Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

Kampf dem Passwort!
Die Authentifizierung der Zukunft.

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

- **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

heinlein

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

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

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

Kampf dem Passwort!elf!!!

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

First things first:

Was bedeutet eigentlich Authentifizierung?!

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

Zugang oder Zugriff

Da darf nicht jeder einfach ran.

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

Zugang oder Zugriff

Da darf nicht jeder einfach ran.

↑

Authorisierung

Person XY darf da ran.

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

Zugang oder Zugriff

Da darf nicht jeder einfach ran.

↑

Authorisierung

Person XY darf da ran.

↑

Authentifizierung

Ich bin Person XY.

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

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.

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

Beispiel: Türschloss

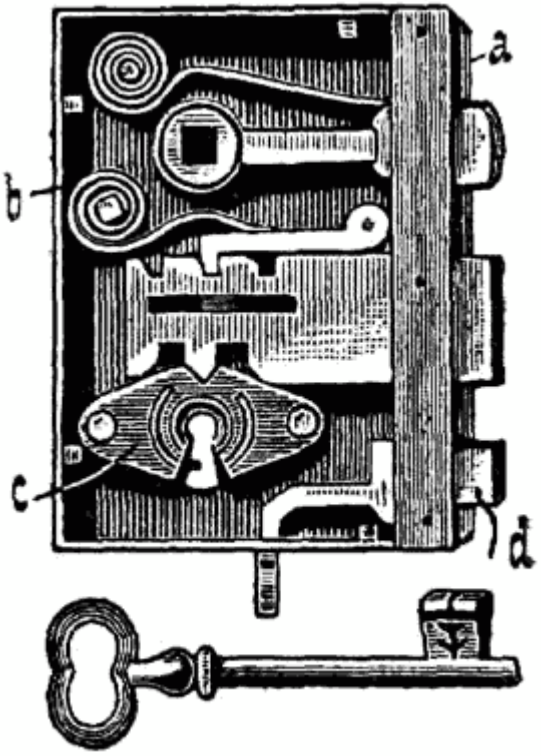


Fig. 5.

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)

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

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

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

Alternativen zur klassischen Authentifizierung

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

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

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

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

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

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

2-Faktor-Authentifizierung mit Yubikey bei mailbox.org

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

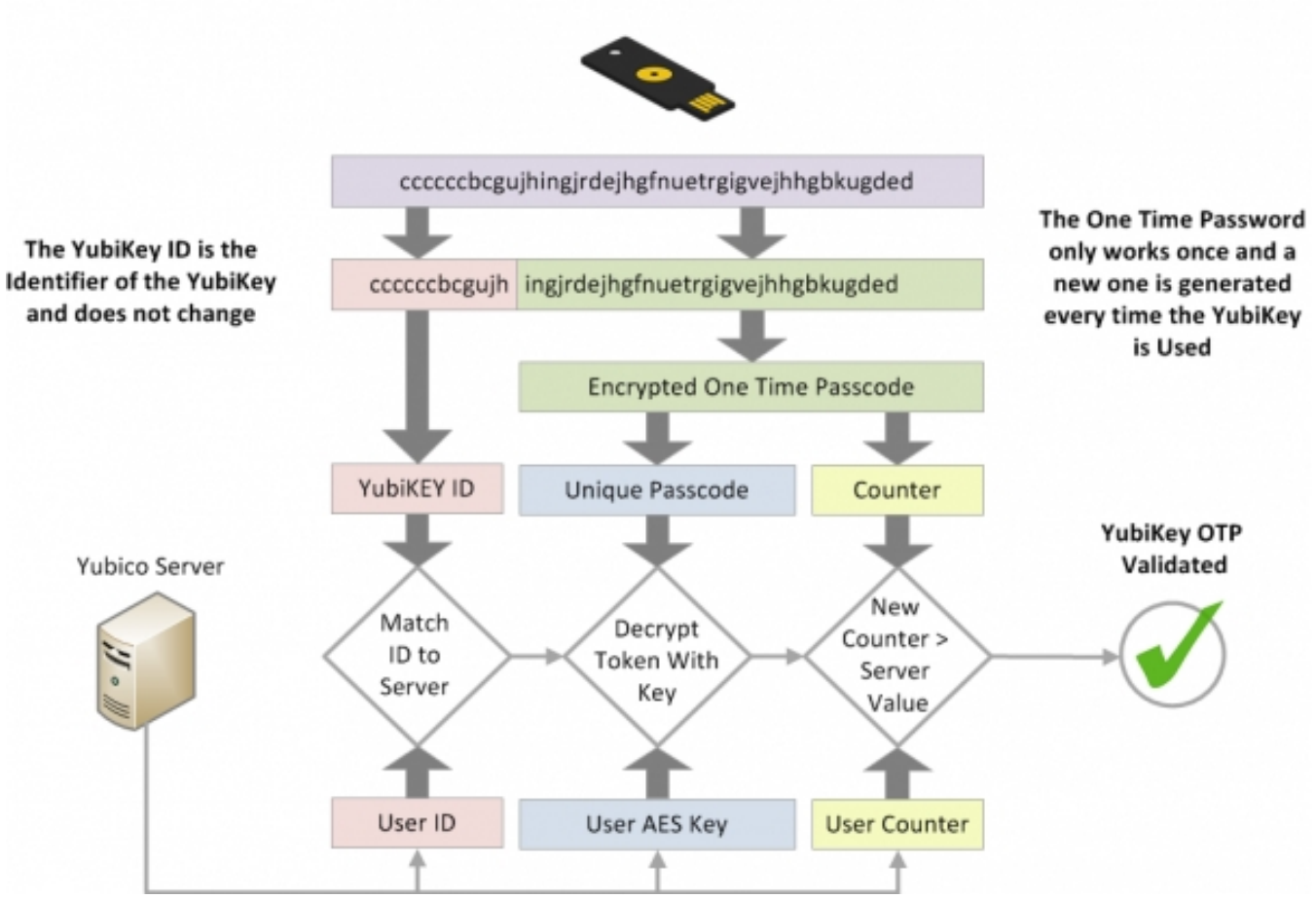
Was ist ein Yubikey?

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

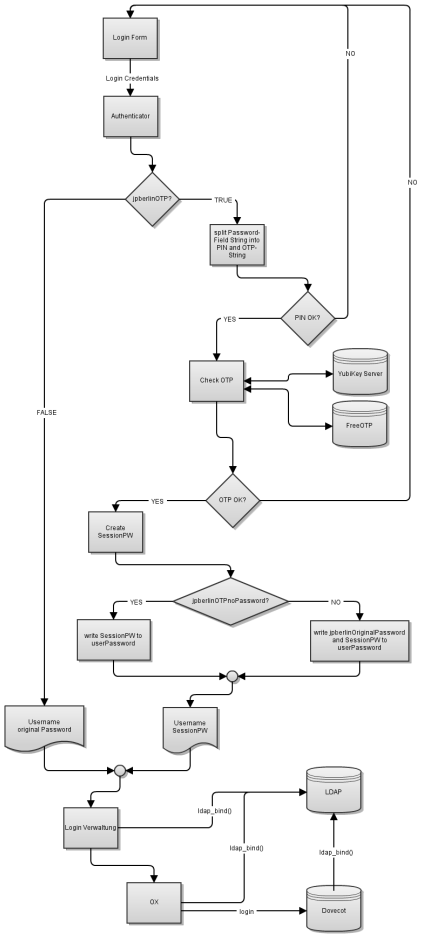
Was ist ein Yubikey?

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

Wie funktioniert Yubikey OTP?



Yubikey bei mailbox.org

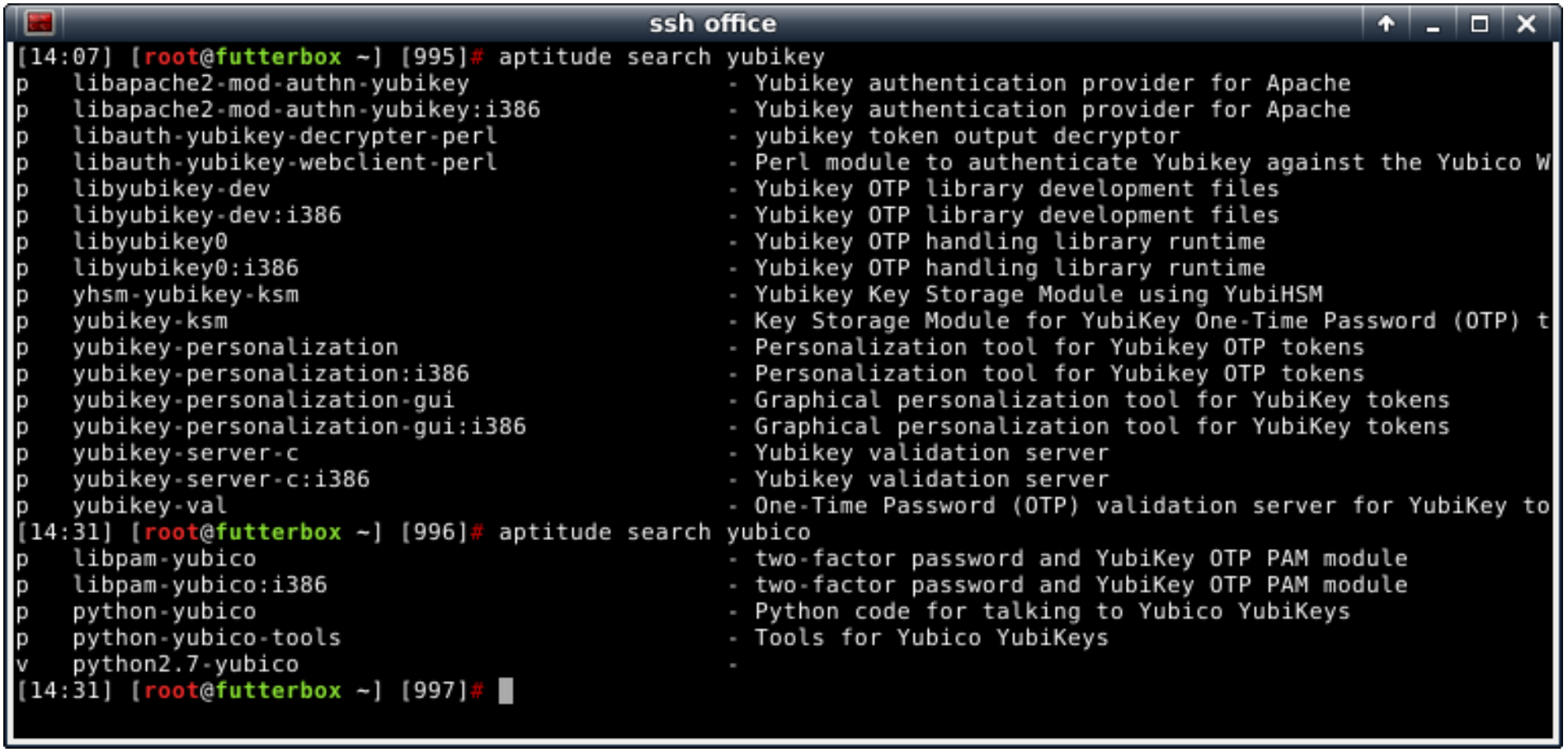


Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

DIY Beispiele:
Yubikey zum selber hacken

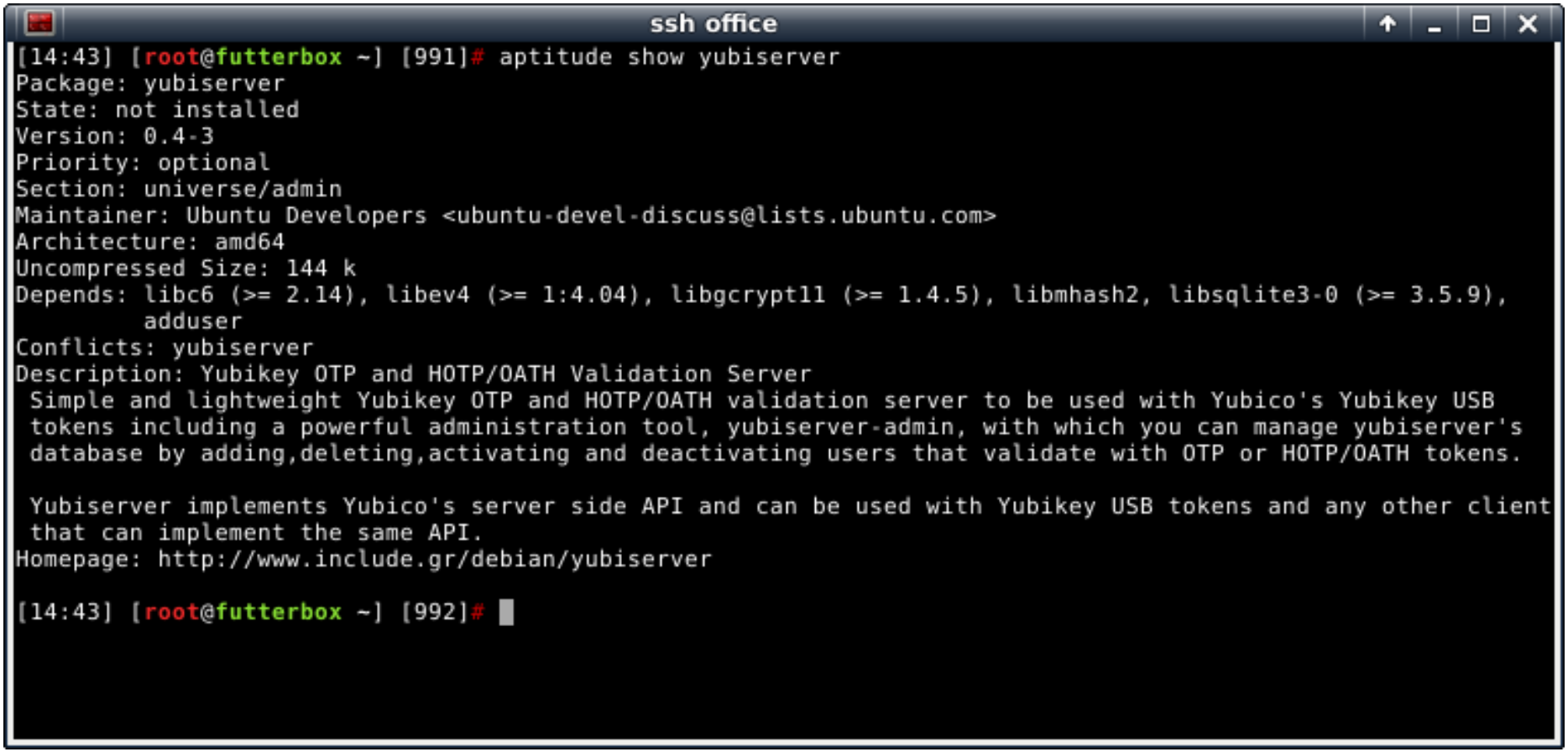
Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

DIY: Yubikey zum selber hacken



Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

DIY: Yubiserver



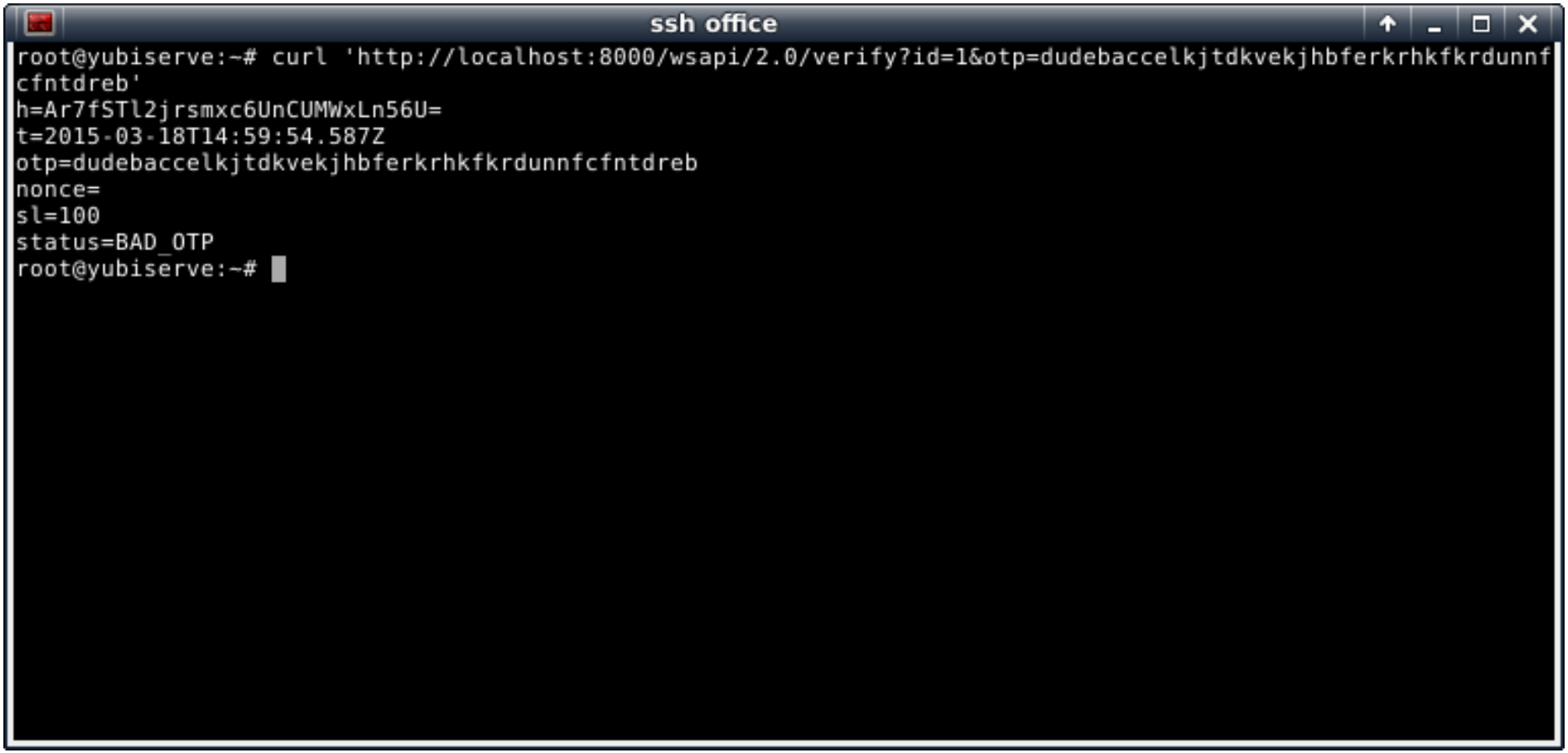
Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

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

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

DIY: Yubiserver



Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

DIY: libpam-yubico

ssh office

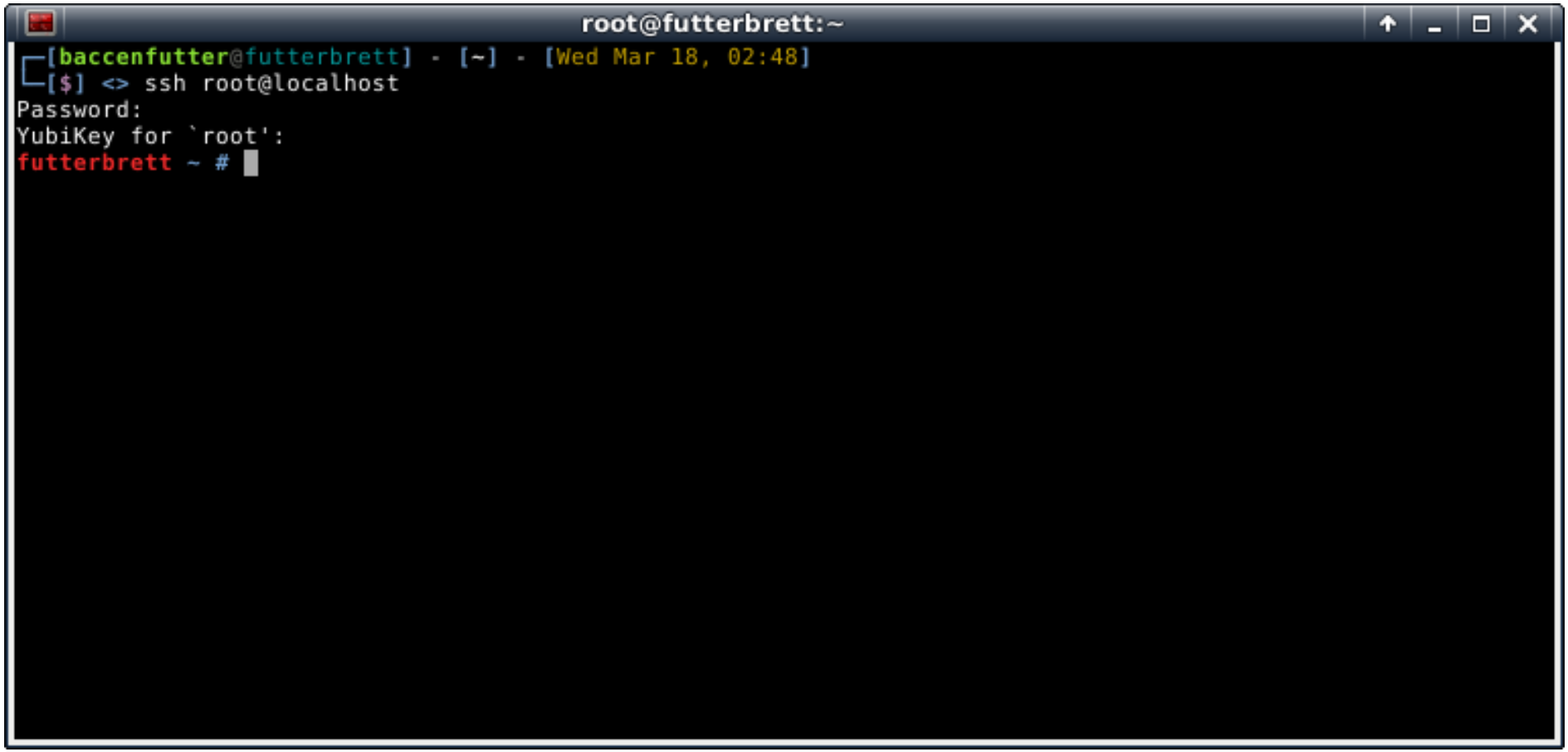
```
[14:45] [root@futterbox ~] [993]# aptitude show libpam-yubico
Package: libpam-yubico
State: not installed
Version: 2.14-1
Priority: optional
Section: universe/admin
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: amd64
Uncompressed Size: 150 k
Depends: libpam-runtime (>= 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]#
```

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

DIY: libpam-yubico

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

DIY: libpam-yubico



Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

Universal 2nd Factor: Die Fido Alliance

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

Fido/U2F

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

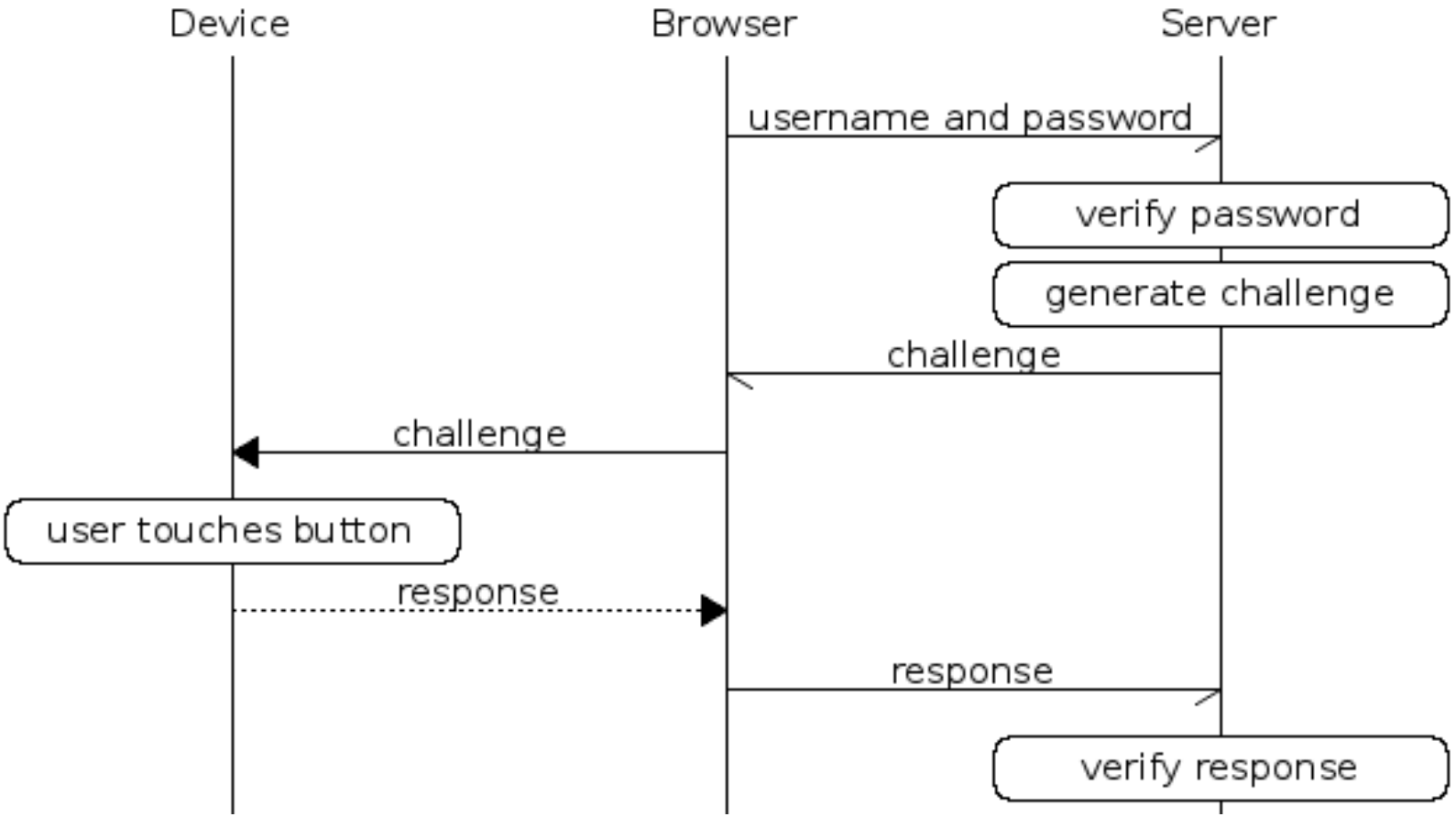
Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

Fido/U2F

- Standard: U2F
  - Universal 2nd Faktor
- Protokoll: UAF
  - Universal Authentication Framework

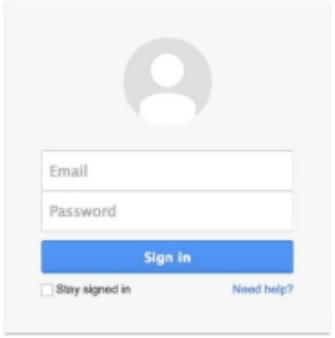
Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

Middleware lebt direkt im Browser



Middleware lebt direkt im Browser

1 ENTER NAME AND PASSWORD



2 INSERT KEY AND TOUCH BUTTON

DONE!

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

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

Telefon: 030/40 50 51 - 42

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

heinlein

Kampf dem Passwort
[Secure Linux Administration Conference 2015]
Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

Ja, diese Folien stehen auch als PDF im Netz...

http://www.heinlein-support.de/vortrag

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

Soweit, so gut.

Gleich sind Sie am Zug:
Fragen und Diskussionen!

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

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

Brian Wiborg & Robert Sander <r.sander@heinlein-support.de>

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.