IpMorph :
« unification de la mystification de la prise d'empreinte »

Guillaume PRIGENT
DIATEAM - Brest

SSTIC - 5 juin 2009

IpMorph : « unification de la mystification de prise d'empreinte»

Contexte

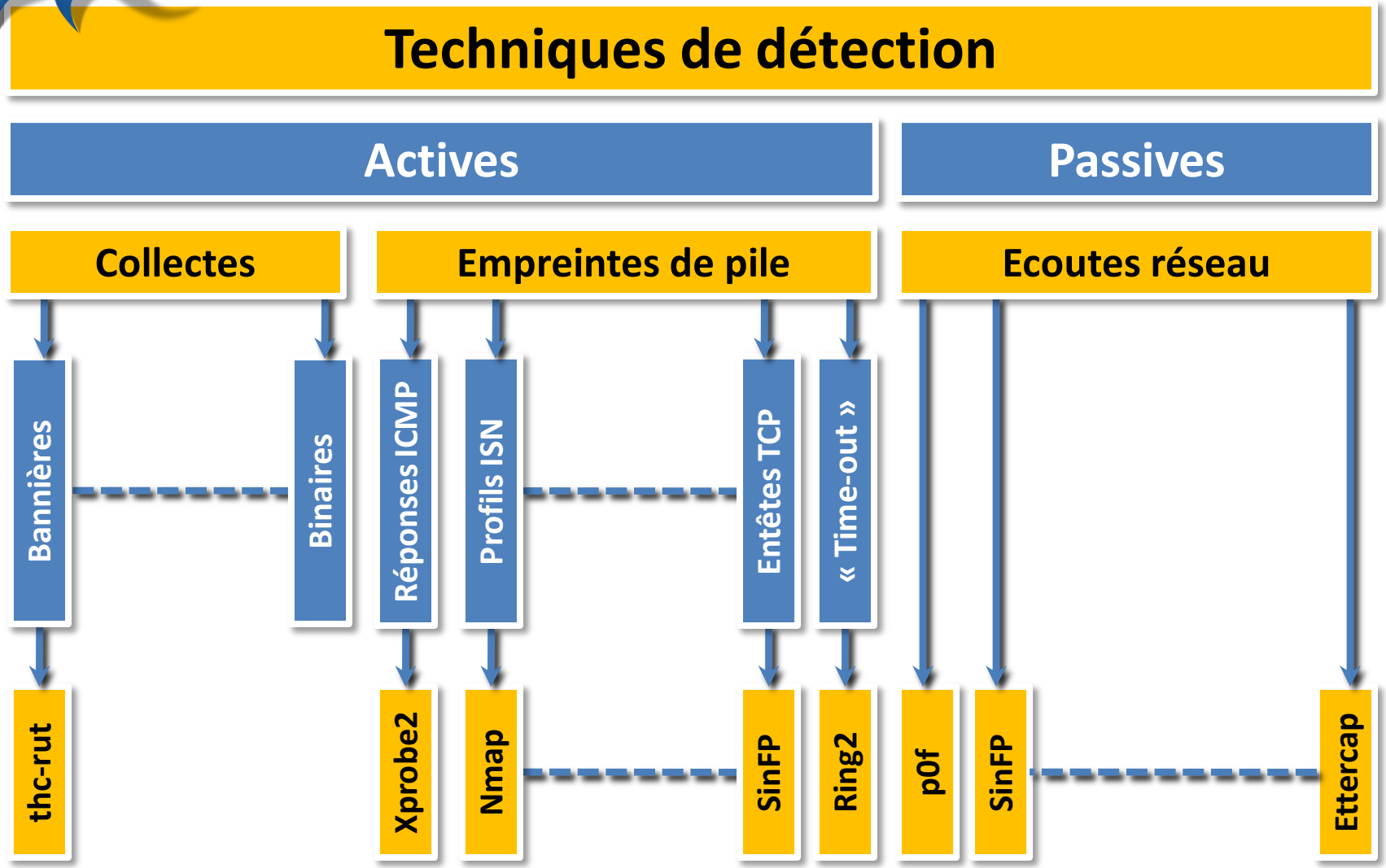
Théorème :

« Vivons heureux, vivons cachés »

Corolaire :

« Si une machine peut falsifier son identité et l'usurper, celle ci minimise l'attrait de l'attaquant et perturbe la pertinence des attaques ciblées à sa nature apparente.»

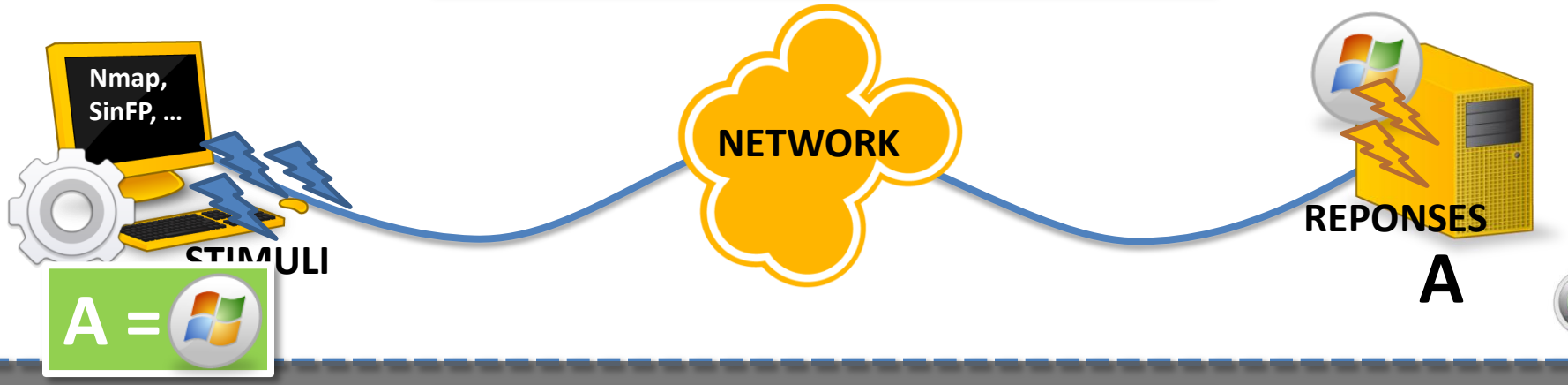
Typologie de la prise d'empreinte



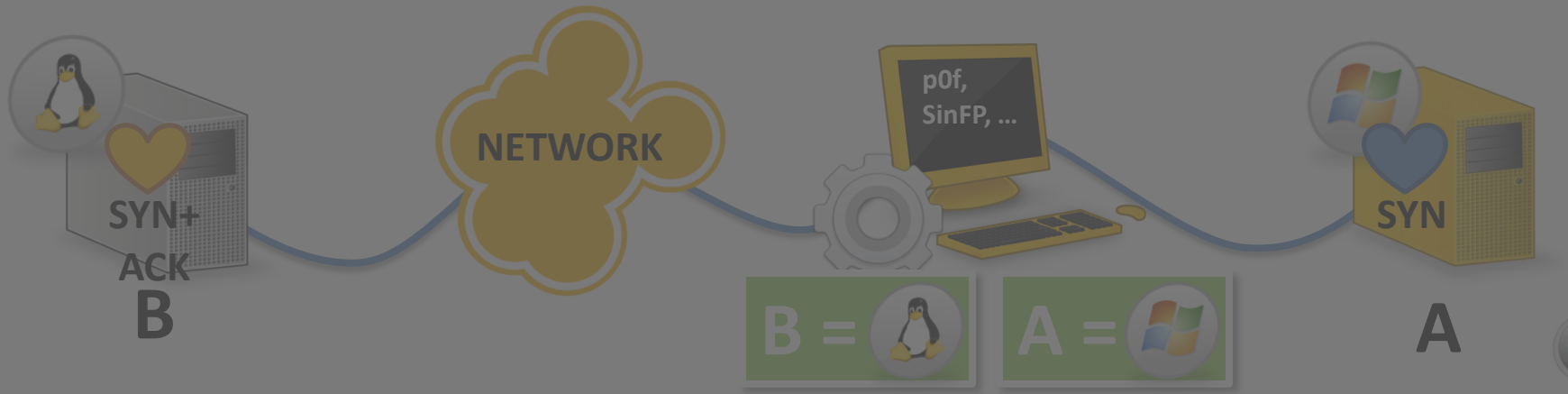
IpMorph : « unification de la mystification de prise d'empreinte»

Principes de détection

Détection active d'empreinte de pile

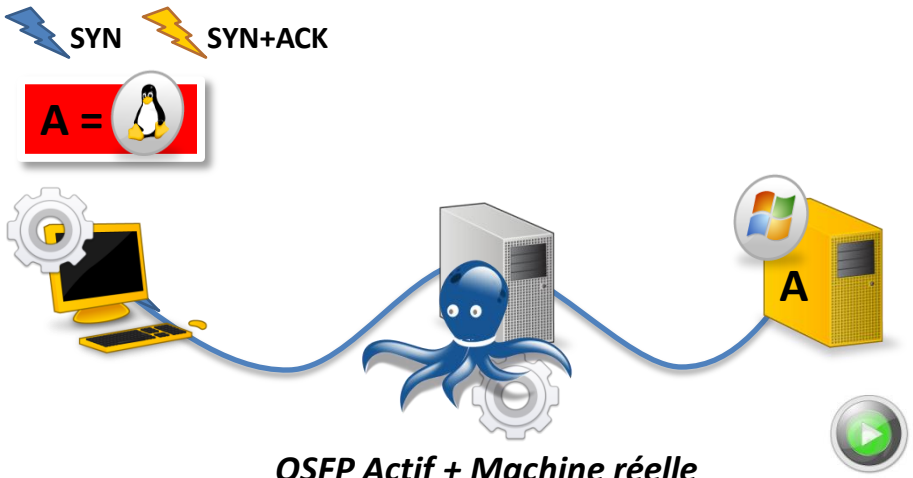


Détection passive d'empreinte de pile

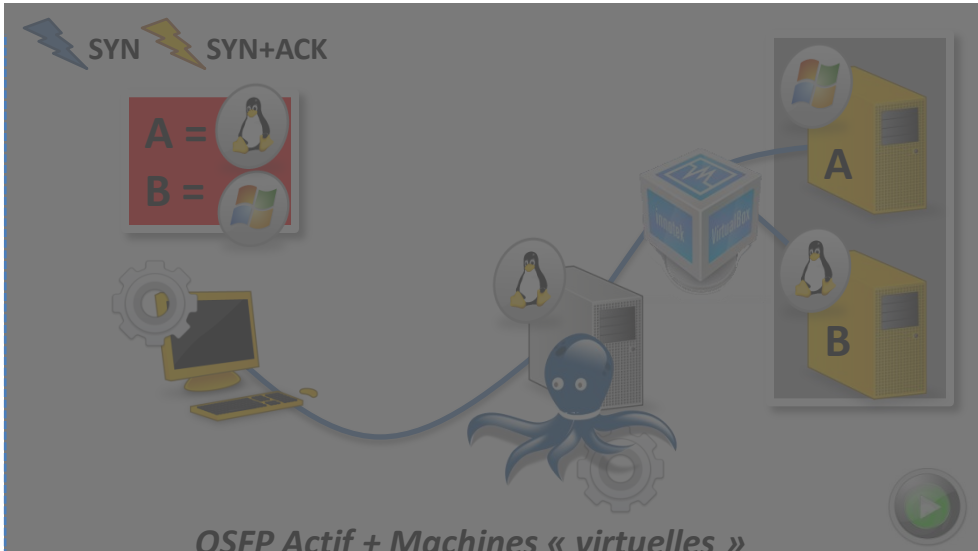


IpMorph : « unification de la mystification de prise d'empreinte»

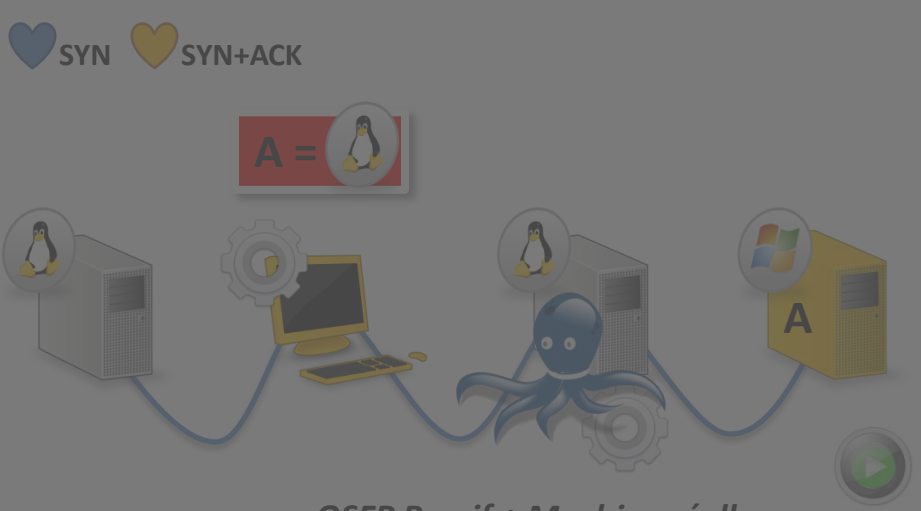
Cas d'utilisation d'IpMorph



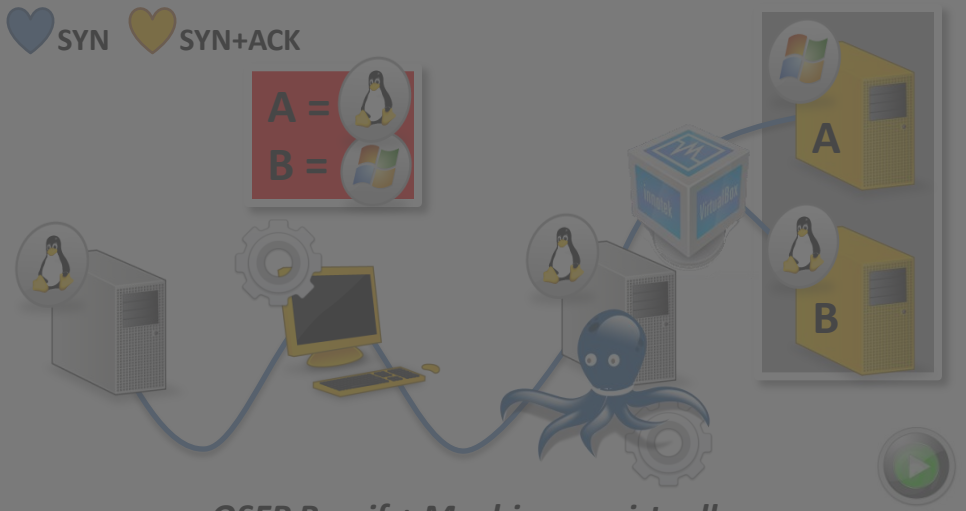
OSFP Actif + Machine réelle



OSFP Actif + Machines « virtuelles »



OSFP Passif + Machine réelle



OSFP Passif + Machines « virtuelles »

IpMorph : « unification de la mystification de prise d'empreinte»

Etat de l'art de la mystification [7]

- **Filtrage**
  - Stealth patch : **Unmaintained as of 2002, GNU/Linux kernel 2.2-2.4** *[14]*
  - Blackhole : **FreeBSD, kernel options** *[16]*
  - IPlog : **Unmaintaned as of 2001, *BSD** *[17]*
  - Packet filter : **OpenBSD** *[18]*
- **Configuration et modification de pile TCP/IP ("host based")**
  - Ip Personality *[19]*
  - Fingerprint Fucker *[12][13]*
  - Fingerprint scrubber *[1]*
  - OSfuscate *[8]*
- **Substitution de pile TCP/IP ("proxy behaviour")**
  - Honeyd *[9]*
  - Packet purgatory / Morph *[10]*

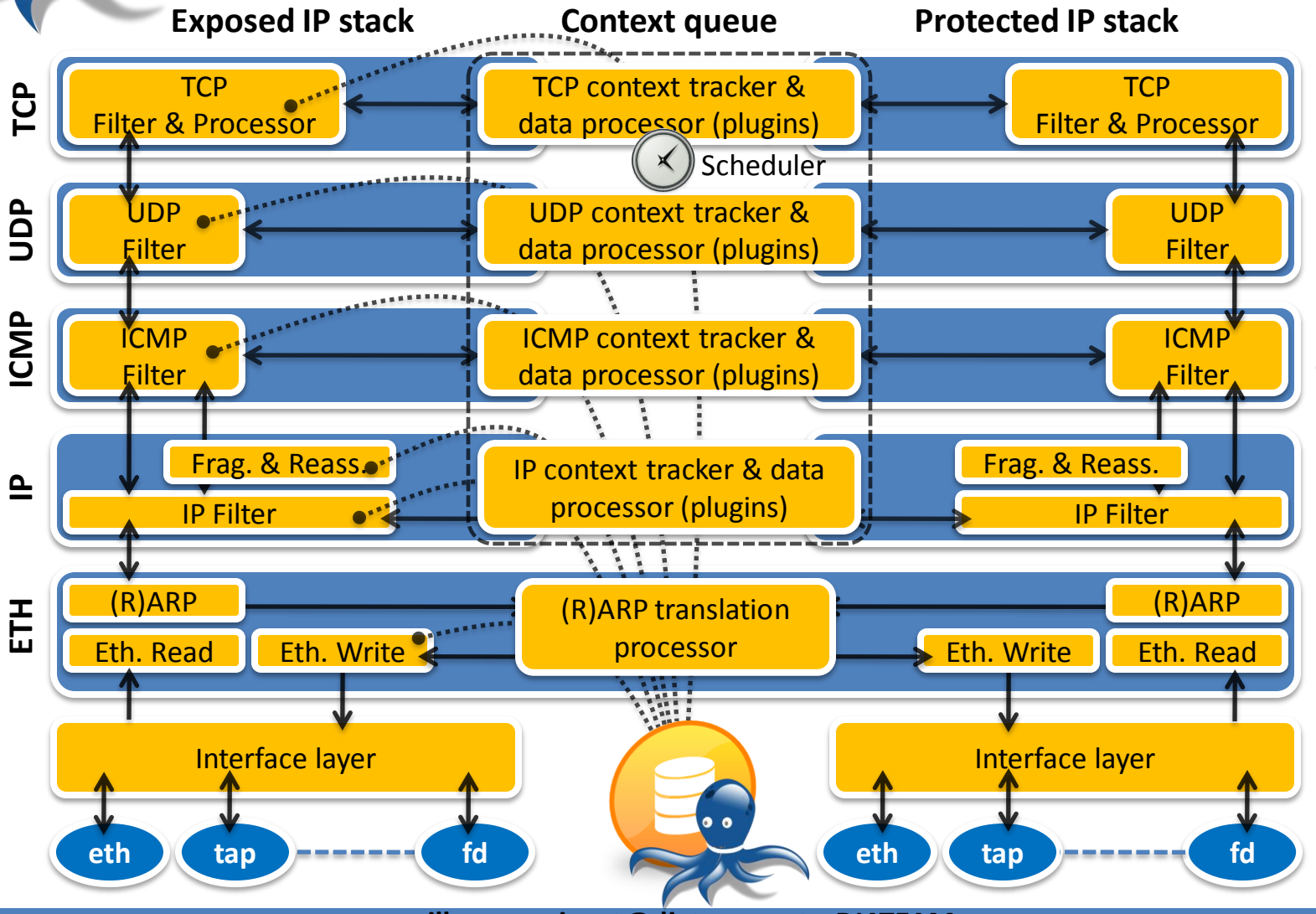
IpMorph : « unification de la mystification de prise d'empreinte»

Socle logiciel

- **Langage C++**
- **Application « *UserLand* »**
- **Utilisation du « *framework* » Qt4**
- **Eléments constituants :**
  - IpMorph (Core)
  - IpMorph Controller
  - IpMorph Personality Manager
  - IpView (IpMorph GUI)
- **Portabilité :**
  - GNU/Linux
  - *BSD, Mac OS
- **License GPLv3**

IpMorph : « unification de la mystification de prise d'empreinte»

Architecture générale



IpMorph : « unification de la mystification de prise d'empreinte»

Nmap : Format d'une signature

SP : TCP ISN Predictability

GCD : TCP ISN Greatest Common Divisor

ISR : TCP ISN counter Rate

TI : TCP IP ID sequence generation algorithm

II : ICMP IP ID sequence generation algorithm

SS : Shared IP ID sequence Boolean

TS : TCP timestamp option algorithm

O1-06: TCP Options (ordering & values)

DF: IP don't fragment bit

T: IP initial time-to-live

TG: IP initial time-to-live guess

```
Fingerprint FreeBSD 7.0-CURRENT
Class FreeBSD | FreeBSD | 7.X | general purpose
SEQ(SP=101-10D%GCD=<7%ISR=108-112%TI=RD%II=RI%TS=20|21|22)
OPS(O1=M5B4NW8NNT11%O2=M578NW8NNT11%O3=M280NW8NNT11%O4=M5B4NW8NNT11%O5=M218NW8NNT11%O6=M109NNT11)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)
ECN(R=Y%DF=Y%T=40%TG=40%W=FFFF%O=M5B4NW8%CC=N%Q=)
T1(R=Y%DF=Y%T=40%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=Y%DF=Y%T=40%TG=40%W=FFFF%S=O%A=S+%F=AS%O=M109NW8NNT11%RD=0%Q=)
T4(R=Y%DF=Y%T=40%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=40%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=40%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=40%TG=40%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
U1(DF=N%T=40%TG=40%TOS=0%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUL=G%RUD=G)
IE(DFI=S%T=40%TG=40%TOSI=S%CD=S%SI=S%DLI=S)
...
```

W1-W6 : TCP initial win size

W: TCP initial win size

S: TCP seq. number

A: TCP ack. number

F: TCP Flags

RD: TCP RST data checksum

Q: TCP misc. quirks

RIPCK: Returned probe IP checksum value

RUCK: Returned probe UDP checksum

TOS: IP type of service

IPL: IP total length

UN: Unused port unreach. field nonzero

RIPL: Returned probe IP total length value

RID: Returned probe IP ID value

RUL: Returned probe UDP length

IpMorph : « unification de la mystification de prise d'empreinte»

SinFP : Base des signatures (sqlite)

SystemClass
- *idSystemClass (PK)*
- systemClass

IpVersion
- *idIpVersion (PK)*
- ipVersion

Vendor
- *idVendor (PK)*
- vendor

Os
- *idOs (PK)*
- os

Signature
- *idSignature (PK)*
- *idIpVersion*
- *idSystemClass*
- *idVendor*
- *idOs*
- *idOsVersion*
- *idOsVersionFamily*
- *idP1PatternBinary*
- *idP1PatternTcpFlags*
- *idP1PatternTcpWindow*
- *idP1PatternTcpOptions*
- *idP1PatternTcpMss*
- ...
- *idP3PatternBinary*
- *idP3PatternTcpFlags*
- *idP3PatternTcpWindow*
- *idP3PatternTcpOptions*
- *idP3PatternTcpMss*
- trusted

OsVersionChildren
- *idSignature*
- *idOsVersion*

OsVersion
- *idOsVersion (PK)*
- osVersion

OsVersionFamily
- *idOsVersionFamily (PK)*
- osVersionFamily

PatternBinary
- *idPatternBinary (PK)*
- patternBinaryHeuristic0
- patternBinaryHeuristic1
- patternBinaryHeuristic2

PatternTcpWindow
- *idPatternTcpWindow (PK)*
- patternTcpWindowHeuristic0
- patternTcpWindowHeuristic1
- patternTcpWindowHeuristic2

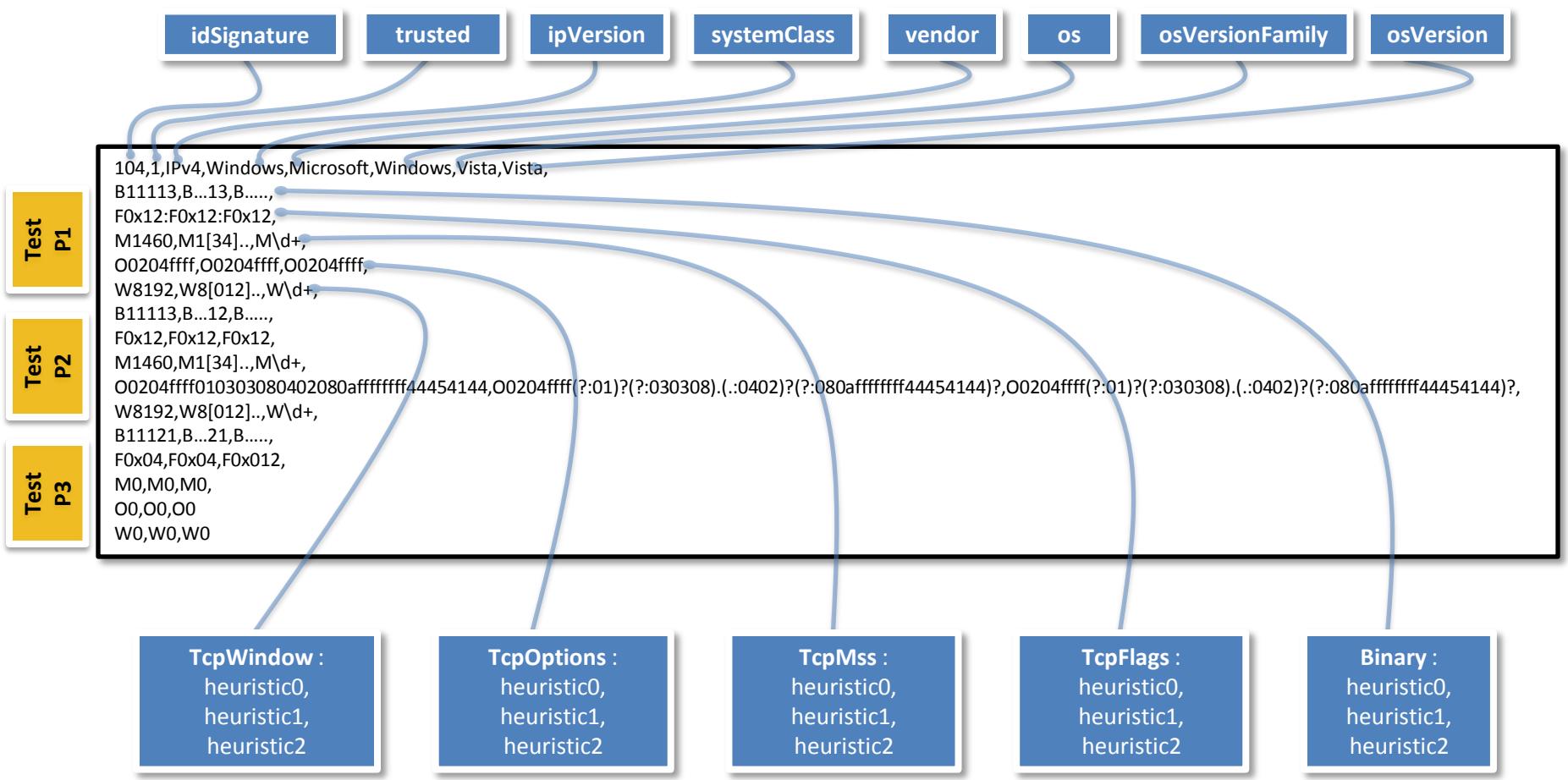
PatternTcpFlags
- *idPatternTcpFlags (PK)*
- patternTcpFlagsHeuristic0
- patternTcpFlagsHeuristic1
- patternTcpFlagsHeuristic2

PatternTcpOptions
- *idPatternTcpOptions (PK)*
- patternTcpOptionsHeuristic0
- patternTcpOptionsHeuristic1
- patternTcpOptionsHeuristic2

PatternTcpMss
- *idPatternTcpMss (PK)*
- patternTcpMssHeuristic0
- patternTcpMssHeuristic1
- patternTcpMssHeuristic2

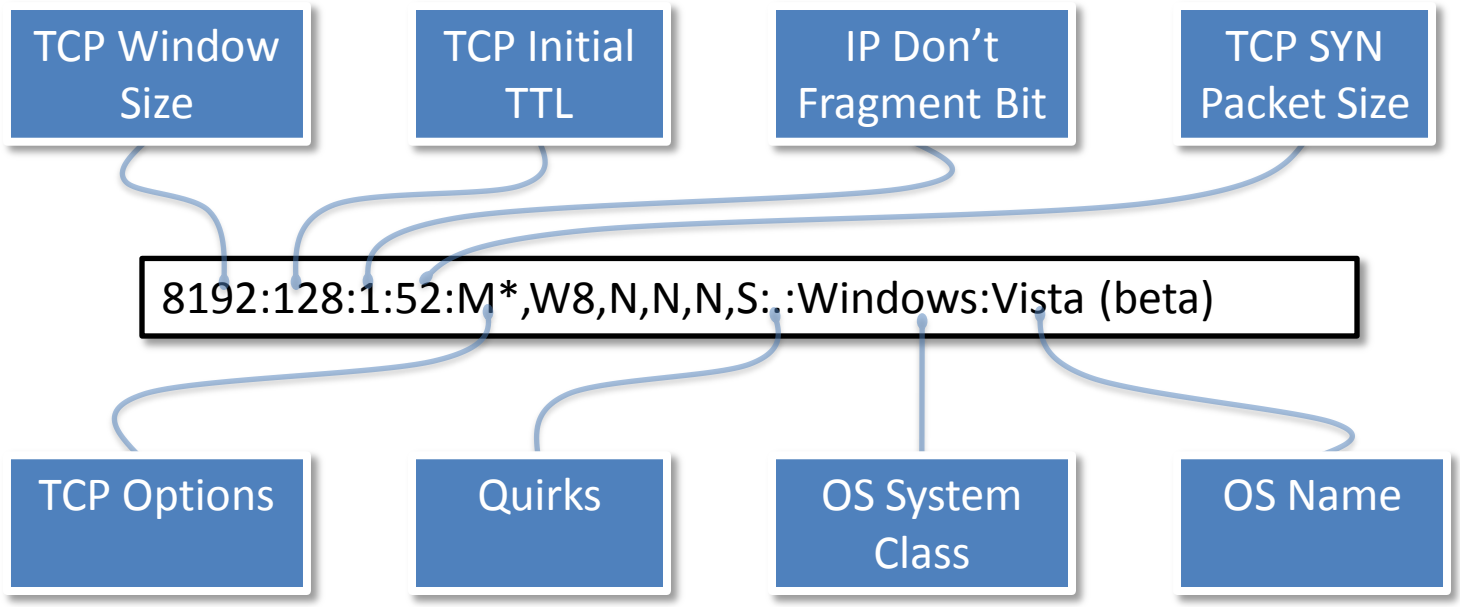
IpMorph : « unification de la mystification de prise d'empreinte»

SinFP : Format d'une signature



IpMorph : « unification de la mystification de prise d'empreinte»

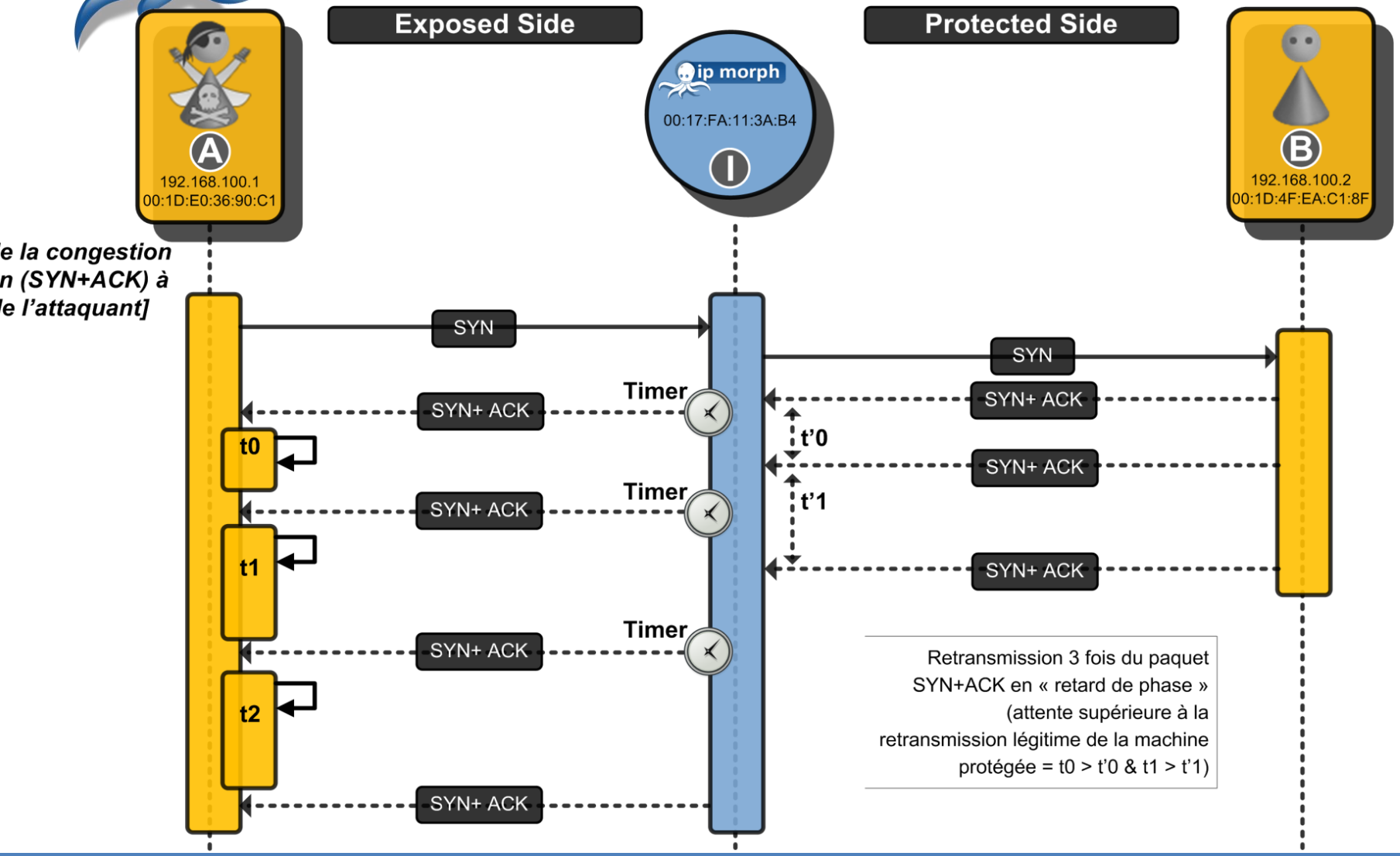
p0f : Format d'une signature



- Version 2.0.8 (2006)
- 6 paramètres d'analyse
- Uniquement sur un SYN (par défaut = p0f.fp)
- Autres fichiers de signatures pour autres modes (expérimentaux)

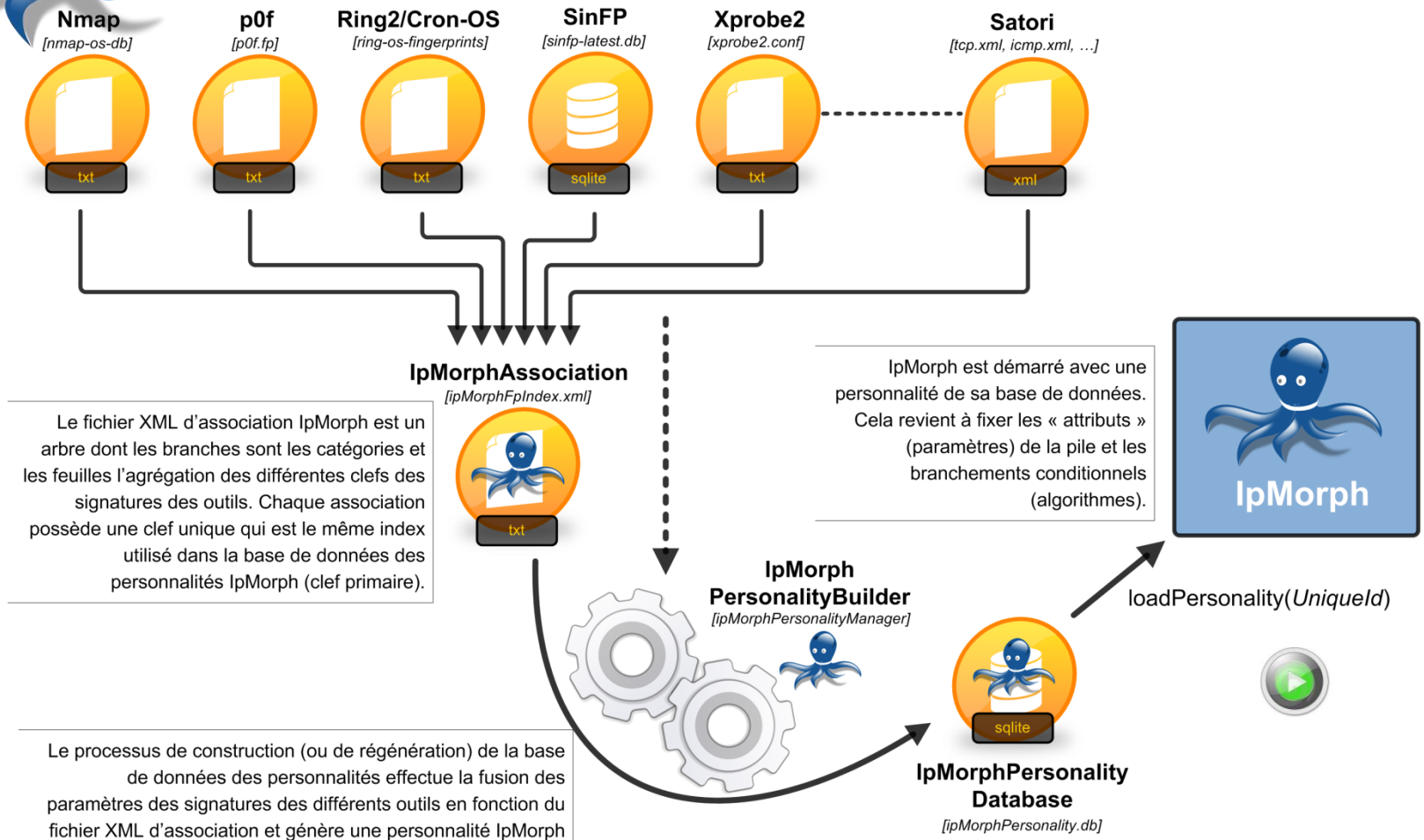
IpMorph : « unification de la mystification de prise d'empreinte»

Ring2 - Mystification de la congestion



IpMorph : « unification de la mystification de prise d'empreinte»

Personality Manager



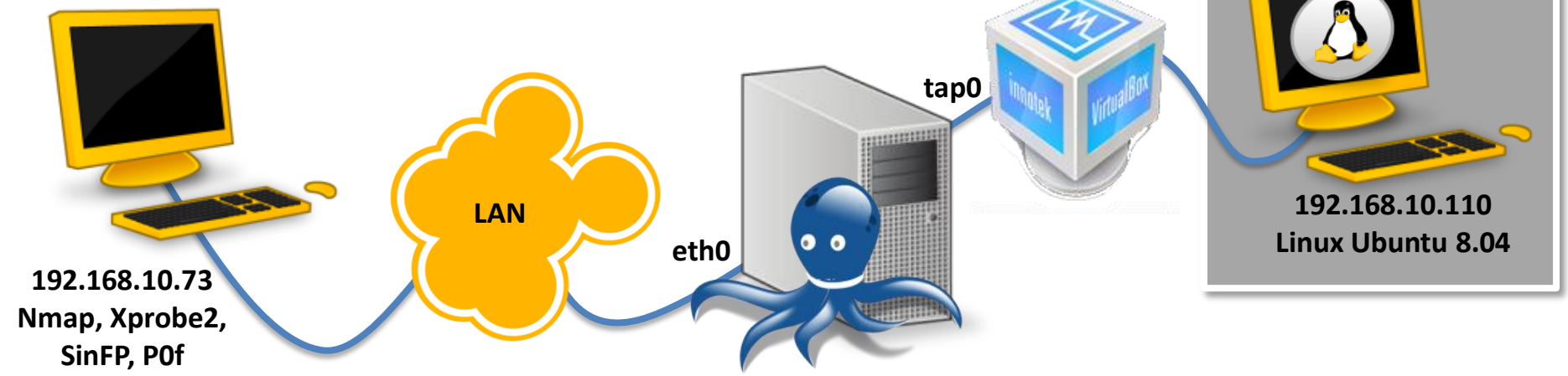
IpMorph : « unification de la mystification de prise d'empreinte»

Perspectives

- **Juin 2009 – SSTIC 2009**
  - Présentation « officielle »
  - « *Beta release* » 0.1 (en « *download* » par courriel)
- **Fin 2009 – Début 2010**
  - « *Refactoring* » (Qt4 ?, uIp !, tests en production …)
  - PersonalityManager, Intégration filtrage, …
  - Version 0.2 en « *download* » Internet
  - Documentation, « *UserGuide* », …
  - Intégration de quelques « *scrubbers* » applicatifs (DNS, SMB, DHCP, …) ?

IpMorph : « unification de la mystification de prise d'empreinte»

Démonstration



Scénario de la démonstration

Configuration

- 1 - Interface tap0
- 2 - VirtualBox
- 3- IpMorph

Prise d'empreinte « active »

- 4 - Xprobe2
- 5 - Nmap
- 6 - SinFp en actif

Prise d'empreinte « passive »

- 7 - SinFp en passif
- 8 - p0f

Merci de votre attention.