
bettercrypto·org

Idee

Keinen Klartext herschenken

Applied Crypto Hardening


bettercrypto·org

Praktischer Crypto Guide

System Administration


PDF

Umfang

Server Tests

Webserver

Mailserver

Schlüssel

Verfahren

Zufallszahlen

VPN

SSH

PGP/GnuPG

Instant Messaging

Datenbanken

Praktische Einstellungen

Kopieren/Einsetzen

Beteiligung

Review

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 in a publicly readable version control system.

Nov 20th, 2013

Tweet

Get the paper

Draft status

PDF

Applied Crypto Hardening PDF

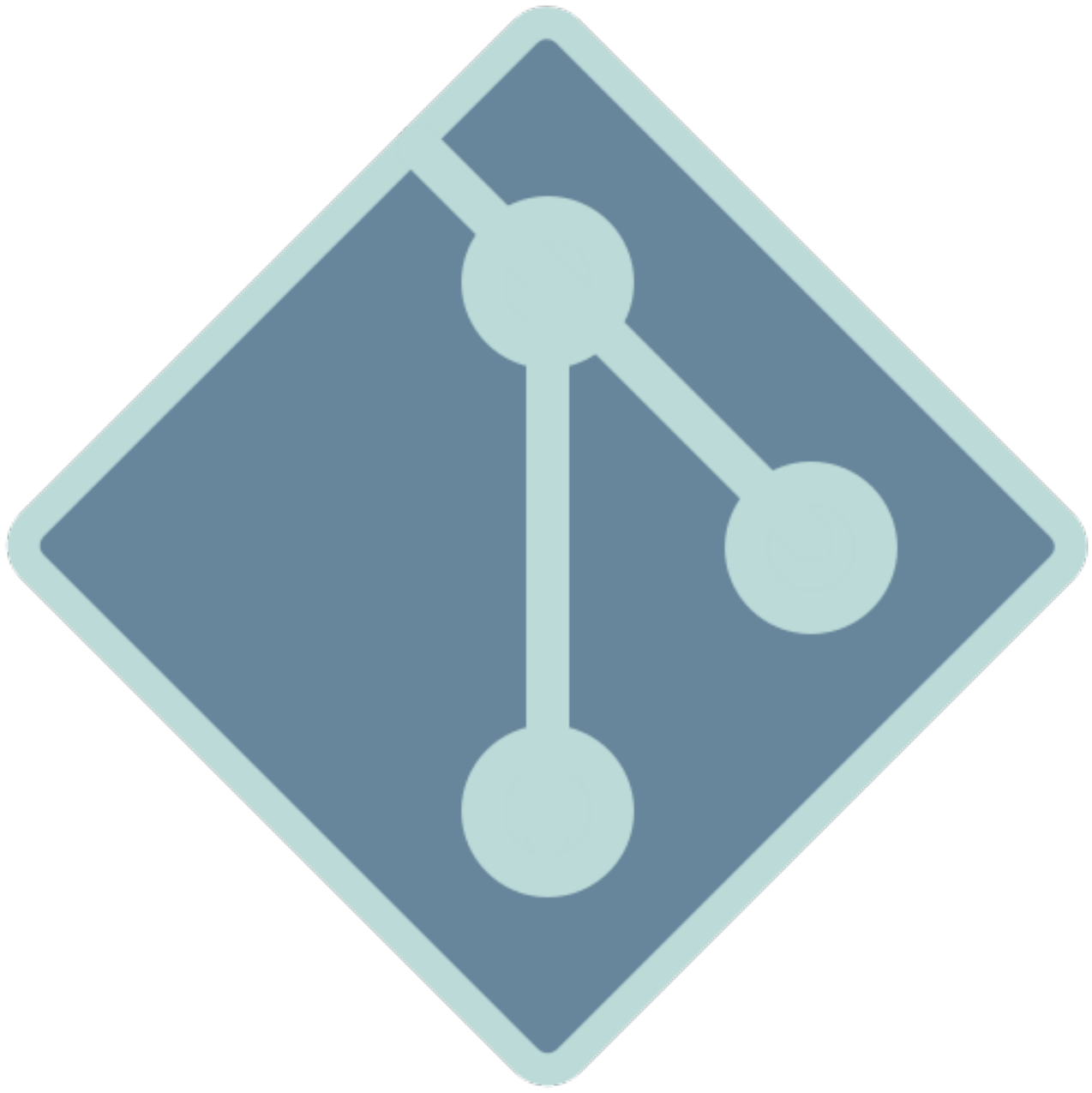
Join the discussion

Public mailing list

Get the sources

Git repository

Github mirror




bettercrypto·org