Advanced Security: Security Services & Privacy

Bruno Martin

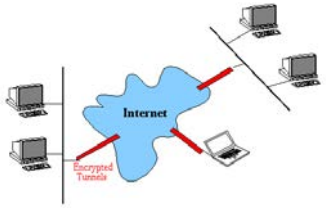
Université Côte d'Azur

M2 Informatique et interactions

Contents

VPN

- Private network which uses the Internet to connect :
  - remote pairs
  - remote sites
- VPN uses virtual connections routed over the Internet towards the remote entity



Functions :

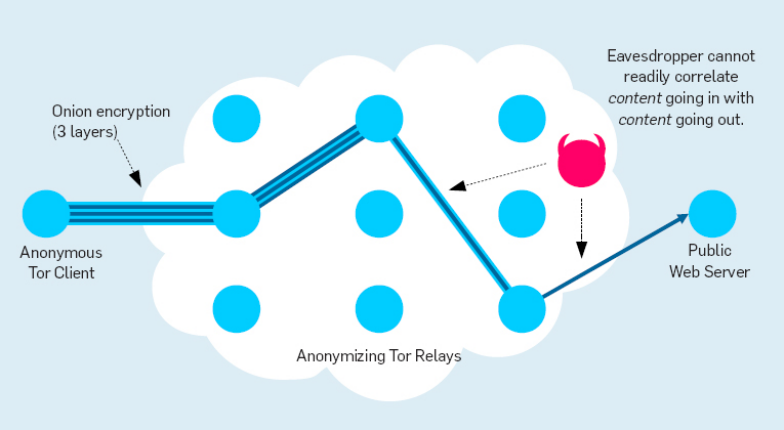
- Extends the connectivity
- improves the security
- reduces the cost compared with a dedicated WAN
- simplifies the network topology

VPN – operation modes

They use the `tun/tap` interface and use different OSI layers.

- **(routed) :** connects remote machines (pairs). Works with the network layer (3) at the IP level. Uses the `tun` interface. Establishes a specific route between distinct network addresses. There is no broadcast. Works point to point.
- **(bridge) :** connects remote networks ; works at the link level (2) by a dedicated protocol `PPTP`, `EoIP`, `IPSec`. Uses the interface `tap`. ifaces VPN and LAN are bridged into a single entity. The VPN address is dynamically provided to the client. Networks are routed by routing tables managed by the VPN server. Allows broadcasting and ensures a full transparency.

Onion routing/TOR

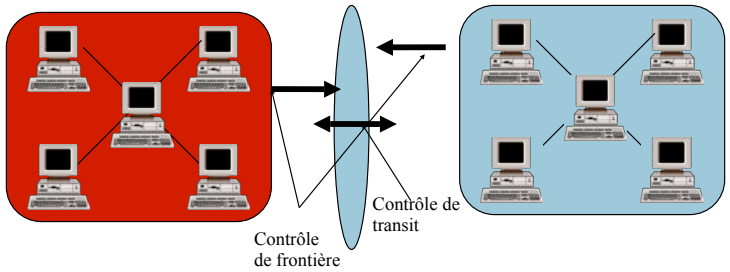


Packet filtering

- Ensured by routers or dedicated hosts
- Principles :
  - redistribute, cancel or track any packet
  - depends on the header contents of the packets
    - source and destination addresses
    - direction (input/output) wrt to the LAN
    - application type by its port number
  - in conjonction with TCP/IP
  - usually at the kernel level of the OS

A firewall denotes a piece of software and/or hardware (appliance) whose role is to apply the network security policy. This security policy tells which communications are allowed or forbidden.

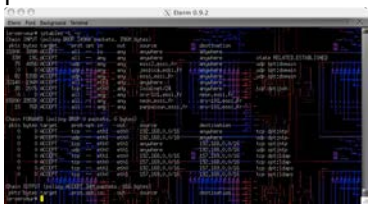
Boundary control



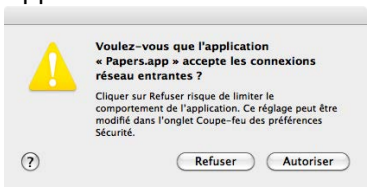
- main problem of lans that are connected to the internet
- **Solution** : use firewalls together with :
  - packet filtering
  - proxies
  - cryptographic mechanisms
- and reduce the number of access points

Kinds of firewalls

packet filters



Application filters



Differents depending on the OS

- **linux** : IPtables/netfilter ... nftables, ufw
  Packet firewall that are available with linux. Made of filtering rules with the next components :
  - chain : ordered list of rules
  - every rule expresses a condition
  - if rule *i* doe not apply, test rule $i + 1$
  - when all the rules have been tested, apply the default policy of the chain (`ACCEPT`,`DROP`)
- **BSD** : 3 different firewalls
  - **IPFILTER** : commande `ipf`
  - **IPFIREWALL** : commande `ipfw`
  - **PacketFilter** : commande `pf`
- **Windows** : Windows defender (or third party)
- **MacOS** : 2 integrated firewalls, one coming from BSD and an application firewall.

What is a virus ?

Originally, it was a self-reproducing automaton designed to generate artificial life. Now, to this kind of software, malicious code is added to propagate to other computers and to infect the hosts. It harms the normal behavior of the machine and can spread by the means of any exchange device, USB dongle, CDs, networks,...

Programs that are often seens as viruses : trojans (that often host ransomware), worms (that just spread).

Limits of a firewall

- all the communications must pass through the firewall
- the firewall must be well configured
- avoid any bypassing of the firewall (by a modem, GSM,...)
- keep track of the traffic by logs
- keep track of intrusions and anomalies

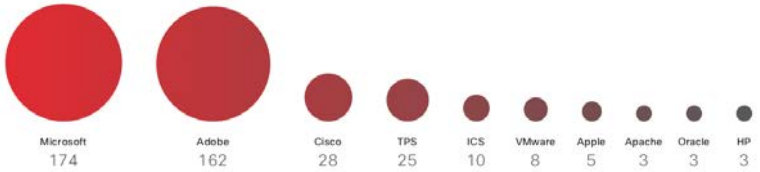
Anti-viruses Programs

They protect the computer against viruses and malware. These programs contain a database with thousands of known viruses' signatures which are known. They can detect such malicious software and remove them.

They also can detect modifications that have been added to standard files to search for new viruses.

There are free anti-viruses like those proposed by Avast, ClamAV, contained in the OS like Windows Defender or sold by third parties like Symantec, Norton, McAfee,...

Favorite Targets



Spam classification

- Advertising : coming most the time from unknown companies offering products you do not care about
- Phishing : more dangerous. A phishing campaign invites you to disclose private information (credit card number, social networks credentials, ...). It can make many damages even with users aware of the risk.
- scams : promise you to win something : the last flagship smartphone, bitcoins,... Do you think you can win something on the Internet ?

What is spam ?

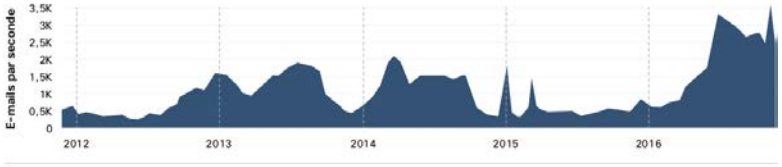
Unsolicited emails are usually used to make advertisement for a product with or without client targeting (see privacy). Spam generalises advertising surface mail and is widely used because of its low cost and to flood recipients.
Spam has a cost :

- for the recipients : the time for filtering good and bad emails
- for mail providers : spams are routed and treated as normal mail before being filtered by the recipient's smtp service.

Almost 75% of the mail traffic is spam.
Spam is also a threat since it often contains viruses or links pointing to malicious software.

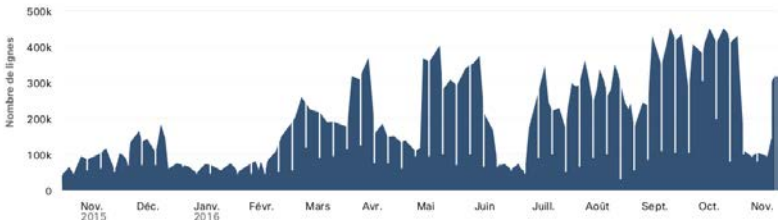
Spam Stats

Figure 15 Volume total de spams



Source : CBL

Figure 16 Taille de la liste de blocage SCBL (SpamCop Blocking List)



Fight again Spam

3 main kind of software :

- anti-spam filter : works with the company smtp server. When a mail is incoming, it is filtered and legitimate email is distributed and the bulk mail put in quarantine.
- anti-spam appliances : sold by providers. No configuration is required. It's plug and p(l)ay. The provider maintains blacklists, greylists and uses more sophisticated filters. Relatively expensive.
- dematerialized service in the cloud. The mail is fetched by the dedicated service, filtered and distributed to the user. Works with paid registration.

Contents

Intrusion Detection

An Intrusion Detection System is a mechanism which tries to find abnormal usage of a specified target. It stores the attacks conducted against a network or a machine.
Three main categories

- NIDS : Network based IDS that manage the activity at the network level (example : `snort`)
- HIDS : Host based IDS that manage the activity at the machine level (example : `tripwire`)
- hybrid IDS : combining NIDS and HIDS

Privacy Definition

Denotes a subjective and abstract concept depending on the field of study, social norms and its context.

- From a legal point of view : the right to be let alone or, everyone can decide which private information can be disclosed and when.
- From a psychological point of view : the freedom to build your own identity in a constrained environment because the construction of one's identity depends on the vision of others ; cf. social networks, profiling, ...

Classification Privacy (Solove, 2006)

- information gathering
  - surveillance
  - interrogation
- information processing
  - aggregation
  - identification
  - insecurity
  - misuse
  - exclusion
- information spreading
  - loss of confidentiality
  - disclosure
  - exposition
  - increased accessibility
  - blackmail
  - appropriation
  - distortion
- invasion
  - intrusion
  - decision interference

RGPD : 6 main principles

- Lawfulness, fairness and transparency : organisations need to ensure their data collelction principles don't break the law.
- Purpose limitation : personal data should be collected for a specific purpose, clearly stated
- Data minimisation : only process the personal data which are required to achieve the processing purpose
- Accuracy : every reasonable step must be taken to erase or rectify data that is inaccurate or incomplete.
- Storage limitation : organisations need to delete personal data when it's no longer necessary.
- Integrity and confidentiality : organisations should encrypt and/or pseudonymise personal data wherever possible, but they should also consider whatever other options are suitable.

Data protection

- 1995 : European Data Protection Directive
- 2016 : GDPR (General Data Protection Regulation)
- applies to "personal data" : any information relative to a person (it doesn't apply neither to national security nor legal activities)
- Regulation on protecting physical people's data and the data movement.

Offline world $\rightarrow$ online world

- information hard to collect, store, search and access
  - F2F talk
  - paper documents
  - cash paiement
  - spinning
  - find your connections
  - dictionnary search
  - ...
- hard to copy, broadcast, easy to destroy
- hard to aggregate, profile and infer
- forgetfulness in time

- information easy to collect, store, search and access
  - instant messaging
  - mails
  - numerical files
  - card paiement
  - geolocation
  - online friends
  - google requests,...
- easy to copy, broadcast, hard to destroy
- easy to aggregate, profile et infer
- information is never lost

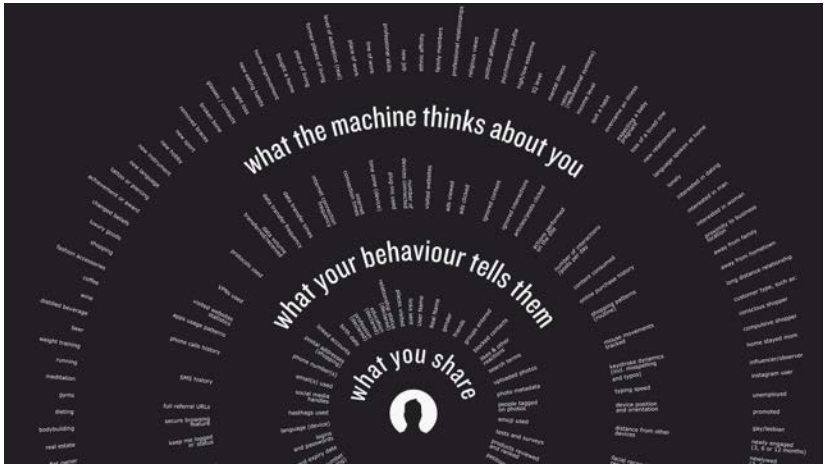
Nothing to hide ?

- the argument “ I have nothing to hide ” is based on the underlying assumption that privacy is to hide negative actions
- What makes a society pleasant to live in is its ability to protect individuals from the intrusion of others in private life. A society without privacy protection would become quickly suffocating.
- Gap between secrecy and privacy :
  - your daily actions, your friends or relations, your conversations, your hobbies, ..
  - all of the above may not be secret but you don’t necessarily want to make these activities public or accessible to others who can analyze and draw conclusions from them

Private life and technology

- red line : our actions and interactions are more and more traced by technology
  - we are tracked all the time
  - those traces are combined, aggregated, analyzed to deduce more information on you and make decisions that will impact you
  - We have no control on the information nor on the inference of them
- Information is never forgotten
  - can sometimes be used out of context

Privacy Levels



Plan

Exemple

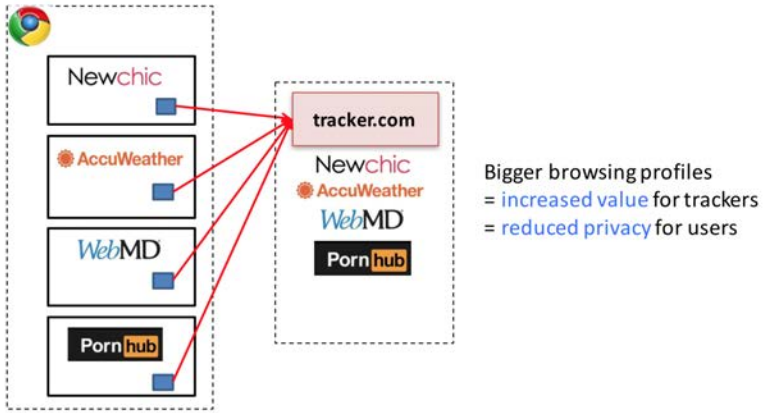
Web browsing on a news site :

With 21 trackers !
From Springer's : " journalistic content is only a excuse for the reader to watch the advertisements. "

Why worry ?

- data collection without agreement
  - on sensitive sites
  - keep track of our browsing habits, our preferences, wishes, humors
- use of these data
  - advertising targetting
  - manipulation

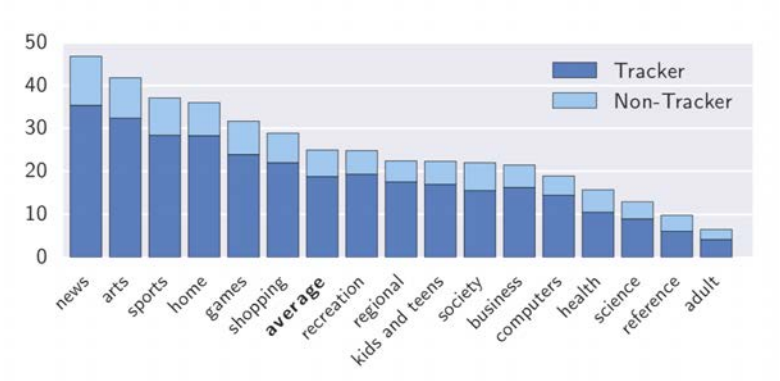
Web tracking (N. Bielova, INRIA)



Bigger browsing profiles
= increased value for trackers
= reduced privacy for users

Cambridge Analytica

How many trackers per site ?



Cookies Authentication

1. a user provides credentials (login/pass) on a website
2. the site returns an identification cookie
3. this cookie is used in the exchanges to identify the user's connexion
4. when the user disconnects, the server closes the connexion and revokes the cookie

The identification cookie is a unique random string, like : D6F8B2BE3ED3040D9A3C10

How it works ?

- With the cookies
- by using other storage mechanisms and zombie cookies
- with large scale measures
- with targetted advertising and cooke synching
- by using your browser's fingerprint

Identity theft by the cookies

An attacker steals the user's cookie and connects at the same time... what happens ?
it steals the legitimate user's identity and can access his account
It can be possible

- by sniffing the `http` traffic and by intercepting the cookie
- same as above but with an adequate MIM atttack
- by stealing the cookie on the computer (OS vulnerability, by social engineering, by a server failure)

Plan

PenTesting steps

- Pre-engagement interaction : négociation with the client : “contract”
- Intelligence gathering : gather all possible information on the client (social networks, scan, footprint,...)
- Threat modeling : use the information from l’IG to identify the vulnerabilities, choose the attacks in accordance with the target
- Vulnerability analysis : find possible attacks by analysing the open ports and vulnerabilities,...
- Exploitation : realisation of exploits
- Post exploitation : whitehat attacks
- Reporting : report the detail of the attacks

Termes

- **Penetration test :** method to evaluate the security of a host or of a network. To that end :
  - search for access points
  - search for vulnerabilities

  with different approaches :
  - **Black box (covert)** : the infrastructure is not known and erasing the tracks is required
  - **White box (overt)** : infrastructure is known in accordance with CSO
  - and variants between both approaches (grey box).
- **Forensics** : comes from the english «computer forensics», is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.

Intelligence gathering

- a good hacker programs a tool for scanning the network
- he publishes it on the Internet (or Darknet)
- a script kiddie uses the tool to find vulnerable systems or weak access points.

Scanner de ports : nmap

A port scanner can scan a large band of IP addresses and return open ports (thus accessible services) as well as OS versions

OS detection

Standard techniques : by banner grabbing ; otherwise

- connects to `smtp`, `snmp` or `telnet` to examine the answers from the server
- in `nmap` fingerprint of the `tcp/ip` stack which allows to identify the system's answer to `tcp` packets with special flags

nmap, operation modes

vanilla attempts to connect on every ports

strobe targets some specific ports

fragment packets focus on fragmented packets (in order to traverse some fw)

udp looks for `udp` ports

sweep connects to the same port of one or several PCs

FTP bounce imitates the behavior of a `ftp` server to appear as legitimate

stealth increases the discretion by avoiding partially the log mechanisms since it never completes TCP connections

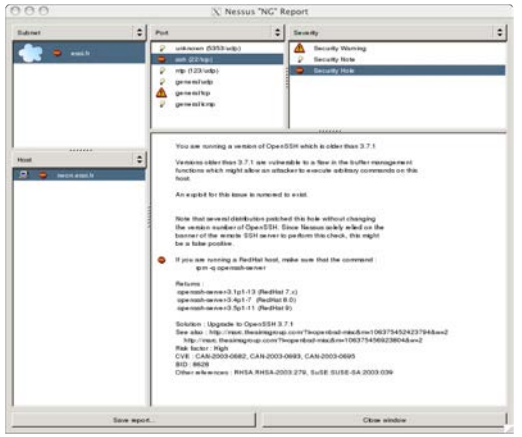
Vulnerabilities

- The script kiddie uses a list of vulnerable IP addresses to gain access to the system
- depending on the weaknesses, he also can create/use a user account or a root account
- this account is the used to make privileges escalade to attack others systems
- example : usurp a legitimate host to attack the network (with `wireshark` or `ettercap`)

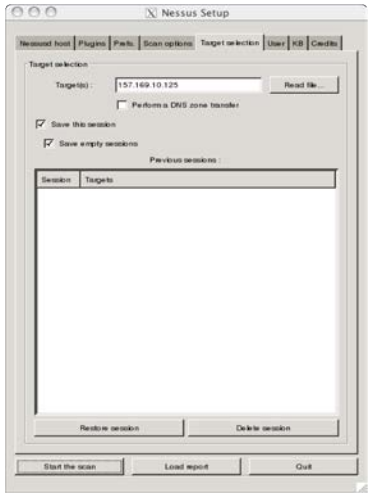
Vulnerabilities scanner – Nessus

The "Nessus" Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner, software which will audit remotely a given network and determine whether someone may break into it, or misuse it. Nessus does not take anything for granted. That is, it will not consider that a given service is running on a fixed port - a web server on port 1234, will be detected it and its security tested. Nessus is fast, reliable and has a modular architecture that allows you to fit it to your needs. Nessus works on Unix-like systems (MacOS X, FreeBSD, Linux, Solaris and more) and a Windows version called NeWT is available.

Nessus : scan



Nessus : target



Nessus - OpenVAS

In 2005, Nessus became expensive.
As an alternative, OpenVAS is the “free” branch of Nessus. As of 2011, it contained more than 23000 vulnerabilities tests which are connected to the database “Common Vulnerabilities and Exposures” CVE on which we can make requests
It is possible to add plugins in the NASL language, as in nessus.
http://www.openvas.org/

Attack

- usually thanks to `rootkits`
- a `rootkit` describes a set of scripts which allow a hacker to hide his commitments and to gain an access to a system
  - changes the `logs`
  - modifies system tools to render detecting the haker more difficult
  - creates a backdoor
  - use the system as an entry point to attack the other hosts of the LAN

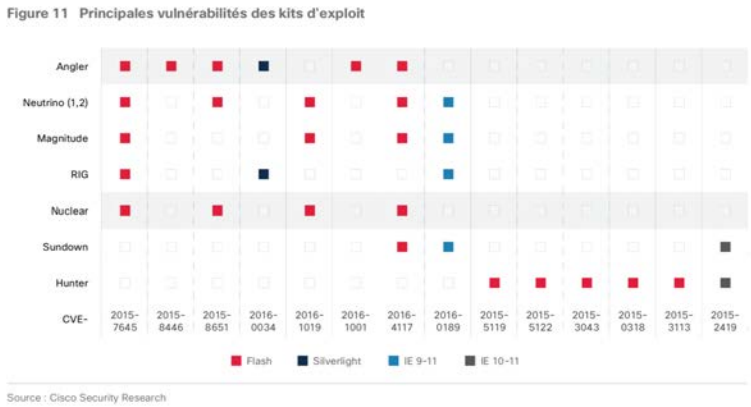
Framework Metasploit

Metasploit (written in `ruby`) is a framework which allows :

- to collect the result of different scanners (port, vulnerability,. . .)
- to automate (and replay) attacks against vulnerabilities (and to add some)

A very powerful tool but which can be hard to use (gui : armitage)

Exploit kits



See the CISCO report

Bug bounty

A bug bounty program rewards individuals for discovering and reporting software bugs. It started in 1995 with Netscape. Bug bounty programs are often initiated to supplement internal code audits and penetration tests as part of an organization's vulnerability management strategy.

Many companies run bug bounty programs, paying out cash rewards to software security researchers and white hat hackers who report software vulnerabilities that have the potential to be exploited. Bug reports must document enough information for for the organization offering the bounty to be able to reproduce the vulnerability. Typically, payment amounts are commensurate with the size of the organization, the difficulty in hacking the system and how much impact on users a bug might have.

In 2015, M. Litchfield claimed he won more than 300000$ by finding breaches. (Source korben)

Plan

The two pillars of security

- **Prevent** : try to prevent an attack as long as possible (by the use of firewalls, antiviruses, keep the soft up to date, check incoming emails)
- **Recovery Plan** : Preventing every risk is impossible. Fruitful attacks can always be conducted. Backups and recovery plan must be prepared in the case of.

The 10 Cammandments of Computer Security

- Install & Update Antivirus/Malware & Firewall Protection
- Secure Your Router
- Set Up & Use A Standard (Non-Administrator) Account
- Keep Your Software & Operating System Updated
- Practice Good Password Use
- Beware Of Scams
- Create & Maintain Backups
- Protect Your Phone & Tablets, Too
- Prevent Spying Through Your Microphone & Camera
- Clean Up After Yourself

Bonus Tip : Disconnect From The Internet (When It Makes Sense)