
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

Ohai #30C3!

To all people at the CCC: We need your help! Good open source cryptography is essential to security. Correctly implementing this is often a complex riddle. This project aims to provide an open source guide to applied crypto hardening.
So what can you do?

1. Read our paper
2. Review it
3. Test it and implement it
4. Give us your feedback on the mailing list
5. Send us patches or pull requests

Thank you for your help and knowledge. Solid reviews by multiple eyes is the key.

Get the paper

Draft status

Applied Crypto Hardening PDF

Join the discussion

Public mailing list

@bettercrypto

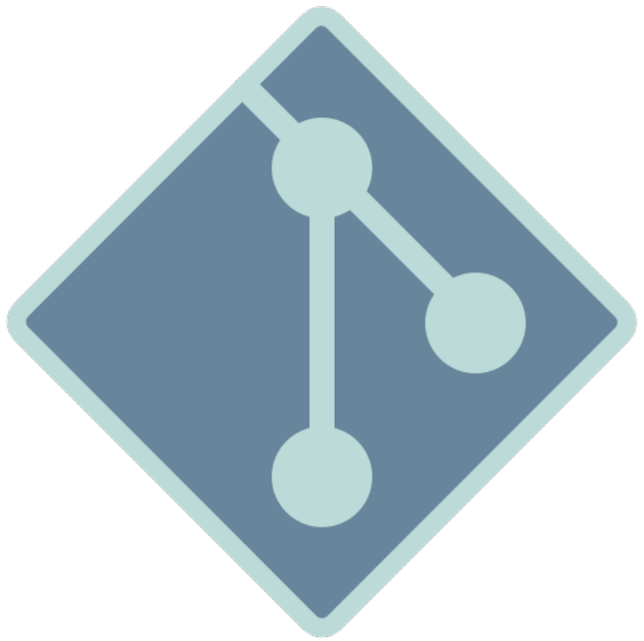
@bettercrypto

Get the sources

Git repository:

Mailinglist

Repository




PDF


bettercrypto·org