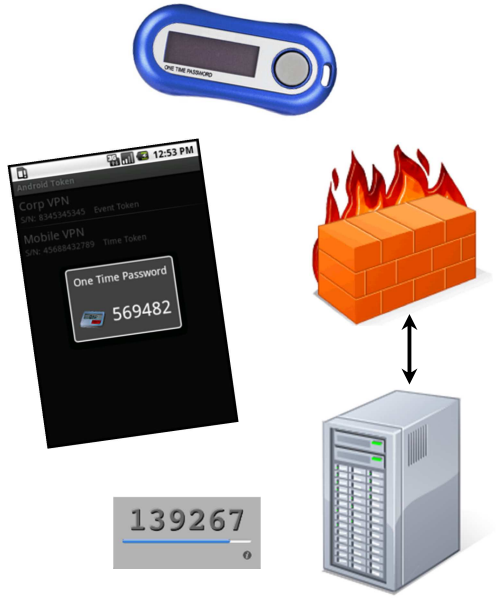
SysCo®

multiOTP

http://www.multiotp.net/

multiOTP Free Strong Authentication Presentation and Deployment for Linux And Windows

(with mOTP, OATH/TOTP and OATH/HOTP support)



André Liechti

Version 3.0.4

September 15, 2010

Contents Overview

1. Introduction

multiOTP is a PHP class and a powerful command line utility developed by SysCo systèmes de communication sa in order to provide a completely free and easy operating system independent server side implementation for strong two factors authentication solution.

Nowadays, spywares, viruses and other hacking technologies are regularly stolen passwords typed by the user.
By using a strong two factors authentication solution, the stolen passwords cannot be stored and used later anymore because each password (called OTP for One-Time Password) is only valid for one authentication and will failed if used a second time.

multiOTP supports hardware and software tokens with different One-Time Password algorithms like OATH/HOTP, OATH/TOTP and mOTP (Mobile-OTP). The data storage of the command line utility is flat files based in order to simplify deployment in a few minutes. **multiOTP** can be easily integrated in free RADIUS servers like FreeRADIUS under Linux or TekRADIUS LT under Windows.

multiOTP can even be installed on laptops, for example if you need strong authentication on your laptops and you are not sure that you will have Internet access during the strong authentication process. This is possible because we have sponsored the development of TekRADIUS LT which is a light RADIUS server for Windows (using SQLite as backend database) that works well with server versions of Windows but also with desktop versions of Windows like XP, Vista or 7.

We are hoping that this whitepaper will be useful for your business. Don't hesitate to contact us by sending an email to developer@sysco.ch if you have suggestions, comments, or if you know related products that can be integrated in this document.

2. Installation and configuration of the multiOTP command line utility

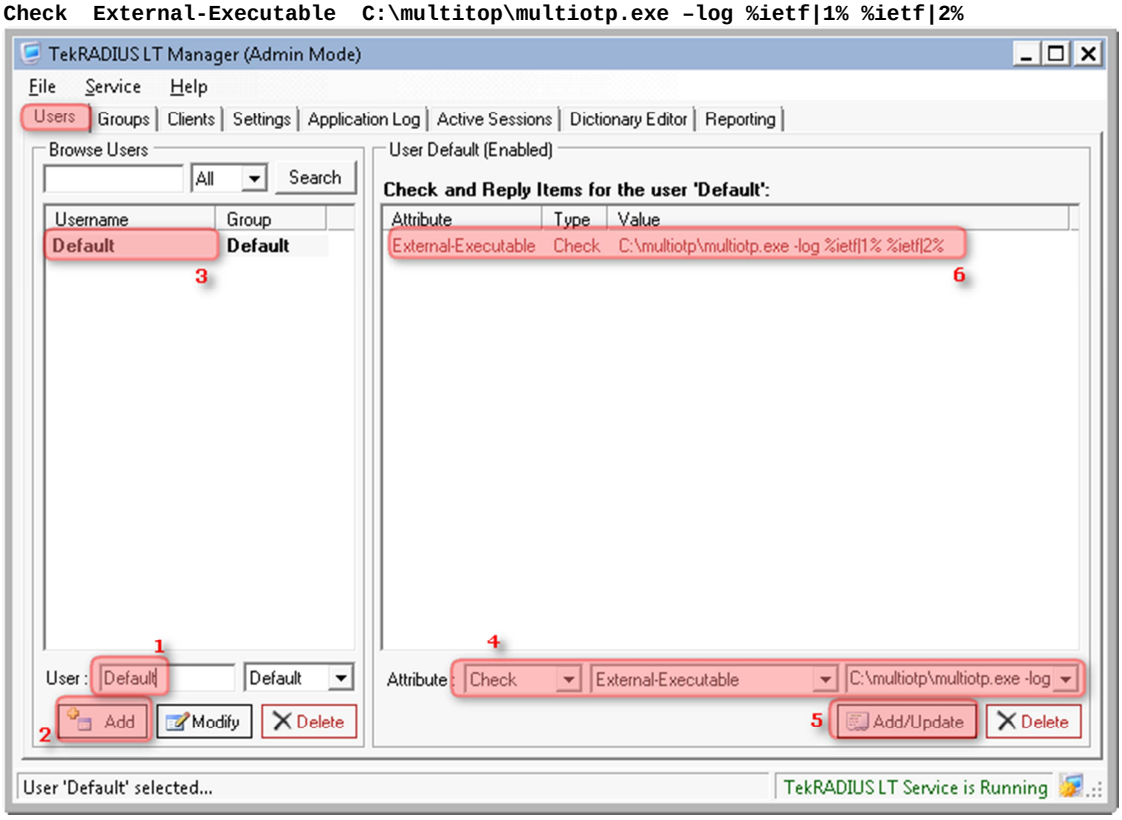
The installation of the multiOTP command line utility is really easy on both Linux and Windows servers. You will have to install first the utility itself, and then you will have to setup your RADIUS server in order to use the command line utility as an external authentication provider.

a) Linux

- Copy the `multiotp.php` file somewhere on your server (for example in the folder `/usr/local/bin/multiotp`) and make it executable by chmod'ing it to +x
- The script needs to have read/write access rights on his folder
- Try to run it. It should display the help page with version information and syntax usage
- You are now already able to create your first token! Try to create the sample token proposed in the RFC 4226:
  ```
  multiotp –log -create test HOTP 31323334353637383930313233343536373839 30 1234 6 0
  ```
- Check that everything is working correctly by typing the first code for the sample token
  ```
  multiotp -debug test 755224
  ```
  You should receive the answer `0 OK: Token accepted`
- Check that the same password is not working anymore
  ```
  multiotp -debug test 755224
  ```
  You should now receive the answer `99 ERROR: Authentication failed`
- Try now to synchronize the sample token with two consecutive values
  ```
  multiotp -debug -resync -status test 338314 254676
  ```
  You should receive the answer `14 INFO: Token has been resynchronized successfully`
- Be sure that FreeRADIUS is installed. If not, please install it using the package installer of your Linux distribution. For a Debian distribution for example:
  ```
  apt-get install freeradius
  ```
- Add a DEFAULT entry in the `/etc/freeradius/users` configuration file like this:
  ```
  DEFAULT Auth-Type = Accept
  Exec-Program-Wait = "/usr/local/bin/multiotp.php %{User-Name} %{User-Password}",
  Fall-Through = Yes,
  Reply-Message = "Hello, %{User-Name}"
  ```
- Add an entry in the `/etc/freeradius/clients.conf` configuration file for the subnet of your devices like this:
  ```
  client 192.168.0.0/24 {
      secret    = mysecret
      shortname = default-secret
  }
  ```
- That's it, you're done!

b) Windows

- Copy the `multiotp.exe` file somewhere on your server (for example in the folder `C:\multiotp\`). Alternatively, you may also launch the `multiotp.msi` installer which will install a smaller `multiotp.exe` and several DLL's. For security reasons, the binary file is digitally signed by SysCo systemes de communication sa.
- The executable needs to have read/write access rights on his folder
- Try to run it. It should display the help page with version information and syntax usage
- You are now already able to create your first token! Try to create the sample token proposed in the RFC 4226:
  `multiotp -log -create test HOTP 31323334353637383930313233343536373839 30 1234 6 0`
- Check that everything is working correctly by typing the first code for the sample token
  `multiotp -debug test 755224`
  You should receive the answer **`0 OK: Token accepted`**
- Check that the same password is not working anymore
  `multiotp -debug test 755224`
  You should now receive the answer **`99 ERROR: Authentication failed`**
- Try now to synchronize the sample token with two consecutive values
  `multiotp -debug -resync -status test 338314 254676`
  You should receive the answer **`14 INFO: Token has been resynchronized successfully`**
- Install TekRADIUS LT which can be freely downloaded at http://www.tekradius.com
- Using the TekRADIUS LT Manager, create a user called **`Default`** that belongs to the existing **`Default`** group with the following attribute:
  `Check External-Executable C:\multitop\multiotp.exe -log %ietf|1% %ietf|2%`



- In the Clients Tab, add a `Default` client with a specific secret. This will be the radius secret for all devices that or not specifically declared in your radius server.
- That's it, you're done!

3. Software tokens

A lot of software tokens exist, for various clients and with different algorithms supports.

a) mOTP (Mobile-OTP)

- **iPhone**: iOTP from PDTS (type iOTP in the Apple AppStore)
- **Android** : Mobile-OTP (http://motp.sf.net/Mobile-OTP.apk)
- **PalmOS**: Mobile-OTP (http://motp.sf.net/mobileotp_palm.zip)
- **Java J2ME** (Nokia and other phones): MobileOTP (http://motp.sf.net/MobileOTP.jad)
- …

b) OATH/HOTP and OATH/TOTP

- **oathtoken** for iPhone: http://code.google.com/p/oathtoken/, AppStore: oathtoken
- **androidtoken** for Android: http://code.google.com/p/androidtoken/
- ...

4. Hardware tokens (commercial)

A lot of manufacturers are providing OATH compatible tokens. If you plan to use your token with more than one authentication server, take if possible an OATH/TOTP (time based) token instead of an OATH/HOTP (event based) one, because for event based token, the next token position is stored on the server side and it could be necessary to resynchronize your token if you have used it several times on other(s) server(s).

- Feitian provides both OATH compliant TOTP and HOTP tokens, and SysCo distributes these tokens in Switzerland 
- ZyXEL provides OATH/HOTP (event based) tokens called ZyWALL OTP v1 (they are rebranded Authenex A-Key 3600) 
- ZyXEL provides new OATH/HOTP tokens called ZyWALL OTP v2 (they are rebranded Aladdin eToken PASS) 
- Seamoon provides OATH/TOTP tokens called Seamoon KingKey
- Verisign, Aladdin, Authenex and others are also providing OATH compatible tokens
- ...

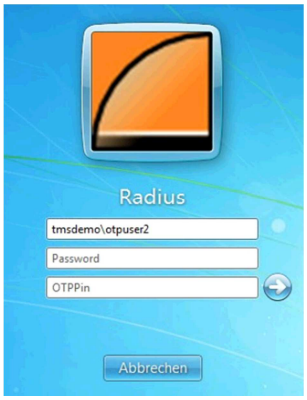
If hardware tokens are shipped with an XML Portable Symmetric Key Container definition (like we do for the Feitian tokens), tokens can be imported directly in the **multiOTP** command line utility. Have a look on the help page of **multiOTP** or in the readme.txt file for more details.

5. Strong authentication compatible software

Some software solutions are ready to provide strong authentication solution compatible with multiOTP. Normally, they are using the RADIUS protocol in order to communicate with the authentication server, but there is also another possibility.

a) Strong authentication logon for Windows XP/2003/2008/7 (commercial)

LSE Leading Security Experts GmbH (http://www.lsexperts.de/) proposes a Windows XP and Windows Server 2003 GINA-Replacement. Credential provider for Windows 7 and Windows Server 2008 is also available. The authentication is using the RADIUS protocol.



On laptops, multiOTP with TekRADIUS LT can be installed locally in order to provide a backup RADIUS server for strong authentication if laptops do not have any Internet access to reach the primary authentication server at the login time.

b) Native PHP implementation without external authentication server

Using the multiOTP class, it is possible to implement in few lines a strong authentication in your own PHP project.

```
(…)
require_once('multiotp.class.php');

$multiotp = new Multiotp();
$multiotp->SetUser($user);

if ($multiotp->CheckToken($token))
{
    echo "Authentication accepted.";
}
else
{
    echo "Authentication rejected.";
}
(…)
```

c) Apache hosted websites on Linux or Windows servers

In order to add strong authentication for Apache hosted websites, you only have to install the mod_auth_radius.

d) Microsoft Internet Information Server hosted websites (commercial)

TCP Data (http://www.tcpdata.com/) provides a RADIUS authentication module for Microsoft Internet Information Server.

6. Strong authentication compatible hardware

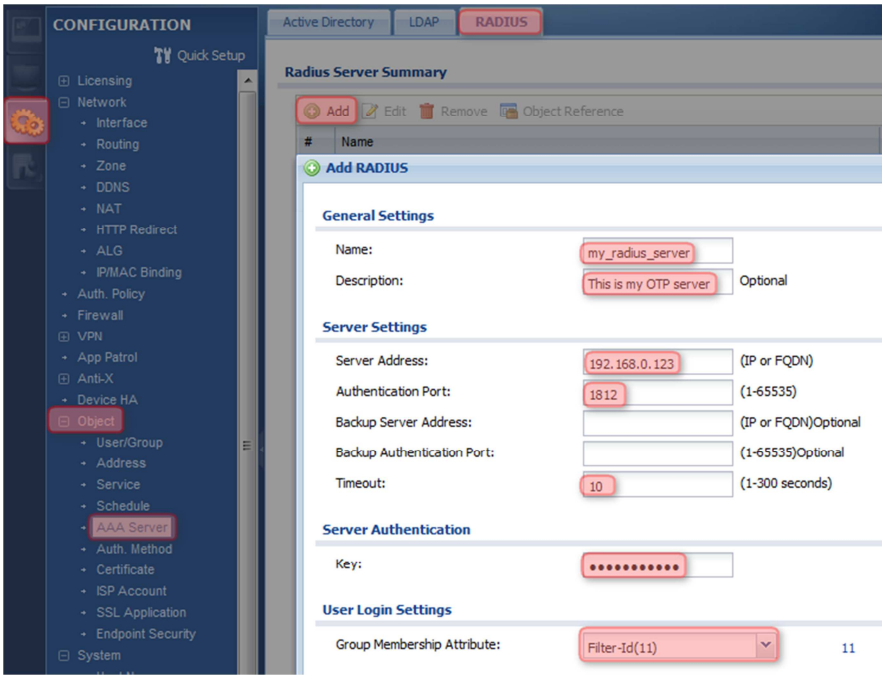
More and more hardware devices like firewalls and appliances are providing external authentications possibilities using also the RADIUS protocol.

a) ZyXEL ZyWALL USG series

The whole series of the Unified Security Gateway from ZyXEL (and the older ZyWALL SSL-10 appliance) are designed to be able to use various external authentication servers like RADIUS, LDAP or Active Directory servers.

Strong authentication can be used to set up VPN, for SSL and SSL-VPN login and also to be able to enable some specific rules in the firewall.

In the **Configuration** menu, expand the **Object** option, click on **AAA Server** and in the **RADIUS** tab, Click on **Add** and add your radius server be specifying a name, a description, the server address, the authentication port (1812), the timeout (10 seconds is fine), the shared secret key (previously defined in your radius server for the subnet of your device) and finally a Group Membership Attribute (Filter-Id(11) is the default value).



Be sure that your device is in the subnet you defined in your radius server, or that you have a Default entry in your radius server configuration, otherwise it will not work.

If you want to use the group membership attribute to manage your users per group in you device rules, you will have to tune a little bit your radius server by creating groups for your different users and by sending back the group name in the Filter-Id(11) attribute.

Now, it is possible to have different levels of authentication. We can simply check that an external radius user is connected (using the **radius-users**), or that a specific radius user is connected (using a specific user defined in the firewall as an **ext-user** user type), or that a specific radius group of users is connected (using a specific user defined in the firewall as an **ext-group-user**).

Users are defined in the **Configuration** menu, expand the **Object** option, User/Group, **+ Add**.

b) DrayTek Vigor 2955 router (and perhaps others)

Draytek has implemented native support for the mOTP (Mobile-OTP) protocol in the Vigor 2955 router, which is pretty cool as you don't need any external server to use it.

7. Useful links

a) multiOTP official website

http://www.multiotp.net – This is the official website were the **multiOTP** project is hosted. Current source files, binary files (for Windows) and other related stuff can be found here.

b) TekRADIUS LT

http://www.tekradius.com - TekRADIUS is a free RADIUS server for Windows. More details about it can be found in the next section.

c) Mobile-OTP

http://motp.sourceforge.net – The Mobile-OTP project was already introduced in 2003. More than 30 independent implementations of the Mobile-OTP algorithm exist around the world.

d) oath - Initiative for Open Authentication

http://www.openauthentication.org – You will find several useful information on this website dedicated to "Strongly authenticating Everyone, Everything and Everywhere".

e) RadiusGINA (2003/XP) and Radius Credential Provider (2008 / 7)

http://www.lsexperts.de – If you are looking to implement strong authentication in your Windows network, **multiOTP** with TekRADIUS LT will be the good choice for the server side, but you will need enhanced logon solution proposed by LSE Leading Security Experts GmbH.

8. About TekRADIUS

TekRADIUS is a RADIUS server for Windows. TekRADIUS development has been started by Yasin KAPLAN in 2005 and first release was in 2007. TekRADIUS is based on latest RADIUS RFC documents RFC 2865 and RFC 2866. TekRADIUS supports PAP, CHAP, MS-CHAP v1-v2, EAP-MD5, EAP-MS-CHAP v2, PEAP (PEAPv0-EAP-MS-CHAP v2) and Digest (draft-sterman-aaa-sip-00.txt) authentication methods. TekRADIUS is a freeware software and can be downloaded from http://www.tekradius.com/.

9. About SysCo systèmes de communication sa

SysCo systèmes de communication sa is a 13 years old Swiss based company installed in Neuchâtel in the French part of Switzerland.

Our team is mainly composed by high level engineers and technicians, and we are mainly providing consulting services and customized development, beside various Internet services and tailored deployments.

Security issues, remote access solutions and communication systems in general are some of our activities for which we provide also several tools to the community.

Beside the **multiOTP** project, we have also provided several PHP tools to the community like a token grid class (to generate and use grids of tokens on paper), a radius client class (to authenticate in pure PHP against a radius server) or also syslog client class (to send syslog information from a PHP script).

We are also monitoring a lot of servers and devices, and therefore, we have developed some free tools like a temperature or power usage monitor for APC UPS devices, logical volumes and drives status monitor for HP RAID controllers, drives and devices monitor for ESXi host servers, etc.

Don't hesitate to contact us if you need some specific support or if you want to develop a project with us. Our main language is French, but we are speaking and reading English and German as well. Community support is only provided per email at developer@sysco.ch.

André Liechti is the 41 years old technical director of the company, with a strong background of electronics, computer sciences and communication systems experience. He is still spending regularly hours to write code lines for their customers, but also for the community.

The strong financial and management knowledge of our 35 years old administrative director, Fabien Paratte, is also shared with our customers to help them managing new projects and challenges.

SysCo systèmes de communication sa
13, rue du Crêt-Taconnet
2000 Neuchâtel
Switzerland

info@sysco.ch / http://www.sysco.ch

tel +41 32 730 11 10
fax +41 32 730 11 09

GPS : 46°59' 52.90" N, +6°56' 32.10" E