Intrusion Detection Systems

Principles, Architecture and Measurements

S3 HUT,6.5.2003, Ville Jussila (vsjussil@netlab.hut.fi)

Supervisor: prof. Jorma Jormakka, HUT - Networking Laboratory

Contents

- Motivation for Intrusion Detection
- Different Types of IDSs
- Simple Process Model for ID
- Advanced Technologies
- NSS Test Results
- Measurements

What is Intrusion Detection

Intrusion detection systems (IDSs) are designed for detecting, blocking and reporting unauthorized activity in computer networks.

“The life expectancy of a default installation of Linux Red Hat 6.2 server is estimated to be less than 72 hours.”

“The fastest compromise happened in 15 minutes (including scanning, probing and attacking)”

“Netbios scans affecting Windows computers were executed with the average of 17 per day”

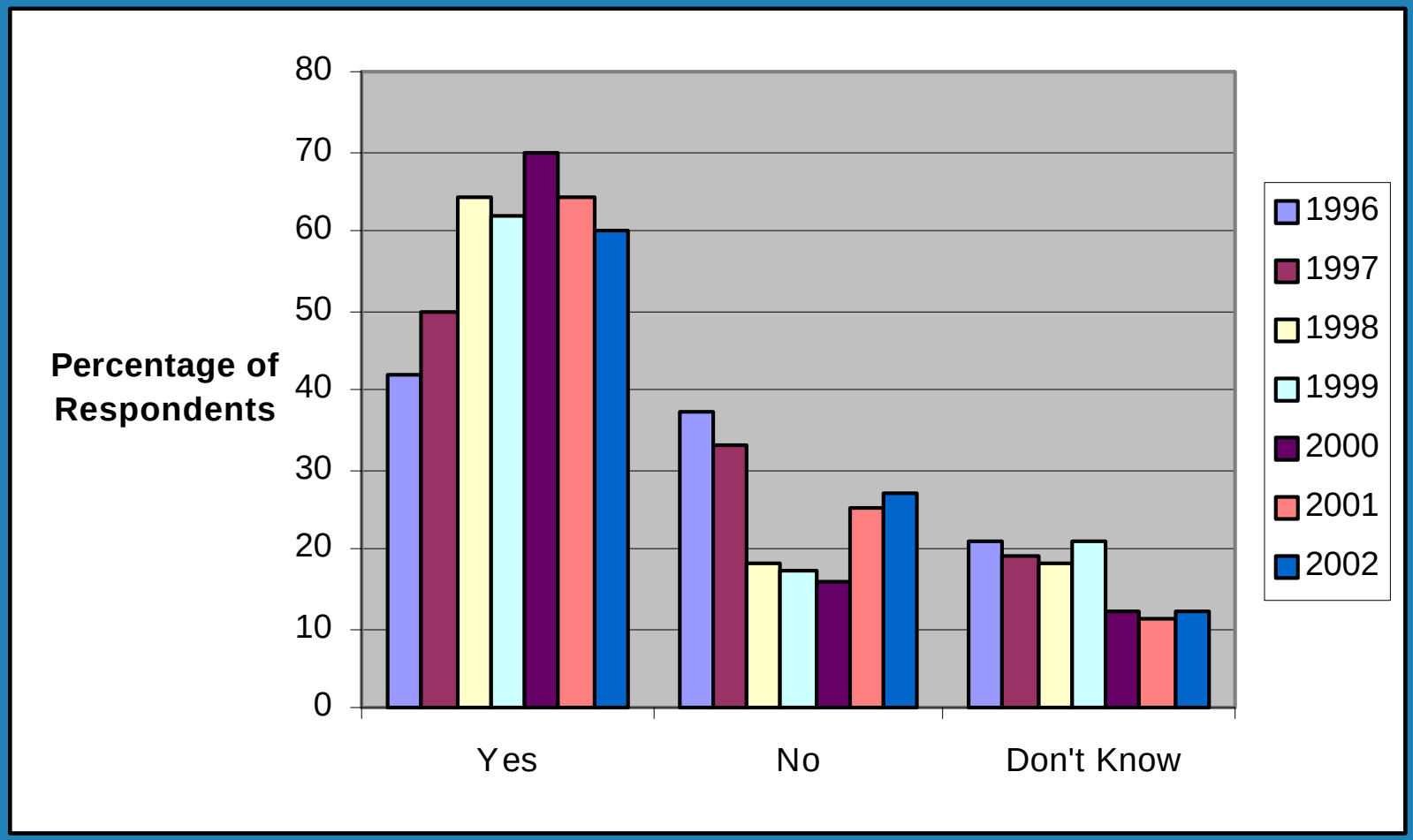
(source: Honeynet Project)

What Was Done in the Thesis

- A detailed literature study and analysis of the current state and problems of intrusion detection.
- Generic architecture planning analysis and two case studies of IDS deployment
- Architecture design based on Snort/ACID + LAMP (Linux, Apache, MySQL, PHP) based IDS + evaluation of this architecture
- Internet hacker activity measurements (about month)

1. Motivation for Intrusion Detection

Unauthorized Use of Computer Systems Within Last 12 Months (source CSI/FBI Study)



1. Motivation for Intrusion Detection

Most Common Attacks (source CSI/FBI)

In year 2002 most common attacks were:

1. Virus (78%)
2. Insider Abuse of Net Access (78%)
3. Laptop theft (55%)
4. Denial of Service and System Penetration (40%)
5. Unauthorized Access by Insiders (38%)

(Yellow color shows the items, which IDSs can decrease)

2. Different Types of IDSs

Application-, Host- and Network IDS

Applications IDS

- Watch application logs
- Watch user actions
- Stop attacks targeted against an application

- **Advantages**
  - Encrypted data can be read

- **Problems**
  - Positioned too high in the attack chain (the attacks reach the application)

2. Different Types of IDSs

Application-, Host- and Network IDS

Host IDS

- Watch kernel operations
- Watch network interface
- Stop illegal system operations
- Drop attack packets at network driver

- **Advantages**
  - Encrypted data can be read
  - Each host contributes to the detection process

- **Problems**
  - Positioned too high in the attack chain (the attacks reach the network driver)

2. Different Types of IDSs

Application-, Host- and Network IDS

Network IDS

- Watch network traffic
- Watch active services and servers
- Report and possibly stop network level attacks

- **Advantages**
  - Attacks can be stopped early enough (before they reach the hosts or applications)
  - Attack information from different subnets can be correlated
- **Problems**
  - Encrypted data cannot be read
  - Annoyances to normal traffic if for some reason normal traffic is dropped

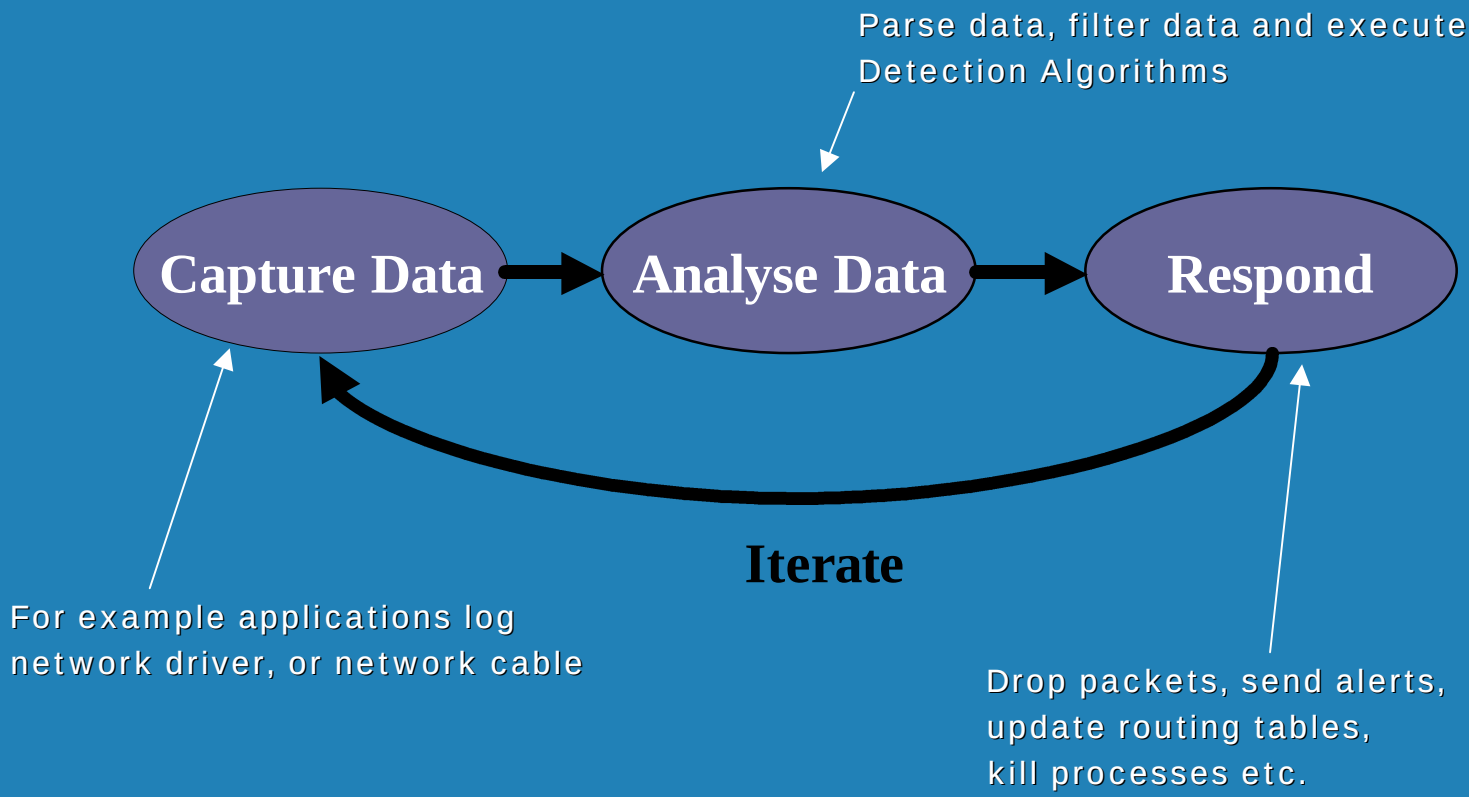
2. Different Types of IDSs

Application-, Host- and Network IDS - Comparison

	Application-based	Host-based	Network-based
Technique	Application monitoring	Host system monitoring	Network segment monitoring
Data Rate	Low	Moderate	High
Placement	Application, userland process	Kernel, system process	Network node
Cost ($)	Low to Moderate	Moderate	High
Maintenance Effort	Moderate	Moderate to High	Low
Encrypted Data	Supported	Supported	Unsupported
Switched Networks	Not problematic	Not problematic	Problematic

3. Simple Process Model for ID

Diagram



3. Simple Process Model for ID

Misuse Detection

– Search attack signatures, which are patterns, byte code or expressions belonging to a specific attack.

– often called signature-based detection

– A signature is created by analysing an attack method

–The patterns are stored inside the IDS

Example Rule:

Alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111

(Content: “|00 01 86 A5|”;msg:”External Mountd access”;)

3. Simple Process Model for ID

Anomaly Detection

"Distinguish abnormal from normal"

Threshold Detection

- X events in Y seconds triggers the alarm

Statistical Measures

- Current traffic profile matches the "normal" profile

Rule-Based Methods

- Jack never logs in at 6 to 8 AM
- If Jack just sent email from Espoo office, he should not send email from New York office at the same time

3. Simple Process Model for ID

Anomaly/Misuse Detection – Comparison

Method	Misuse Detection	Anomaly Detection
Technique	Detect Patterns of Interest	Deviations from Learned Norms
Generalization	Problematic	Yes
Specifity	Yes	No
Sensitivity	High	Moderate
False Alarms	Low	Moderate
Adaptation	No	Yes

3. Simple Process Model for ID

Responses

- Alerts and notifications: email, SMS, pager (important issue: alert path must be bulletproof)
- Increase Surveillance: log more
- Throttling: slow down malicious traffic
- Blocking Access: drop data, update firewall/router
- Nuke the Attacker: Eye for an eye tactics
- Honey Pots and Padded Cells: route the hacker to a fake system and let him play freely

3. Simple Process Model for ID

Detection Rate

Bayesian Detection rate

(no false positives)

$$P(Intrusion \mid Alarm)$$

differs from Detection rate

(true and false positives)

$$P(Alarm \mid Intrusion)$$

- True positive, TP, is a malicious attack that is correctly detected as malicious.
- True negative, TN, is a not an attack and is correctly classified as benign.
- False positive, FP, is not an attack but has been classified as an attack.
- False negative, FN, is an attack that has been incorrectly classified as a benign.

Detection rate is obtained by testing the IDS against set of intrusive scenarios

"...The false alarm rate is the limiting factor for the performance in an IDS".

4. Advanced Technologies

Techniques used in the Intrusion Detection

For Protection

- Stream Reassembly: follow connections and sessions
- Traffic Normalization: see that protocols are followed
- Bayesian Networks: Data mining and decision networks
- Graphical IDSs (for example GrIDS): use graphs to model attacks
- Feature equality heuristics: port stepping, packet gap recognition
- Genetic Programming, Human immune systems
- Tens of research systems exist

For Attacks

- Evasion methods (fragmentation, mutation etc.)
- IDS trashing (DoS tools to like stick/snot to crash IDS capability

6. Measurements

Goals

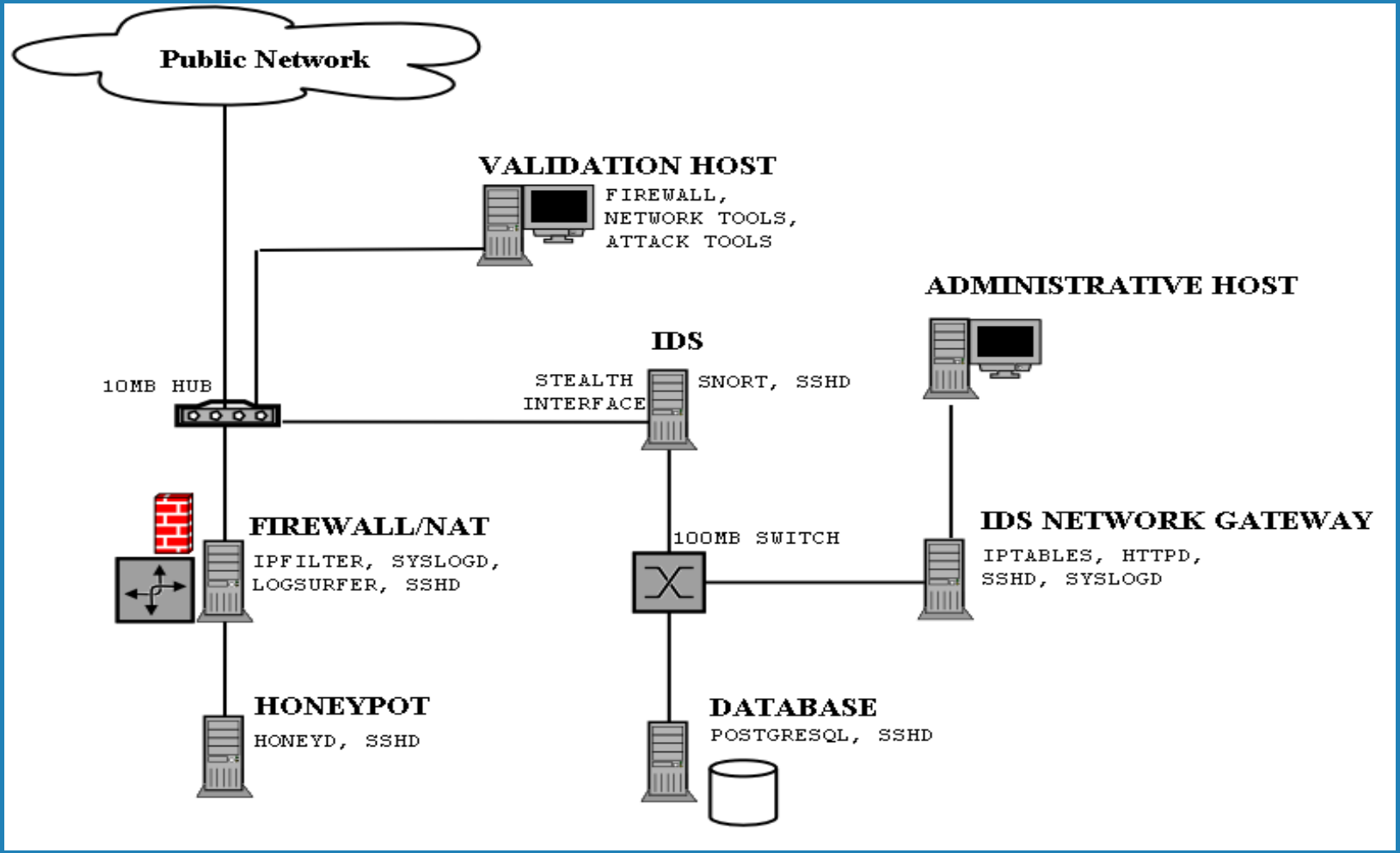
Evaluate the performance of the architecture.

Verify the following hypothesis:

- There is first a probe or a scan and then an attack.
- An attack is a likely consequence of browsing hacker sites and newsgroups.
- There are daily variations in hostile activities.
- There are geographical variations in hostile activities.

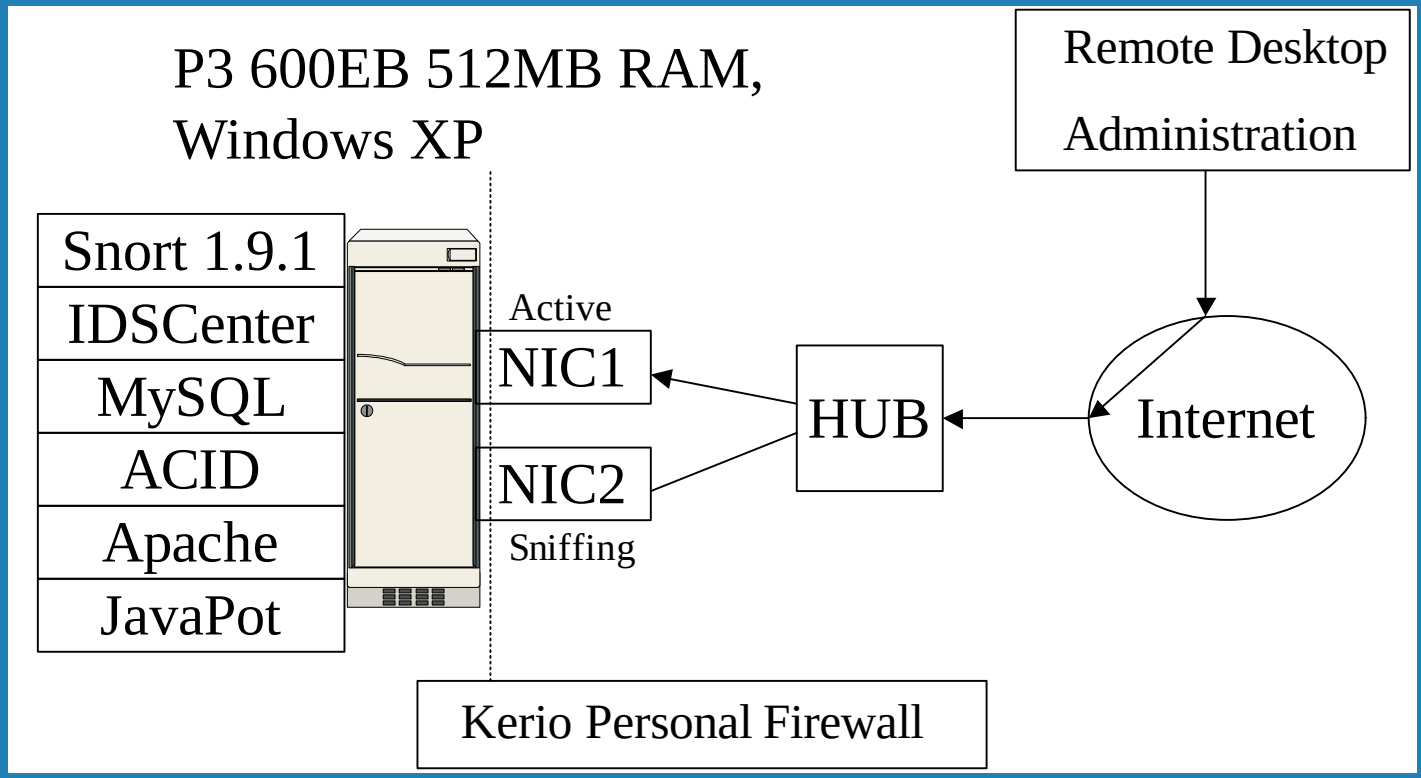
6. Measurements

Architecture (laboratory)



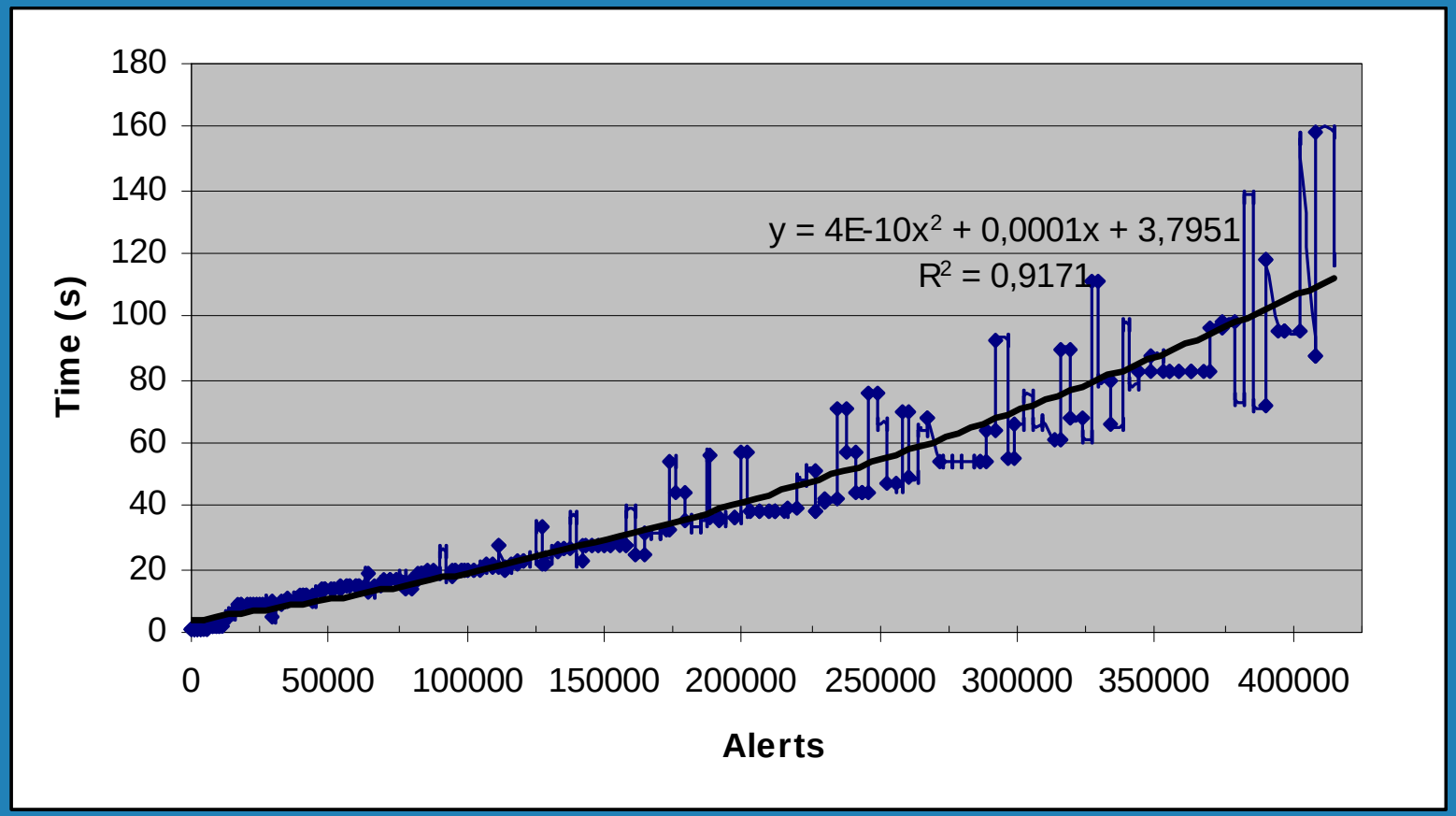
6. Measurements

Architecture (home)



6. Measurements

Architecture Evaluation: Alert Throughput (lab)



Number of Alerts vs. ACID Main Page Load Time During a DoS Attack

6. Measurements

Compilation of Results

	HOME: Period 1	HOME: Period 2	LABORATORY
Measurement period	40	7	28
Total number of alerts	8403	1790	5965
Unique alerts	174	46	199
Alerts per Day	210	255	213
Port scans	150	18	37
Port scans per Day	3,8	2,6	1,3
Unique source addresses	670	163	375
Proper DNS entry (%)	74	not checked	67
CAIDA coordinate mapping (%)	21	not checked	9,6
Source ports (TCP/UDP)	2051 / 42	561 / 12	2256 / 14
Destination ports (TCP/UDP)	904 / 25	270 / 4	1241 / 2
Traffic Profile (TCP/ICMP/UDP)	92% / 7% / 1%	98 % / 1% / 1%	92 % / 8% / << 1%

1. Microsoft Internet Information Server related attacks (97,2% home, 46,79% lab)
2. Brute-force or random FTP-login attempts (0,19% home, 38,19 % lab)
3. POP3 bad logins and USER overflow attempts (0% home, 11,09% lab)
4. Bad Port 0 UDP or TCP traffic (0,66% home, 1,53% lab)
5. MS-SQL Worm Propagation attempt (0,98% home, 0,74% lab)

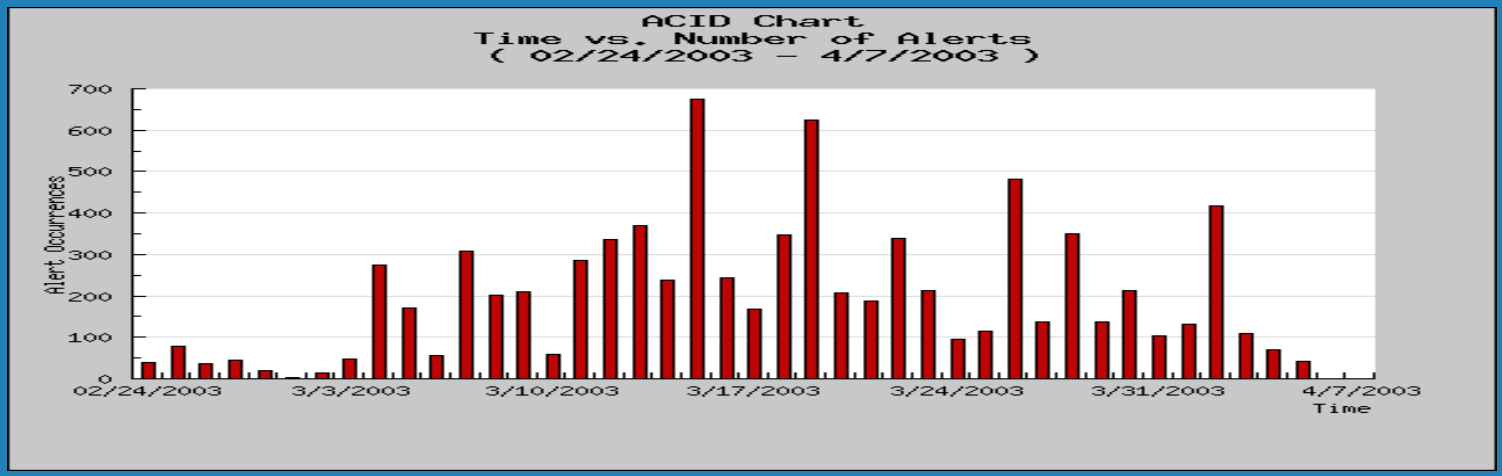
6. Measurements

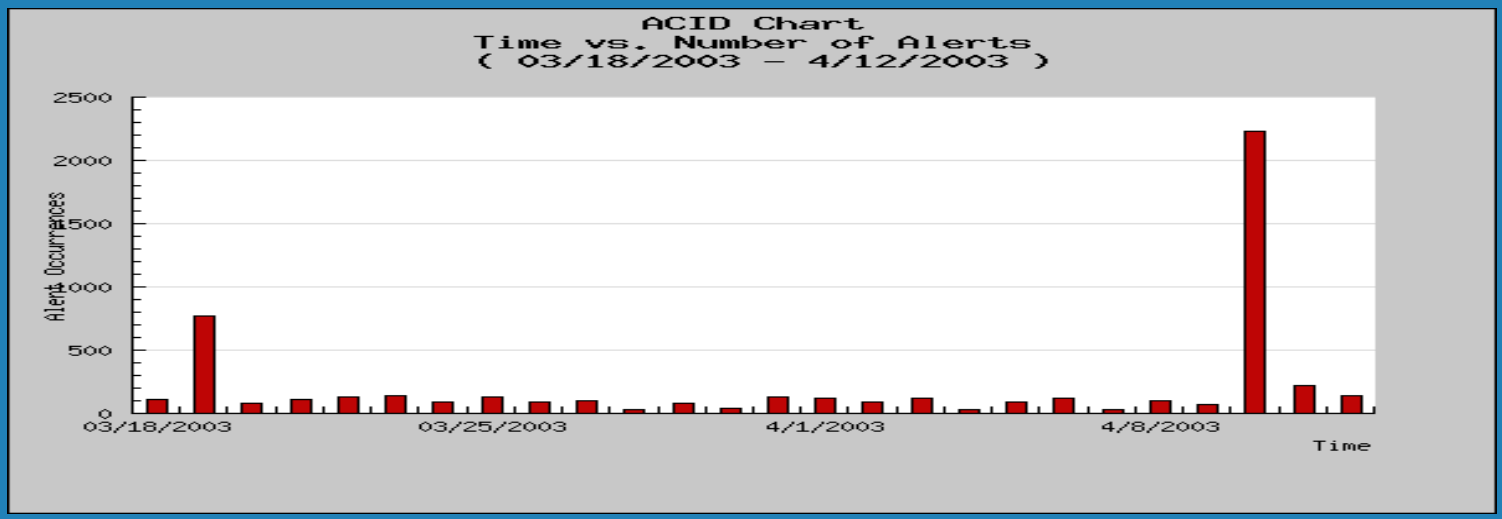
Is there any reconnaissance before an attack?

- No reconnaissance events before an attack could be identified
- There were no reconnaissance events and attack events from the same IP-address.
- Time recurrence could not be used as a reconnaissance to attack mapping variable, as there is very much noise traffic – mostly generated by Microsoft Internet Information Server related worm attacks.
- Attacks are mostly worm related, automated or executed randomly.

6. Measurements

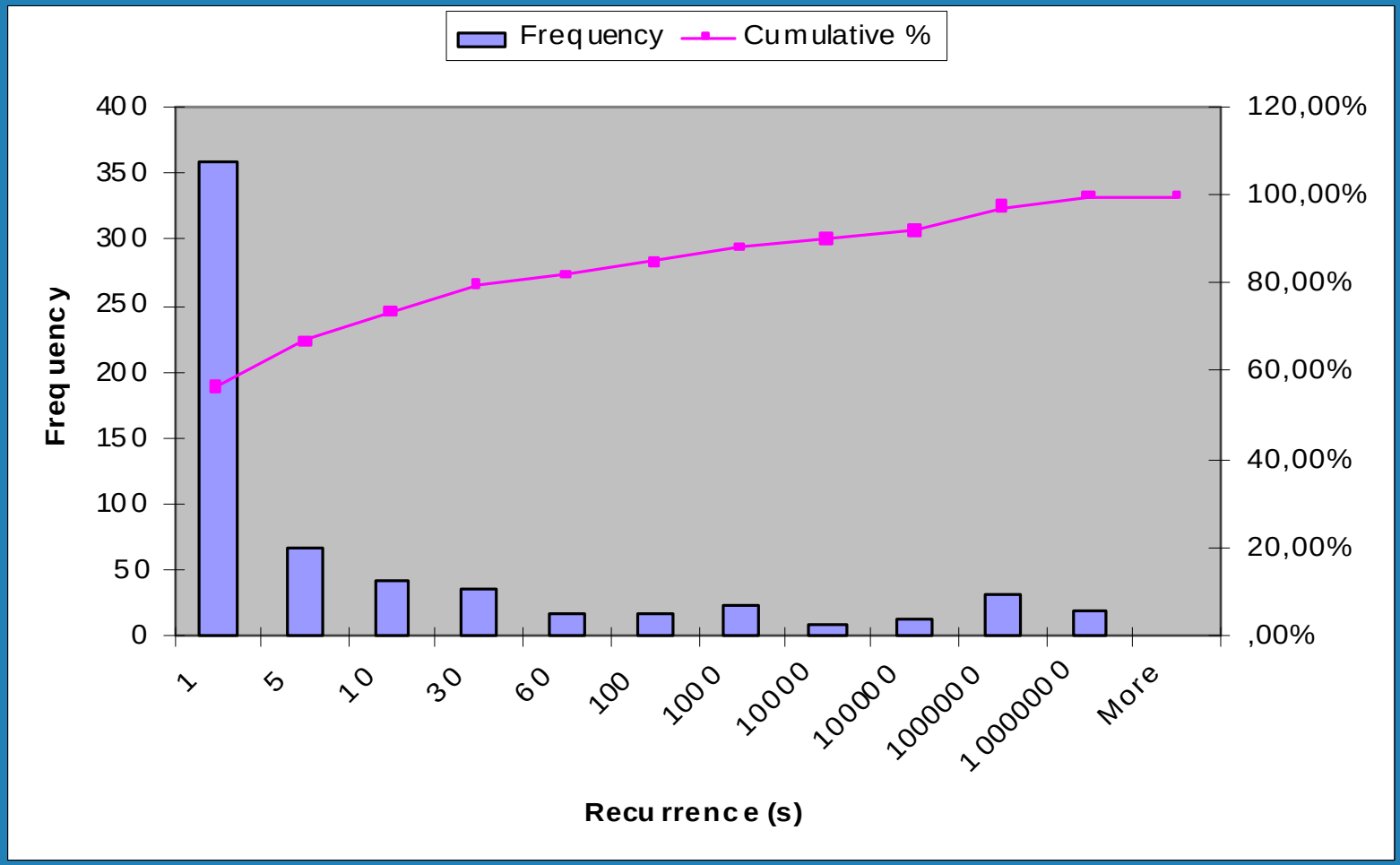
Is there any reconnaissance before an attack?





6. Measurements

Is there any reconnaissance before an attack?



6. Measurements

Does hacker site browsing result in increased attack frequency?

- During the seven-day “hacking period”, notorious hacker and terrorist group sites were visited, pinged and scanned.

- The increase of alerts per day was only 21% and it could result from short-term changes in the attack activities.

6. Measurements

Do hostile activities have any daily or hourly variations?

- Thursday seemed to be most active – weekend was not very active

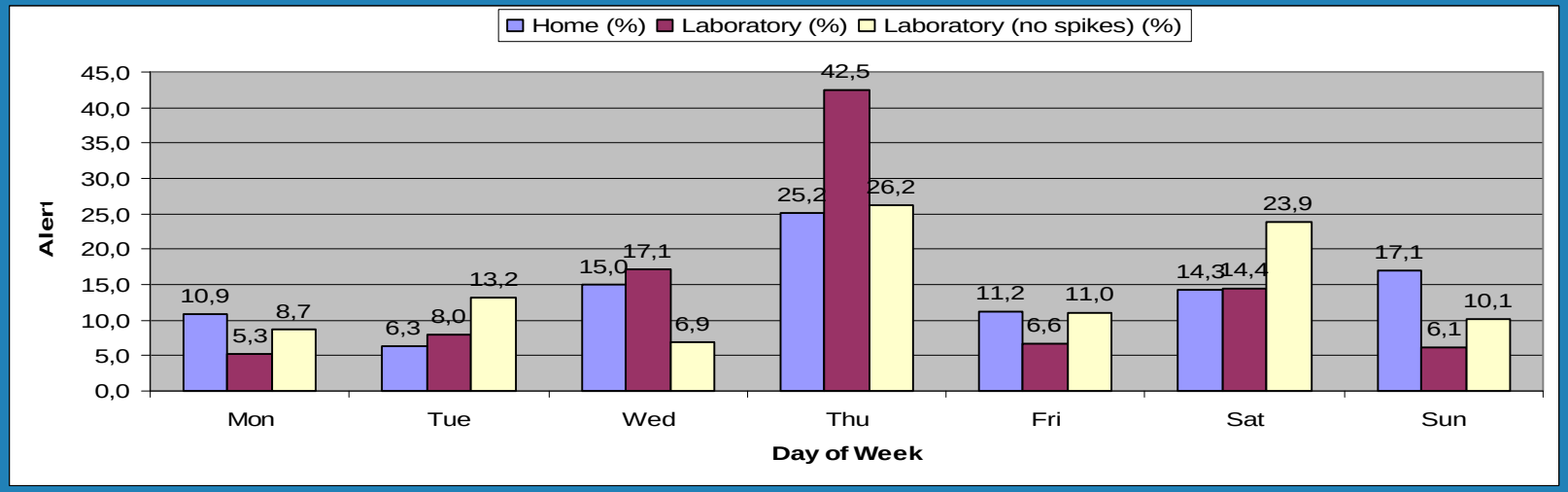
- Afternoon and evening hours seem to be quite active
- Morning hours are the most quiet

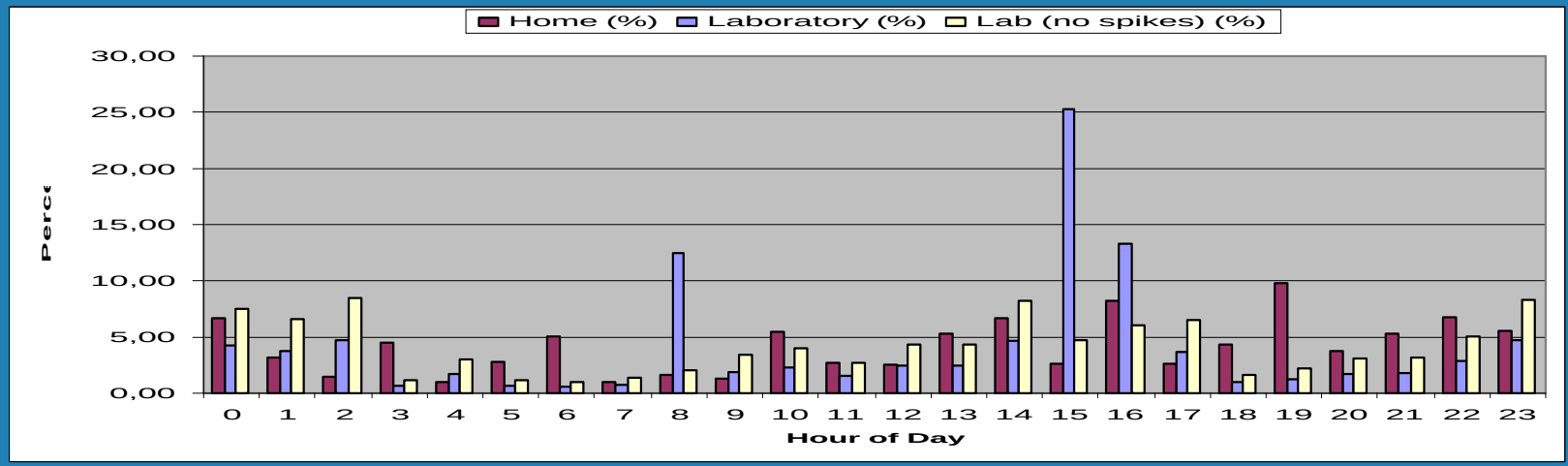
- There is a high variance in daily and hourly activities

→ This prohibits the use of variations in for example human resources planning (for example how many system administrators guard the network in the night)

6. Measurements

Do hostile activities have any daily or hourly variations?





6. Measurements

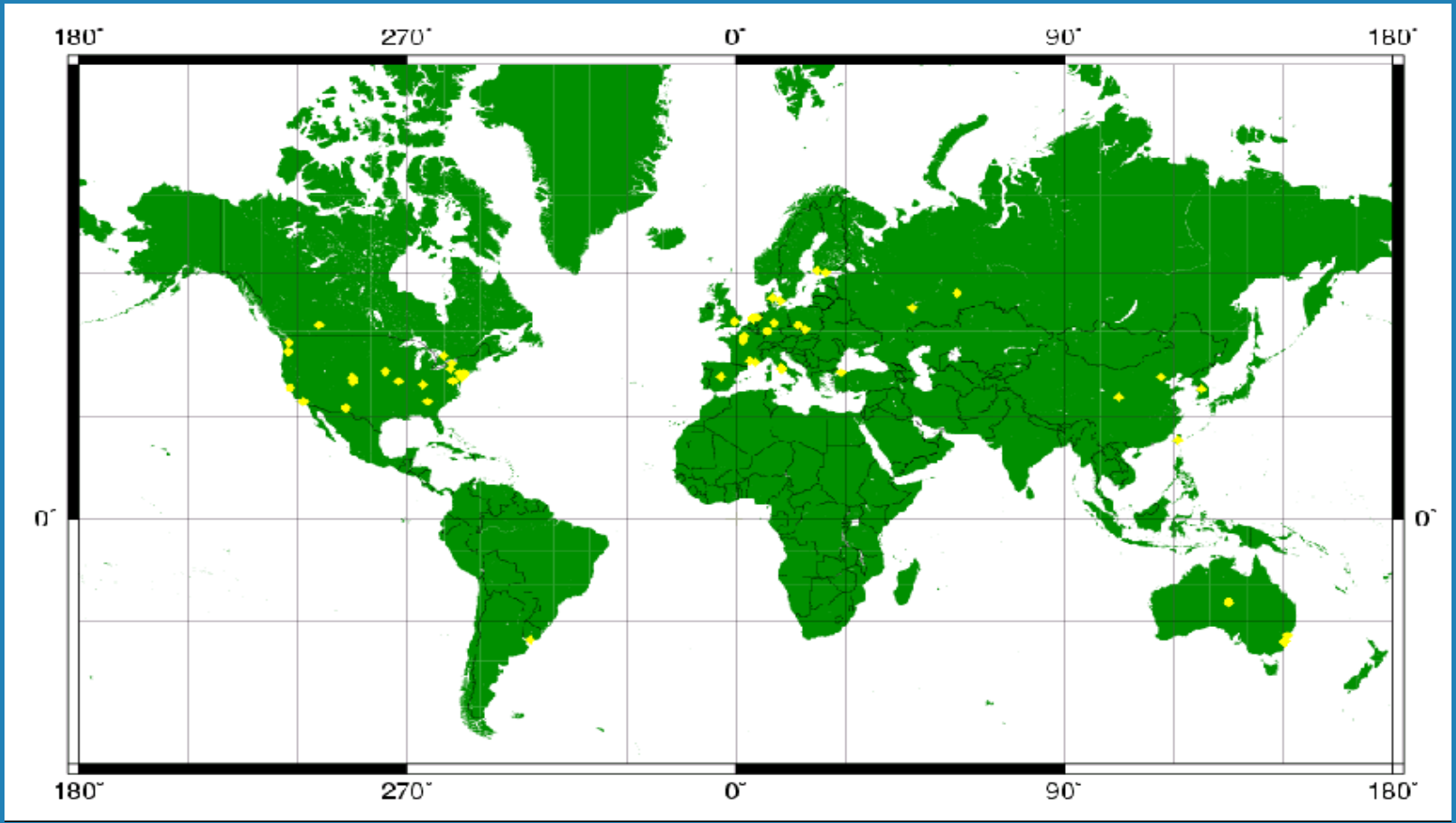
Do attack activities vary by geographical location?

- Most attacks come from developed countries, which have lots of computers and Internet connections. Unlike expected, the traditional evil-axis countries like Romania and Israel were not very active.

- About 70% of addresses had a proper DNS entry and they could be resolved to some domain. Table 24 shows the most active domains. Only 20% (home) and 10% (laboratory) of addresses could be mapped to geographical coordinates using CAIDA's service and a custom built mapping tool.

6. Measurements

Do attack activities vary by geographical location?



Suggestions and Improvements

- Do not run Microsoft IIS web-server

- A random home computer with Internet connection received over 3000 attacks in one month → Use Firewalls at your home!!

- Network IDS cannot catch all attacks like browser hijacking. For this reason, a host IDS is required too (personal firewalls bundled with real-time virus-scanners are almost like host IDSs already). Is somebody reinventing the wheel?

- Some paranoia is just for good:

"I pull the network cable every time I leave the office"

Okay

Completed

Thank you!

Any Questions?