# Distress Detection (DD)

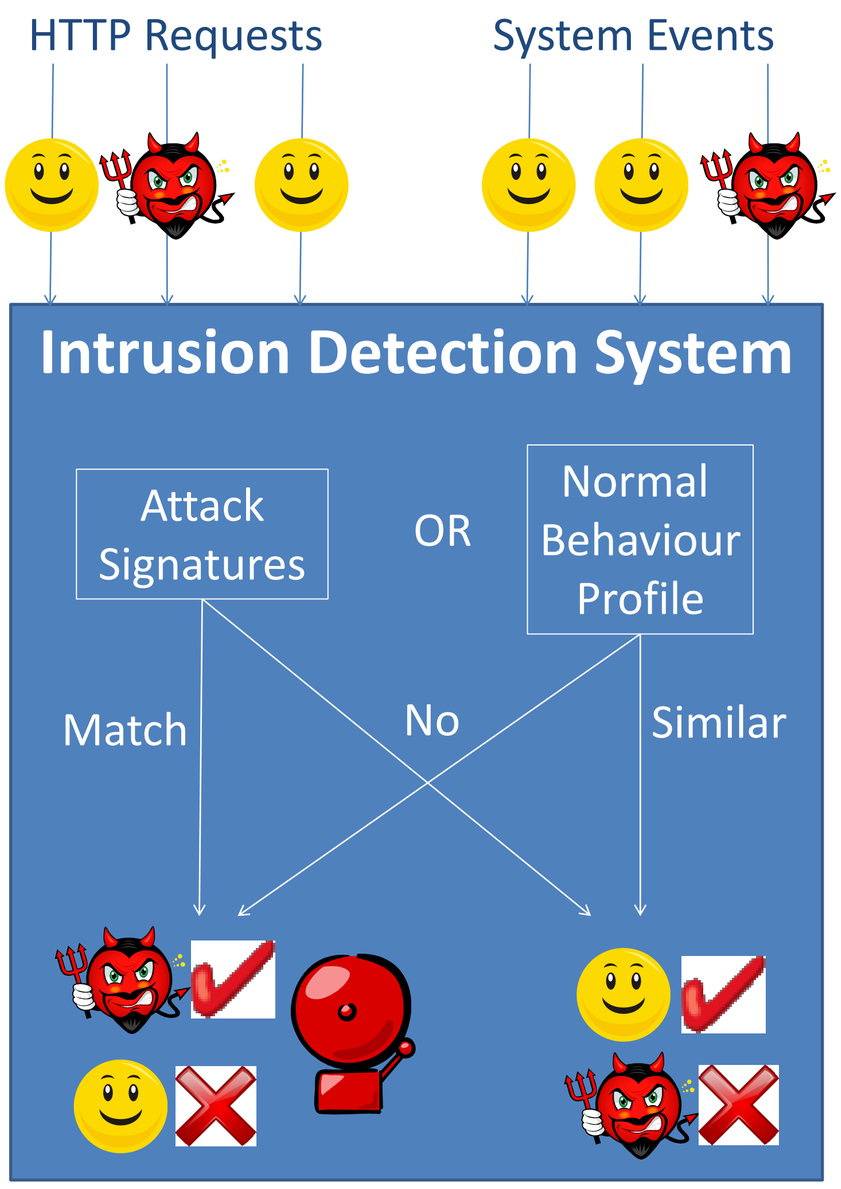
## A first step towards self-protecting web systems

Sotirios Terzis and Marc Roper
Department of Computer and Information Sciences

### 1. Web attacks are a major concern


In 2011 Symantec blocked
4,595 web attacks per day and uncovered
4,989 new vulnerabilities
403 million unique malware variants
55,294 unique malicious domains
3,065,030 bot zombies

### 2. IDS attempt to solve the problem



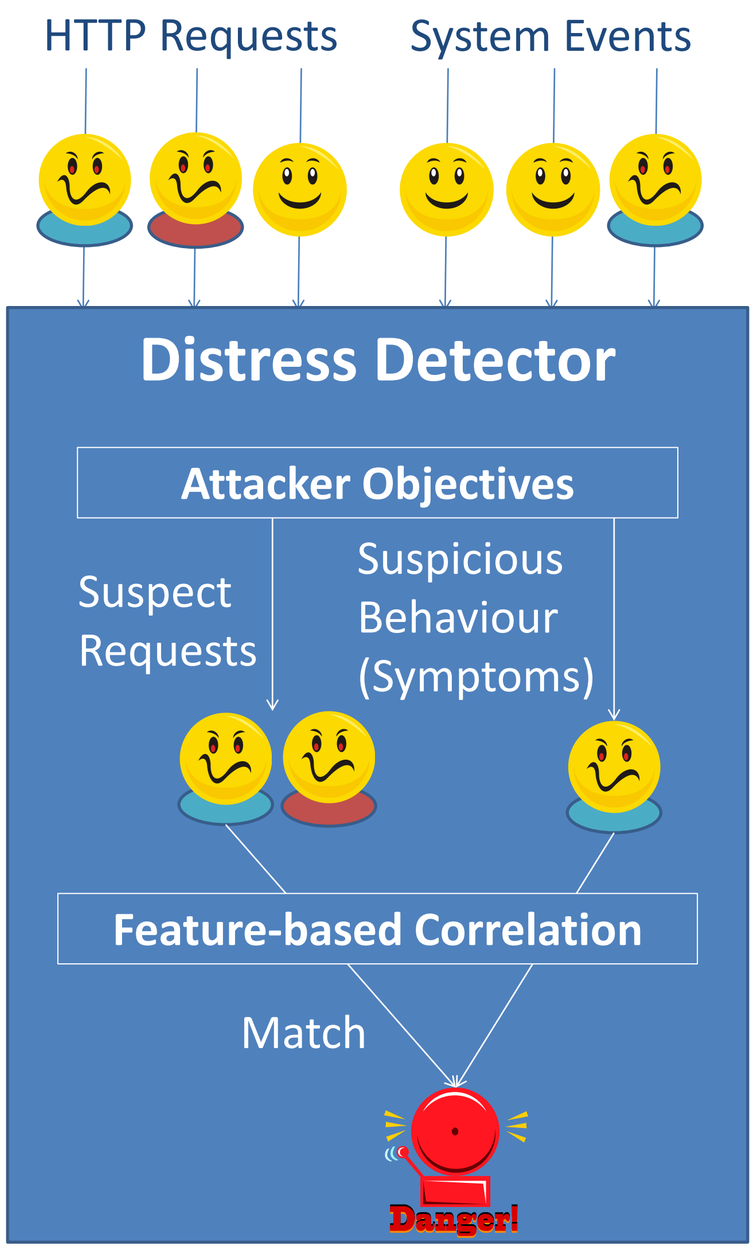

The aim is to maximize attacks detected and minimize erroneously classified normal events, **but it is difficult to generalize beyond known attack or normal behaviour**

### 3. DD addresses this challenge

Immuno-inspiration: Danger Theory

- Activation of targeted response to pathogens through correlation of signals of infection

Our premise: attacks are launched by suspicious requests that result in suspicious behaviour




### 4. DD provides novel attack resilience with minimal errors

- Three prototype detectors developed
- Experimentation platform
  - Web forum with injected vulnerabilities
  - Dataset comprising various attacks and realistic normal traffic

Baseline: 1231 requests

| | Requests | Attacks | Suspects | Symptoms | TP | FP |
|---|---|---|---|---|---|---|
| DD 1 | 18054 | 14 | 60 | 15845 | 14 | 0 |
| DD 2 | 6280 | 12 | 52 | 995 | 12 | 0 |
| DD 3 | 18173 | 14 | 262 | 497249 | 14 | 10 |