J'ai pas de TUN et je m'en TAP

rafioz0

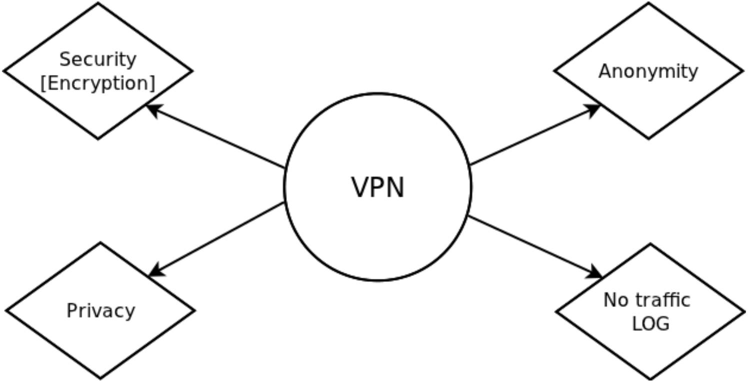
February 23 2012

FIXME
HACKERSPACE LAUSANNE

Table of Contents

1. VPN: what, where, who
2. Very brief recall of how it works
3. The attack and results
4. The reaction of a VPN provider
5. Conclusion

What a VPN provides



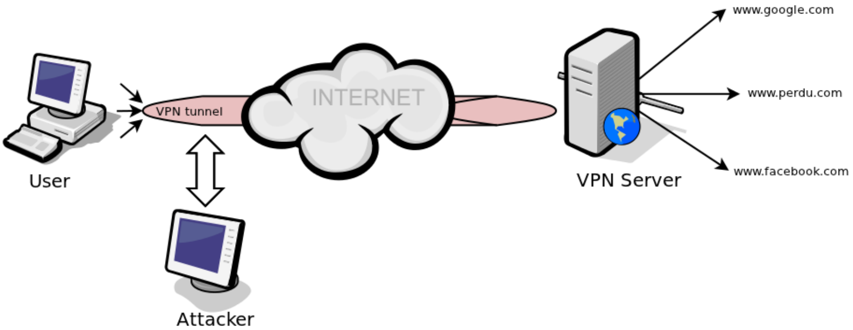
Who uses VPNs ?

- Anti Hadopi people, to download as crazy
- People under restrictive laws (China, Iran, etc)
- People who want to hide themselves

Who ?

Simply people who don't trust their ISPs

And they are right...



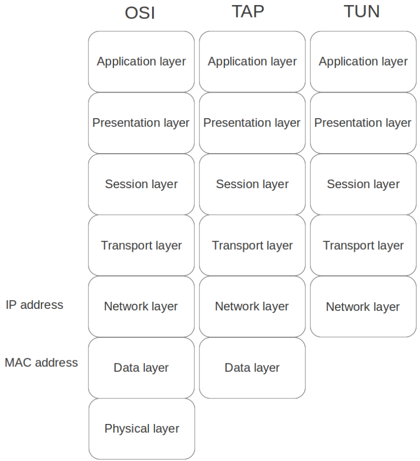
An attacker will not see the traffic being transfered in the VPN tunnel (VPN provides encryption).

TUN / TAP

- VPNs tend to use TUN / TAP provided by the kernel as a virtual network kernel device.
- TAP (as in network TAP): simulates an Ethernet device and it operates with layer 2 - same switch
- TUN (network TUNnel): simulates a network layer device and it operates with layer 3 packets - same router

Simpletun[1] is a very tiny implementation to understand how it works.

The OSI layers



	OSI	TAP	TUN
	Application layer	Application layer	Application layer
	Presentation layer	Presentation layer	Presentation layer
	Session layer	Session layer	Session layer
	Transport layer	Transport layer	Transport layer
IP address	Network layer	Network layer	Network layer
MAC address	Data layer	Data layer	
	Physical layer		

An oversimplified view:

- TAP: you will have a MAC address and an IP address.
- TUN: you will have only an IP address.
- We won't take into account the encapsulation.

tic-TAP attack

- Would you let a stranger use your private network ?
- VPN providers offer TAP devices, because they are simpler to deploy.

TAP == LAN

Your computer behaves the same as if it were on your LAN !

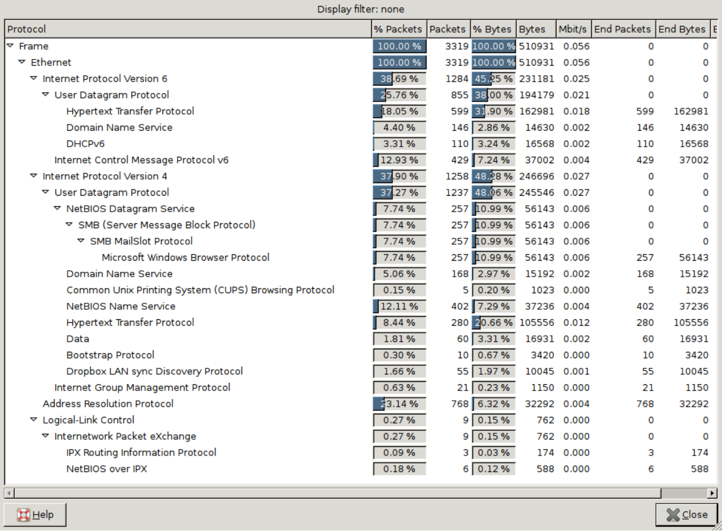
So what ?

- Your computer will broadcast a lot of information to the broadcast / multicast address.
- Layer 2 attacks are now possible: Man in the middle (ARP poisoning, STP attacks, etc).

A privacy issue

- A lot of people put their firstname/lastname as their machine name, Windows will broadcast them (LLMNR protocol[6]).
- You are not anonymous anymore.
- (Although Windows 7 doesn't really trust TAP)...

The stats before the MITM

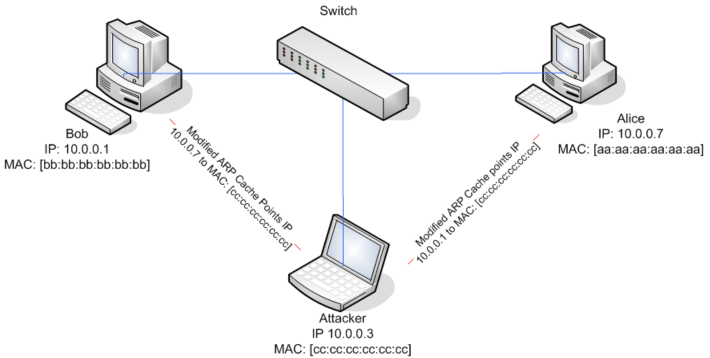


Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	E
Frame	100.00 %	3319	100.00 %	510931	0.056	0	0	
Ethernet	100.00 %	3319	100.00 %	510931	0.056	0	0	
Internet Protocol Version 6	38.69 %	1284	45.25 %	231181	0.025	0	0	
User Datagram Protocol	25.76 %	855	38.00 %	194179	0.021	0	0	
Hypertext Transfer Protocol	18.05 %	599	31.90 %	162981	0.018	599	162981	
Domain Name Service	4.40 %	146	2.86 %	14630	0.002	146	14630	
DHCPv6	3.31 %	110	3.24 %	16568	0.002	110	16568	
Internet Control Message Protocol v6	12.93 %	429	7.24 %	37002	0.004	429	37002	
Internet Protocol Version 4	37.90 %	1258	48.28 %	246696	0.027	0	0	
User Datagram Protocol	37.27 %	1237	48.06 %	245546	0.027	0	0	
NetBIOS Datagram Service	7.74 %	257	10.99 %	56143	0.006	0	0	
SMB (Server Message Block Protocol)	7.74 %	257	10.99 %	56143	0.006	0	0	
SMB MailSlot Protocol	7.74 %	257	10.99 %	56143	0.006	0	0	
Microsoft Windows Browser Protocol	7.74 %	257	10.99 %	56143	0.006	257	56143	
Domain Name Service	5.06 %	168	2.97 %	15192	0.002	168	15192	
Common Unix Printing System (CUPS) Browsing Protocol	0.15 %	5	0.20 %	1023	0.000	5	1023	
NetBIOS Name Service	12.11 %	402	7.29 %	37236	0.004	402	37236	
Hypertext Transfer Protocol	8.44 %	280	20.66 %	105556	0.012	280	105556	
Data	1.81 %	60	3.31 %	16931	0.002	60	16931	
Bootstrap Protocol	0.30 %	10	0.67 %	3420	0.000	10	3420	
Dropbox LAN sync Discovery Protocol	1.66 %	55	1.97 %	10045	0.001	55	10045	
Internet Group Management Protocol	0.63 %	21	0.23 %	1150	0.000	21	1150	
Address Resolution Protocol	23.14 %	768	6.32 %	32292	0.004	768	32292	
Logical-Link Control	0.27 %	9	0.15 %	762	0.000	0	0	
Internetwork Packet eXchange	0.27 %	9	0.15 %	762	0.000	0	0	
IPX Routing Information Protocol	0.09 %	3	0.03 %	174	0.000	3	174	
NetBIOS over IPX	0.18 %	6	0.12 %	588	0.000	6	588	

Man in the middle

It exists a lot of different ways and (script-kiddies) tools to MITM someone: **arp cache poisoning**. Ettercap[3] was used here.


Switch
Bob
IP: 10.0.0.1
MAC: [bb:bb:bb:bb:bb:bb]
Alice
IP: 10.0.0.7
MAC: [aa:aa:aa:aa:aa:aa]
Modified ARP Cache Points IP 10.0.0.7 to MAC: [cc:cc:cc:cc:cc:cc]
Modified ARP Cache points IP 10.0.0.1 to MAC: [cc:cc:cc:cc:cc:cc]
Attacker
IP 10.0.0.3
MAC: [cc:cc:cc:cc:cc:cc]

After MITM

During a test of 5 minutes:

- Password were stolen: NNMP, POP, HTTP accounts.
- Credentials from sites like Facebook / private trackers (cookies, whole URL).
- A lot of porn sites...
- Samba user and hash(pwd).
- Possibility to kill TCP connections, massively degrade the VPN service.

Looking for you

- If someone (Feds) is looking for you he can just look at your destination IP to know which VPN service you use.
- Create an account to the same VPN provider.
- Do the same attacks as presented.

Can we secure that ?

- VPN providers could provide TUN instead of TAP.
- Layer2 attacks are difficult to protect against: ignore ARP, use static routes, etc.
- On linux, you can use **iptables**[4] for layer3, **ebtables**[5] for layer2.

Exchange of emails

> *Hi,*
> *One of the reason is that TUN requires 4 ips per connection. I cant give you a straight answer but I”ll speak to our technical engineer and see he has to say. Can you show me some proof? Print screens or something.*

[...]

> *Hi,*
> *I spoke to my tech engineer and he told me that we can’t filter it. If we’re gonna use TUN, it takes 4 IPs per connection. Every custom have a /30 net. 1 for customer, 1 for gateway, 1 for broadcast and 1 for net. We’ll see if we can install a new VPN with TUN.*

Conclusion

- For strong anonymity, don't use a "public" VPN, even if you pay for it.
- Don't do like the lulzsec with the hidemyass provider[2].
- However, some VPN providers seem to be more security focused (use TUN, have firewalling rules, etc).

Questions ?

Questions ?

[Davide Brini, 2009]
A simplistic, simple-minded, naive tunnelling program using tun/tap interfaces and TCP.
http://www.cis.syr.edu/ wedu/seed/Labs/VPN/files/simpletun.c

[Hide My Ass, 2011]
The Lulzec fiasco
http://blog.hidemyass.com/2011/09/23/lulzsec-fiasco/

[Ettercap NG 0.7.4-Lazarus, 2011]
Ettercap NG 0.7.4-Lazarus
http://ettercap.sourceforge.net/

[iptables]
iptables is the userspace command line program used to configure the Linux 2.4.x and 2.6.x IPv4 packet filtering ruleset.
http://www.netfilter.org/

[ebtables]
The ebtables program is a filtering tool for a Linux-based bridging firewall.
http://ebtables.sourceforge.net/

[llmnr]
Link-Local Multicast Name Resolution (LLMNR)
https://www.ietf.org/rfc/rfc4795.txt