Collection and Analysis of Attack Data based on Honeypots deployed on the Internet

E. Alata[1], M. Dacier[2], Y. Deswarte[1], M. Kaâniche[1], K.Kortchinsky[3],
V.Nicomette[1], V.H. Pham[2], F. Pouget[2]

LAAS-CNRS[1], Eurecom[2], CERT-RENATER[3]

Mohamed.Kaaniche@laas.fr

Partially funded by the French research action
ACI "Sécurité & Informatique" (http://acisi.loria.fr)

First Workshop on Quality of Protection, Milano, Italy, September 15, 2005

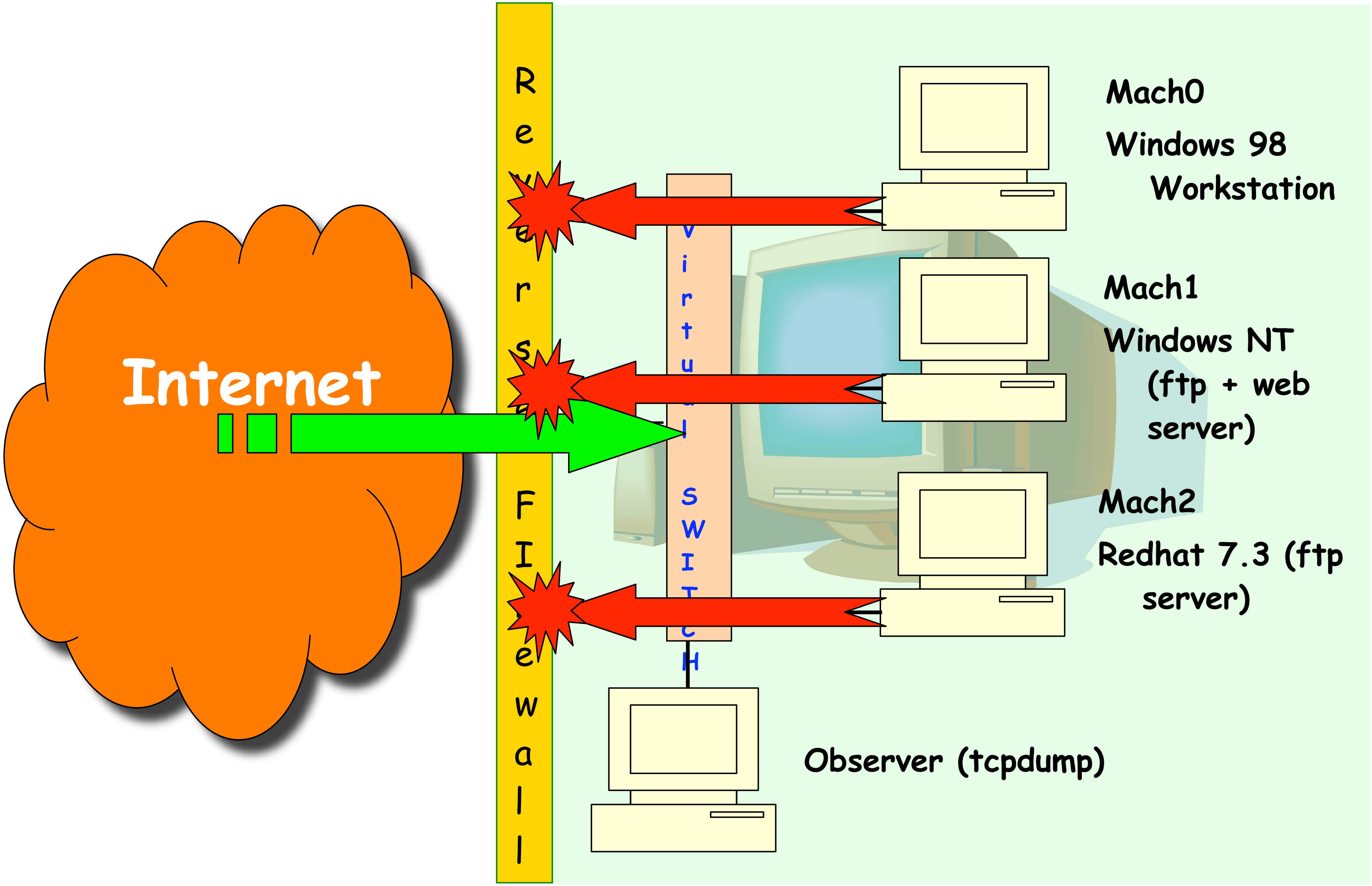
Objectives

- Build and deploy on the Internet a distributed platform of identically configured low-interaction honeypots in a large number of diverse locations

- Carry out various analyses based on the collected data to better understand threats and build models to characterize attack processes

- Analyze and model the behavior of malicious attackers once they manage to get access and compromise a target
  - High-interaction honeypots

Deployed platform



30 platforms, 20 countries, 5 continents

in Europe …

Europe
Serbia and Montenegro have asserted the formation of a joint independent state, but this entity has not been formally recognized as a state by the United States.
Macedonia has proclaimed independent statehood but has not been formally recognized as a state by the United States.
Greenland (DENMARK)
Jan Mayen (NORWAY)
Greenland Sea
Norwegian Sea
Barents Sea
White Sea
Arctic Circle
ICELAND
Reykjavík
Tórshavn
Faroe Islands (DENMARK)
Shetland Islands
Orkney Islands
Hebrides
Rockall (U.K.)
North Atlantic Ocean
North Sea
NORWAY
SWEDEN
FINLAND
DENMARK
RUSSIA
ESTONIA
LATVIA
LITHUANIA
BELARUS
POLAND
UNITED KINGDOM
IRELAND
NETHERLANDS
BELGIUM
LUX.
GERMANY
FRANCE
SWITZ.
LIECH.
AUSTRIA
CZECH REPUBLIC
SLOVAKIA
HUNGARY
ROMANIA
MOLDOVA
UKRAINE
SLOVENIA
CROATIA
BOSNIA AND HERZEGOVINA
Serbia
Montenegro
ALB.
Macedonia
BULGARIA
GREECE
TURKEY
ITALY
SAN MARINO
VATICAN CITY
MONACO
ANDORRA
SPAIN
PORTUGAL
MOROCCO
ALGERIA
TUNISIA
MALTA
Hammerfest
Narvik
Kiruna
Murmansk
Arkhangel'sk
Umeå
Gulf of Bothnia
Trondheim
Tampere
Helsinki
Gulf of Finland
St. Petersburg
Lake Onega
Lake Ladoga
Bergen
Oslo
Gävle
Stockholm
Åland Islands
Tallinn
Skagerrak
Göteborg
Gotland
Riga
Copenhagen
Öland
Bornholm
Vilnius
Minsk
Smolensk
Gdańsk
Rostock
Hamburg
Berlin
Hannover
Poznań
Warsaw
Brest
Kiev
Leipzig
Wrocław
Kraków
L'viv
Bonn
Amsterdam
Belfast
Dublin
Irish Sea
Isle of Man (U.K.)
Liverpool
Newcastle
Cardiff
London
English Channel
Guernsey (U.K.)
Jersey (U.K.)
Le Havre
Paris
Luxembourg
Strasbourg
Stuttgart
Munich
Nantes
Bay of Biscay
Bern
Geneva
Lyon
Vienna
Bratislava
Budapest
Graz
Cluj-Napoca
Chişinău
Odesa
Bordeaux
Milan
Venice
Turin
Genoa
Ljubljana
Zagreb
Pécs
Belgrade
Sarajevo
Bucharest
Constanța
Black Sea
Varna
Florence
Marseille
Adriatic Sea
Podgorica
Sofia
Tirane
Skopje
İstanbul
Bilbao
Porto
Madrid
Barcelona
Corsica
Rome
Thessaloniki
Tagus
Lisbon
Valencia
Sardinia
Naples
Tyrrhenian Sea
Ioánnina
Corfu
Aegean Sea
Balearic Islands
Sevilla
Málaga
Mediterranean Sea
Palermo
Sicily
Ionian Sea
Athens
Peloponnisos
Rhodes
Crete
Strait of Gibraltar
Gibraltar (U.K.)
Ceuta (SPAIN)
Melilla (SPAIN)
Algiers
Tunis
Valletta
Rabat
Danube
Dnieper
Scale 1:19,500,000
Lambert Conformal Conic Projection, standard parallels 40°N 56°N
0 300 Kilometers
0 300 Nautical Miles
802176 (R01083) 9-93

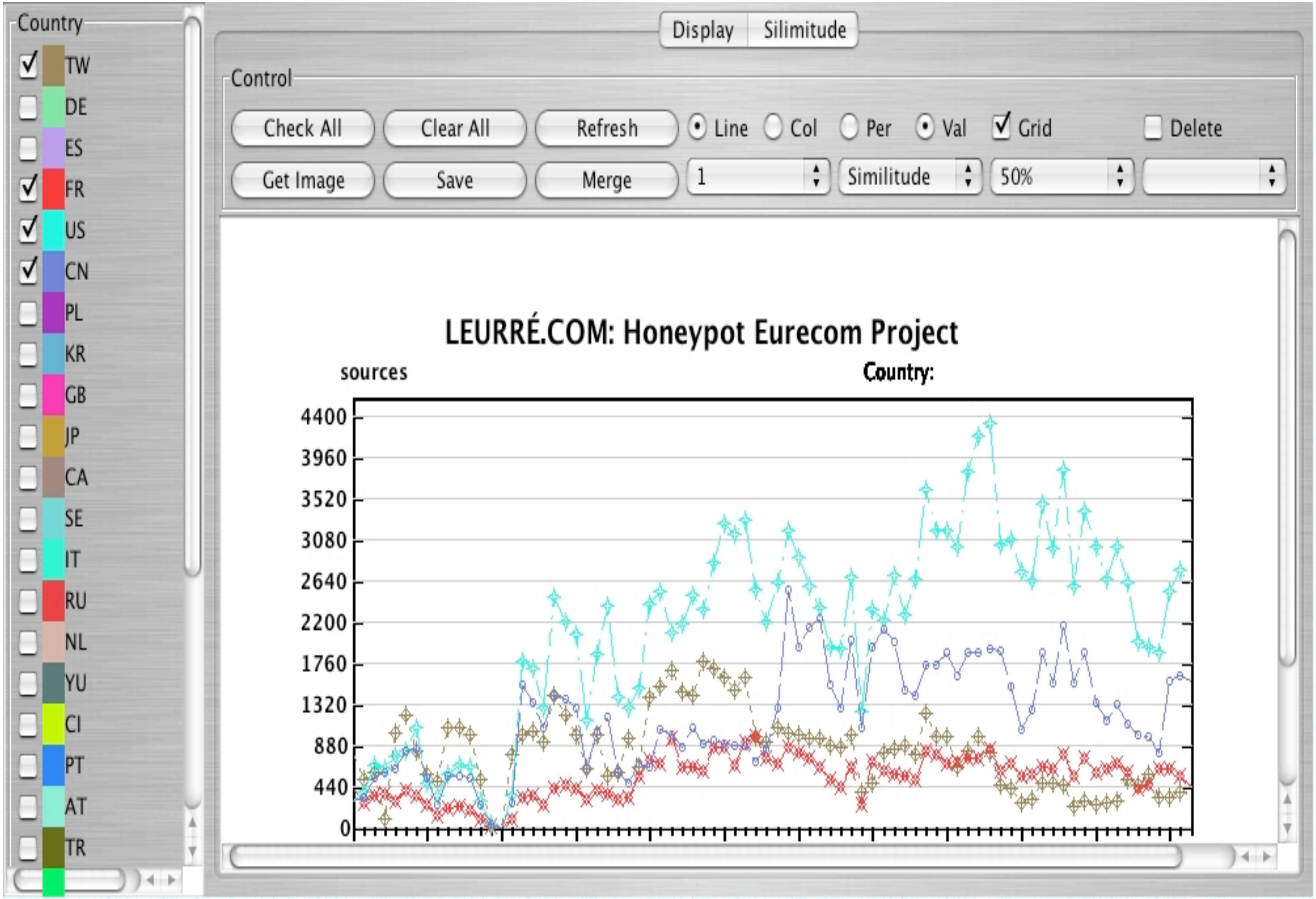
Win-Win Partnership

- Interested partners provide…
  - One old PC (pentium II, 128M RAM, 233 MHz…),
  - 4 routable IP addresses,

- EURECOM offers …
  - Installation CD Rom
  - Remote collection of logs + integrity checks
  - Access to the whole SQL database

Data analysis

- Data collection since 2003
  - *Vmware* and *honeyd* platforms
- Information extracted from the logs + additional tools
  - IP address of the attacking machine
  - Time of the attack and duration
  - Targeted virtual machines and ports
  - Geographic location of the attacking machine (*Maxmind*)
  - Os of the attacking machine (*p0f, ettercap, disco*)
- Deep analyses are necessary to extract useful trends and identify hidden phenomena from the data
  - Clustering techniques, Time series analysis, etc.
- Interesting results obtained so far
  - Publications available at: www.eurecom/~pouget/papers.htm



Country

☑ TW
□ DE
□ ES
☑ FR
☑ US
☑ CN
□ PL
□ KR
□ GB
□ JP
□ CA
□ SE
□ IT
□ RU
□ NL
□ YU
□ CI
□ PT
□ AT
□ TR

Control

● Line ○ Col ○ Per ● Val ☑ Grid □ Delete

1 | Similitude | 50%

Modeling and quantitative evaluation

- Identify probability distributions that best characterize attack occurrence and attack propagation processes

- Model the time relationships between attacks coming from different sources (or to different destinations)

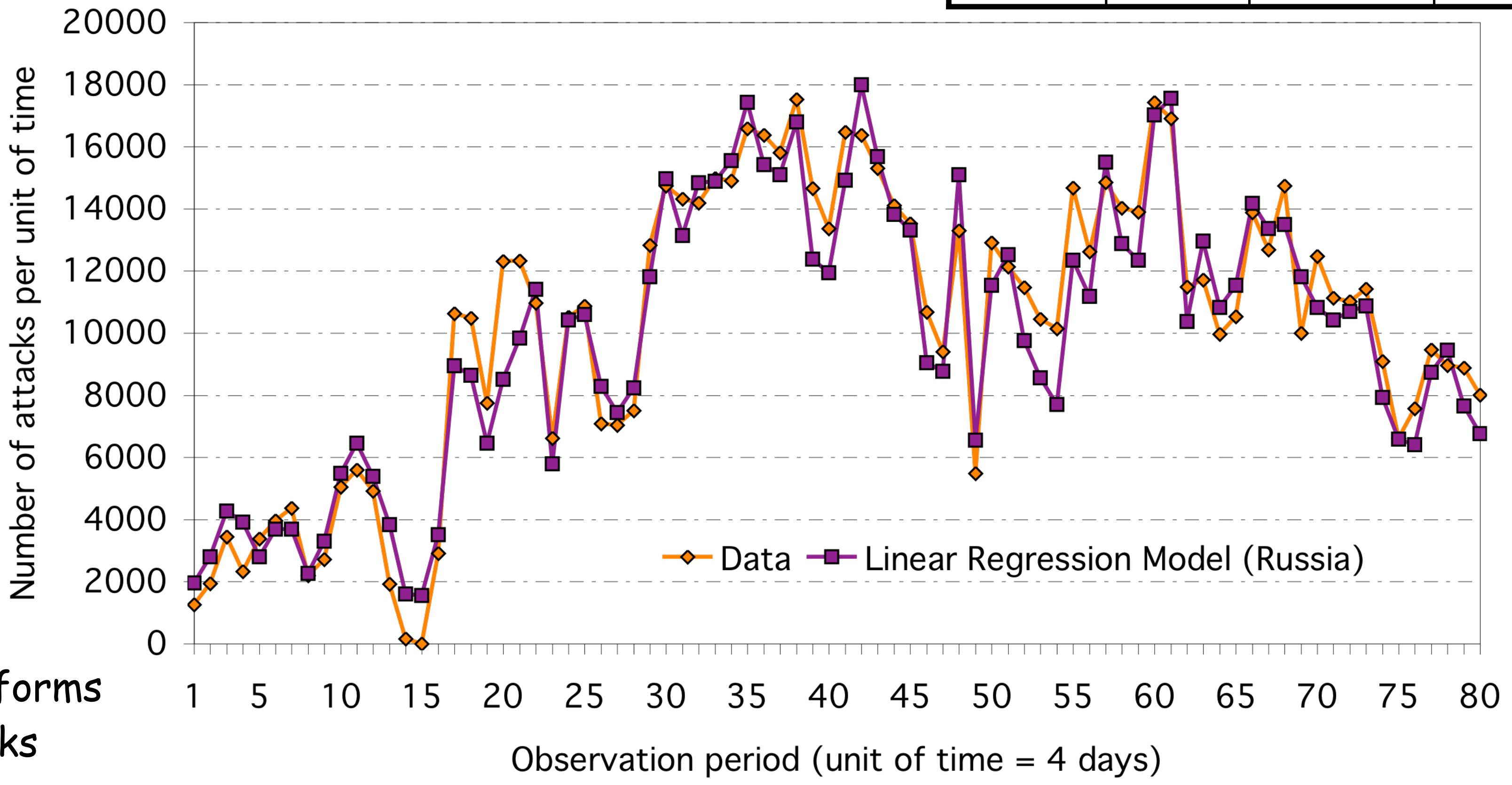
- Predict occurrence of new attacks on a given platform based on past observations on this platform and other platforms

- Estimate impact of attacks on security of target systems
  - High-interaction honeypots to analyze attackers behavior once they compromise and get access to a target

The number of attacks per unit of time, considering a single platform or all platforms, can be described as a linear regression of the attacks originating from a single country only

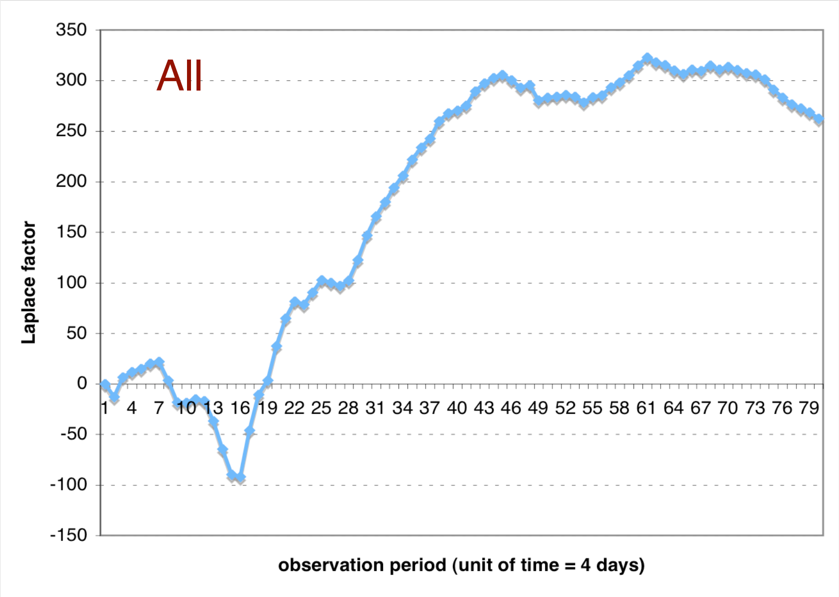
$$Y(t) = \alpha_j X_j(t) + \beta_j$$

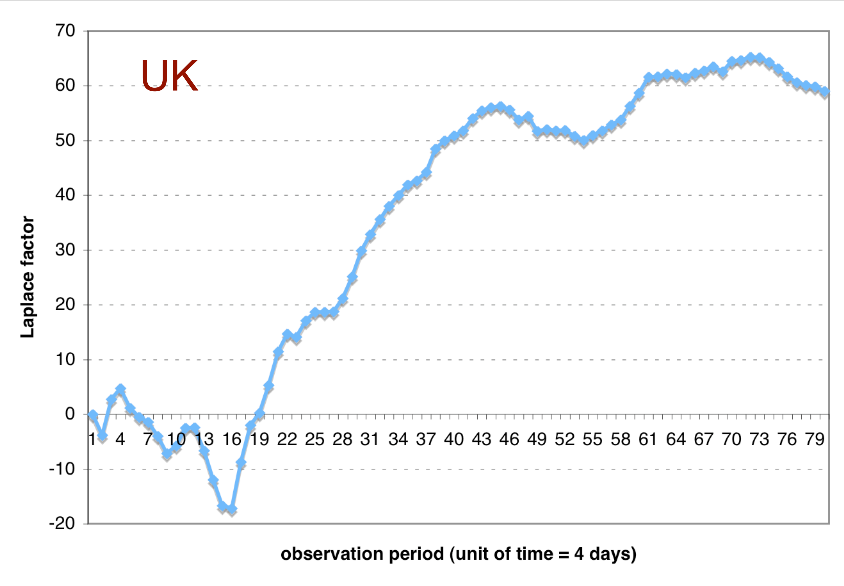
	α_j	β_j	R^2
Russia	44.57	1555.67	0.93
USA	5.13	759.1	0.94
UK	25.93	438.03	0.94

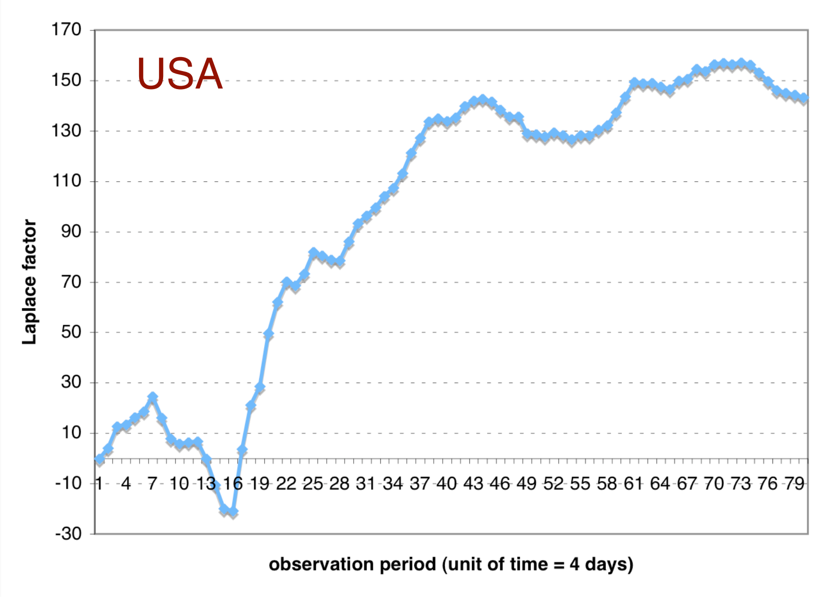


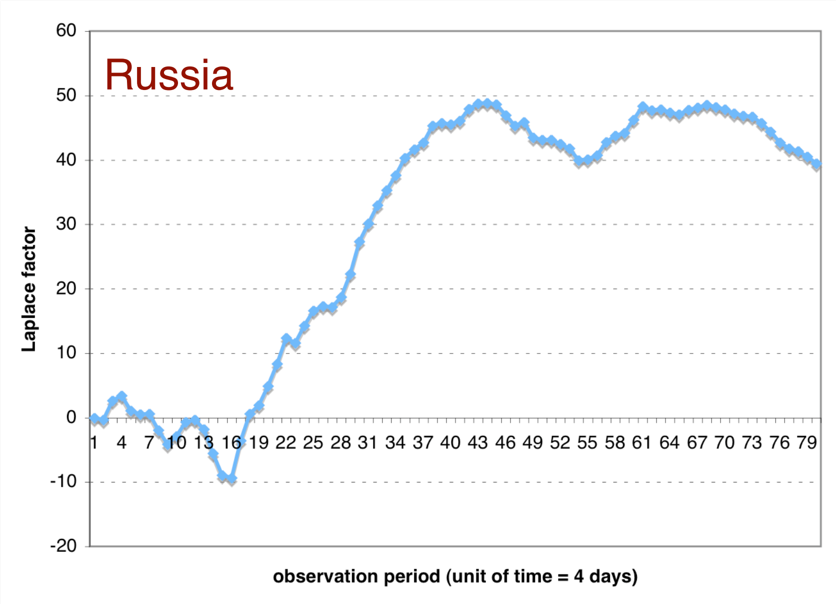
14 platforms
46 weeks

Trend: Laplace

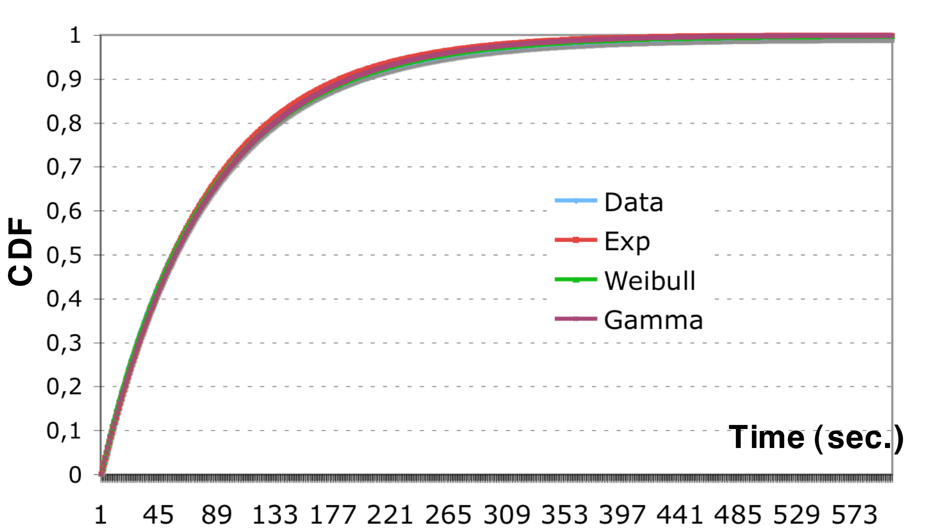




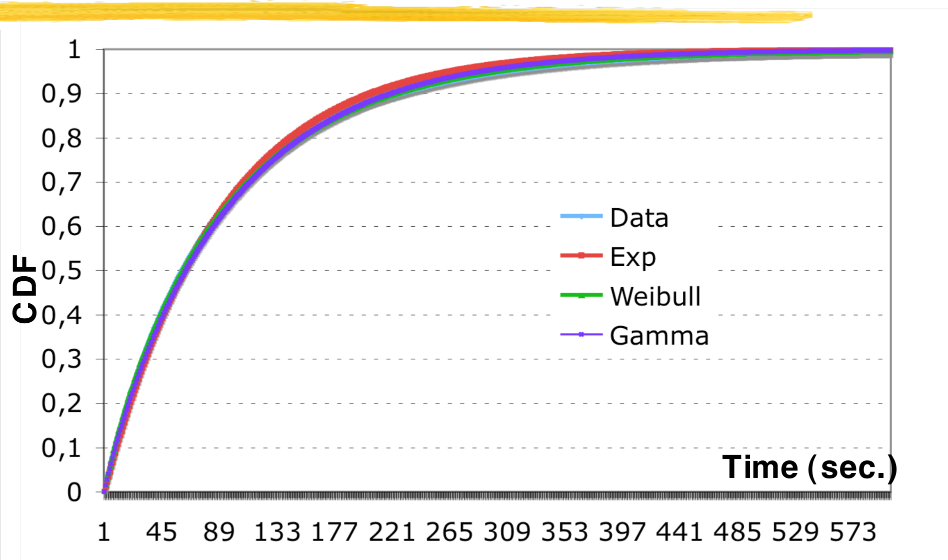




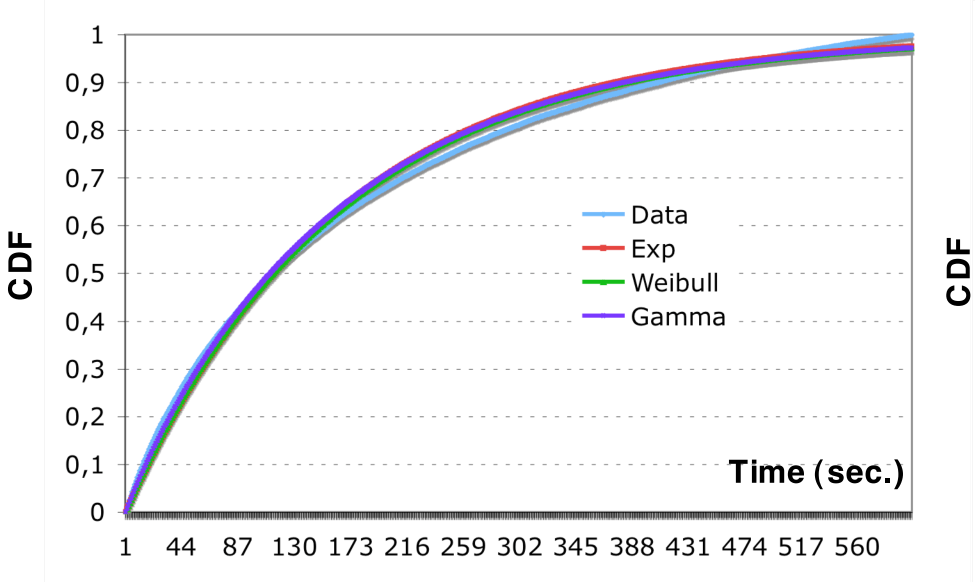
“Times between attacks” distribution



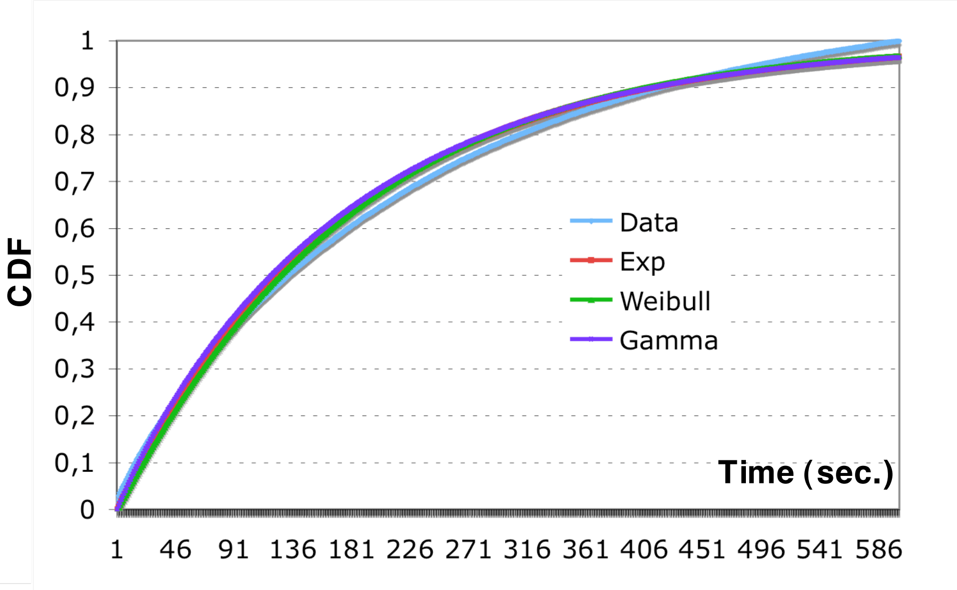
Platform 20



Platform 6



Platform 8



Platform 5

High-Interaction honeypots

- Analyze behavior of skilled attackers once they get access to a target
  - Identify attack scenarios
  - Estimate systems capacity to resist to attacks

- Validate a theoretical model for quantitative evaluation of security developed by LAAS in the 90's
  - Privilege graph to describe vulnerabilities and attack scenarios
  - METF "Mean Effort To security Failure" to quantify security
  - Assumptions about intruders behaviors

Conclusion

- Interesting conclusions derived from the data collected so far

- Some open issues with respect to modeling are under investigation

- The more data we have, the more we can say about threats and how to model them

  - Participation to data collection and analysis effort is open to all interested partners who accept to install a honeypot in their premises

  - Contact: dacier@eurecom.fr