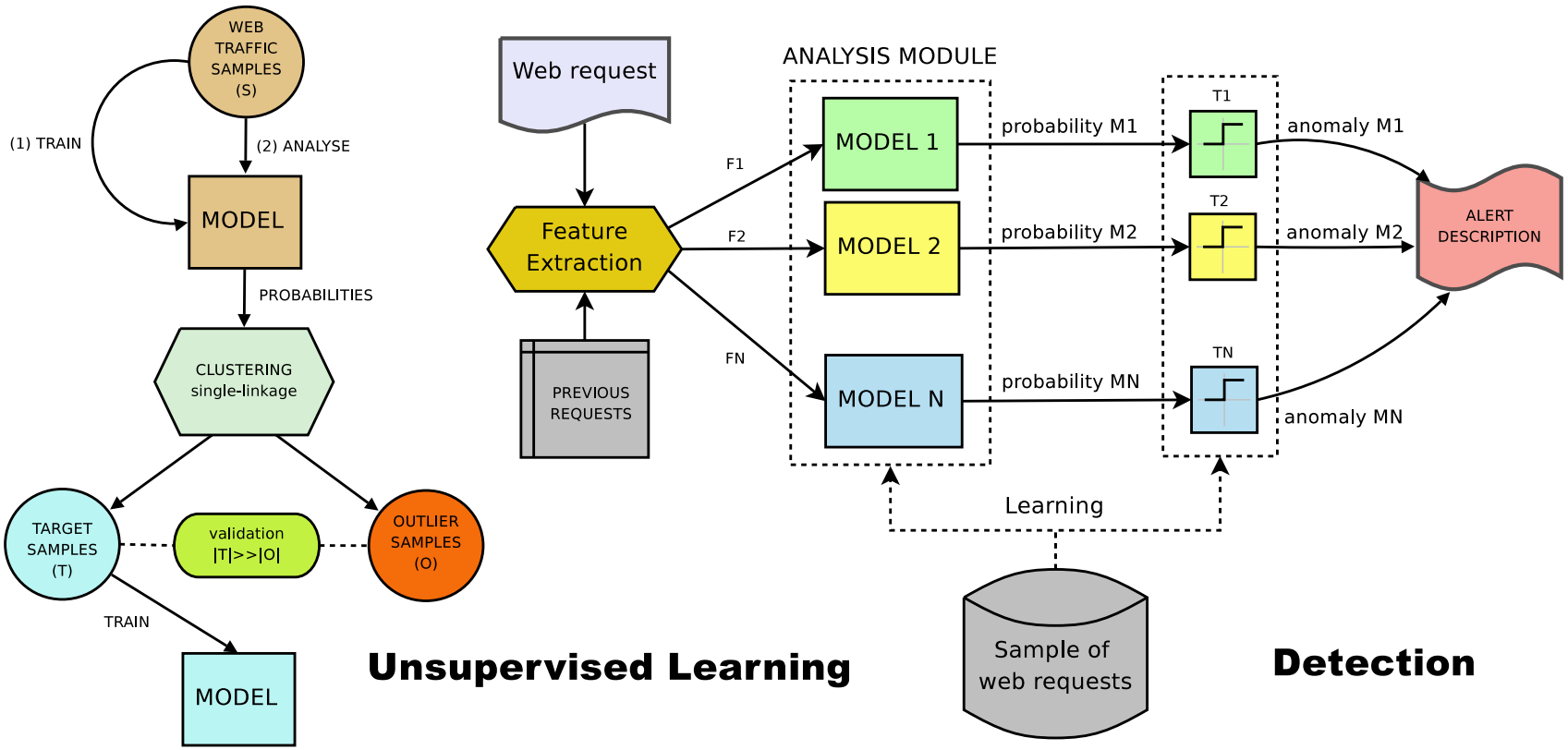
Detection of Server-side Web attacks

Igino Corona and **Giorgio Giacinto**
Pattern Recognition and Applications Group
Department of Electrical and Electronic Engineering
University of Cagliari, Italy

1 September 2010
Workshop on Applications of Pattern Analysis
Cumberland Lodge, Windsor, UK

Problem overview

- Web services are the typical target of computer attacks
- Well-crafted *malicious* input may divert the expected behavior of web services
- Due to the ad-hoc nature of web applications, it is difficult to prevent such attacks



Conclusions

Unsupervised Learning that is able to cope with noise (attacks) inside the training set

General approach: new traffic features and models can be easily added

Multiple and independent models allow for a meaningful and detailed description of known/unknown attacks

High detection accuracy

Challenges and future work

Further false alarm rate reduction

How about targeted attacks against the learning framework?

Extensive testing on multiple web servers

Parameter	Dataset	Value
detection rate	$\Lambda = \Sigma \cup T$	232 attacks out of 232, 100%, ∼39alerts/day
	Φ	505 attacks out of 507, 99.6%
false alarm rate	Λ	1,252alerts/447,178reqs, 0.28%, ∼209alerts/day
	Σ	450alerts/200,000reqs, 0.22%, ∼150alerts/day
	T	802alerts/247,178reqs, 0.32%, ∼267alerts/day
response time	Λ	1.2 milliseconds

This work is founded by

PROGRAMMA OPERATIVO FSE SARDEGNA 2007-2013
LEGGE REGIONALE 7 AGOSTO 2007, N. 7
PROMOZIONE DELLA RICERCA SCIENTIFICA E DELL' INNOVAZIONE TECNOLOGICA IN SARDEGNA

EUROPEAN UNION
REPUBLIC OF ITALY
REGIONE AUTONOMA DELLA SARDEGNA