privacy
 - your data, your choice?

Techie stuff

How the internet works



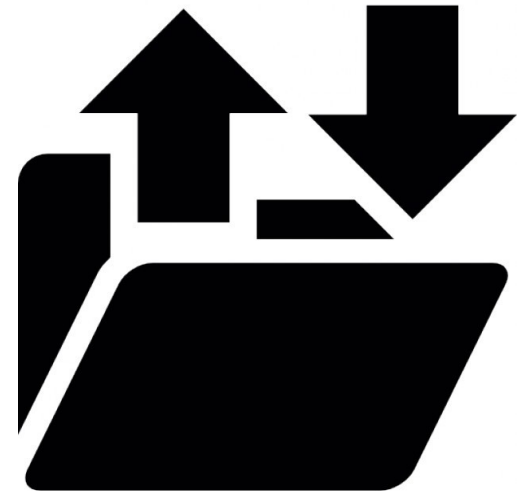
Quick intro to protocols



WWW
(HTTP)



email
(SMTP, IMAP, POP3)



file transfer
(FTP)

Sniffing tra

Stream Content

```
GET /wp-content/uploads/2015/11/KingCrab-600x450-e1447290106304.jpg HTTP/1.1
Host: www.wired.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101
Firefox/38.0 Iceweasel/38.3.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.7,da;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://www.wired.com/
Cookie: s_pers=%20ev1%3Dundefined%7C1430484412452%3B%20_dr%3Dhttp%253A%252F%
252Ft.co%252Fsurk4bxrrc%253Ft%253D1%2526cn%
253Dcmvjb3nfbmv0d29ya19kawdlc3rfdhjz2dlcmvk%2526sig%
253D3f620772241154883cf6b7a67bbcb97ae89b86fb%2526al%253D1%2526iid%
253Dfcfe5079100643e8a23d151eb5e73962%2526autoactions%253D1434116494%2526uid%
253D2459555580%2526nid%253D244%252B288%7C1434121785720%3B%20s_nr%
3D1442206176301%7C1444798176301%3B%20s_vnum_m%3D1448924400785%2526vn%253D24%
7C1448924400785%3B%20s_fid%3D501DE23E63384F67-065D39EE4BE571CA%
7C1510526230490%3B%20s_campaign%3Dundefined%7C1447369630494%3B%20sinvisit_m%
3Dtrue%7C1447369630497%3B%20s_eVar10%3Dundefined%7C1447369630500%3B%20s_depth%
3D14%7C1447369630502%3B%20gpv_p5%3DHomepage%7C1447369630506%3B; s_vi=[CS]v1|
24824444851026D_4000060800002041CE1_62-CAL_2_728206012_1426740846_
```

http Expression... Clear Apply Save

Time	Source	Destination	Protocol	Length	Info
6	73.31565200	10.0.20.125	107.23.243.205	HTTP	2828 GET / HTTP/1.1
5	73.61362700	10.0.20.125	23.235.43.239	HTTP	581 GET / HTTP/1.1
7	298.2497280	10.0.20.125	23.235.43.239	HTTP	710 GET / HTTP/1.1
0	83.53702300	10.0.20.125	23.235.43.239	HTTP	706 GET /2015/11/lego-xwing-death-star/ HTTP/1.1
2	191.9046740	10.0.20.125	23.235.43.239	HTTP	729 GET /2015/11/lego-xwing-death-star/ HTTP/1.1
3	88.75307800	10.0.20.125	205.251.219.19	HTTP	531 GET /5640d91361646d0497000015/97f5a98a-00b0-4e7d-829d-
9	88.98241300	10.0.20.125	205.251.219.19	HTTP	535 GET /5640d91361646d0497000015/97f5a98a-00b0-4e7d-829d-
5	88.81501800	10.0.20.125	205.251.219.19	HTTP	534 GET /5640d91361646d0497000015/97f5a98a-00b0-4e7d-829d-
2	88.71043600	10.0.20.125	205.251.219.19	HTTP	531 GET /5640d95b61646d049d00000a/824584a7-b60f-4fd9-89e1-
4	191.9293760	10.0.20.125	205.251.219.19	HTTP	531 GET /5640d95b61646d049d00000a/824584a7-b60f-4fd9-89e1-

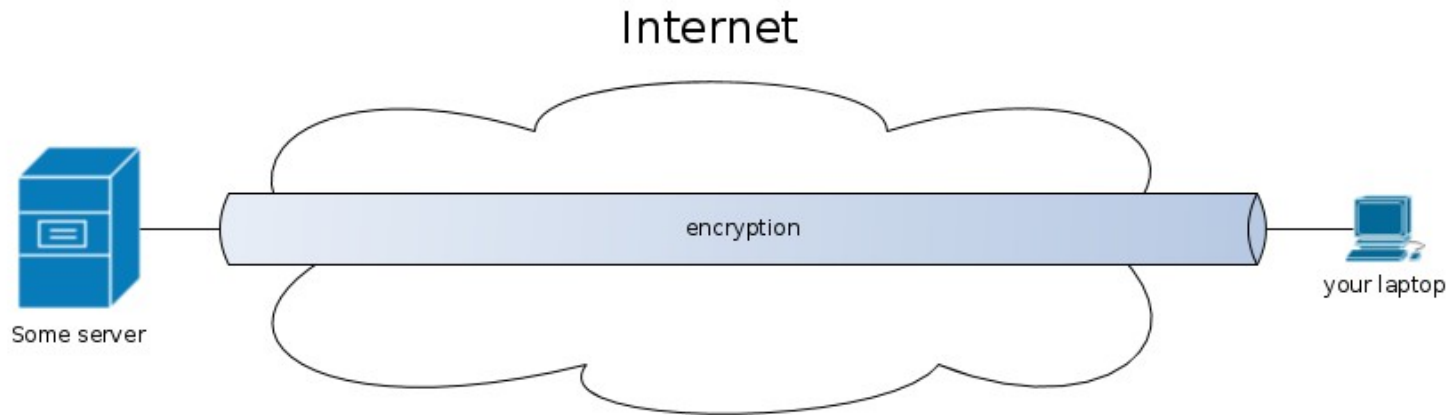
me 30: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits) on interface 0
ernet II, Src: IcpElect_d6:1e:06 (00:08:9b:d6:1e:06), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
ernet Protocol Version 4, Src: 10.0.20.113 (10.0.20.113), Dst: 239.255.255.250 (239.255.255.250)
r Datagram Protocol, Src Port: 1900 (1900), Dst Port: 1900 (1900)
ertext Transfer Protocol



btw

no confidentiality
and
no integrity

Encryption





Privacy

Sharing data



Friends and family

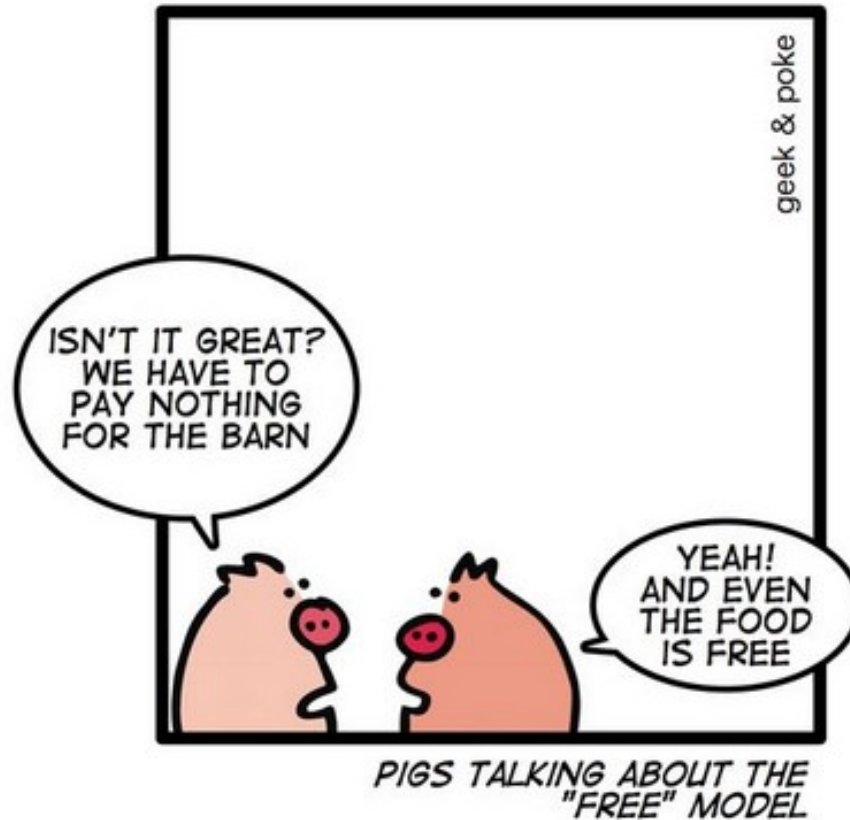


Doctor



Large corporation
e.g insurance

Product vs. costumer



SoMe



3rd parties

politikken.dk

13 Trackers

- Adform
- ADTECH
- ChartBeat
- Criteo
- Gemius
- Google AJAX Search ...
- Google Analytics
- Krux Digital
- Nugg_Ad
- Realtime
- ScoreCard Research B...
- TNS
- Visual Website Optimi...

b.dk

10 Trackers

- Adform
- ChartBeat
- Digital Analytix
- Emediate
- Facebook Connect
- Gemius
- Google AdServices
- Google Tag Manager
- TNS
- Visual Website Opti...

wired.com

15 Trackers

- Adobe Audience Ma...
- Adobe TagManager
- Adobe Test & Target
- Amazon Associates
- ChartBeat
- Disqus
- FreeWheel
- Google AdServices
- Media Innovation Gr...
- Optimizely
- Polar Mobile
- Rubicon
- ScoreCard Research...
- Typekit by Adobe
- Yieldbot

3rd parties

















who do you talk to?

politikken.dk







-  **Forbid politikken.dk**
-  Forbid jppol.dk
-  Forbid google.com
-  Forbid google-analytics.com
-  Forbid webspectator.com
-  Forbid adform.net
-  Forbid chartbeat.com
-  Forbid criteo.com
-  Forbid nuggad.net
-  Forbid gemius.pl
-  Forbid visualwebsiteoptimizer.com
-  Forbid krxd.net
-  Forbid adtech.de
-  Recently blocked sites ▸
-  Allow Scripts Globally (dangerous)
-  Revoke Temporary Permissions
-  Make page permissions permanent

Options...

b.dk

-  **Forbid b.dk**
-  Forbid adform.net
-  Forbid googletagservices.com
-  Forbid googletagmanager.com
-  Forbid berlingskemedi.net
-  Forbid chartbeat.com
-  Forbid gemius.pl
-  Forbid visualwebsiteoptimizer.com
-  Forbid cloudfront.net
-  Forbid facebook.net
-  Forbid tns-gallup.dk
-  Forbid emediate.dk
-  Recently blocked sites ▸
-  Allow Scripts Globally (dangerous)
-  Revoke Temporary Permissions
-  Make page permissions permanent

Options...

-  Forbid mediavoice.com
-  Forbid googletagservices.com
-  Forbid Disqus.com
-  Forbid typekit.net
-  Forbid chartbeat.com
-  Forbid zqtk.net
-  Forbid cnevids.com
-  Forbid condenastdigital.com
-  Forbid cloudfront.net
-  Forbid demdex.net
-  Forbid yldbt.com
-  Forbid optimizely.com
-  Forbid amazon-adsystem.com
-  Forbid mookie1.com
-  Forbid adobedtm.com
-  Forbid rubiconproject.com
-  Forbid fwmm.net
-  Forbid wired.com
-  **Recently blocked sites** ▸
-  Allow Scripts Globally (dangerous)
-  Revoke Temporary Permissions
-  Make page permissions permanent

Options...

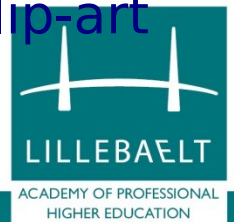
Closing comment

Privacy by design
vs.
Privacy by policy

Credits & licences



- Content by Morten Bo Nielsen
License: Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.
[\(http://creativecommons.org/licenses/by-nc-sa/3.0/\)](http://creativecommons.org/licenses/by-nc-sa/3.0/)
- EAL logo might be an issue, please check before you use it
- Friends:
http://www.clipartpanda.com/clipart_images/23-best-friends-clip-art-2841017
- doctor:
http://www.clipartpanda.com/clipart_images/doctor-clip-art-13-282x300-2122002



Credits & licences



- some icons:
<http://www.cliparthut.com/black-and-white-social-media-icons-free-clipart-UvsuZq.html>
- umbrella logo
<http://www.clipartsheep.com/umbrella-corporation-clipart-37358.html>
- email icon:
http://www.freepik.com/free-icon/black-envelope_755015.htm
- ftp icon:
http://www.freepik.com/free-icon/ftp-file-transfer-protocol_755286.htm
- www icon http://www.freepik.com/free-icon/browser_755553.htm
- pigs:
<http://geekandpoke.typepad.com/geekandpoke/2010/12/the-free-model.html>

