embedded projects GmbH

User Manual

picosafe login

2th November 2012

Holzbachstraße 4, D-86152 Augsburg
Tel +49 (0) 821 279599-0
Fax +49 (0) 821 279599-20
shop.embedded-projects.net

Inhaltsverzeichnis

Holzbachstraße 4, D-86152 Augsburg
Tel +49 (0) 821 279599-0
Fax +49 (0) 821 279599-20
shop.embedded-projects.net

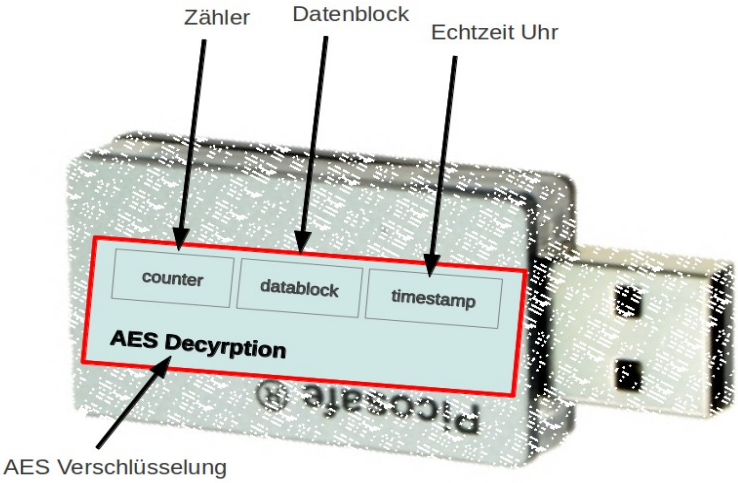
1 Introductory Information

1.1 Introduction

1.2 Features

- Works as USB keyboard
- Secure Flash for AES Key + Datablock
- Hardware based Timestamp

1.3 Security Concept



The increased safety for the registration process is that the USB hardware issues a unique key, can verify that only the server. This is similar to a radio car keys. Datagram as a packet is

Holzbachstraße 4, D-86152 Augsburg
Tel +49 (0) 821 279599-0
Fax +49 (0) 821 279599-20
shop.embedded-projects.net

transmitted, that is composed of several components:

- Counter that is incremented each key press
- Current date and time
- Specific data block

This datagram is encrypted with an AES key. The AES key is written by the owner of the website in the memory stick. This can then never read again - ensures the safety of the microprocessor.

2 Manage Picosafe Login

Administrators of the the Picosafe Login Sticks needs some small tools to configure the tokens.

2.1 Install software tools

```
cd libpiocsafelogin

sudo apt-get install python-dev libc6-dev libusb-dev gcc
sudo python setup.py install
```

2.2 Initialize empty Picosafe Key

```
sudo python init.py -c "Firma A" -o "Hans Bieber" -p soopu9goBoay9vongooth2ooLu8keed1eeng5jo7th -d "Beschreibung"
```

2.3 Show Stick Informations

```
sudo python show.py
```

2.4 Check Password

```
python verify.py -s soopu9goBoay9vongooth2ooLu8keed1eeng5jo7th
```

Then press the button on the key and the <enter> on your keyboard. Something like this should appeare:

```
yQ59ZWTrcuDFkYQt9f9TE7g..
(1, 73, 1351942937)
yJt84-df2nDebDKRF1AA55g..
(1, 74, 1351942942)
ygMB4cy70nX70y5cNBcTFFA..
(1, 75, 1351942943)
```

Every time the button is pressed the internal counter of the picosafe key is increment. As last number the actual timestamp of the internal rtc of the key is printed on the screen.

Holzbachstraße 4, D-86152 Augsburg
Tel +49 (0) 821 279599-0
Fax +49 (0) 821 279599-20
shop.embedded-projects.net

2.5 Reset Picosafe Key with Master Key

Open the file reset.py. Change master key to your own.

```
sudo python reset.py
```

3 Integration PHP Application

Der USB-Stick ist eine Ergänzung zu Benutzername und Passwort. In der bestehenden Anwendung hat man irgendwo die Prüfung ob Benutzername und Passwort stimmen. Genau an dies Stelle kommt die Picosafe Login Funktion.

Damit die Picosafe Klasse jederzeit durch eine neue ausgetauscht werden kann muss man dieser einzeln für den aktuellen Benutzer die notwendigen Datenfelder für die Hardware mitgeben:

Das ganze sieht dann grob so aus:

```
include("class.picosafelogin.php");
$myPicosafe = new PicosafeLogin();

// die Variablen $aes, $datablock, $counter muss man selber zuvor füllen.
$myPicosafe->SetUserAES($aes);
$myPicosafe->SetUserDatablock($datablock);
$myPicosafe->SetUserCounter($counter);

if($username == $check_username && $password_hash == md5($password) &&
$myPicosafe->LoginOTP($token))
{
     echo "Anmeldung erfolreich!";
     // Synchronisation Counter
     $newcounter = $myPicosafe->GetLastValidCounter();
     // BITTE PROGRAMMIEREN: newcounter in die eigene Datenstruktur übertragen

} else {
     echo "Fehler! Falcher Benutzername, Passwort oder Token";
}
```

3.1 Schritte

Um den USB-Stick als Erweiterung für das Verfahren Benutzername + Passwort verwenden zu können muss man im wesentlichen drei Schritte machen:

- Erweiterung HTML Formular
- Erweiterung Benutzertabelle für neue Stick Felder
- Erweiterung der Loginfunktion mit einer weiteren Bedingung (die für den Stick)

Holzbachstraße 4, D-86152 Augsburg
Tel +49 (0) 821 279599-0
Fax +49 (0) 821 279599-20
shop.embedded-projects.net

HTML Formular

Das Formular muss im ein Feld erweitert werden, so dass man dort wo Benutzername und Passwort vom Server entgegen genommen werden noch das Feld token hinzufügen kann. Der Stick gibt wie eine Tastatur das Passwort aus. Man muss nur den Cursor im richtigen Textfeld stehen haben.

```
<input type="text" size="20" name="token">
```

3.2 Benutzertabelle mit Stick Felder

Entweder erweitert man die eigene Tabelle oder erstelle eine neue.

3.3 Eigene Datenbank erweitern

Zusätzlich neben dem Benutzername und Passwort bzw. Passworthash werden benötitg

- aes varchar(32)
- datablock varchar(10)
- counter int(11)

Im Feld aes wird der AES Schlüssel hinterlegt. Der Schlüssel aes und datablock liegt auf einer Karte dem Stick bei Lieferung bei, bzw. kann man mit den Tools diese jederzeit selber ändern. Der Counter wird später nach jedem Login um eins erhöht. Server und Stick synchronisieren so regelmäßig Ihren Counter.

3.4 Vorgeschlagens Datenbank Schema verwenden

Alternativ kann man eine extra Tabelle für diese Informationen erstellen.

```
CREATE TABLE IF NOT EXISTS picosafelogin (
   user varchar(255) NOT NULL,
   aes varchar(255) NOT NULL,
   datablock varchar(255) NOT NULL,
   counter int(11) NOT NULL,
   hw int(11) NOT NULL,
   locked int(1) NOT NULL,
   PRIMARY KEY (`user`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1;
```

3.5 Typische Fehler

3.5.1 Uhrzeit auf Server falsch

Die Uhrzeit vom Server wir aktuell in der class.picosafelogin.php in der Methode GetServerTimestamp() mit time() ermittelt. Es wird ein Unix-Timestamp zurückgegen. Der Stick gibt die Uhrzeit als UTC Timestamp aus.

Holzbachstraße 4, D-86152 Augsburg
Tel +49 (0) 821 279599-0
Fax +49 (0) 821 279599-20
shop.embedded-projects.net

Um zu prüfen was der Stick für einen Timestamp geschickt hat man in der Methode

```
function LoginOTP($givenOtp)
```

nach der Zeile:

```
$result = $this->ParseOTP($givenOtp,$key,$datablock);
```

folgendes einfügen:

```
echo "Hardware Zeit: ".$result["timestamp"]." Server Zeit: ".time();
```

So sieht man am schnellsten ob alles passt.

3.5.2 Schluessel falsch bzw. falsche Laenge

Am Ende von der Methode

```
function ParseOTP($givenOtp,$key,$datablock)
```

Kann man folgende Zeilen aktivieren:

```
//echo "Nummer: " . $n . "\n";
//echo "Datenblock: " . $plain . " (" . $data . ") \n";
//echo "Timestamp: " . $timestamp . "\n";
//echo "Datetime: " . date("d.m.Y H:i:s",$timestamp) . "\n";
```

So sieht man immer ob die Entschlüsselung passt. Wechselt der Timestamp wie verrückt herum oder ist der Datenblock jedesmal nach einem Tastendruck auf den Stick neu deutet es auf einen falschen bzw zu kurzen oder zu langen Schlüssel hin.

3.6 Administrations Oberfläche

Im Ordner php liegt eine Datei admin.php. Diese ermöglicht eine einfache Administration von Sticks für Benutzer, wenn man keine eigene Admin Oberfläche hat oder schreiben möchte.

Holzbachstraße 4, D-86152 Augsburg
Tel +49 (0) 821 279599-0
Fax +49 (0) 821 279599-20
shop.embedded-projects.net

picosafe

List Create Logout

Please Login

Database:

User:

Password:

Login

picosafe

List Create Logout

User	AES	Datablock	Counter	HW	Lock
demo	iQRyGAidN5d6olJFndzUnb9wJA0TsHq1	tbmKSfSDPF	0	1	0
demo2	UXPTAnEtlWGLZHwPnaQsUdWSuwHV63hx	Jdy3s1ntrf	0	1	0
max	S7mWXviQaDhvTlnWWlK2q26gZsRsKxyy	OIGZTLkDoj	0	1	0

Holzbachstraße 4, D-86152 Augsburg
Tel +49 (0) 821 279599-0
Fax +49 (0) 821 279599-20
shop.embedded-projects.net

Last edited by embeddedprojects,

4 Flash own Master Key

To flash an own Master Key you need the Picosafe Key Programmer. Connect it with an USB cable to your Linux PC.

Holzbachstraße 4, D-86152 Augsburg
Tel +49 (0) 821 279599-0
Fax +49 (0) 821 279599-20
shop.embedded-projects.net

Abbildung 1: Picosafe Key Programmer

Install Toolchain for Picosafe Key

```
sudo apt-get install gcc-avr gdb-avr binutils-avr avr-libc avrdude
```

cd firmware

```
gedit picosafelogin.c
```

Find row:

```
const prog_char MASTER_PASSWORD[] = "coa7Heeh8ChaiR9XaikeeRei4fuo2kah";
```

Change the master password (32 Signs) and save file. Compile the firmware with your new master key:

```
make
```

Connect an Picosafe Key with the Programmer

Holzbachstraße 4, D-86152 Augsburg
Tel +49 (0) 821 279599-0
Fax +49 (0) 821 279599-20
shop.embedded-projects.net

Abbildung 2: Picosafe Key connected with the programmer

Programm Fuse Bits:

```
make fuse
```

Programm firmware:

```
make program
```

Lock Firmware (After this step you can never change the master key!)

```
make lock
```


Holzbachstraße 4, D-86152 Augsburg
Tel +49 (0) 821 279599-0
Fax +49 (0) 821 279599-20
shop.embedded-projects.net