The state of mass surveillance

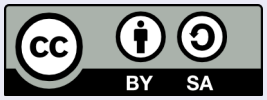
OWASP
The Open Web Application Security Project

OWASP
Austrian Chapter

First things first

OWASP
The Open Web Application Security Project

- Language: German ok?
  - slides are in English, just in case
- Interaction is fun!
- Talk and slides are CC-BY-SA



OWASP
Austrian Chapter

About Me

- Simon Hornbachner

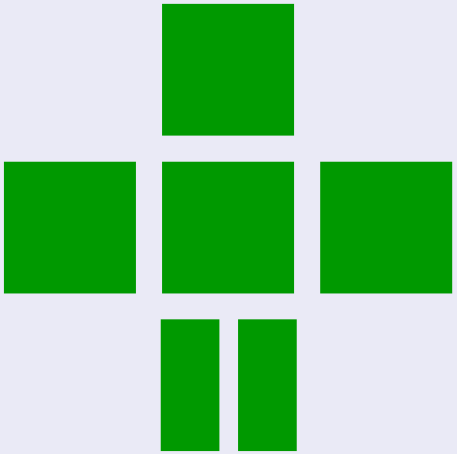
About Me

- Simon Hornbachner
- Alumni of FH OÖ, SI Bachelor
- Currently looking for a job ...

About Me

OWASP
The Open Web Application Security Project

- Simon Hornbachner
- Alumni of FH OÖ, SI Bachelor
- Currently looking for a job ...
- Coordinator of FSFE Group Linz



OWASP
Austrian Chapter

This talk

OWASP
The Open Web Application Security Project

- ...is not about
  - Political issues behind mass surveillance

OWASP
Austrian Chapter

This talk

OWASP
The Open Web Application Security Project

- ...is not about
  - Political issues behind mass surveillance
  - Conspiracy theories

OWASP
Austrian Chapter

This talk

OWASP
The Open Web Application Security Project

- ...is not about
  - Political issues behind mass surveillance
  - Conspiracy theories

→ Happy to discuss this issues afterwards

OWASP
Austrian Chapter

This talk

OWASP
The Open Web Application Security Project

- ...is about
  - Providing an overview over NSA/GCHQ mass surveillance programs

OWASP
Austrian Chapter

This talk

OWASP
The Open Web Application Security Project

- ...is about
  - Providing an overview over NSA/GCHQ mass surveillance programs
  - Taking a look at the technology

OWASP
Austrian Chapter

This talk

OWASP
The Open Web Application Security Project

- ...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

OWASP
Austrian Chapter

NSA

- Biggest U.S. intelligence agency

NSA

- Biggest U.S. intelligence agency
- Strict focus on overseas surveillance

NSA

- Biggest U.S. intelligence agency
- Strict focus on overseas surveillance
- Run by General Keith Alexander

NSA

- Biggest U.S. intelligence agency
- Strict focus on overseas surveillance
- Run by General Keith Alexander
- Overseen by congressional committees and Foreign Intelligence Surveillance Court

GCHQ

- Government Communications Headquater

GCHQ

- Government Communications Headquater
- UK's answer to NSA

GCHQ

OWASP
The Open Web Application Security Project

- 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

OWASP
Austrian Chapter

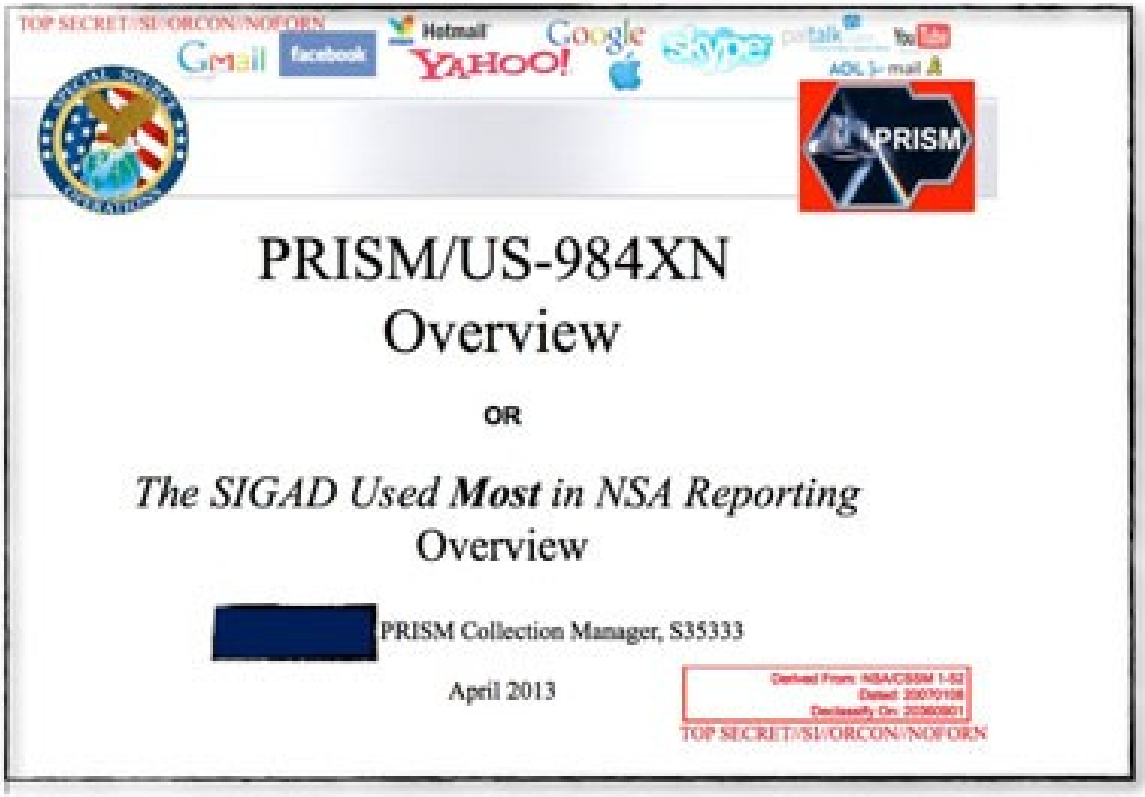
GCHQ

OWASP
The Open Web Application Security Project

- 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

OWASP
Austrian Chapter

PRISM


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
skype
AOL mail
PRISM
PRISM/US-984XN
Overview
OR
The SIGAD Used Most in NSA Reporting
Overview
[redacted] PRISM Collection Manager, S35333
April 2013
TOP SECRET//SI//ORCON//NOFORN

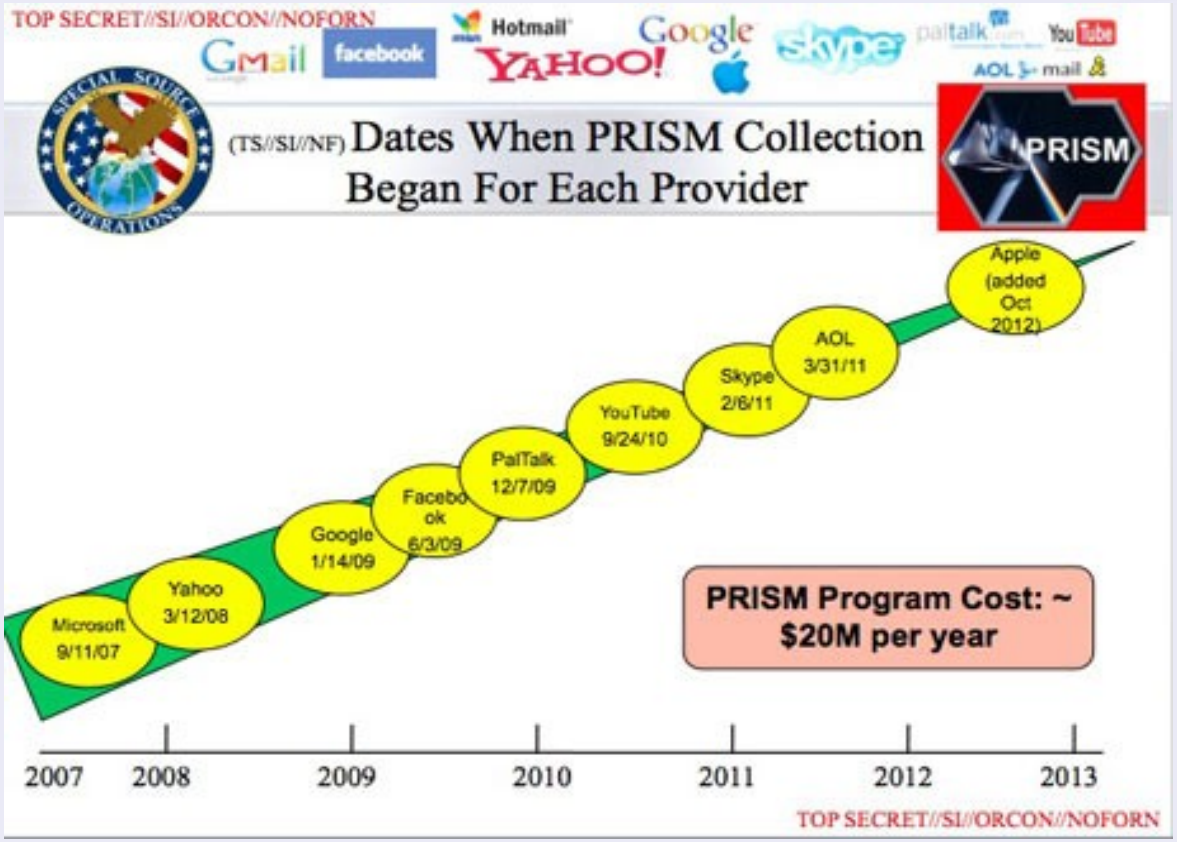
PRISM

OWASP
The Open Web Application Security Project

- Top secret, $20m-a-year surveillance program
- Used to gain information on targets stored on Servers of U.S. technology firms

OWASP
Austrian Chapter

PRISM


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk
YouTube
AOL mail
(TS//SI//NF) Dates When PRISM Collection Began For Each Provider
PRISM
Microsoft 9/11/07
Yahoo 3/12/08
Google 1/14/09
Facebook 6/3/09
PalTalk 12/7/09
YouTube 9/24/10
Skype 2/6/11
AOL 3/31/11
Apple (added Oct 2012)
PRISM Program Cost: ~ $20M per year
2007
2008
2009
2010
2011
2012
2013
TOP SECRET//SI//ORCON//NOFORN

PRISM

OWASP
The Open Web Application Security Project

- PRISM (allegedly) gives access to
  - Emails
  - Chat conversations
  - Voice calls

- Yet unclear, what PRISM exactly is

OWASP
Austrian Chapter

PRISM

OWASP
The Open Web Application Security Project

- Believed to be upstream monitoring of cable communications

OWASP
Austrian Chapter

PRISM

OWASP
The Open Web Application Security Project

- Believed to be upstream monitoring of cable communications
- Leaked documents describe it as „direct access to servers“

OWASP
Austrian Chapter

PRISM

OWASP
The Open Web Application Security Project

- Believed to be upstream monitoring of cable communications
- Leaked documents describe it as „direct access to servers“
- Upstream monitoring → different program: „Upstream“

OWASP
Austrian Chapter

PRISM/Upstream

OWASP
The Open Web Application Security Project

OWASP
Austrian Chapter

Upstream

OWASP
The Open Web Application Security Project

- Collecting huge amounts of phone and internet communication

OWASP
Austrian Chapter

Upstream

OWASP
The Open Web Application Security Project

- Collecting huge amounts of phone and internet communication
- Achieved by working with telecom companies like AT&T and Verizon

OWASP
Austrian Chapter

Upstream

OWASP
The Open Web Application Security Project

- 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

OWASP
Austrian Chapter

Xkeyscore

Approx. 150 sites, over 700 servers
(cited from NSA slides)

XKeyscore

OWASP
The Open Web Application Security Project

- Framework to search the „Digital Network Intelligence“ (DNI)

OWASP
Austrian Chapter

XKeyscore

OWASP
The Open Web Application Security Project

- Framework to search the „Digital Network Intelligence“ (DNI)
- DNI = (apparently) data stored by NSA as well as real-time monitoring of internet traffic

OWASP
Austrian Chapter

XKeyscore

OWASP
The Open Web Application Security Project

- 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

OWASP
Austrian Chapter

What now?

OWASP
The Open Web Application Security Project

- Use free software

OWASP
Austrian Chapter

What now?

OWASP
The Open Web Application Security Project

- Use free software
  - prism-break.org → freie Alternativen

OWASP
Austrian Chapter

What now?

OWASP
The Open Web Application Security Project

- Use free software
  - prism-break.org → freie Alternativen
- Need to review our trust

OWASP
Austrian Chapter

What now?

OWASP
The Open Web Application Security Project

- Use free software
  - prism-break.org → freie Alternativen
- Need to review our trust
  - istruecryptauditedyet.com

OWASP
Austrian Chapter

What now?

OWASP
The Open Web Application Security Project

- Use free software
  - prism-break.org → freie Alternativen
- Need to review our trust
  - istruecryptauditedyet.com
- Use european providers
  - mykolab.com
  - autistici.org

OWASP
Austrian Chapter

What now?

OWASP
The Open Web Application Security Project

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

OWASP
Austrian Chapter

What now?

OWASP
The Open Web Application Security Project

- Use encryption where possible
  - GnuPG for E-Mail
  - OTR for IM → otr.cypherpunks.ca
- Best alternative: self-hosted

OWASP
Austrian Chapter

Reach me

OWASP
The Open Web Application Security Project

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

OWASP
Austrian Chapter

OWASP
The Open Web Application Security Project

Thank you

OWASP
Austrian Chapter