Einen sicheren Laptop mit Ubuntu einrichten

Stefan Schumacher

sicherheitsforschung-magdeburg.de
stefan.schumacher@sicherheitsforschung-magdeburg.de

30.04.2016

Über Mich

Über Mich

- Geek, Nerd, Hacker seit knapp 20 Jahren
- Berater für Finanzinstitute, Regierungen, Sicherheitsbehörden
- Direktor des Magdeburger Instituts für Sicherheitsforschung
  Forschungsprogramme zur Unternehmenssicherheit
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`

Schulungs- und Beratungsangebote

- Sicher unterwegs im Internet
- Anonymität und Überwachung im Internet
- Security Awareness Kampagnen konzipieren
- Netzwerke absichern/Penetration Testing
- Die psychologischen Grundlagen des Social Engineerings
- Der digitale Untergrund: zur aktuellen Bedrohungslage im Internet
- Kryptographie - Konzepte, Methoden und Anwendungen
- Strategien im Wirtschaftskrieg
- Selbstschutz in Krisengebieten

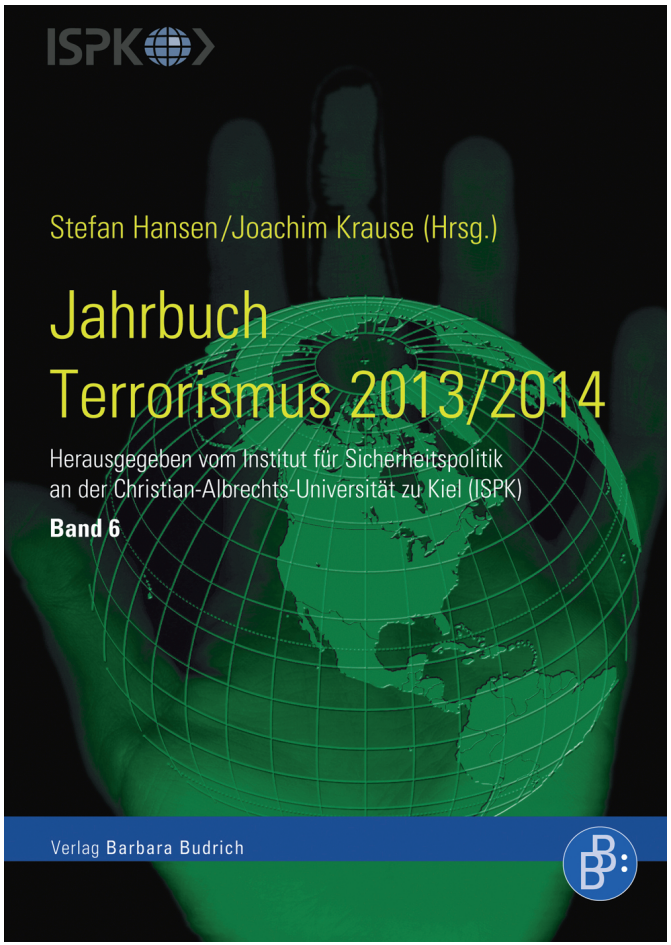
Informationstechnologie und Sicherheitspolitik

Sambleben, J. und Schumacher, S. (Herausgeber)

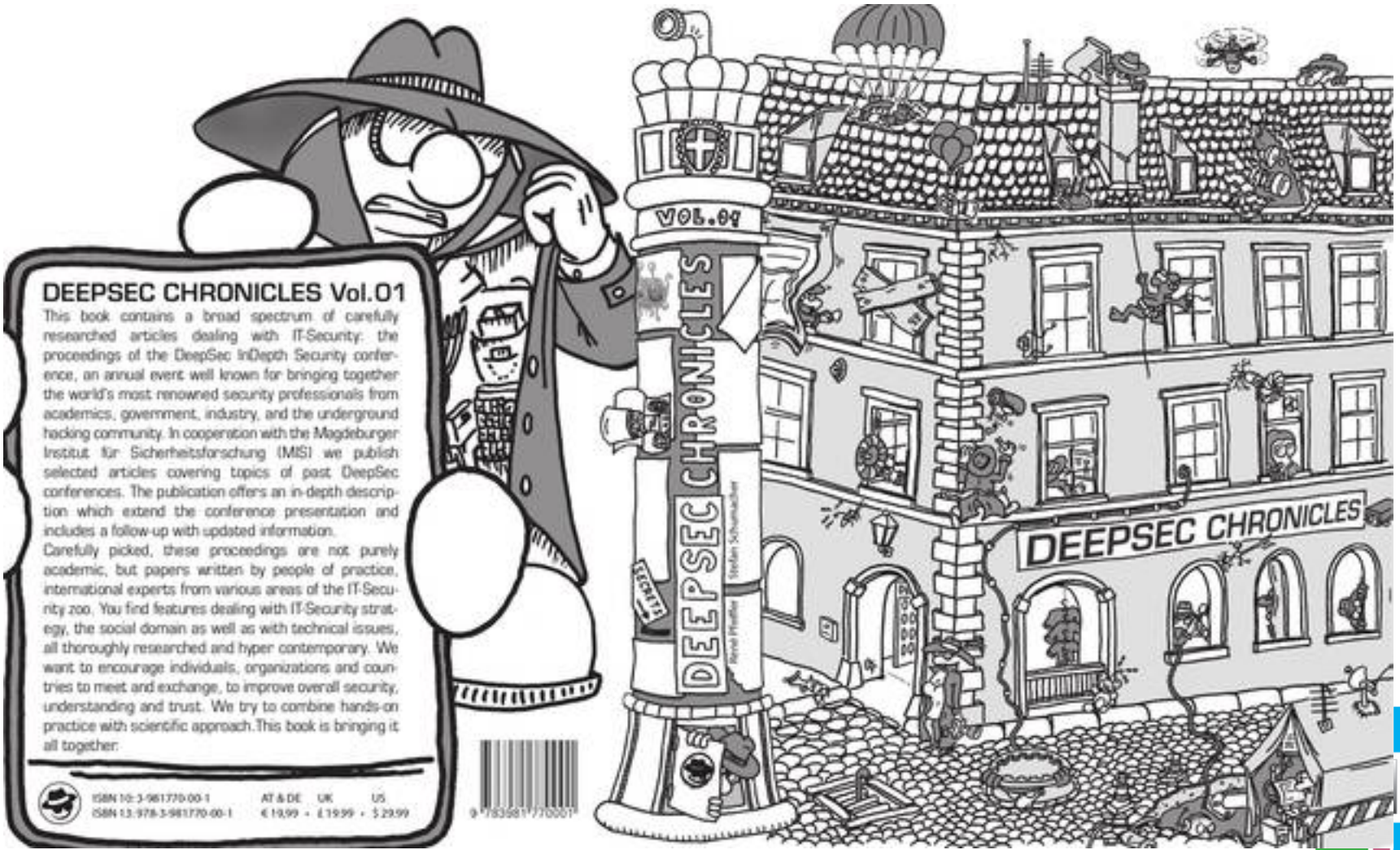
sicherheitsforschung-magdeburg.de/buecher.html

Jahrbuch Terrorismus 2013/2014

Hansen, S. und Krause, J. (Herausgeber, Institut für Sicherheitspolitik Kiel)



Stefan Schumacher:
Cyber-Terrorismus:
Reale Bedrohung oder Mythos?
S. 159 – 180


DEEPSEC CHRONICLES Vol.01
This book contains a broad spectrum of carefully researched articles dealing with IT-Security: the proceedings of the DeepSec InDepth Security conference, an annual event well known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. In cooperation with the Magdeburger Institut für Sicherheitsforschung (MIS) we publish selected articles covering topics of past DeepSec conferences. The publication offers an in-depth description which extend the conference presentation and includes a follow-up with updated information.
Carefully picked, these proceedings are not purely academic, but papers written by people of practice, international experts from various areas of the IT-Security zoo. You find features dealing with IT-Security strategy, the social domain as well as with technical issues, all thoroughly researched and hyper contemporary. We want to encourage individuals, organizations and countries to meet and exchange, to improve overall security, understanding and trust. We try to combine hands-on practice with scientific approach.This book is bringing it all together.
ISBN 10: 3-981770-00-1
ISBN 13: 978-3-981770-00-1
AT & DE UK US
€ 19,99 £ 19,99 $ 29,99
vol.01
DEEPSEC CHRONICLES
DEEPSEC CHRONICLES

- Stefan Schumacher and René Pfeiffer (editors)
- In Depth Security – Proceedings of the DeepSec Conference
- 360 Pages
- Magdeburger Institut für Sicherheitsforschung
- 978-3981770001
- `http://www.amazon.de/Depth-Security-Stefan-Schumacher/dp/3981770005/ref=sr_1_1?ie=UTF8&qid=1448888706`

Inhaltsverzeichnis

Bedrohungslage

- Schadsoftware greift Rechner an
- mobile Rechner gehen verloren oder werden gestohlen
- Manipulationen einfach möglich bei physischer Kontrolle
- Daten abschöpfen im Hotel
- Trojaner aufspielen bei »Zollkontrolle«
- sensible Daten schützen

Warum Linux?

- kostenlos, frei, offen
- Open Source - Backdoors verstecken schwierig
- Unix-Sicherheitsmodell
- gute Hardwareunterstützung
- vielfältige Software verfügbar

Warum Ubuntu?

- Ubuntu recht einfach nutzbar
- unterstützt von Canonical
- viele Anwendungen verfügbar
- 2 Releases pro Jahr (.04 und .10)
- LTS mit 5 Jahren Laufzeit (16.04., 14.04, 12.04)
- Alternate Install/Server existiert

- Abwägung Aufwand und Kosten vs. Bedrohung und Sicherheit
- Was bedroht mich?
- Risikoanalyse!
- Grundlage der Journalistenschulung für Syrien

Inhaltsverzeichnis

Hardware

- professionelle Laptops mit ordentlichem BIOS/UEFI
- Lenovo Thinkpad, Dell Latitude, HP Elitebook
- Thinkpad-BIOS besonders geschützt
- BIOS: User, Admin und Festplattenpasswort setzen
- gebrauchten Wegwerflaptop/Netbook
- z.B. Lapstore
- Hardwaremanipulationen existieren - Rechner nicht aus den Augen lassen

Hardware

- SSD: Samsung 850 Pro 1TB ab 360 Euro
- SSD: Samsung 850 Evo 1TB ab 260 Euro
- SSHD: Seagate ST1000LM015 1TB ab 85 Euro
- Hardwareverschlüsselung in AES
- immer aktiviert
- Festplattenpasswort im BIOS setzen
- cf: OPAL TCG

Hardware

Inhaltsverzeichnis

Ubuntu Download

- `http://www.ubuntu.com/download/server`
- Ubuntu Server 16.04 LTS
- Minimal-Installation
- Anwendungen per Internet nachinstallieren
- Installation per CD/DVD oder USB-Stick
- nur Ubuntu auf Platte sehr einfach
- Dualboot komplexer, nicht empfohlen

Verschlüsselung

- Verschlüsselung der gesamten Festplatte (LVM LUKS)
- Verschlüsselung von user durch ecryptfs
- Verschlüsselung beliebiger Verzeichnisse durch encfs
- Verschlüsselung einzelner Dateien durch mcrypt, OpenSSL oder GnuPG
- sicheres Passwort!
  min. 12 Zeichen, Groß/Kleinbuchstaben, Ziffern, Sonderzeichen, keine Wörter aus dem Wörterbuch

Verschlüsselung

- Verschlüsselung der gesamten Festplatte (LVM LUKS)
- Verschlüsselung von user durch ecryptfs
- Verschlüsselung beliebiger Verzeichnisse durch encfs
- Verschlüsselung einzelner Dateien durch mcrypt, OpenSSL oder GnuPG
- sicheres Passwort!
  min. 12 Zeichen, Groß/Kleinbuchstaben, Ziffern, Sonderzeichen, keine Wörter aus dem Wörterbuch

Verschlüsselung

- Partitionierung: /boot (1GB), Swap (RAM), / (Rest)
- 3 Partitionen
- /boot unverschlüsselt, beinhaltet Startsystem
- / wird per LVM und dm-crypt verschlüsselt
- Swap ist Auslagerungsspeicher, wird verschlüsselt mit Zufallspasswort

Verschlüsselung

- `Geführt - gesamte Platte mit verschlüsseltem LVM`
- `Manuell`
- `http://wiki.ubuntuusers.de/System_verschlüsseln/Alternate_Installation`
- `/` kann kaum mehr manipuliert werden, `/boot` schon
- `/boot` auf USB-Stick verschieben
- kann auch für USB-Sticks oder USB-Platten eingesetzt

Verschlüsselung

- eCryptFS: verschlüsselt das Benutzerverzeichnis (`/home/stefan/`)
- verschlüsselt im Dateisystem, Passwort automatisch aus User-Passwort abgeleitet
- wird automatisch bei der Installation mit eingerichtet
- Nutzung transparent
- schützt aber nur Nutzerdateien, nicht Systemdateien

Verschlüsselung

- encfs: verschlüsselt ein beliebiges Verzeichnis
- verschlüsselt im Dateisystem, Passwort muss übergeben werden
- muss nachinstalliert werden (apt-get -y install encfs)
- kann beliebig ineinander gestapelt werden

Beispiel

- Kunde1 | Kunde2 | Kunde3 | Buchhaltung jeweils mit encfs
- verschlüsseltes /home/stefan mit eCryptFS
- Festplattenverschlüsselung LVM
- hardwareverschlüsselte SSD/SSHD

externe Datenträger

- USB-Stick oder SD-Karte verschlüsseln
- Dateisystem mit LUKS
- Verzeichnisse mit encfs
- sensible Daten auslagern
- SD-Karte im Portemonnaie mitführen

Live-Systeme

- starten von CD/DVD oder USB-Stick
- fassen Festplatte nicht an
- können ständig mitgeführt werden
- TAILS: https://tails.boum.org/download/index.de.html
- c't Surfix: http://www.heise.de/ct/projekte/c-t-Surfix-Sicher-im-Web-1380126.html

Dateien verschlüsseln

- mcrypt, GnuPG, OpenSSL
- GnuPG hat standardisiertes Format
- portabel und austauschbar: Linux, *BSD, OS X, Windows
- OpenSSL recht weit verbreitet
- Dateien in tar-Ball packen, verschlüsseln und im Internet ablegen
- Nach der Einreise auf Laptop ziehen
- vor Ausreise wieder löschen

Datensicherung

- Backups! Backups! Backups!
- Offline, Offsite, Archiv!
- Verschlüsseln
- `tar cpf Backup-`date +%y%m%d%H%M`.tar /home/.ecryptfs/stefan/`

Manipulationen erkennen

- Fingerabdruck des Systems erstellen
- AIDE automatisiert dies
- Datenbank von /boot erstellen und vergleichen
- `/etc /bin /sbin /usr/bin /usr/sbin`
- Nach jedem Update aktualisieren
- Prüfung nicht im Live-System sondern via CD/Stick

Manipulationen erkennen

- chkrootkit: Scannt nach Anzeichen von Rootkits
- clamav: freier Virenscanner
- regelmäßige Scans sinnvoll, aber von Live-CD/Stick
- können nicht alle Schadsoftware erkenne
- c't Desinfec't

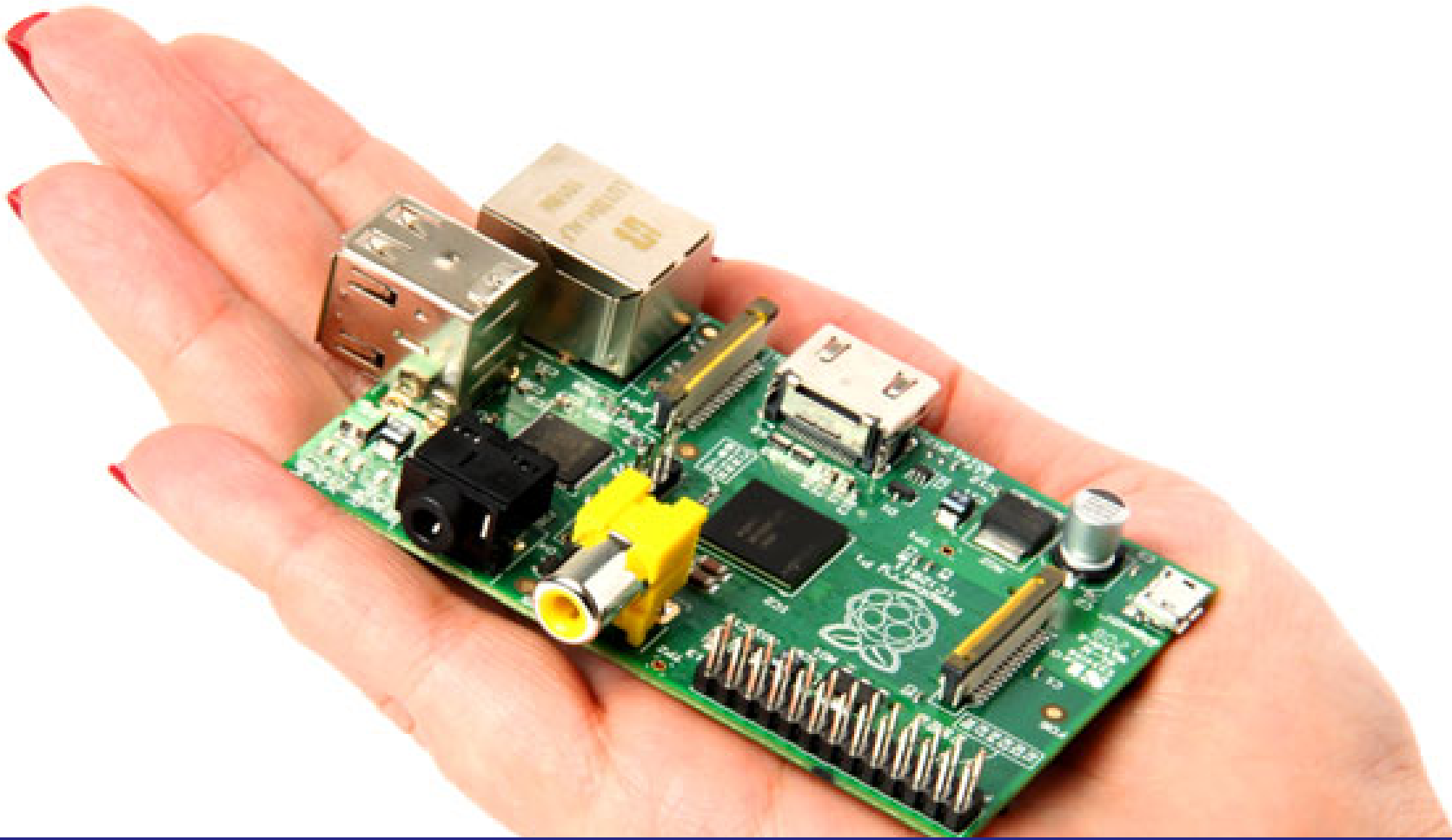
Anwendungen

- so wenig wie möglich installieren
- regelmäßig updates einspielen - sofort
- LibreOffice als Ersatz für MS Office
- nach Möglichkeit vermeiden
- Desktop Environments (KDE, Gnome, LXDE etc.) meiden

VPN

- Virtual Private Network - verschlüsselt Verbindung zwischen Laptop und Server
- Server zu Hause oder im Unternehmensnetz
- Laptop kann auf Unternehmensserver etc. zugreifen
- Server einfach einrichten z.B. Raspberry PI mit Raspbian, PC mit Ubuntu oder Hardwarelösung (Fritzbox, ASUS)
- Miet-Lösungen
- sichert Verbindungen ins Internet ab
- umgeht Zensurmaßnahmen im Internet
- eventuell verboten und geblockt
- Updates möglichst bei VPN-Verbindung einspielen

Himbeerkuchen



Anonymität mit TOR

- Internetverbindungen zurückverfolgbar
- TOR anonymisiert diese durch kaskadierende Proxys
- Anwender - Tor1 - Tor2 - Tor3 - Webseite
- Tor Browser Bundle
- TorBox/Whonix: Virtuelle Maschine
- TAILS: USB-Stick oder Virtuelle Maschine

Browser

- zentrales Einfallstor für Schadsoftware
- Chromium derzeit am sichersten, AddBlocker installieren (μBlock)
- Midori ist klein und schnell
- auf Flash, Java und Javascript möglichst verzichten
- ggf. mehrere Browser einsetzen

OwnCloud

- OwnCloud: eigenen Cloud-Server aufsetzen
- kann z.B. Google auf Android ersetzen, iOS App verfügbar
- Kalender, Aufgaben, Adressbuch, Dokumentenverwaltung etc.
- Keine Auslieferung der Daten an Google, Apple, Dropbox und Co.
- Betrieb mittels VPN zusätzlich absichern

Virtuelle Maschinen

- VirtualBox `https://www.virtualbox.org/`
- Open Source, Virtuelle Maschine
- Linux, Windows, Android, FreeBSD, NetBSD ...
- virtuelle Maschinen voneinander abgrenzen

AppArmor

- Kernelmodul, steuert Zugriffsrechte der Prozesse
- automatisch installiert
- Profile für bekannte Programme existieren und werden automatisch eingerichtet
- eigene Progile können erstellt werden
- sichert insbesondere komplexe Programme (Thunderbird, Evolution)


Yubico
Yubico
fido

U2F Unterstützung

- Google, Dropbox, Github, PAM,
- Wordpress, Django, Ruby on Rails
- OpenSSH, Login, OpenVPN, FreeRADIUS via PAM
- LastPass, Dashlane, Password Safe, Passpack, Password Tote, pwSafe, KeePass

U2F Unterstützung

- Google, Dropbox, Github, PAM,
- Wordpress, Django, Ruby on Rails
- OpenSSH, Login, OpenVPN, FreeRADIUS via PAM
- LastPass, Dashlane, Password Safe, Passpack, Password Tote, pwSafe, KeePass

Web.de unterstützt U2F nicht

- OATH-HOTP im Yubikey Personalization Tool einrichten, Secret Key generieren
- KeePass installieren und einrichten, Plugin OtpKeyProv installieren, Secret Key hinterlegen
- sicheres Passwort für Keepass vergeben
- Zufallspasswort (256HEX Bit) generieren und bei Web.de eintragen

  `09137f0ac6627f9e94e2af2342d2610bf20ff0ee929114d27b3629e3823e11ea`
- KeePass mit dem Webbrowser via Plugin verbinden
- KeePass-Datenbank mit Passwort und Token entschlüsseln, Browser holt User/Passwort für Web.de via Plugin aus DB.

- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html

- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher