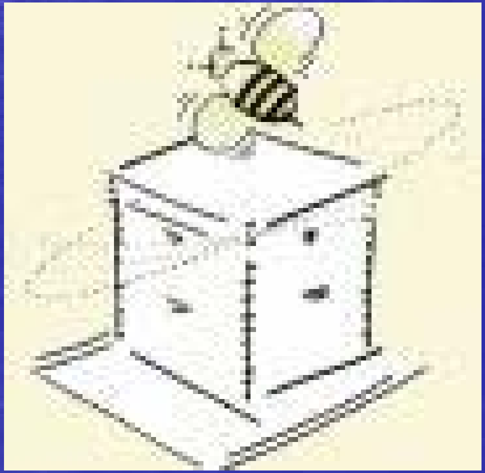
A Pointillist Approach for Comparing Honeypots

Fabien Pouget, Thorsten Holz



EURECOM
Sophia Antipolis

RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

Motivations

- What are the Modus Operandi of the perpetrators?
- Who has data to validate in a rigorous way any kind of taxonomy and/or profiling model?
- Are the threats changing?
- How can we figure out if we are facing script kiddies and/or « organized crime » ?

Motivations (ctd.)

- Darknets and Internet telescopes are based on the assumption that lessons learned from the observation of attacks at a given place can be extrapolated to the whole Internet.
- How do we know if that assumption holds?
- What about a deployment of small honeypot sensors placed in a lot of various locations?

Honeypot Families

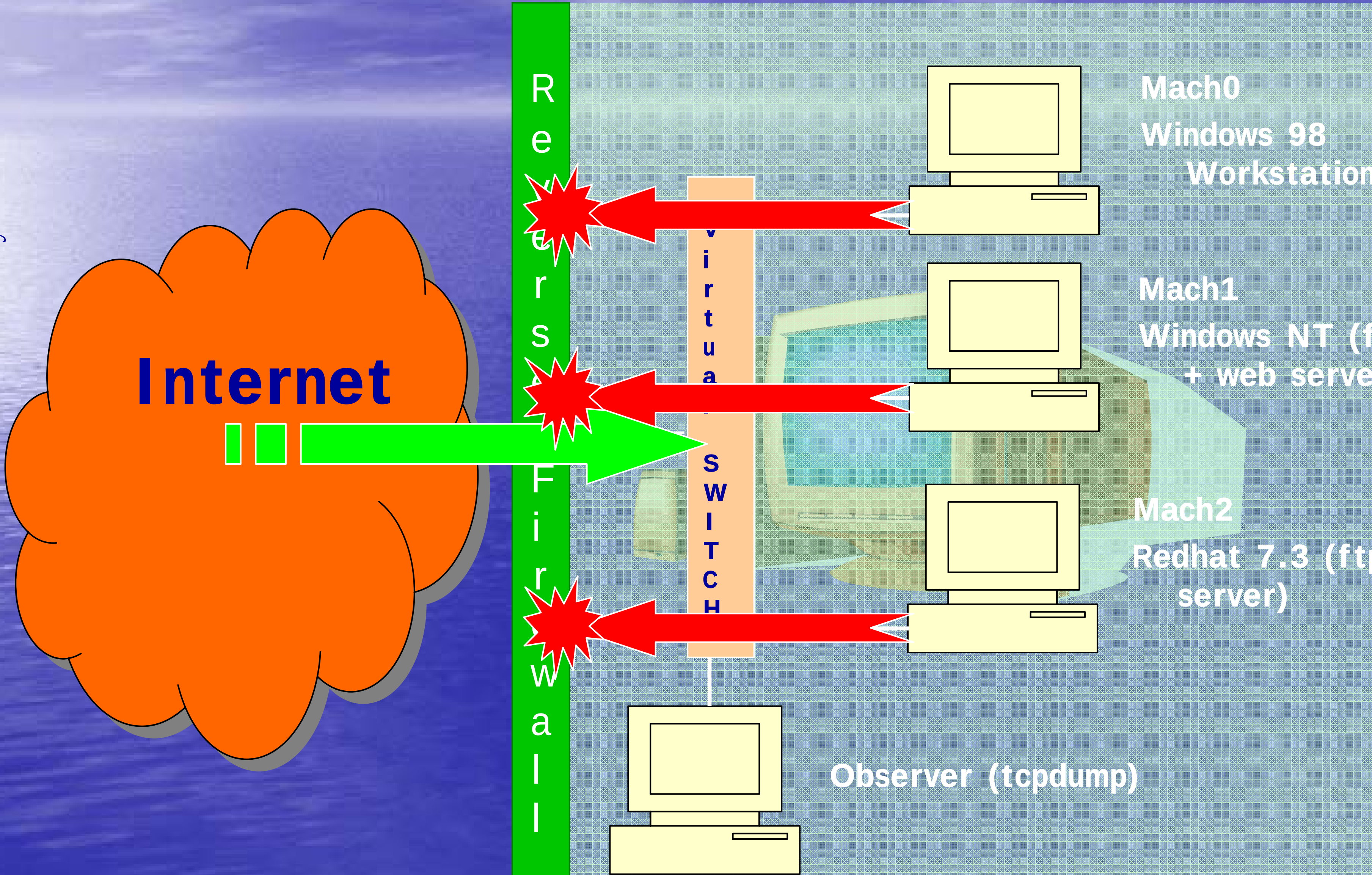
- **High-Interaction**
  - Real Environments at the mercy of attackers
  - Record hacker shell commands
  - Hard monitoring, legal issues
  - Costful (resources, maintenance, licenses, etc)
- **Low-Interaction**
  - Superficial Behavior
  - Safer
  - Scalable and flexible
  - Cheap (many open projects or home-built tools)

- Any qualitative and quantitative comparison?

First Honeypot Environment: H1

- **High Interaction Experimental Setup H1**
  - **VMWare-based**
  - **Ethernet switch**
  - **Non-persistent disks**
  - **ARP Spoofing**
  - **Three virtual machines: IPs=X.X.X.1, X.X.X.2, X.X.X.3**

Experimental Set Up



Internet

Reverse Firewall

Virtual SWITCH

Mach0

Windows 98 Workstation

Mach1

Windows NT (f + web serve

Mach2

Redhat 7.3 (ftp server)

Observer (tcpdump)

Second Honeypot Environment: H2

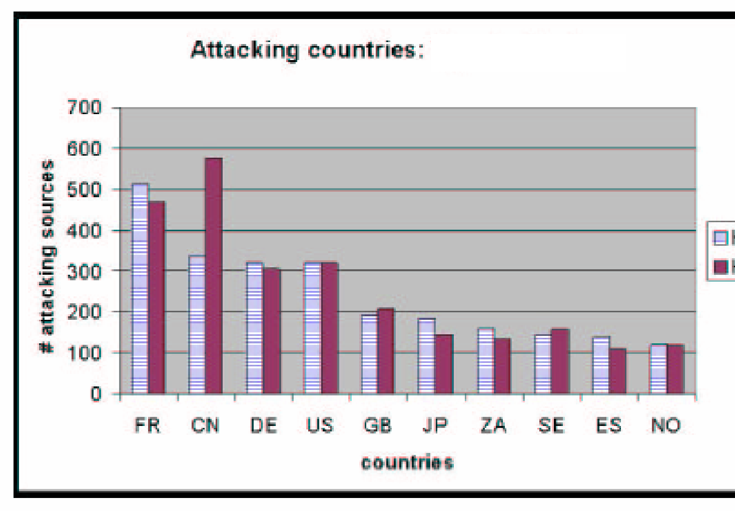
- **Low Interaction Experimental Setup H2**
  - **Honeyd-based**
  - **ARP Proxy**
  - **3 Operating Systems Profiles (from nmap & xprobe fingerprints database)**
  - **Port Status (from scanning)**
  - **Emulated Services**
  - **Three virtual machines IPs=X.X.X.7, X.X.X.8, X.X.X.9**

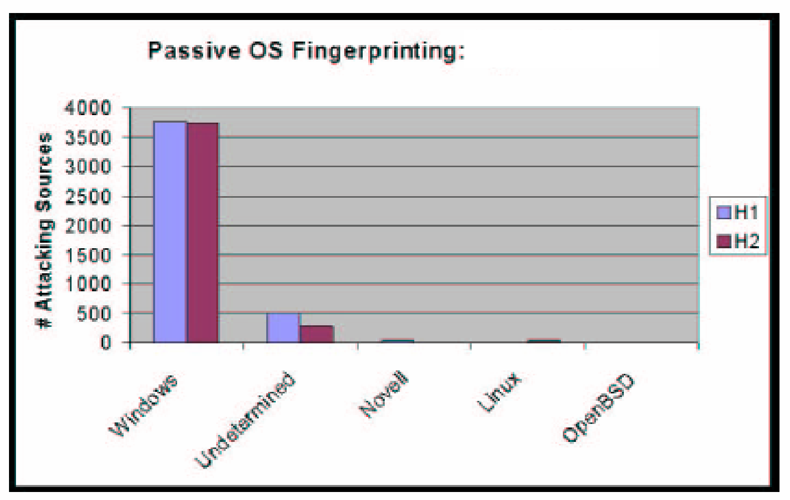
Comparison: In Short...

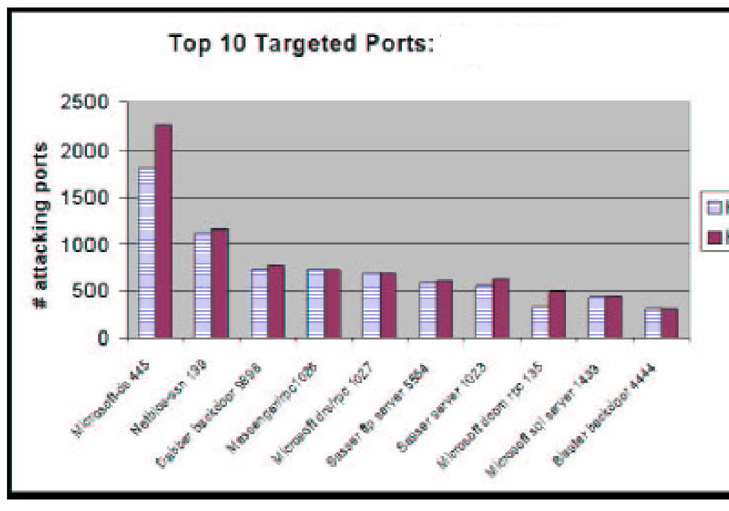
- H1 and H2 are in a French academic Network
- 3 months (August-October 2004) of data collection
- Not hidden behind a firewall
- Data daily collected and stored in a SQL database.
  - Enriched Information (geographical location, Passive OS fingerprinting, whois queries, TCP stats...)
  - Analysis
    - Grouping of attacks sharing same fingerprint on the platform into clusters
    - Particular Attention to losses and reordering (with IPID fields, TCP sequence numbers, etc)
    - And others (time series)
- H1: 480700 received packets (40x more than H2)

Global Statistics Analysis

- Attacking Countries
- Passive OS Fingerprinting
- Top10 Targeted Ports

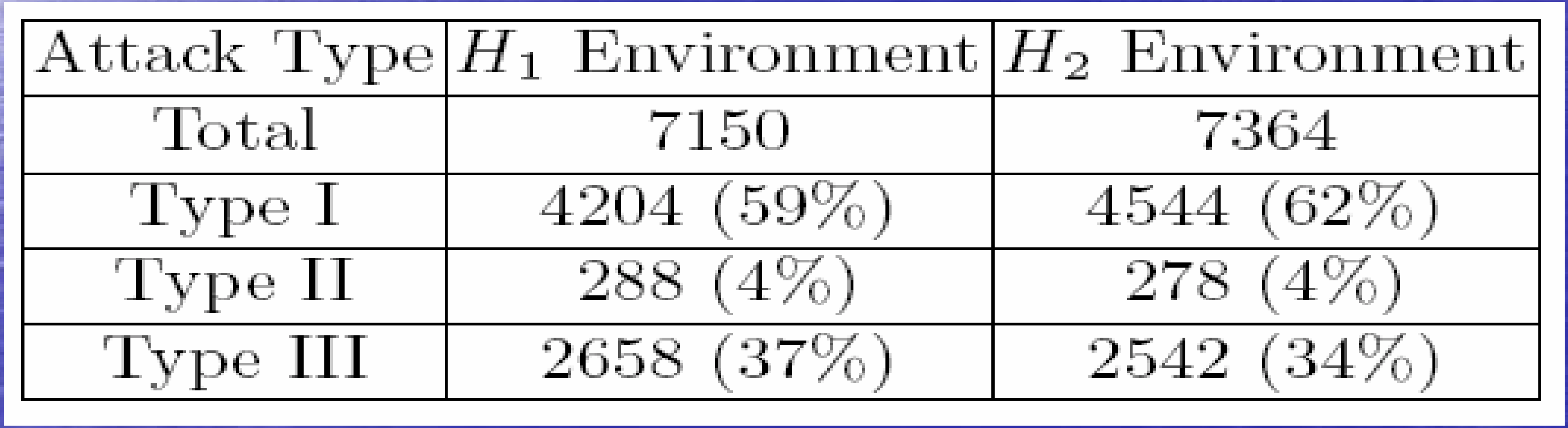






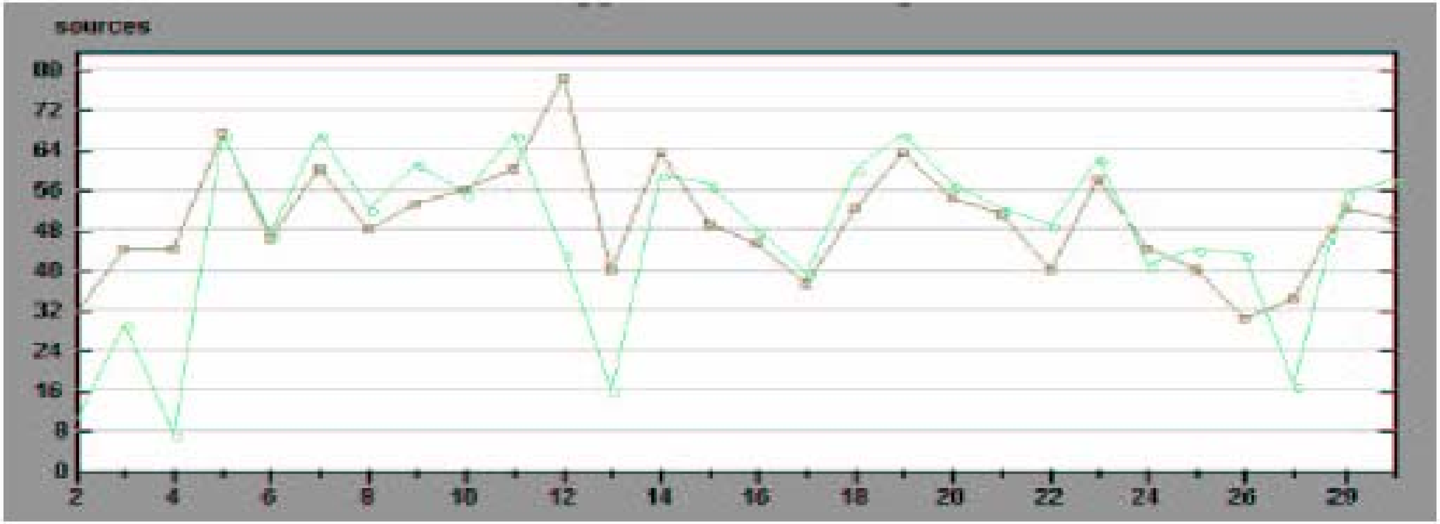
Attack Categories

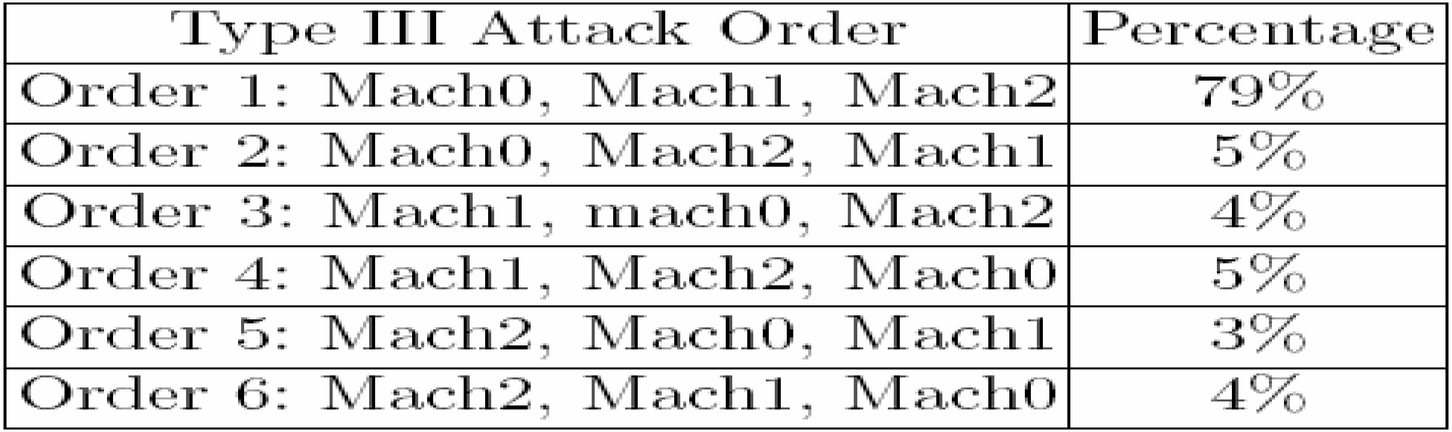
Grouping attacks according to the number of Virtual Machines they have targeted on each Honeypot Environment



Attack Type	H_1 Environment	H_2 Environment
Total	7150	7364
Type I	4204 (59%)	4544 (62%)
Type II	288 (4%)	278 (4%)
Type III	2658 (37%)	2542 (34%)

Type III Attacks





Type III Attack Order	Percentage
Order 1: Mach0, Mach1, Mach2	79%
Order 2: Mach0, Mach2, Mach1	5%
Order 3: Mach1, mach0, Mach2	4%
Order 4: Mach1, Mach2, Mach0	5%
Order 5: Mach2, Mach0, Mach1	3%
Order 6: Mach2, Mach1, Mach0	4%

Type III Attacks (cont.)

-All IPs are common to both environments
-They send very few packets in general
-Impact of packet losses

⇒ Broad-sweeping scans

⇒ On the usefulness of deploying honeypots using hundreds of IP addresses?

⇒ In-sequence Scanning
(New IP = current IP +1)

⇒ What about blacklisting the IPs?

Type II Attacks

- 88% => Residus of Type III attacks (many confirmation techniques)

- 9% => Scanning one out of two IPs (new IP = current IP + 2)

- 3% => Attacks on the sole two Windows virtual machines. Where is coming the information?

Type I Attacks

- 60 % of the observed attacks
- Similar global stats
- But...
- Here, IPs are not observed on both H1 and H2...
- Could we also determine if they are associated to same attack processes?

Type I Attacks (cont.)

- Very few broad-sweeping scans residus (i.e. two packet losses at least)

- Random Propagation Strategy
  - Identification by using the *clustering* method we have developed
    - Large clusters, some of them being identified and labeled
    - Attack fingerprints found on both H1 and H2
    - No favorite target (i.e. machines are equally targeted)

- And the others...

... particular to each platform H1 or H2.... And to a given virtual machine...

→ **focused and original Attacks**

Examples

- Example 1

<u>Attacks on port 25666</u>
<u>Of Mach0 (H1) only</u>

✓ **Observed 387 times**
✓ **From 378 distinct IPs**
✓ **During three months**
✓ **Very regular (day after day)**

✓ **Source ports=80,8080**
✓ **TCP flag set=RST-ACK**

✓ **Residus of DoS attacks on web servers (*Backscatters*)**

- Example 2

<u>Attacks on port 5000</u>
<u>Of Mach1 (H2) only</u>

✓ **From 75 distinct IPs**
✓ **Half a dozen TCP Syn packets**
✓ **No payload**

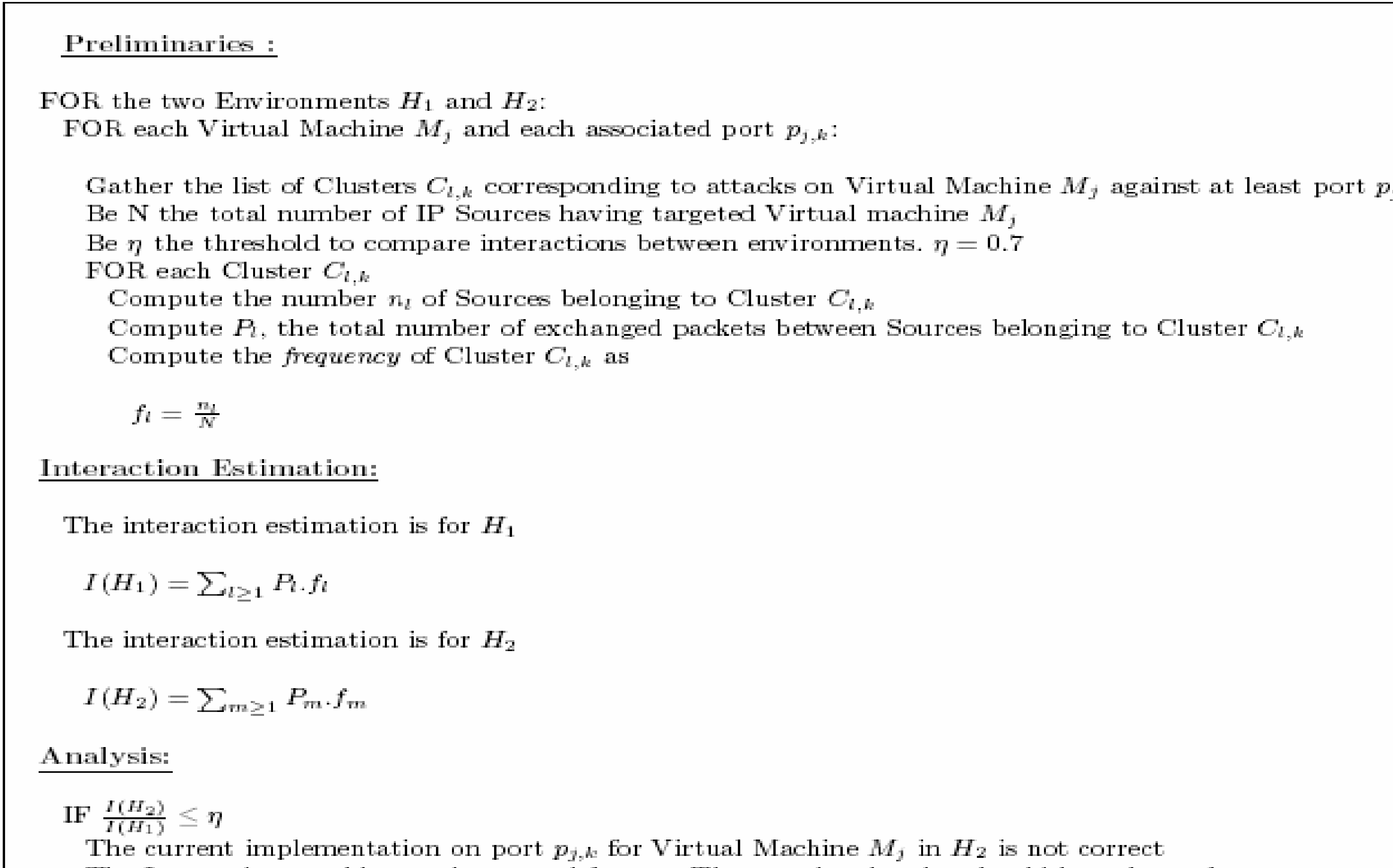
✓ **UPnP port 5000**
✓ **often associated to Bobax or Kibuv worms... but... does not match their random scanning activities**

✓ **So?**

Interaction Differences

- How to periodically validate the relevance of H2 configuration wrt to H1 data?
- Are the actions bound to each port sufficient in H2?
- Idea: the more different attacks interact with a port (from H1 observation), the more important it is that Honeyd runs an interactive script behind the port.

Interaction validation



Preliminaries :

```
FOR the two Environments $H_1$ and $H_2$:
  FOR each Virtual Machine $M_j$ and each associated port $p_{j,k}$:

    Gather the list of Clusters $C_{l,k}$ corresponding to attacks on Virtual Machine $M_j$ against at least port $p_j$
    Be N the total number of IP Sources having targeted Virtual machine $M_j$
    Be $\eta$ the threshold to compare interactions between environments. $\eta = 0.7$
    FOR each Cluster $C_{l,k}$
      Compute the number $n_l$ of Sources belonging to Cluster $C_{l,k}$
      Compute $P_l$, the total number of exchanged packets between Sources belonging to Cluster $C_{l,k}$
      Compute the frequency of Cluster $C_{l,k}$ as

        $f_l = \frac{n_l}{N}$
```

Interaction Estimation:

```
  The interaction estimation is for $H_1$

    $I(H_1) = \sum_{l \geq 1} P_l . f_l$

  The interaction estimation is for $H_2$

    $I(H_2) = \sum_{m \geq 1} P_m . f_m$
```

Analysis:

```
  IF $\frac{I(H_2)}{I(H_1)} \leq \eta$
    The current implementation on port $p_{j,k}$ for Virtual Machine $M_j$ in $H_2$ is not correct
```

Interaction validation

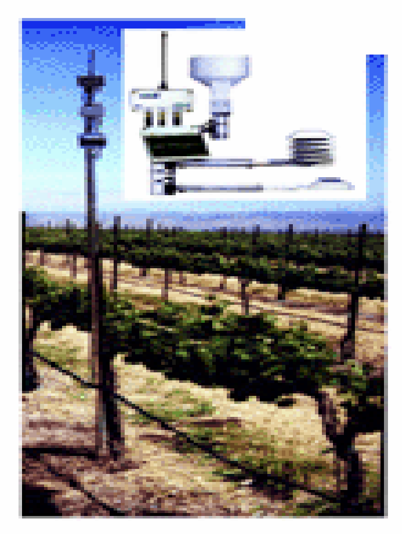
- It is often sufficient just to open a port ex: 111 (RPC), 515 (LPRng).
- Few scripts are not interactive enough (on netbios ports especially)

- These tendencies might change over months...

First conclusion

- Comparison between H1 and H2 brings three concrete outcomes:
  - Relevance of the configuration of Low Interaction honeypots
  - Low Interaction honeypots capture interesting information, without introducing particular bias.
  - Surprising attacks specific to a given machine
- Low Interaction honeypots provide a good representative source of information. High-Interaction honeypots are good etalon systems.

Analogies?



- Weather forecast

- Volcanic/sismic activities

Leurré.com

- This project aims at deploying the very same honeypots in a large number of diverse locations.
- Early results demonstrate the complementarity of this approach to so-called *Internet telescopes* and *Darknets*.
- You can see this as a simple, widely distributed, fine grained network monitoring system

- Partially funded by the French ACI Security named CADHO (see acisi.loria.fr)

CADHO: Collection and Analysis of Data from HOneypots

- Joint work with CERT/RENATER, France
- Joint work with LAAS/CNRS

- Complete this preliminary study on High-Interaction Honeypots in a large-scale network of combined interactions.

35 platforms, 20 countries, 5 continents

In Europe ...

Greenland Sea
Norwegian Sea
Barents Sea
ICELAND
NORWAY
SWEDEN
FINLAND
ESTONIA
RUSSIA
North Atlantic Ocean
North Sea
DENMARK
UNITED KINGDOM
IRELAND
NETH.
BELGIUM
LUX.
GERMANY
POLAND
LITHUANIA
BELARUS
UKRAINE
SLOVAKIA
AUSTRIA
HUNGARY
MOLDOVA
ROMANIA
SWITZ.
FRANCE
Bay of Biscay
ITALY
Serbia
BULGARIA
ALB.
GREECE
TURKEY
PORTUGAL
SPAIN
Mediterranean Sea
Tyrrhenian Sea
Ionian Sea
MALTA
MOROCCO
ALGERIA
TUNISIA

Win-Win Partnership

- The interested partner provides ...
  - One old PC (pentiumII, 128M RAM, 233 MHz...),
  - 4 routable IP addresses,
- EURECOM offers ...
  - Installation CD Rom
  - Remote logs collection and integrity check.
  - Access to the whole SQL database by means of a secure web access.

Conclusions

- The more platforms we get, the better the analysis we can carry out.
- Assumptions made by Internet telescopes do not always hold.
- Threats are changing.
- Attacks are as frequent as before but try to stay more stealthy.

- You should join our distributed platform !!!
  - Contact : **pouget@eurecom.fr**

References

- More information on the French ACI Security available at acisi.loria.fr
- F. Pouget, M. Dacier, “Honeypots-based Forensics”, *Proc. Of the AusCERT2004 Conference* (refereed stream), May 23-27 2004, Brisbane, Australia.
- M. Dacier, F. Pouget, H. Debar, “Attack Processes found on the Internet”, *Proc. NATO Symposium on Adaptive Defense in Unclassified Networks*, April 2004.
- M. Dacier, F. Pouget, H. Debar, “Honeypots: Practical Means to Validate Malicious Fault Assumptions on the Internet”, *Proc. 10th IEEE International symposium Pacific Rim Dependable Computing (PRDC10),*March 2004, pages. 383-388.

Exhaustive and up to date list of publications available at http://www.eurecom.fr/~pouget/papers.htm

http://www.leurrecom.org

Thank you for your attention !

Questions?