New Techniques in Application Intrusion Detection

Al Huizenga, Mykonos Product Manager

May 2010

Today

- Who am I?
  - Director of Product Management, Mykonos
  - 11 years experience marketing Web-based products and technologies
  - Canadian. Eh.
- The Agenda
  - The problem of Web application abuse
  - Current options
  - Application intrusion detection and response
  - AppSensor vs. Mykonos Security Appliance

The Problem

The Cost of Web Application Abuse

Fraud!

Defacement!

Identify Theft!

Loss of business!

Brand damage!

Economic Growth!

mykonos

How Big is the Problem?

Big, and Getting Bigger

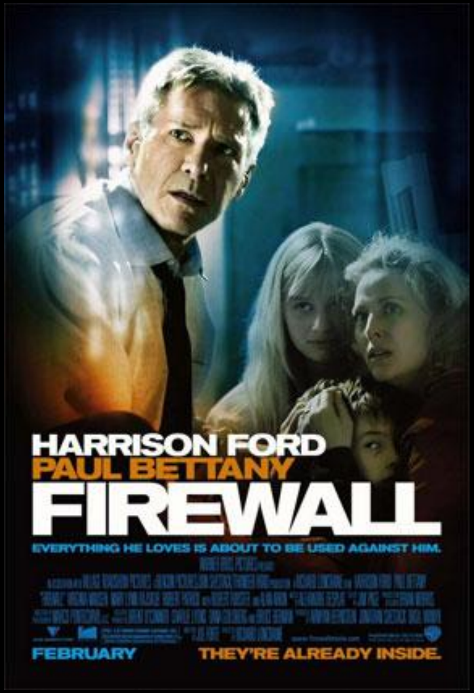
- **$4.0B** in Fraud
  (2008 Cybersource)
- **$50B** in Identity Theft
  (2009 FTC)
- **$16B** Credit Card Fraud
  (2008 Mercator Advisory Group)
- **$204** - Cost of Data Breach per Customer Record
  (Ponemon Institute 2009)
- **$1T** - Global Cost of Cyber Crime
  (McAfee 2008)

mykonos

The Challenge

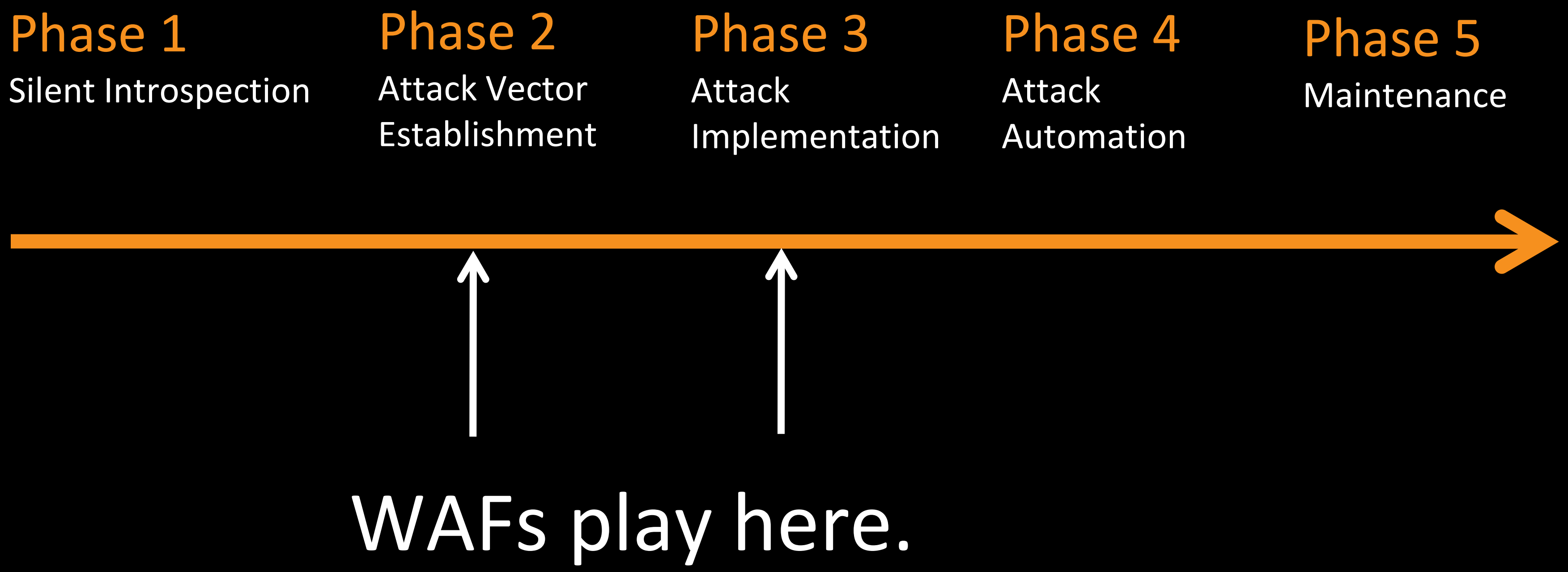
How to Secure Legacy Apps from Abuse

Fix It.



Firewall It.

The Anatomy of a Web Attack



Phase 1
Silent Introspection

Phase 2
Attack Vector Establishment

Phase 3
Attack Implementation

Phase 4
Attack Automation

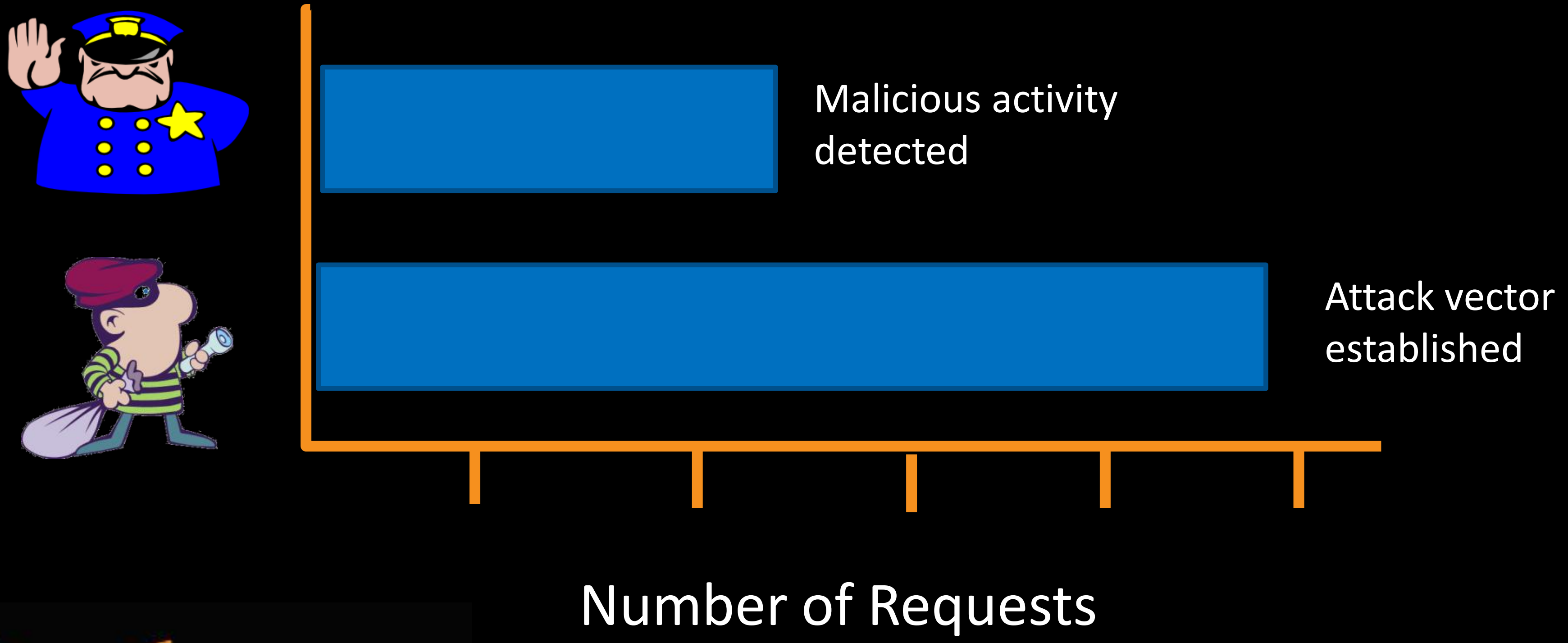
Phase 5
Maintenance

WAFs play here.

mykonos

Early Detection

What about all the requests before an attack is delivered?



mykonos

Is there another way?

Add Security Logic to the App

- Can you extend legacy apps to detect malicious activity from within the app itself, before a user is able to identify and exploit a vulnerability?
  - E.g. Manipulating cookies, query parameters, input fields…

Approaches

OWASP AppSensor Project

A conceptual framework for implementing intrusion detection capabilities into existing applications

http://www.owasp.org/index.php/Category:OWASP_AppSensor_Project

AppSensor

42 Detection Points

Exception	# Detection Points
Request	4
Authentication	11
Access Control	6
Session	4
Input	2
Encoding	2
Command Injection	4
File IO	2
User Trend	4
System Trend	3

AppSensor

How is it implemented?

- A little unclear…
- Two recommendations
  - At the business layer (aka in code), preferably using the OWASP ESAPI
  - As a ‘cross-cutting concern’ in an Aspect-Oriented Programming approach (e.g. Java Filters)

AppSensor

Strengths and Challenges

Strengths

- It’s smart
- A great reference for determining malicious intent, categorizing and rating incidents

Challenges

- Takes development time
- No tools or pre-fab solutions yet
- Project advances very slowly

Approaches

The Mykonos Security Appliance

A high speed HTTP processing engine that extends Web application code with intrusion detection and response capabilities at serve time.

http://www.mykonossoftware.com

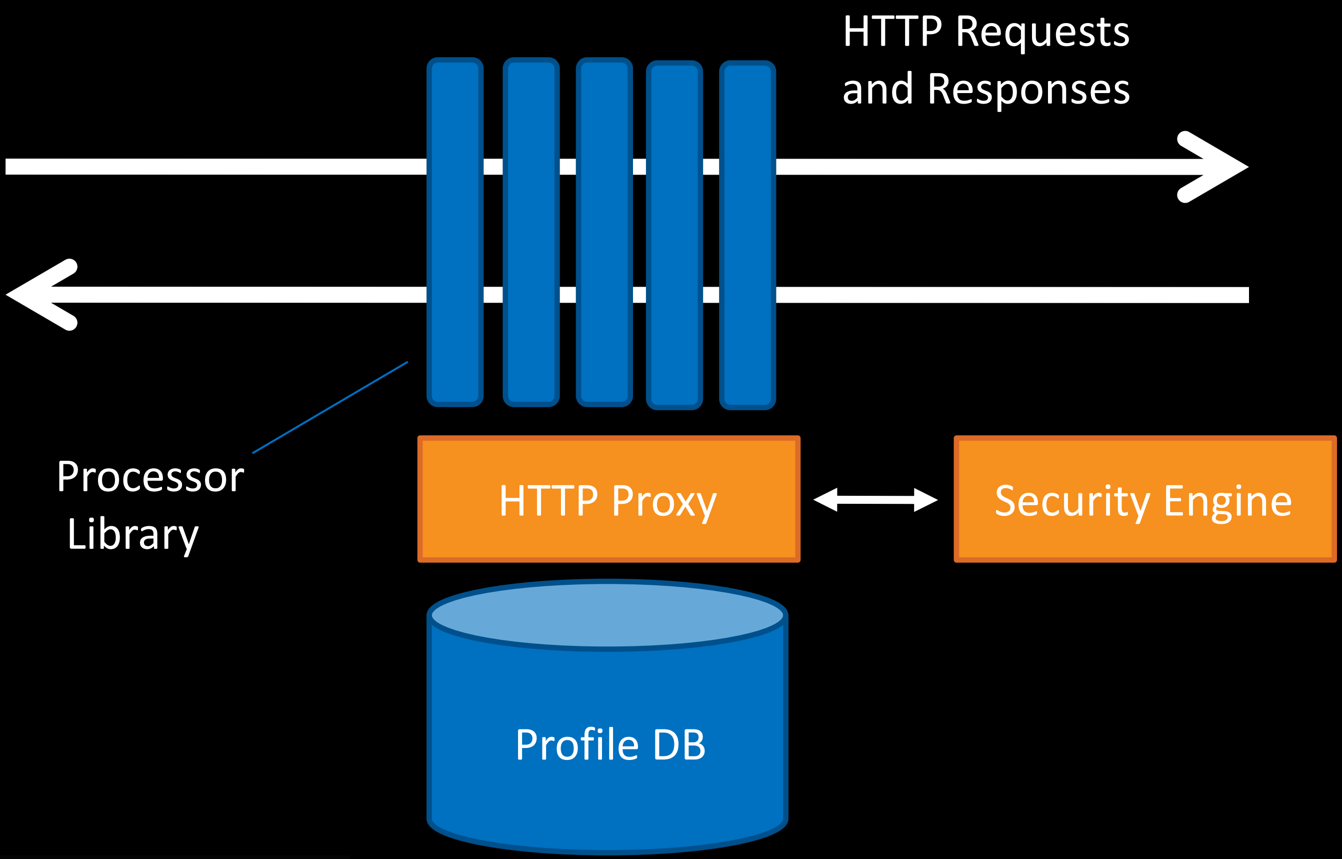
The Mykonos Security Appliance

26 Detection Points

Processor	# Detection Points
Authentication	4
Cookies	1
Errors	2
Files	2
Headers	7
Inputs	1
Links	3
Request Methods	3
Query Parameters	1
Spiders	2

The Mykonos Security Appliance

How is it implemented?



The Mykonos Security Appliance

Strengths and Challenges

Strengths

- It’s smart
- Code-aware w/o dev participation
- Easy to configure

Challenges

- Inline proxy
- Throughput and latency
- Transparency – don’t break the app!

The Mykonos Security Appliance

Demo