

# **Kampf dem Passwort!**

## **Die Authentifizierung der Zukunft.**

## → **Heinlein Support**

- IT-Consulting und 24/7 Linux-Support mit ~25 Mitarbeitern
- Eigener Betrieb eines ISPs seit 1992
- Täglich tiefe Einblicke in die Herzen der IT aller Unternehmensgrößen
- Macher hinter mailbox.org

## → **24/7-Notfall-Hotline: 030 / 40 50 5 - 110**

- 25 Spezialisten mit LPIC-1, LPIC-2 und LPIC-3
- Für alles rund um Linux & Server & DMZ
- Akutes: Downtimes, Performanceprobleme, Hackereinbrüche, Datenverlust
- Strategisches: Revision, Planung, Beratung, Konfigurationshilfe

- Warum eigentlich kämpfen?
- 2-Faktor-Auth bei mailbox.org
- Do-it-yourself (DIY)
- Universal 2<sup>nd</sup> Faktor (Fido/U2F)

# Kampf dem Passwort!elf!!!



**First things first:**

**Was bedeutet eigentlich Authentifizierung?!**

# Zugang oder Zugriff

Da darf nicht jeder einfach ran.

# Zugang oder Zugriff

Da darf nicht jeder einfach ran.



# Authentifizierung

Person XY darf da ran.

# Zugang oder Zugriff

Da darf nicht jeder einfach ran.



## Authorisierung

Person XY darf da ran.



## Authentifizierung

Ich bin Person XY.

# Zugang oder Zugriff

Da darf nicht jeder einfach ran.



## Authorisierung

Person XY darf da ran.



## Authentifizierung

Ich bin Person XY.

## Was bedeutet also Authentifizierung?

- Authentifizierung ist der Nachweis, dass man der ist, der man vorgibt zu sein.
- Ist dieser Nachweis glaubhaft, wird man von der Gegenstelle authentifiziert.
- Glaubhaftigkeit entsteht durch geheimes Wissen oder limitierten Besitz - also z. B. Schlüssel oder Passwörter.

## Beispiel: Türschloss

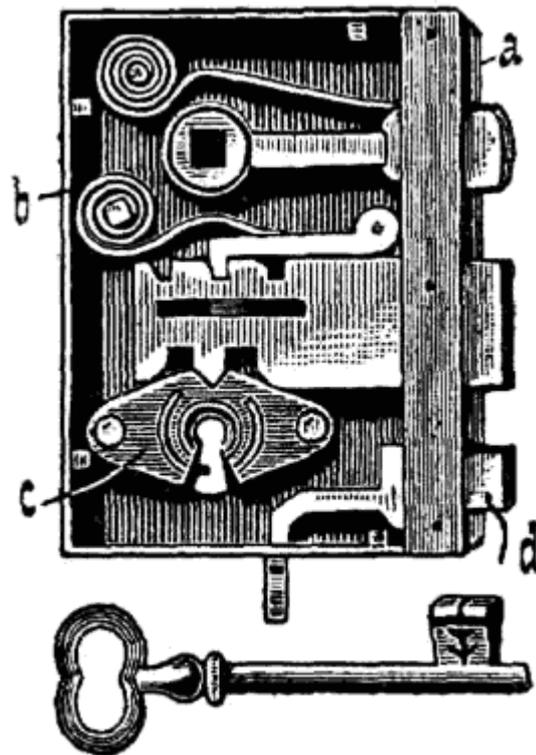


Fig. 5.

## Probleme der klassischen Authentifizierung

→ Passwörter „besitzt“ man nicht, Passwörter weiß man.

# Probleme der klassischen Authentifizierung

- Passwörter „besitzt“ man nicht, Passwörter weiß man.
- „Wissen“ allein ist ein Problem!
  - Leicht zu kopieren (Wire-Tapping, Replay-Attacks, Client/Server/DB Compromization)
  - Leicht zu erraten (Bruteforce-Attacks, Dictionary-Attacks)

## Probleme der klassischen Authentifizierung

- Passwörter „besitzt“ man nicht, Passwörter weiß man.
- „Wissen“ allein ist ein Problem!
  - Leicht zu kopieren (Wire-Tapping, Replay-Attacks, Client/Server/DB Compromization)
  - Leicht zu erraten (Bruteforce-Attacks, Dictionary-Attacks)
- Die Gegenstelle braucht das gleiche Wissen!
  - Risiko des Datendiebstahls
  - Salted HASHs in der Datenbank schützen nur bedingt

# Alternativen zur klassischen Authentifizierung

- Smart-Cards und Dongles
  - Sind die Schlüssel der digitalen Welt
  - „Besitz“ statt „Wissen“
  - Enthalten statisches Geheimnis
    - Vorteil? Nachteil?

# Alternativen zur klassischen Authentifizierung

- Smart-Cards und Dongles
  - Sind die Schlüssel der digitalen Welt
  - „Besitz“ statt „Wissen“
  - Enthalten statisches Geheimnis
    - Vorteil? Nachteil?
  
- One-Time-Passwords (OTP) (*Yubikey/FreeOTP*)
  - Algorithmischer Generator für Einweg-Passwörter
  - Eigentliches Geheimnis wird nie preisgegeben
  - Jedes Passwort ist genau ein einziges Mal gültig

# Alternativen zur klassischen Authentifizierung

- „Besitz“ allein ist auch ein Problem!
  - Diebstahl
  - Verlust
  - Defekt

# Alternativen zur klassischen Authentifizierung

- „Besitz“ allein ist auch ein Problem!
  - Diebstahl
  - Verlust
  - Defekt
  
- Lösung → 2-Faktor-Authentifizierung
  - „Wissen“ und „Besitz“ vereint
  - Die Nachteile beider wiegen sich auf
  - Die Vorteile beider komplementieren sich

## **2-Faktor-Authentifizierung mit Yubikey bei mailbox.org**

## Was ist ein Yubikey?

- Legacy USB-Tastatur
- Generiert 44-stelliges OTP
- Payload ist ein Zähler

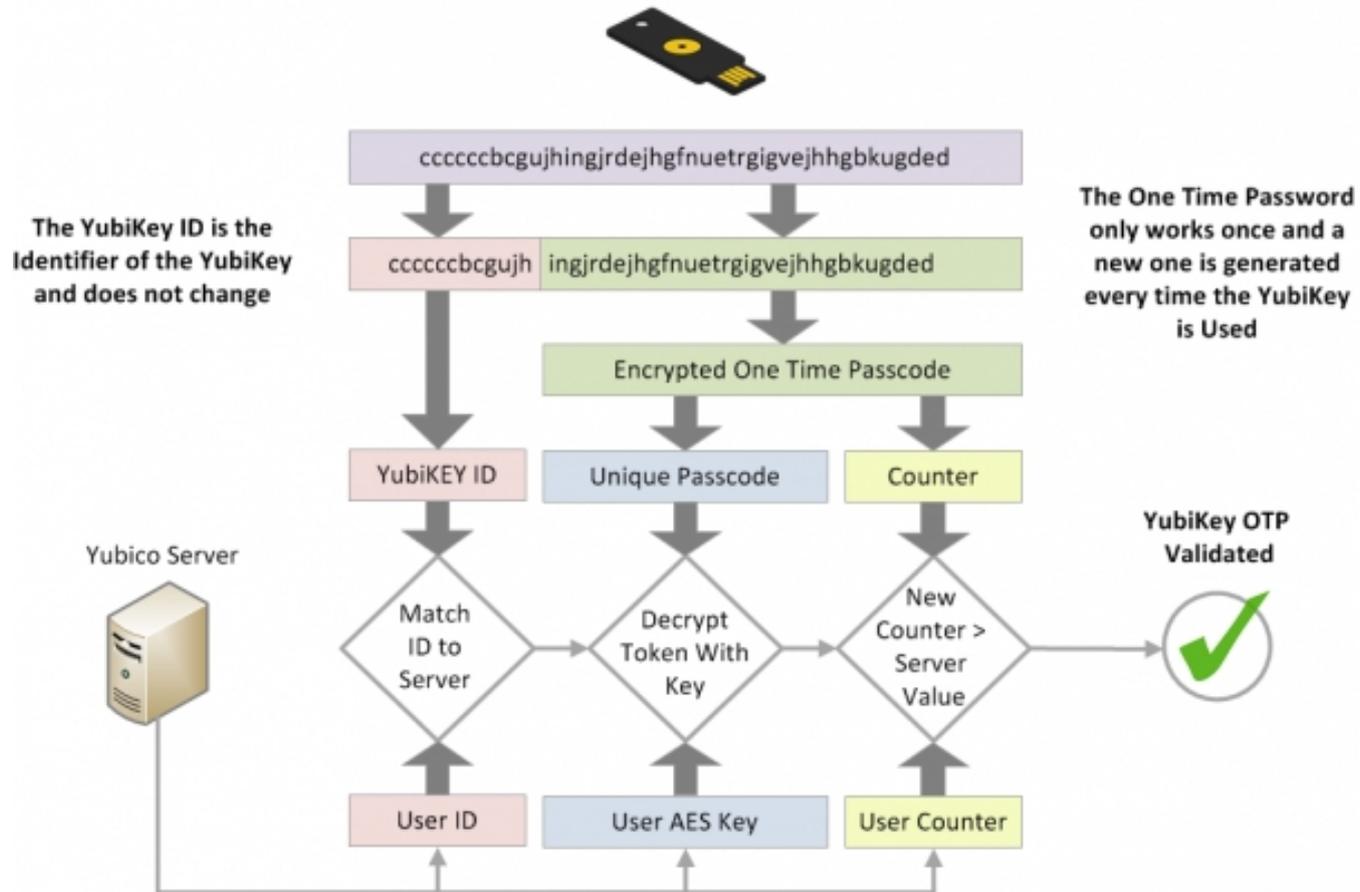


## Was ist ein Yubikey?

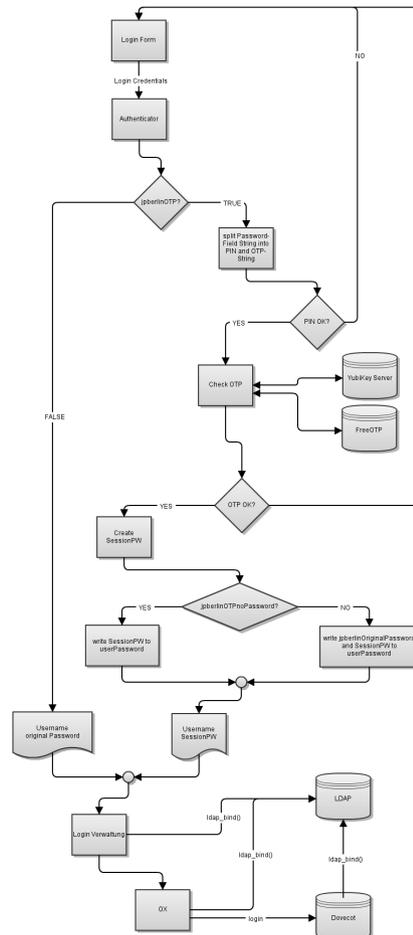
- Standard
- NANO (*ultra-small*)
- NEO (*mit NFC*)



# Wie funktioniert Yubikey OTP?



# Yubikey bei mailbox.org



# DIY Beispiele: Yubikey zum selber hacken

## DIY: Yubikey zum selber hacken

```
ssh office
[14:07] [root@futterbox ~] [995]# aptitude search yubikey
p  libapache2-mod-authn-yubikey          - Yubikey authentication provider for Apache
p  libapache2-mod-authn-yubikey:i386     - Yubikey authentication provider for Apache
p  libauth-yubikey-decrypter-perl       - yubikey token output decryptor
p  libauth-yubikey-webclient-perl      - Perl module to authenticate Yubikey against the Yubico W
p  libyubikey-dev                       - Yubikey OTP library development files
p  libyubikey-dev:i386                  - Yubikey OTP library development files
p  libyubikey0                           - Yubikey OTP handling library runtime
p  libyubikey0:i386                      - Yubikey OTP handling library runtime
p  yhsm-yubikey-ksm                      - Yubikey Key Storage Module using YubiHSM
p  yubikey-ksm                           - Key Storage Module for YubiKey One-Time Password (OTP) t
p  yubikey-personalization              - Personalization tool for Yubikey OTP tokens
p  yubikey-personalization:i386         - Personalization tool for Yubikey OTP tokens
p  yubikey-personalization-gui          - Graphical personalization tool for YubiKey tokens
p  yubikey-personalization-gui:i386    - Graphical personalization tool for YubiKey tokens
p  yubikey-server-c                     - Yubikey validation server
p  yubikey-server-c:i386                - Yubikey validation server
p  yubikey-val                           - One-Time Password (OTP) validation server for YubiKey to
[14:31] [root@futterbox ~] [996]# aptitude search yubico
p  libpam-yubico                         - two-factor password and YubiKey OTP PAM module
p  libpam-yubico:i386                    - two-factor password and YubiKey OTP PAM module
p  python-yubico                          - Python code for talking to Yubico YubiKeys
p  python-yubico-tools                   - Tools for Yubico YubiKeys
v  python2.7-yubico                       -
[14:31] [root@futterbox ~] [997]# █
```

## DIY: Yubiserver

```
ssh office
[14:43] [root@futterbox ~] [991]# aptitude show yubiserver
Package: yubiserver
State: not installed
Version: 0.4-3
Priority: optional
Section: universe/admin
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: amd64
Uncompressed Size: 144 k
Depends: libc6 (>= 2.14), libev4 (>= 1:4.04), libcrypt11 (>= 1.4.5), libmhash2, libsqlite3-0 (>= 3.5.9),
        adduser
Conflicts: yubiserver
Description: Yubikey OTP and HOTP/OATH Validation Server
 Simple and lightweight Yubikey OTP and HOTP/OATH validation server to be used with Yubico's Yubikey USB
 tokens including a powerful administration tool, yubiserver-admin, with which you can manage yubiserver's
 database by adding, deleting, activating and deactivating users that validate with OTP or HOTP/OATH tokens.

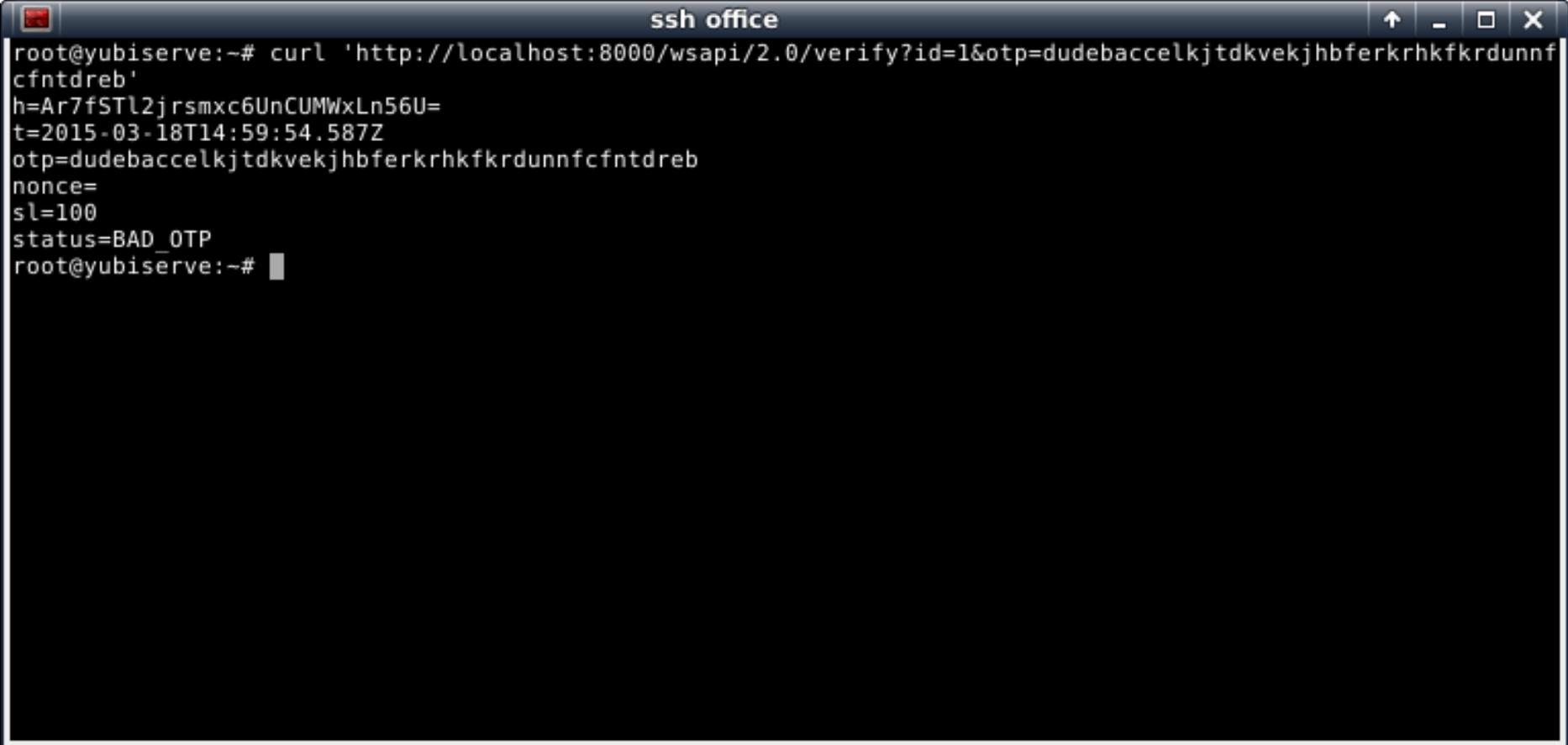
 Yubiserver implements Yubico's server side API and can be used with Yubikey USB tokens and any other client
 that can implement the same API.
Homepage: http://www.include.gr/debian/yubiserver

[14:43] [root@futterbox ~] [992]# █
```

## DIY: Yubiserver

- Kleiner Python Daemon
- Bei den gängigen Distros enthalten
- Webserver auf Port 8000
- Nimmt GET Requests mit Parametern entgegen
- Führt Yubikey OTP-Validierung durch
- Antwortet mit ASCII-Response

## DIY: Yubiserver



```
ssh office
root@yubiserve:~# curl 'http://localhost:8000/wsapi/2.0/verify?id=1&otp=dudebaccelkjtdkvekjhbfkerkrhkfkrdunnf
cfntdreb'
h=Ar7fSTl2jrsmxc6UnCUMWxLn56U=
t=2015-03-18T14:59:54.587Z
otp=dudebaccelkjtdkvekjhbfkerkrhkfkrdunnfcbntdreb
nonce=
sl=100
status=BAD_OTP
root@yubiserve:~#
```

## DIY: libpam-yubico

```
ssh office
[14:45] [root@futterbox ~] [993]# aptitude show libpam-yubico
Package: libpam-yubico
State: not installed
Version: 2.14-1
Priority: optional
Section: universe/admin
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: amd64
Uncompressed Size: 150 k
Depends: libpam-runtime (>= 1.0.1-6~), libykclient3 (>= 2.9), libldap-2.4-2 (>= 2.4.7), libykpers-1-1 (>= 1.12.0), debconf (>= 0.5) | debconf-2.0, libc6 (>= 2.14), libpam0g (>= 1.1.3), libyubikey0 (>= 1.5)
Conflicts: libpam-yubico
Description: two-factor password and YubiKey OTP PAM module
 This package provides the Yubico PAM module. It enables the use of two-factor authentication, with existing logins and passwords plus a YubiKey One-Time Password that is validated against an online validation service. The default is the free YubiCloud, but it is easy to set up a custom service.

 A second mode of operation is available using the YubiKey's HMAC-SHA-1 Challenge-Response functionality. This allows for offline validation using a YubiKey, for example on a laptop computer. However, this only works for local logins, not for instance SSH logins.
Homepage: http://code.google.com/p/yubico-pam/

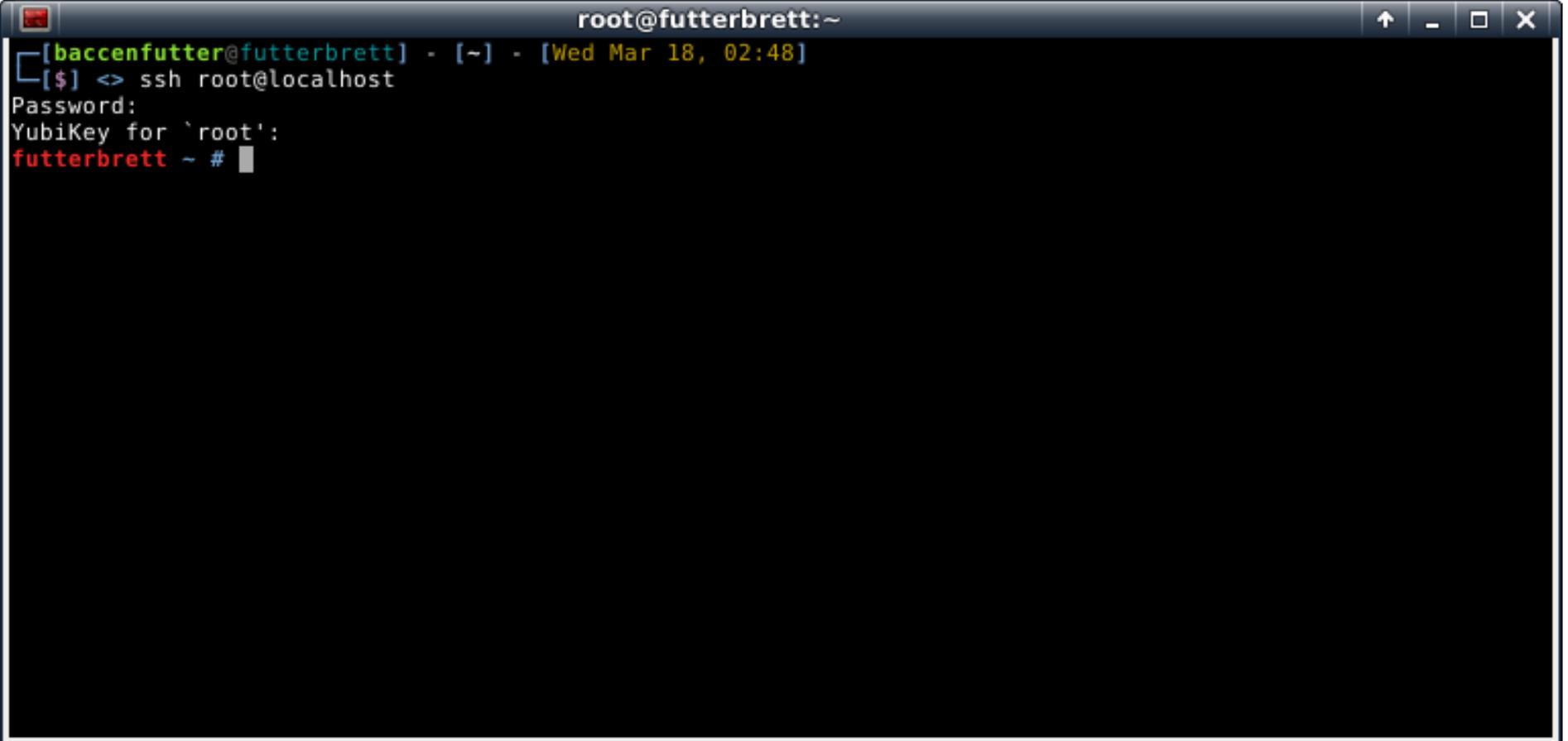
[14:45] [root@futterbox ~] [994]# █
```

## DIY: libpam-yubico



```
sudo bash
auth    include    system-remote-login
account include    system-remote-login
password include    system-remote-login
session include    system-remote-login
auth    sufficient pam_yubico.so id=1 url=http://localhost:8000/wsapi/2.0/verify?id=%d&otp=%s
/etc/pam.d/sshd [dec= 0] hex=00] [pos=0005:0001][83% of 6]
```

## DIY: libpam-yubico



```
root@futterbrett:~  
[baccenfutter@futterbrett] - [~] - [Wed Mar 18, 02:48]  
[$] <> ssh root@localhost  
Password:  
YubiKey for `root`:  
futterbrett ~ #
```

# Universal 2<sup>nd</sup> Factor: Die Fido Alliance

## Fido/U2F



- Fido Alliance
  - Google
  - Yubico
  - NXP Semiconductors
- Universal 2<sup>nd</sup> Factor (U2F)
  - Industrie-Standard für eine allgemein anwendbare 2-Faktor-Authentifizierung
- Free and Open-Source Software

## Fido/U2F



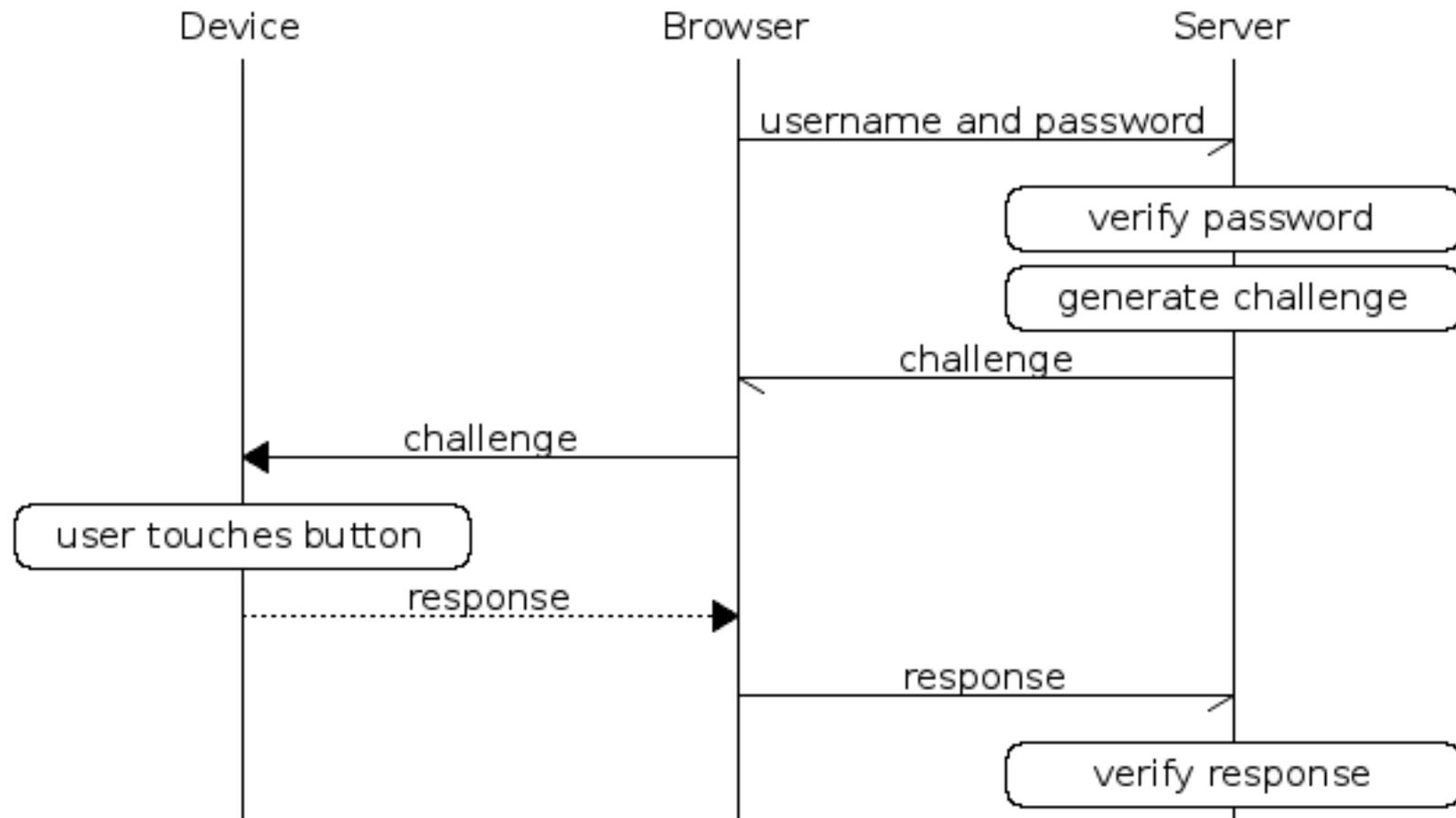
Ready



Ready

- Standard: U2F
  - Universal 2<sup>nd</sup> Faktor
- Protokoll: UAF
  - Universal Authentication Framework

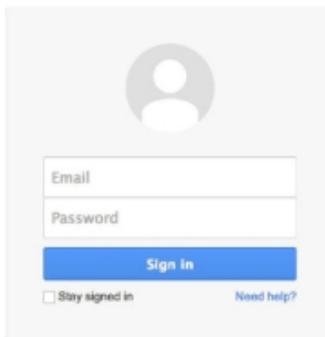
## Middleware lebt direkt im Browser



# Middleware lebt direkt im Browser

①

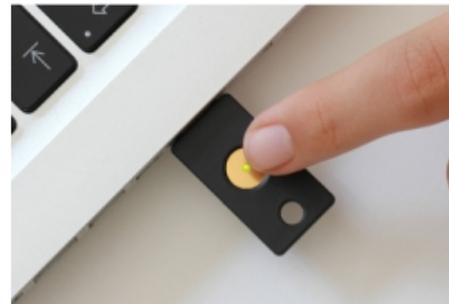
**ENTER NAME  
AND PASSWORD**



A screenshot of a web login form. At the top is a grey circle containing a white person icon. Below it are two input fields: 'Email' and 'Password'. A blue 'Sign in' button is positioned below the fields. At the bottom left, there is a checkbox labeled 'Stay signed in'. At the bottom right, there is a link labeled 'Need help?'.

②

**INSERT KEY AND  
TOUCH BUTTON**



**DONE!**



## Fido/U2F: Besondere Merkmale

- Herstellerunabhängigkeit
- Betriebssystemunabhängigkeit
- Geräteunabhängigkeit
- Protokollunabhängigkeit
- Anbieterunabhängigkeit
- Lizenzfreiheit
- Unabhängigkeit von Patentinhabern
- Öffentlich zugängliche Verfahrensbeschreibung

## Fido/U2F: Links

### → Nützliche Links

- <http://de.wikipedia.org/wiki/U2F>
- <http://fidoalliance.org/news/item/fido-1.0-specifications-published-and-final>
- <http://www.yubico.com/products/yubikey-hardware/fido-u2f-security-key/>
- <http://www.test.de/Internetsicherheit-Yubikey-Standard-kleiner-Schluessel-fuer-grossen-Schutz-4807972-0/>

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich auf neue Kontakte.



Peer Heinlein

Mail: [p.heinlein@heinlein-support.de](mailto:p.heinlein@heinlein-support.de)

Telefon: 030/40 50 51 - 42

- Wenn's brennt:
  - Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110



Unser Unternehmen

Jobs bei uns

Publikationen

Howtos

**Vorträge**

- / 11 Gebote zum IT-Management
- / Amavisd-new
- / Best Practice für stressfreie Mailserver
- / Cloud Computing
- / Disaster Recovery/P2V mit ReaR
- / Dovecot IMAP-Server
- / Dovecot-Server

## UNSERE VORTRÄGE ZUM NACH- UND ZUHÖREN...

Wir halten viele Vorträge: LinuxTage, CeBIT, Unternehmensveranstaltungen oder Branchen-Messen. Hier finden Sie eine Auswahl der populärsten Vorträge. Oft nicht nur mit Folien-PDFs, sondern auch mit Video- oder Tonaufzeichnungen.

**[Vortrag von uns] Best Practice für stressfreie Mailserver**

Ein Mailserver ist ein sensibles Geschöpf: Auch wenn oberflächlich alles läuft, d.h. Mails akzeptiert und versandt werden, lauern im Detail viele kleine Fallstricke und Haken. Hier entscheidet sich, ob der Mailverkehr sauber und reibungslos läuft, in der Annahme die Spreu vom Weizen getrennt wird und ob im Versand die Kommunikation mit anderen Mailservern problemlos klappt. [Mehr →](#)

 [Mailserver-Best-Practice.pdf](#)

**[Vortrag von uns] amavisd-new: Schöne Geheimnisse und komische Ideen.**

Amavisd-new ist ein beliebtes Mittel, um Mails nach Spam und Viren zu filtern: Schnell, robust.

### Blog: Heinlein Support

- DDoS-Attacke durch recursive DNS-Queries
- Wenn unser Support an seine Grenzen stößt
- Mailman-Listen mit gleichem Localpart / unter mehreren Domains

### News

Wir suchen: Sekretärin, Linux-Consultant & PHP-Anwendungsentwickler

Neue Schulung: "Bacula Administration" ab 22.10.12

**Ja, diese Folien stehen auch als PDF im Netz...**  
**<http://www.heinlein-support.de/vortrag>**

**Soweit, so gut.**

**Gleich sind Sie am Zug:  
Fragen und Diskussionen!**

**Wir suchen neue Kollegen für:**

**Helpdesk, Administration, Consultanting!**

**Wir bieten:**

**Spannende Projekte, Kundenlob, eigenständige  
Arbeit, keine Überstunden, Teamarbeit**

**...und natürlich: Linux, Linux, Linux...**

**<http://www.heinlein-support.de/jobs>**

## Und nun...



- Vielen Dank für's Zuhören...
- Schönen Tag noch...
- Und viel Erfolg an der Tastatur...

**Bis bald.**

# Heinlein Support hilft bei allen Fragen rund um Linux-Server

## HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

## HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

## HEINLEIN CONSULTING

Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

## HEINLEIN ELEMENTS

Hard- und Software-Appliances und speziell für den Serverbetrieb konzipierte Software rund ums Thema eMail.