Project „ACH“
(Applied Crypto Hardening)

kaplan@cert.at

Don‘t give them anything for free

It‘s your home, you fight

Idea

- Do at least something against the **Cryptocalypse**
- Check SSL, SSH, PGP crypto Settings in the most common services and certificates:
  - Apache, Nginx, lighthttp
  - IMAP/POP servers (dovecot, cyrus, ...)
  - openssl.conf
  - Etc.
- Create **easy, copy & paste-able settings** which are „OK“ (as far as we know) for **sysadmins.**
- **Many eyes must check this!**

Current ToC

1. Abstract
2. Disclaimer
3. Motivation
4. Overview common crypto systems
5. Keylenghts
6. PRNGs
7. **Practical settings**
8. PKIs
9. Tools
10. Further research

ToC so far - Practical settings

- SSL
  - Apache
  - Nginx
  - Overview different SSL libs: openssl/gnutls/...
  - Openssl.conf settings
- IMAPs
- SMTP: opportunistic TLS
- SSH
- OpenVPN
- PGP
- PRNG settings in the kernel

Participation

- Authors: cryptologists, sysadmins, hackers
- Apply for write-perms
- World-readable

Current state as of 2013/11/04

- Initial ongoing work in the git repository
- More testing needed. Especially compatibility with clients and when to simply ignore old clients (RC4,...)
- Need to fill in other sections (nginx, ...)

Code

https://rhodecode.plunge.at/ach/ach-master

Mailinglist: ach@lists.cert.at

http://lists.cert.at/cgi-bin/mailman/listinfo/ach