The state of mass surveillance
• Language: German ok?
  – slides are in English, just in case

• Interaction is fun!

• Talk and slides are CC-BY-SA
About Me

• Simon Hornbachner
Simon Hornbachner
Alumni of FH OÖ, SI Bachelor
Currently looking for a job ...
• Simon Hornbachner
• Alumni of FH OÖ, SI Bachelor
• Currently looking for a job …
• Coordinator of FSFE Group Linz
• ...is not about
  – Political issues behind mass surveillance
This talk

• ...is not about
  – Political issues behind mass surveillance
  – Conspiracy theories
This talk

• ...is not about
  – Political issues behind mass surveillance
  – Conspiracy theories

→ Happy to discuss this issues afterwards
This talk

• ...is about
  – Providing an overview over NSA/GCHQ mass surveillance programs
This talk

• ...is about
  – Providing an overview over NSA/GCHQ mass surveillance programs
  – Taking a look at the technology
This talk

• ...is about
  – Providing an overview over NSA/GCHQ mass surveillance programs
  – Taking a look at the technology
  – Talking shortly about where to go from here
• Biggest U.S. intelligence agency
• Biggest U.S. intelligence agency
• Strict focus on overseas surveillance
• Biggest U.S. intelligence agency
• Strict focus on overseas surveillance
• Run by General Keith Alexander
• Biggest U.S. intelligence agency
• Strict focus on overseas surveillance
• Run by General Keith Alexander
• Overseen by congressional committees and Foreign Intelligence Surveillance Court
• Government Communications Headquater
• Government Communications Headquater
• UK's answer to NSA
• Government Communications Headquater
• UK's answer to NSA
• permitted to spy in the interests of national security, preventing serious crime, or defending the UK’s economic interests
• Government Communications Headquater
• UK's answer to NSA
• permitted to spy in the interests of national security, preventing serious crime, or defending the UK’s economic interests
• Answers to foreign secretary, overseen by the Intelligence and Security Committee
PRISM/US-984XN Overview

OR

The SIGAD Used Most in NSA Reporting Overview

PRISM Collection Manager, S35333

April 2013
• Top secret, $20m-a-year surveillance program
• Used to gain information on targets stored on Servers of U.S. technology firms
• PRISM (allegedly) gives access to
  – Emails
  – Chat conversations
  – Voice calls

• Yet unclear, what PRISM exactly is
• Believed to be upstream monitoring of cable communications
• Believed to be upstream monitoring of cable communications
• Leaked documents describe it as „direct access to servers“
• Believed to be upstream monitoring of cable communications
• Leaked documents describe it as „direct access to servers“
• Upstream monitoring → different program: „Upstream“
PRISM/Upstream

FAA702 Operations
Two Types of Collection

Upstream
- Collection of communications on fiber cables and infrastructure as data flows past.
  (FAIRVIEW, BLARNEY,)

You Should Use Both

PRISM
- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube, Apple.

TOP SECRET/SI/ORCON/NOFORN

OWASP
The Open Web Application Security Project

OWASP
Austrian Chapter
• Collecting huge amounts of phone and internet communication
Upstream

• Collecting huge amounts of phone and internet communication
• Achieved by working with telecom companies like AT&T and Verizon
• Collecting huge amounts of phone and internet communication
• Achieved by working with telecom companies like AT&T and Verizon
• Metadata obtained by Upstream is fed into a DB → MARINA
Approx. 150 sites, over 700 servers
(cited from NSA slides)
• Framework to search the „Digital Network Intelligence“ (DNI)
• Framework to search the „Digital Network Intelligence“ (DNI)
• DNI = (apparently) data stored by NSA as well as real-time monitoring of internet traffic
• Framework to search the „Digital Network Intelligence“ (DNI)
• DNI = (apparently) data stored by NSA as well as real-time monitoring of internet traffic
• Suggested read → guardian has full NSA presentation on XKS
• Use free software
• Use free software
  – prism-break.org → freie Alternativen
What now?

• Use free software
  – prism-break.org → freie Alternativen
• Need to review our trust
• Use free software
  – prism-break.org → freie Alternativen
• Need to review our trust
  – istruecryptauditedyet.com
What now?

• Use free software
  – prism-break.org → freie Alternativen
• Need to review our trust
  – istruecryptauditedyet.com
• Use european providers
  – mykolab.com
  – autistici.org
• Use encryption where possible
  – GnuPG for E-Mail
  – OTR for IM → otr.cypherpunks.ca
What now?

• Use encryption where possible
  – GnuPG for E-Mail
  – OTR for IM → otr.cypherpunks.ca

• Best alternative: self-hosted
Reach me

- lfodh@fsfe.org
  - GPG KeyID D61C4FCF
- lfodh@jabber.fsfe.org
- irc.freenode.net (SSL on port 7000)
  - #owasp-owaspat, nick: lfodh
Thank you