

2nd MAP-Tele Workshop
2nd December 2009, Porto, Portugal

Methodologies for Intrusion Detection in Communication Networks

Eduardo Rocha
Paulo Salvador
António Nogueira

INSTITUIÇÕES ASSOCIADAS:



INSTITUTO
SUPERIOR
TÉCNICO



Faculdade de Ciências
e Tecnologia da
Universidade de Coimbra

universidade
de aveiro



Inovação

SIEMENS
Communications



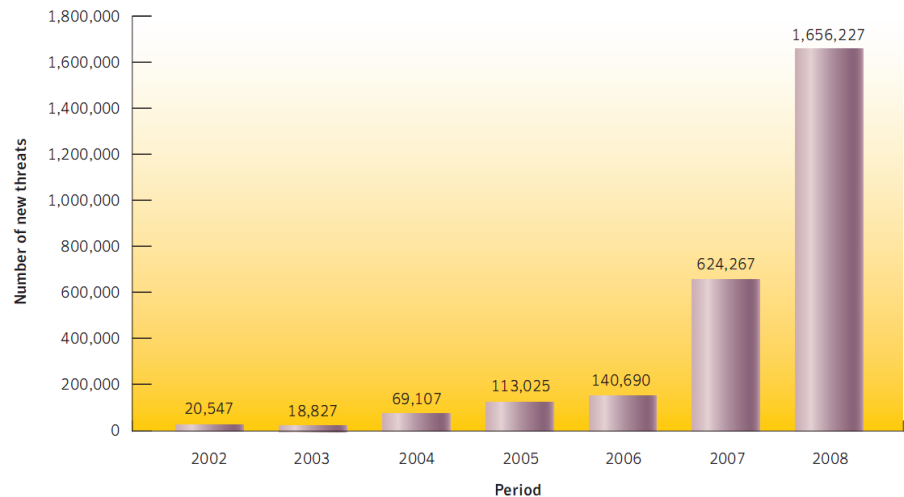
instituto de
telecomunicações

creating and sharing knowledge for telecommunications

© 2005, it - instituto de telecomunicações. Todos os direitos reservados.

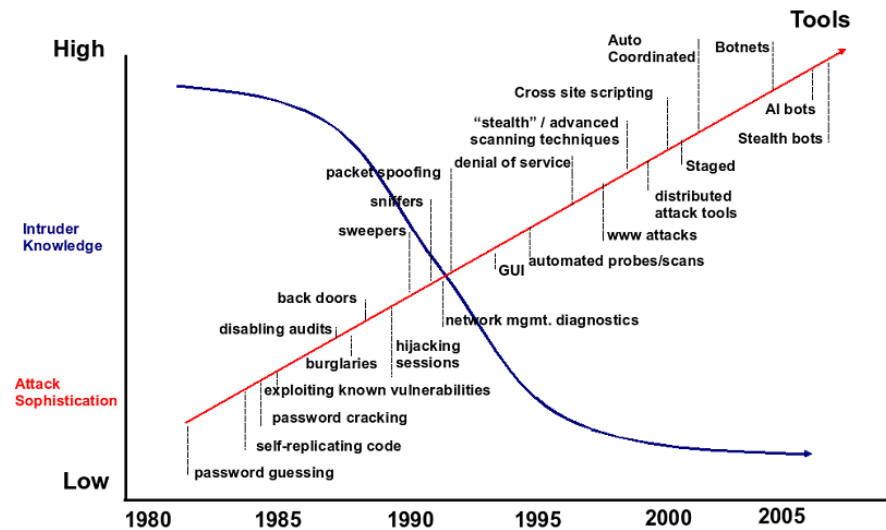
Introduction

- Immense increase in the use of Internet:
 - Counts with thousands of millions of sites;
 - The most powerful communication medium;
 - Used for an extensive array of activities:
 - Web Browsing;
 - Video Streaming;
 - Voice Calls;
 - And many many more...
 - Several means and targets for attackers:
 - Number of attacks has increased.



Introduction

- Continuous publication of exploits and vulnerabilities;
- Availability of tools for launching attacks:
 - Reduces the level of expertise;
- Conventional security approaches:
 - Create a “shield” around the host and/or network;
 - However:
 - Vulnerabilities associated;
 - Not sufficient for a complete protection.



Botnets

- *Botnets* are used for various illegitimate activities
 - Sources of massive exploit activity;
 - Recruit new vulnerable systems to expand their reach;
 - Due to their volume, capabilities and robustness, *botnets* pose a significant and growing threat;
 - Detection is hard:
 - Traditional network security systems are unable to do it.

New iPhone worm steals
builds botnet

New Spamming Botnet On
The Rise
steals online banking codes,

Report: botnets sent over 80% of all June spam

Botnet Command and Control Server Hosted on
Google App Engine
Cloud-based services increasingly appeal to bot herders

INSTITUIÇÕES ASSOCIADAS:



2nd MAP-Tele Workshop

2nd December 2009, Porto, Portugal



instituto de
telecomunicações

Botnets

- *Botnet* detection is very difficult using traditional methods:
 - *Antivirus* and *antispyware* can only detect and remove known viruses or Trojan horses:
 - Cannot prevent new and stealth threats;
 - Firewalls can be an effective tool to avoid PC infection:
 - Require an average know-how level and special attention by the user;
 - Network-based Intrusion Detection Systems:
 - Most of the IDSs are only able to detect known attacks;
 - *Botnet* threats are distributed and hard to detect;
 - Botnets are evolving and are very flexible:
 - The protocols used for Command and Control (C&C) evolved from IRC to others;
 - The structure evolved from centralized to distributed.

Intrusion Detection

- Active field for more than 20 years;
- Based upon the belief that an intruder's behaviour is different from a legitimate user's behaviour;
- IDSs are gaining more acceptance as they constitute a valuable resource;
- IDSs can be deployed with other security mechanisms such as access control and authentication;
- Methodologies become inappropriate due to the evolution and appearance of new Internet services.

Identified Flaws

- Most of the tools are software components which analyse data in an isolated manner:
 - Not able to detect stealth and coordinated attacks;
- These systems may become overwhelmed by the amount of information;
- Not able to perform intrusion detection in encrypted traffic scenarios;
- Do not correlate information from network's elements.

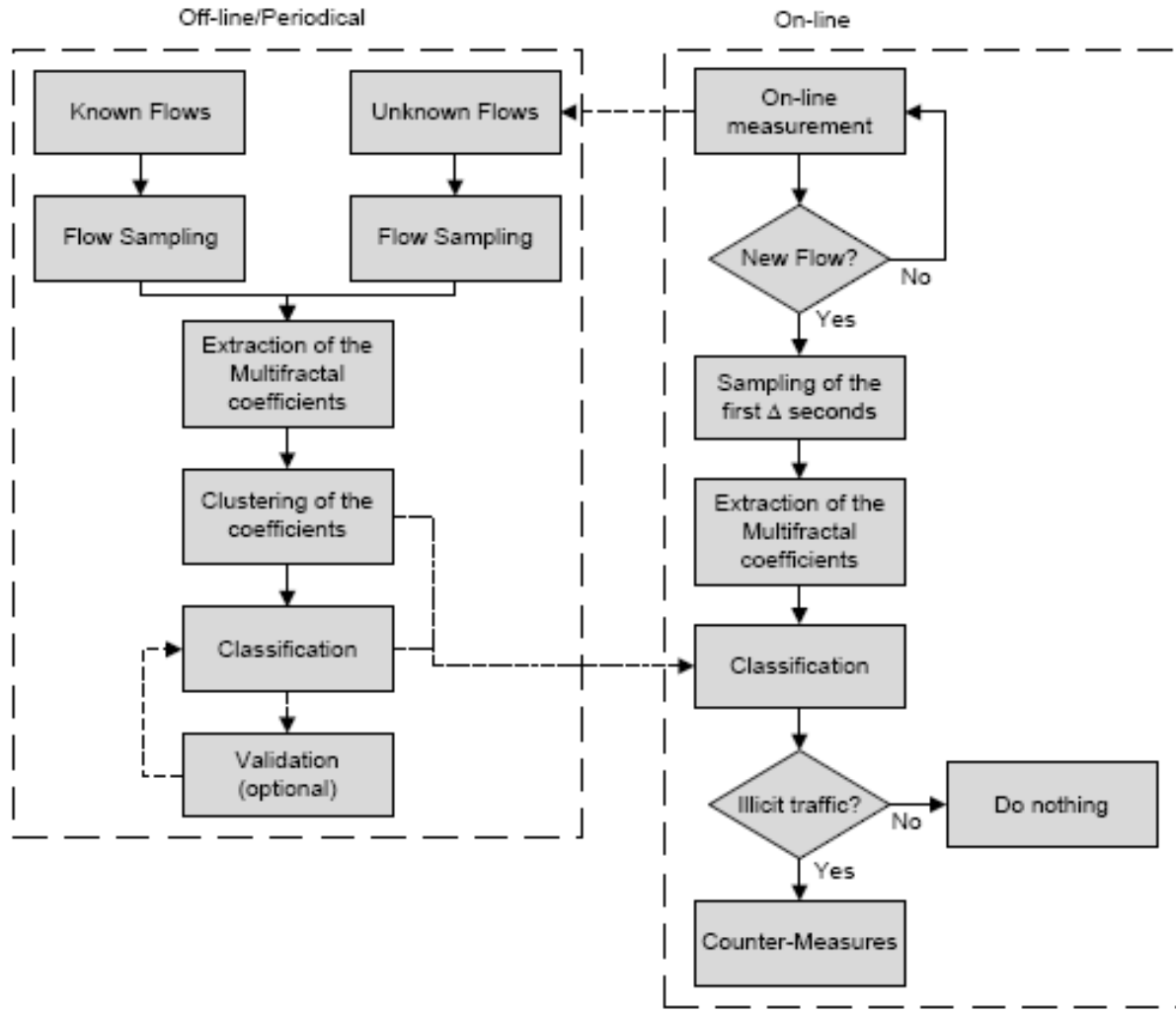
Workplan Objectives

- The implementation of novel methodologies which can act in encrypted and non-encrypted traffic scenarios:
 - analysis and correlation of all available and relevant network data:
 - traffic statistics;
 - networks equipments' and servers' logs;
- The study of an architecture which combines isolated data analysis with distributed correlation of the several network data;
- Provide response actions to intrusions.

Developed Work

- Development of a novel methodology for traffic classification and identification of Internet-based attacks:
 - Relies on the multiscale analysis of sampled TCP/IP traffic flows;
 - Estimation, analysis and pattern recognition of the multiscaling coefficients;
 - Immune to confidentiality restrictions;
 - Analyses are based on traffic raw statistics.

Classification Methodology



Test Scenarios – Legitimate Traffic

- Selected applications:
 - Web-browsing;
 - Streaming;
 - BitTorrent.
- Passively collected on the network of the University of Aveiro;
- Composed of all TCP and UDP traffic in the upload and download directions;
- First 68 bytes captured:
 - Full packet's headers and some payload bytes.

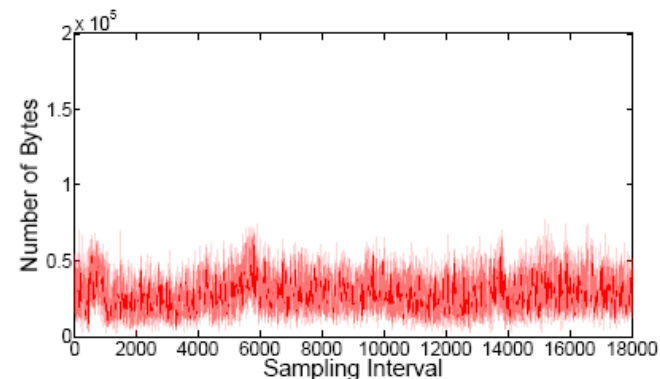


Fig. 1. Number of bytes for a Torrent flow.

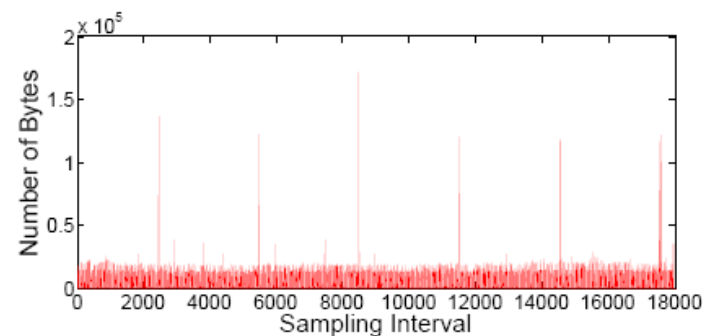


Fig. 2. Number of bytes for a Streaming flow.

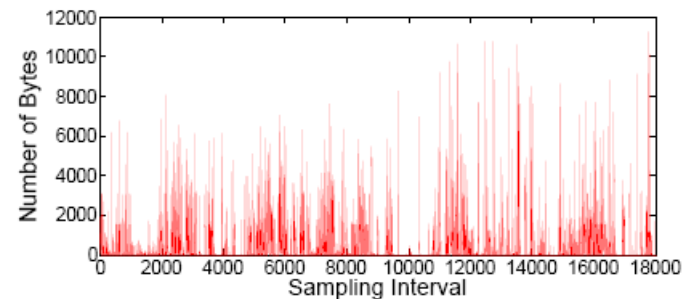


Fig. 3. Number of bytes for an HTTP flow.

Test Scenarios – Legitimate Traffic: Results

- Very accurate identification results;
- Proved that multiscale analysis is an accurate technique for traffic classification.

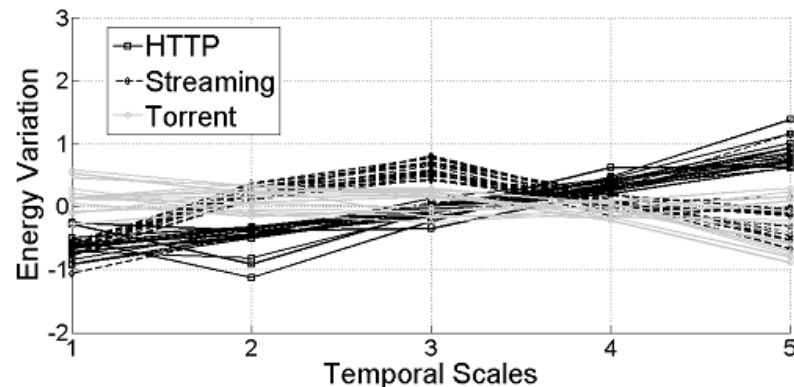


TABLE I
PERCENTAGE OF FLOWS CORRECTLY CLASSIFIED

Moment	HTTP	Streaming	Torrent
1	100%	93,3%	93,3%
2	40%	53,3%	73,3%
3	40%	60%	73,3%
4	40%	60%	73,3%
5	53,3%	60%	60%

Test Scenarios – Legitimate and Illegitimate Traffic

- Selected applications:
 - Port scans;
 - Snapshots.
- Experimentally generated:
 - Nmap flows:
 - Discrete scan profile;
 - Sequential port scan with one second interval;
 - Snapshot flows:
 - Capture of a small fixed size image;
 - Every time the user performs a click.

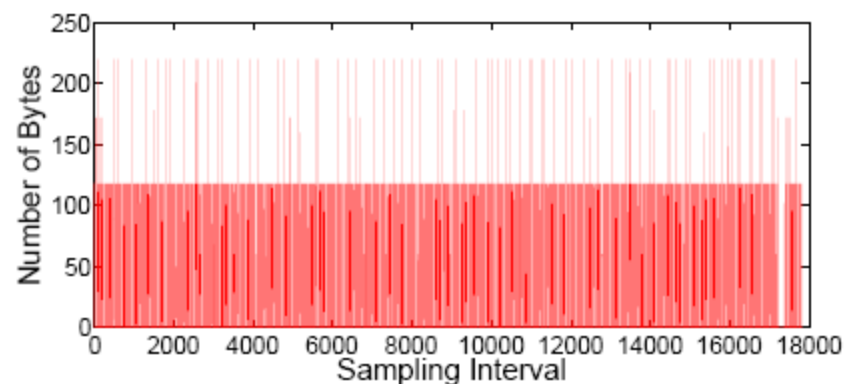


Fig. 5. Number of bytes for a NMap flow.

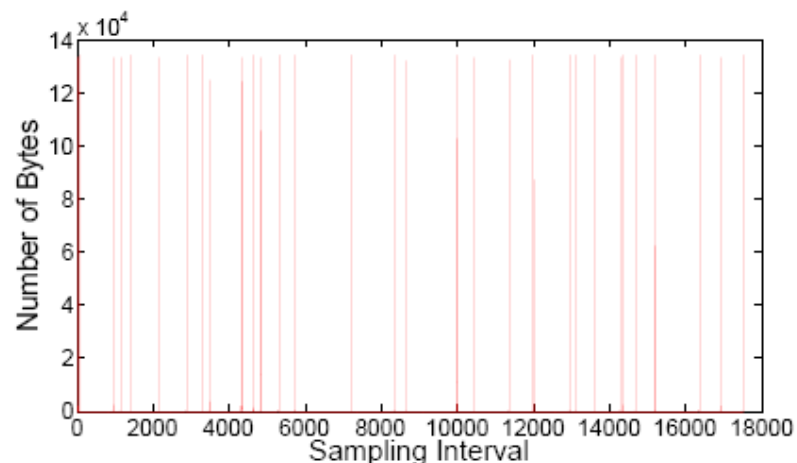
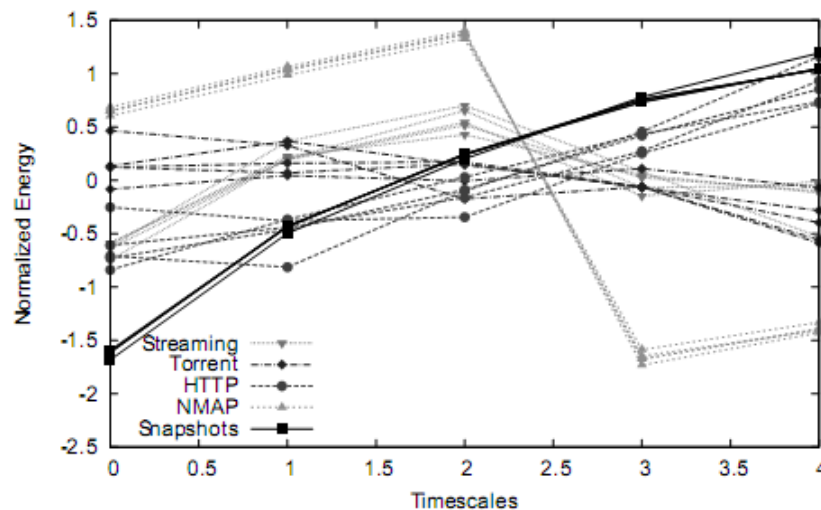


Fig. 6. Number of bytes for a Snapshot flow.

Test Scenarios – Legitimate and Illegitimate Traffic: Results

- Very identification results;
- All illicit traces were correctly identified:
 - Important for identification of *botnets*.



Flows	Classified as				
	<i>NMAP</i>	<i>Snapshot</i>	<i>HTTP</i>	<i>Streaming</i>	<i>Torrent</i>
NMAP	100%	0%	0%	0%	0%
Snapshot	0%	100%	0%	0%	0%
HTTP	0%	0%	100%	0%	0%
Streaming	0%	0%	6.67%	93.3%	0%
Torrent	0%	0%	6.67%	0%	93.3%

Future Work

- Three main aspects:
 - The data to analyze:
 - network equipments' and servers' logs and other traffic statistics;
 - The study of the more appropriated statistics that can be extracted from this data for the identification of new and stealth threats;
 - The study of more adequate methodologies for the correlation and classification of the statistics:
 - Pattern recognition techniques.

Final Remarks

- Work developed in this year:
 - Development and study of a methodology for the identification of Internet attacks;
 - Able to act in encrypted and non-encrypted traffic scenarios;
- Future Work:
 - Continuation of the analysis of traffic's and logs' informations;
 - Continuation of the analysis of the statistics extracted from the mentioned data;
 - Analysis of techniques for the correlation of the mentioned data;
 - Still many aspect left open:
 - Which statistics and logs to analyze?
 - How should these data be correlated?
 - Data reduction.
- Our workplan addresses important, and still open, aspects of Intrusion Detection research.

- 
- Thank you!
 - Questions?

INSTITUIÇÕES ASSOCIADAS:



2nd MAP-Tele Workshop

2nd December 2009, Porto, Portugal



instituto de
telecomunicações