



Improving Security Management through Passive Network Observation

Yohann THOMAS - Hervé DEBAR

France Télécom R&D - Caen, France

Benjamin MORIN

Supélec - Rennes, France



(Unrestricted)

What are we talking about ? (1)



→ Intrusion Detection

- Second security level above intrusion prevention
- Sensors aiming at detecting unauthorized actions
 - Matching of attack signatures or behavior anomaly detection
 - Reporting of alerts in case of characterized attacks
- Limitations:
 - Operators overwhelmed over huge amounts of alerts
 - Large number of false positives
 - Poor alert semantic

} Need for additional processing



Alert Correlation

(Unrestricted)

What are we talking about ? (2)



→ Alert Correlation

- Improve intrusion detection diagnosis by merging low-level alerts (or events) to produce “better” alerts

- Consider vulnerability assessment
 - Enable alert severity mitigation
 - Provide false positive recognition
- } Need for additional information
(not only alerts/events)



What are we talking about ? (3)



→ Host Profiles

- Inventory of the hosts of an information system
 - IP addresses / DNS names
 - Operating Systems
 - Services and Clients
 - Various software
- Deduction of host functions

→ Network Mapping

- Acquisition of host profiles from the network

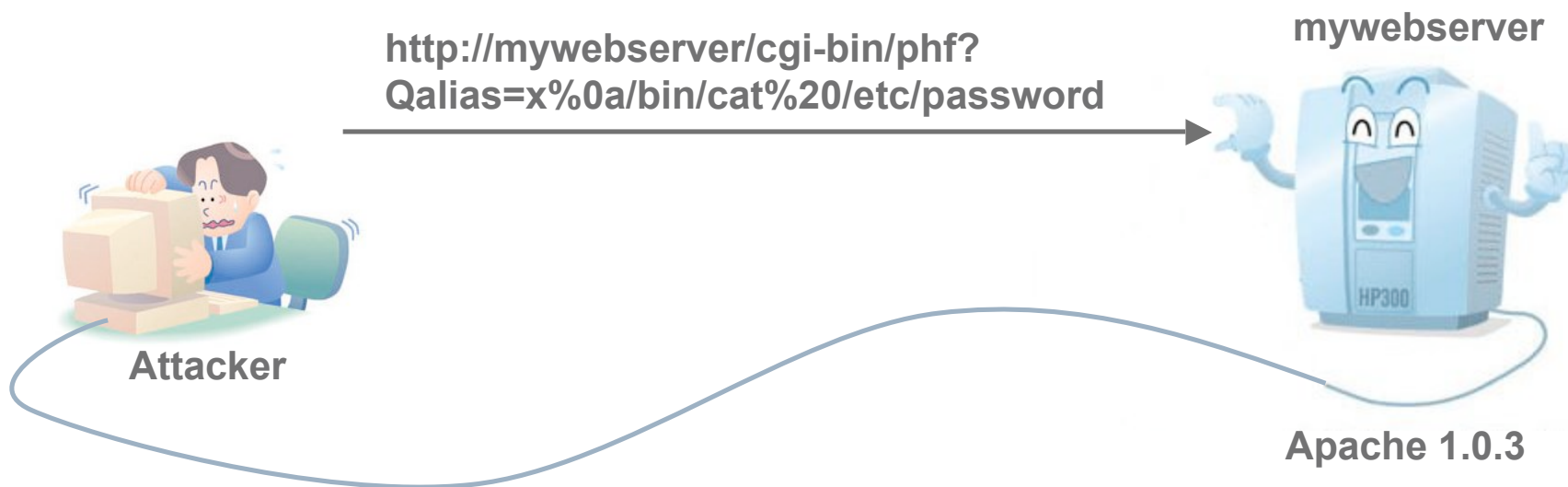
→ Passive Network Mapping

- Innocuous method to acquire hosts profiles, that is only observing the traffic

Objective: Correlation with vulnerabilities (1)



→ PHF attack over a vulnerable webserver



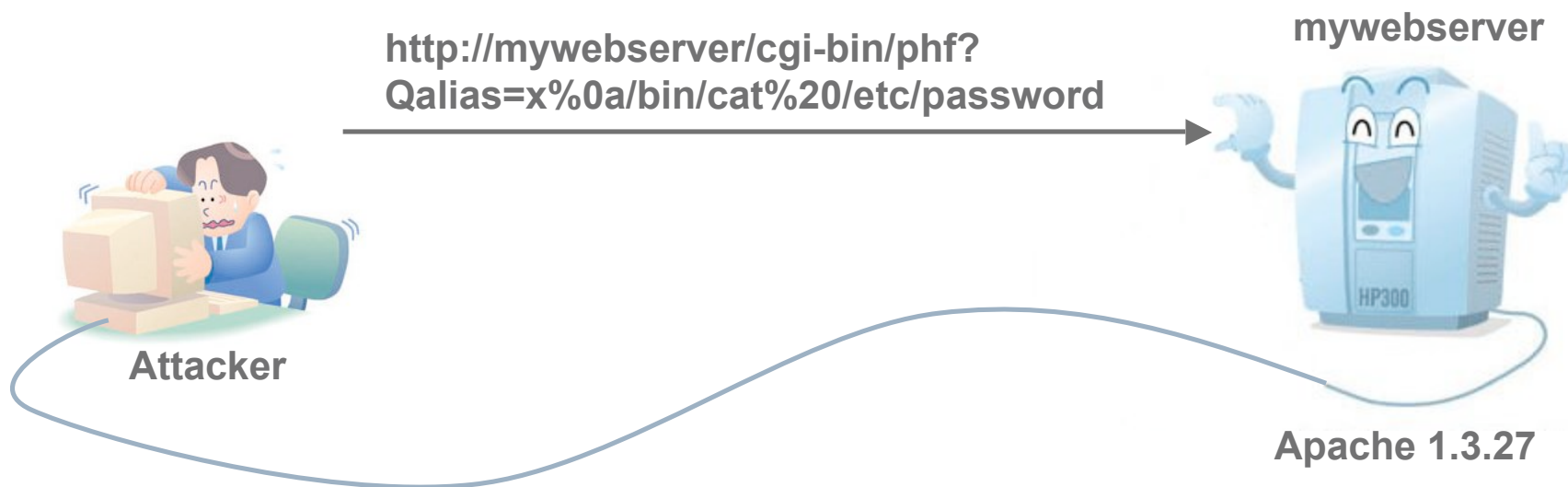
→ OSVDB 136: Apache 1.0.3 is vulnerable

Increase alert severity

Objective: Alert Severity Mitigation (2)



➔ PHF attack over a non-vulnerable webserver



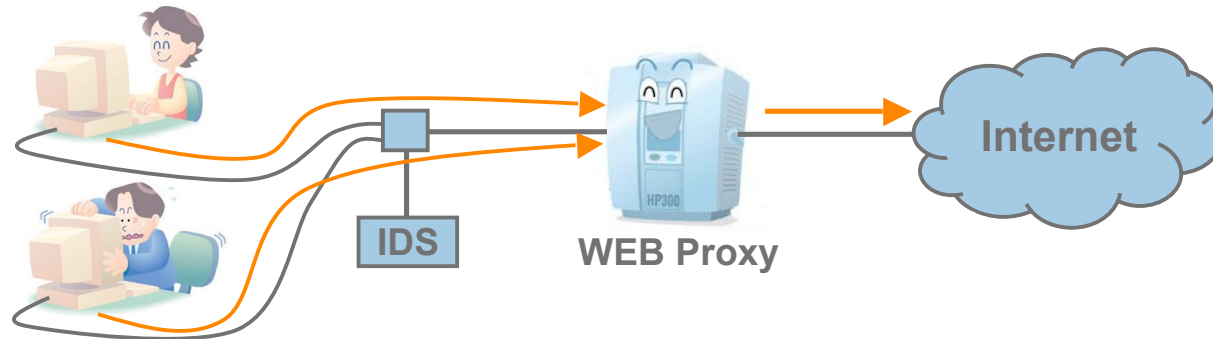
➔ OSVDB 136: Apache 1.3.27 is **not** vulnerable

Decrease alert severity

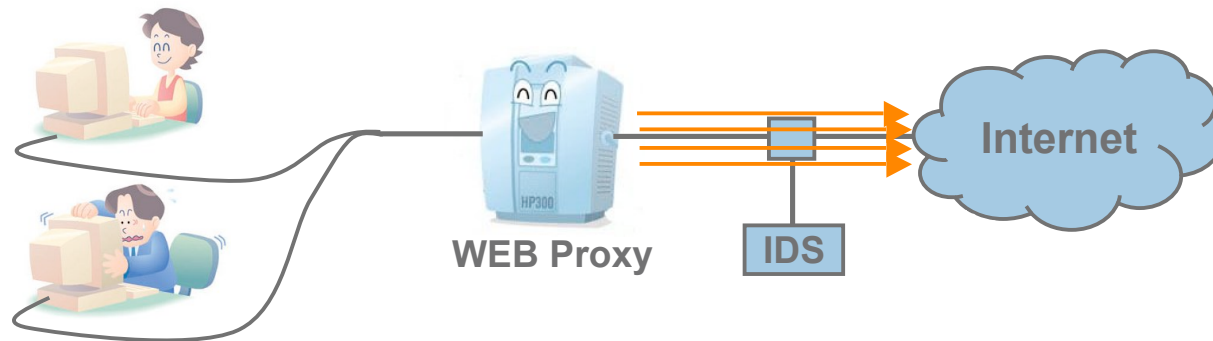
Objective: False Positive Recognition (3)



- ➔ Configurations prone to false positives (Ex: HTTP Proxy)
 - "HTTP Proxies seen as victims of web attacks (flooding)"



- "HTTP Proxies seen as IP-Sweep attackers"



Why not use existing active approaches ?



- Some tools exist, e.g. nmap, ettercap, nessus, etc.
- Several major drawbacks, among which:
 - Additional traffic generated on the monitored network
 - Harmful side-effects for the environment (ex: stimulation)
 - Difficulty of deployment and maintenance (ex: agents)
 - Discovery of server-side characteristics only (not client-side)
 - Long-time acquisition process
 - Lack of reactivity
 - ...



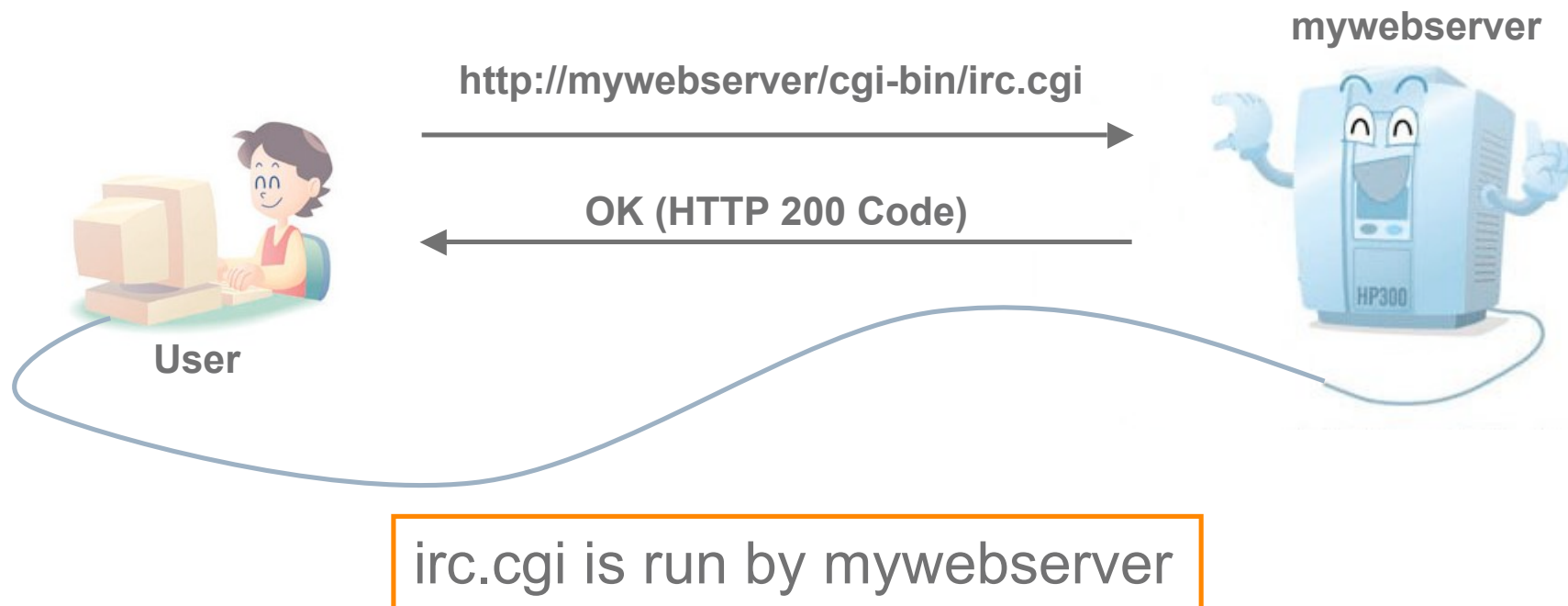
We prefer the **passive** approach

Innovative functionalities (1)



→ Stateful analysis

- Single packets analysis is not sufficient
- Session analysis



Innovative functionalities (2)



➔ Applicative protocol decoding

- Obtain precise properties
- Ex: HTTP

```
GET http://c-xe159b/ HTTP/1.1.
Host: c-xe159b.
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.6)
Gecko/20040405 Firefox/0.8.
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1.
Accept-Language: en-us,en;q=0.5.
Accept-Encoding: gzip,deflate.
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7.
Keep-Alive: 300.
Proxy-Connection: keep-alive.
```

URL

WEB Client

OS

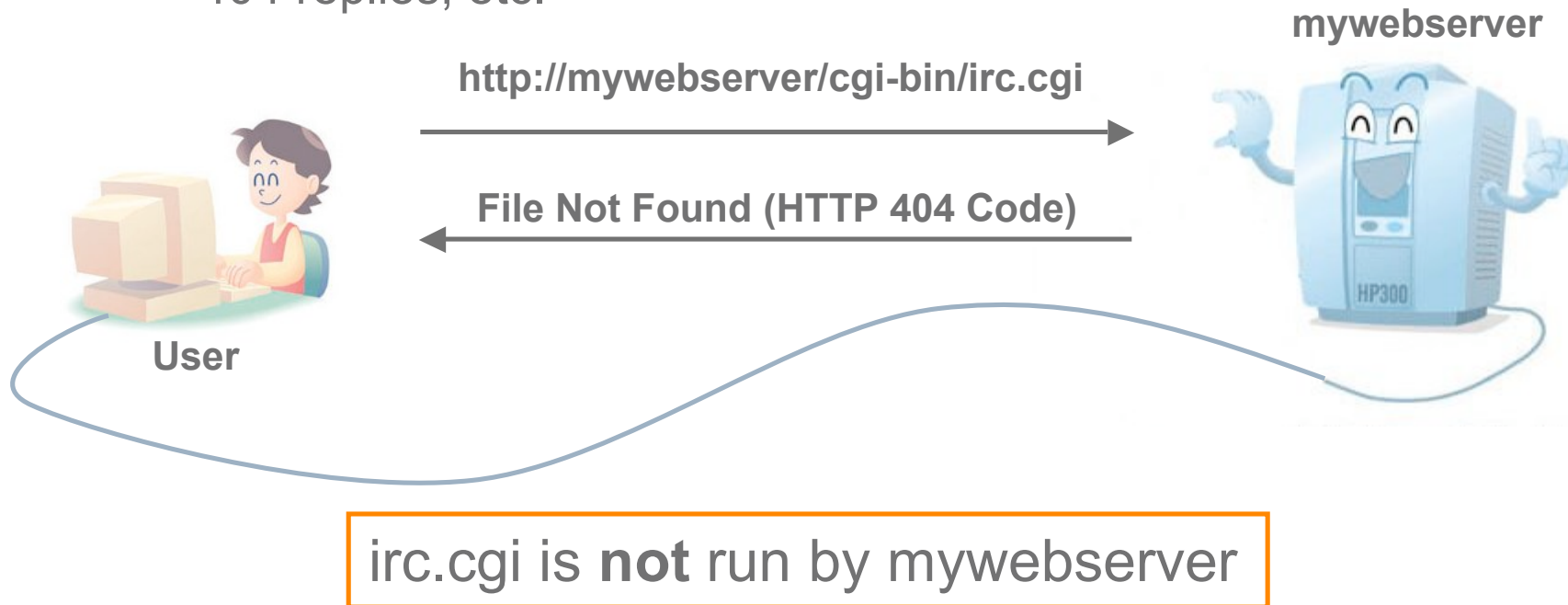
(Unrestricted)

Innovative functionalities (3)



➔ Absence of features

- Avoid closed world assumption
- Need for absence of properties discovery (non-existent software)
- Ex: ICMP « host unreachable », TCP failed connections, HTTP 404 replies, etc.



Innovative functionalities (4)

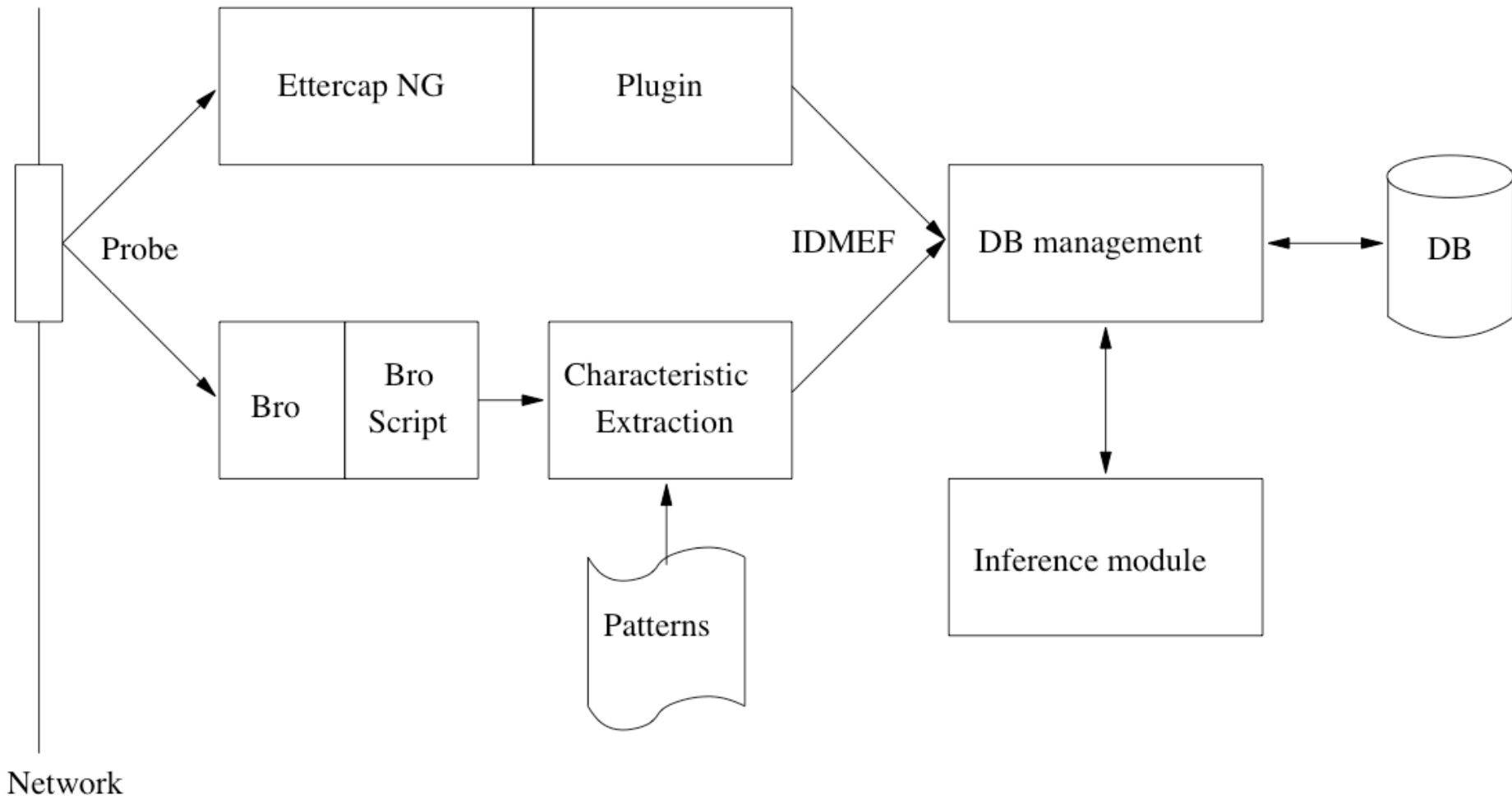


→ Property inference

- Deduct non-observed properties
- Infirm, confirm or update observation
- Detect inconsistencies in host properties



Prototype



Experiments



- Prototype installed on an exploitation network at France Télécom R&D
- Five captures of 2 minutes, during a working day
- Observation of:
 - IP addresses / DNS names
 - Operating systems
 - Services (based on open ports)
 - Web clients and web servers (HTTP decoding)
 - CGI applications (HTTP decoding)

Results



Identified objects	Capture number					TOTAL
	1	2	3	4	5	
Hosts	344	342	323	274	322	742
Products	165	116	150	93	118	223
Runs	927	907	877	635	879	2162
Names	35	24	32	18	20	63
OSes	24	24	26	22	25	31
Web servers	39	35	34	38	47	71
Web clients	15	14	11	11	16	24
CGIs	1	0	0	0	0	1

- 702 hosts have been assigned at least one OS
- Among 2162 runs relations, 760 associate OSes with hosts

Conclusion & perspectives



- A limitation: characteristics are discovered for a host only if it is involved in a communication, but...
- Corollary: whenever a host communicates, the system is susceptible to observe and update properties.

- Possible new active functionalities in the mapping system
 - ex: DNS requests to keep up-to-date name-IP mappings
 - Current implementation of passive mapping system works in complement of active systems

Questions?

