bettercrypto·org

Idea

No more plaintext

The definitive guide

Applied crypto hardening

System Administration

bettercrypto·org

Scope

Testing

Webservers

Mailservers

Keylengths

Algorithms

Random numbers

VPNs

SSH

PGP/GnuPG

Instant messaging

Databases

bettercrypto·org

Tested configs

copy/paste

nginx

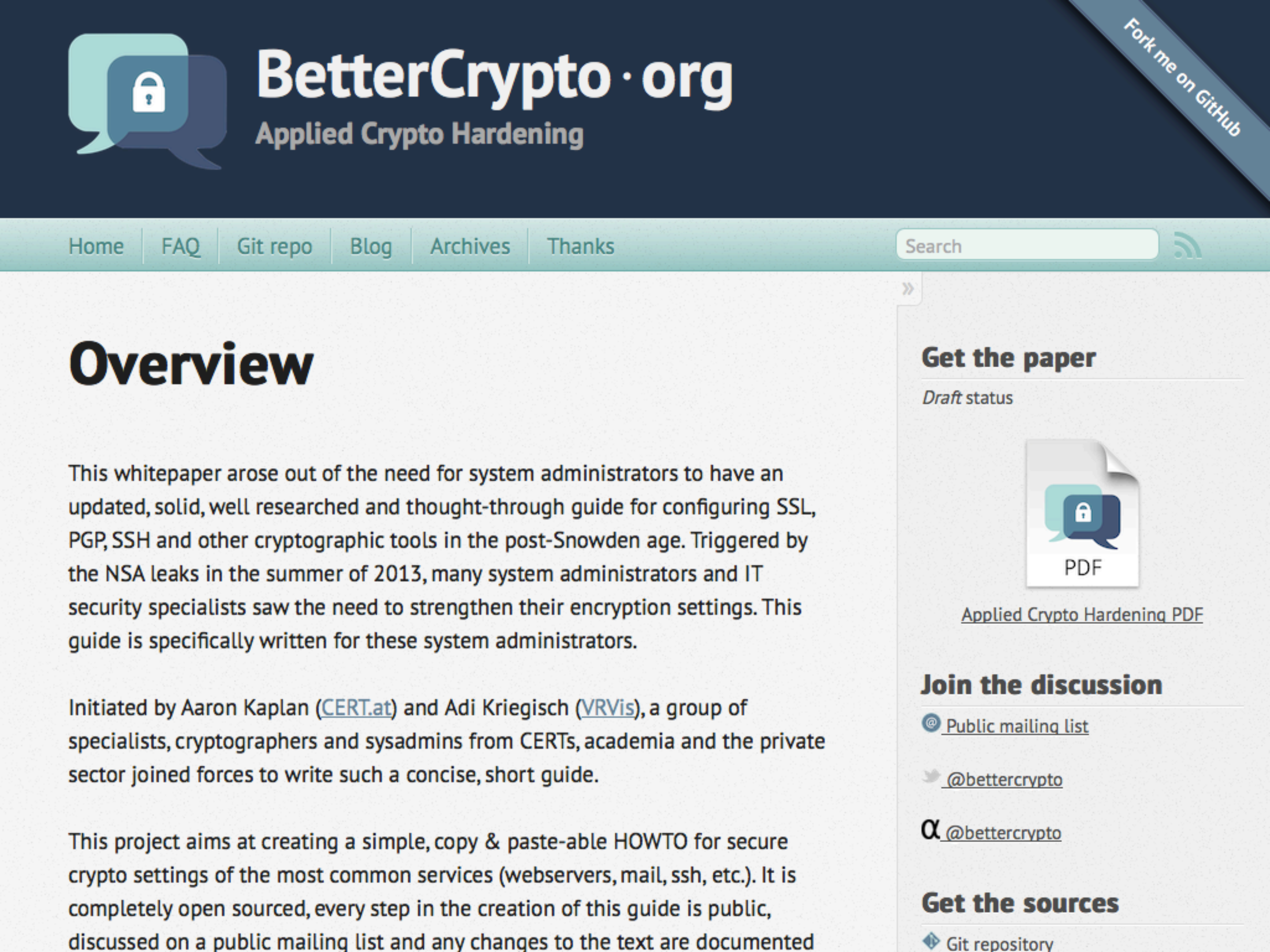
```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl_prefer_server_ciphers on;
ssl_ciphers 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA
+AESGCM:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:
+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!
aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!
RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256-
SHA:CAMELLIA128-SHA:AES128-SHA';
ssl_ecdh_curve secp384r1;

rewrite ^(.*) https://$host$1 permanent;
add_header Strict-Transport-Security max-age=2592000;
```

Participate!

Review

Write

Deploy hard crypto



BetterCrypto·org

Applied Crypto Hardening

Overview

This whitepaper arose out of the need for system administrators to have an updated, solid, well researched and thought-through guide for configuring SSL, PGP, SSH and other cryptographic tools in the post-Snowden age. Triggered by the NSA leaks in the summer of 2013, many system administrators and IT security specialists saw the need to strengthen their encryption settings. This guide is specifically written for these system administrators.

Initiated by Aaron Kaplan (CERT.at) and Adi Kriegisch (VRVis), a group of specialists, cryptographers and sysadmins from CERTs, academia and the private sector joined forces to write such a concise, short guide.

This project aims at creating a simple, copy & paste-able HOWTO for secure crypto settings of the most common services (webservers, mail, ssh, etc.). It is completely open sourced, every step in the creation of this guide is public, discussed on a public mailing list and any changes to the text are documented

Get the paper

Draft status

Applied Crypto Hardening PDF

Join the discussion

@ Public mailing list

@bettercrypto

α @bettercrypto

Get the sources

Git repository

Mailinglist

@

Repository

PDF

bettercrypto·org