OpenVPN

Amoocon 2010

Felix Kronlage <kronlage@bytemine.net>
@felixkronlage

bytemine GmbH

Who am I?

- Founder of bytemine GmbH
- (idle) OpenBSD developer
  - fkr@openbsd.org
- More or less active member of the OpenVPN e.V.
- Twitter: @felixkronlage

Whats to come

- Introduction VPN
- Introduction OpenVPN
- Why and where use OpenVPN
- Various usage scenarios
- Upper layer: *bytemine-manager*
- Lower layer: socket-wrapper *ut*
- Questions and Answers

Introduction VPN

- Confideniality
- Integrity
- Authenticity
- Replay protection

Confidentiality

- Ensure it is hard for anyone but the receiver to understand what data has been communicated.
  - Ensuring the secrecy of passwords when logging into a remote machine over the Internet.
- Not only company data needs to be protected – more and more sniffing in private environments!

Authenticity and Integrity

- Authenticity and Integrity come together
- **Authenticity**
  - Sign your data so that others can see that it is really you that sent it. It is clearly nice to know that documents are not forged.
- **Integrity**
  - Guarantee that the data does not get changed in transit.

Replay Protection

- An attacker should not be able to record a connection an replay it later

Use cases for VPN

- Site-to-site within one company
- Roaming road-warriors
- Encryption of wireless connections
- Secure client-server connections
- Interconnection within one building
- Ensuring your privacy!

VPN technologies

- IPsec
- L2TP - Layer 2 Tunneling Protocol
- **OpenVPN**
- mesh'ed VPNs
  - CloudVPN
- SSH based ad-hoc
- pptp – Point-to-Point tunneling protocol

OpenVPN Overview

- Layer-7
  - *application layer*
  - SSL-based
    - Secure Socket Layer
  - NAT-T not needed
- Offers routed und bridged mode
- Protokoll is similar to https
  - Even works in proxied environments
- Much effort needed to detect

OpenVPN Overview (2)

- Standard-port (since version 2)
  - 1194
- Since version 2.1 port-sharing possible
  - security by obscurity?
- Layer-2 traffic in bridged-mode posssible
  - dhcp
  - IPX
  - Microsoft netservices

OpenVPN CLI client

- Free-, Net- und OpenBSD and DragonFly
- Linux in all its variations
- Solaris / OpenSolaris
- Mac OS X
- Win32 since windows 2000

OpenVPN GUI clients

- Integration into Gnome
  - network manager plugin
- Integration into KDE
- Tunnelblick and viscosity for Mac OS X
- “OpenVPN GUI” and “OpenVPN Admin” for Windows based platforms

OpenVPN on the phone

- Snom has integrated OpenVPN
  - At least in the 3xx line
- Android via TunnelDroid
  - http://sourceforge.net/projects/tunneldroid
- Windows Mobile works
- No iPhone nor Symbian client yet
  - Problem: tun-interface not available

OpenVPN Servers

- All unix flavors that offer the CLI client can act as a server
- Zerina / IPCop
- OpenWRT
- Various other embedded firewall projects

OpenVPN authentication

- Pre-shared key
- Username / Password
  - User database
  - s/key
  - token-based
- Certificate based
- Dual-Factor Authentification possible

OpenVPN Auth Plugins

- PAM
- bsdauth
- LDAP
- Radius
- MySQL
- Sqlite
- Samba
- POP3

OpenVPN plugins

- Sadly no central place for plugins (yet)
- A compilation can be found in a forum
  - http://forum.openvpn.eu/viewtopic.php?f=1&t=3663

OpenVPN configuration

- First: *routed* or *bridged*
  - *Bridged* is not as efficient
  - IP-address conflicts possible
  - Harder to restrict
  - Broadcast services possible
- OpenVPN Software can be a client or a server
  - Mode is decided upon configuration

Certificate Authority

- A journey through the world of X509
- One of the “big” burdens going to OpenVPN
- The “hard” way:
  - *easy-rsa*
- The “easy” way:
  - tinyCA
  - *bytemine-manager*

Certificate games

- Root Certificate Authority
  - Possibly going through an intermediate
- Server Certificate
- Client Certificate
- Certificate Revocation List (CRL)
- Diffie-hellmann params

easy-rsa

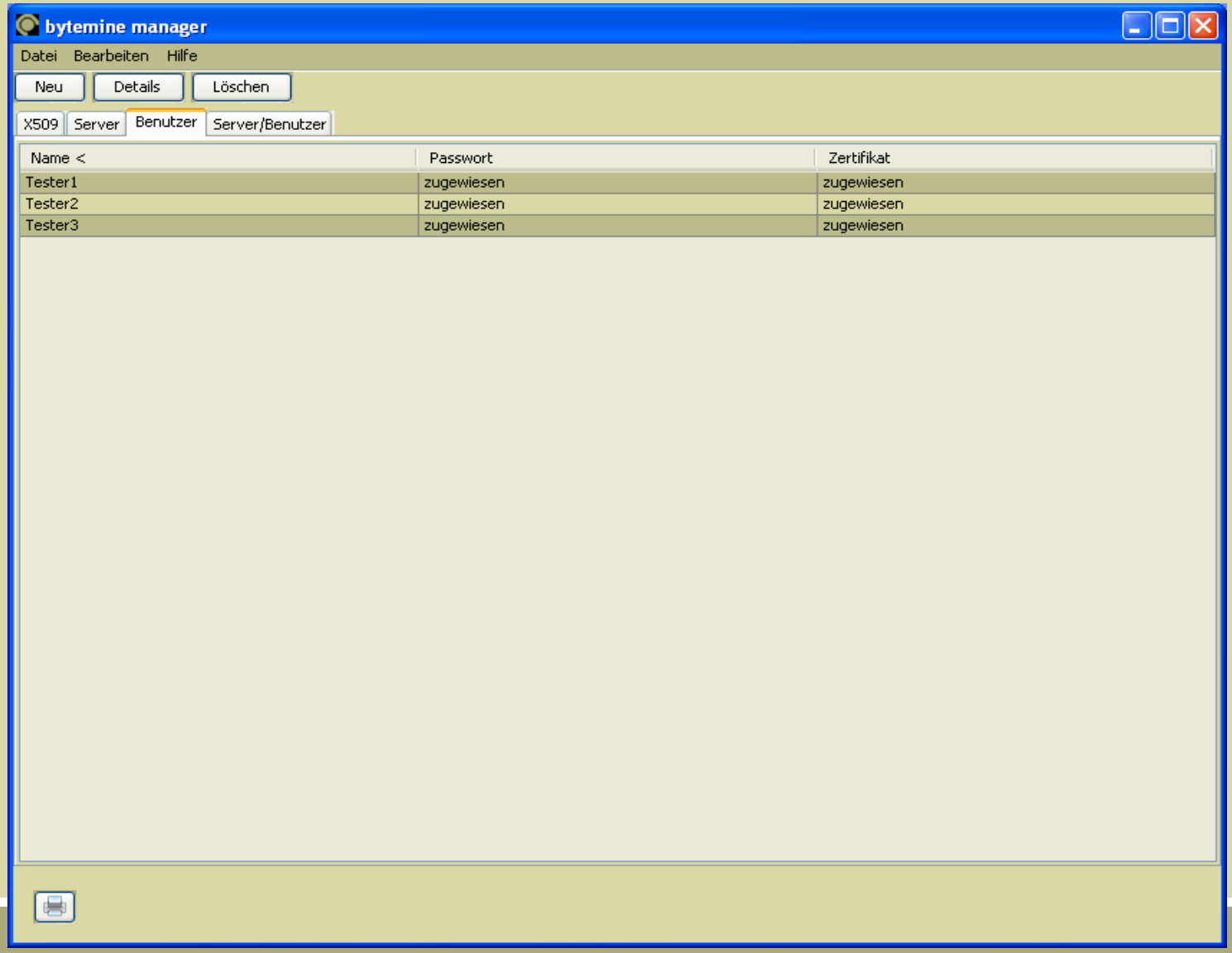
- Collection of scripts coming from OpenVPN
  - */usr/local/share/examples/openvpn/easy-rsa*
- Edit *vars*
  - *./build-ca*
  - *./build-key-server*
  - *./build-key client1*
  - *./build-dh*
- Adding further clients via script

Leaving the old way

- *bytemine manager*
- Java-based desktop software
  - Why not a web-app?
- Released under bsd 2-clause license at this years CeBIT
- Bundles certificate management as well as administration

bytemine-manager

bytemine-manager (2)



Communication - *ut*

- Communication to the concentrator via ssh
- *ut* – Socket Wrapper
- A simple multiplexer
- Executing *ut* over the SSH channel
- Since OpenVPN 2.1rc13 the management interface supports unix domain socket
- bsd licensed as well

OpenVPN server config

- */etc/openvpn/*
- ca.crt, server.crt, server.key, crl.pem
- example: server-udp.conf
- tun / tap interface

```
01 for _conf in $(find /etc/openvpn -name '*.conf' -maxdepth 1 -type f); do
02             test -r $_conf || continue
03             echo "starting OpenVPN($(basename $_conf))"
04             /usr/local/sbin/openvpn --config $_conf --daemon \
05                     --cd /tmp --script-security 2
06 done
```


OpenVPN Server config (2)

```
01 local 134.106.146.206
02 port 8080
03 proto udp
04 dev tun1
05 ca /etc/openvpn/keys/ca.crt
06 cert /etc/openvpn/keys/server.crt
07 key /etc/openvpn/keys/server.key  # This file should be kept secret
08 dh /etc/openvpn/keys/dh1024.pem
09 server 192.168.4.0 255.255.255.0
10 ifconfig-pool-persist ipp.txt
11 push "route 192.168.1.0 255.255.255.0"
12 push "redirect-gateway"
13 push "dhcp-option DNS 192.168.1.1"
14 keepalive 10 120
15 comp-lzo
16 user nobody
17 group nobody
18 status /var/log/openvpn/openvpn-status.log
19 management /var/run/management-udp unix
20 auth-user-pass-verify /usr/local/sbin/auth.pl via-file
```


OpenVPN Client config

```
01 client
02 dev tun0
03 proto udp
04 remote 134.106.146.206 8080
05 resolv-retry infinite
06 user nobody
07 group daemon
08 persist-key
09 persist-tun
10 ca ca.crt
11 cert fkr_49.crt
12 key fkr_49.key
13 ns-cert-type server
14 comp-lzo
15 auth-user-pass
```


OpenVPN and the wish for reduncancy

- Redundancy only possible as a way of 'load-balancing'
- carp(4) to the rescue!
- How do you take over a SSL-connection?
  - Fool, you don't!
  - SSL/TLS Client-Key-Renogiation
  - Man-in-the-middle attack

Scaling OpenVPN

- Load-balancing mode
- client configuration is being configured *N* servers
- server-configuration identical except for the virtual IP address pool

Monitoring OpenVPN

- Process checks via nagios / icinga
- TCP- and process checks are easy
- What about UDP?
- monitoringexchange.org for more

- Zabbix (or other flavors?) anyone?

OpenVPN *Best-Practices*

- Keep the concentrator simple!
- Use dual-factor auth
- Activate *tls-auth* and *ns-cert-type*
- Use unprivileged users
  - user/group *nobody*
- *chroot* the process
- Restrict the users on the IP level
- Port 443 (https)

The OpenVPN Community

- Since 2010 openvpn.net goes new ways
  - Samoli as Community Manager
  - Experimental branch(?)
- The german *OpenVPN e.V.*
  - http://www.openvpn.eu/
- Why is it important to push OpenVPN?

OpenVPN Books

- *Beginning OpenVPN 2.0.9*
  - Markus Feilner
  - ISBN-10: 184719706X
  - ISBN-13: 978-1847197061
- *OpenVPN – Kurz und Gut*
  - Sven Riedel
  - ISBN-10: 3897215292
  - ISBN-13: 978-3897215290

Commercial OpenVPN?

- OpenVPN AS
- bytemine GmbH
  - bytemine openbsd appliance
  - OpenVPN consultency, development und support
- SecurePoint GmbH
  - UTM Appliances, OpenVPN Client

Commercial OpenVPN (2)

- Funkwerk / Bintec
  - UTM Appliances
- OpenSource Training
  - OpenVPN Training
  - http://www.os-t.de/

Ressources

- Official website
  - http://www.openvpn.net/
- Official, central development site
  - https://community.openvpn.net/openvpn
- English web forum
  - http://www.ovpnforum.com/
- German forum and home of OpenVPN e.V.
  - http://www.openvpn.eu/

Ressources (2)

- Things we do at bytemine
  - http://blog.bytemine.net/
- Our released code
  - http://github.com/bytemine/

The famous (almost) last page!

- Thanks Stefan for Amoocon!
- Further infos regarding the following, ask me after the talk:
  - OpenBSD
  - OpenVPN
  - VPN stuff
  - The OpenVPN e.V.
  - German beer

Thanks for listening!

bytemine GmbH

Marie-Curie-Str. 1
26129 Oldenburg

info@bytemine.net
http://www.bytemine.net
http://blog.bytemine.net
+49-441-3091970