MAGENTO SECURITY

DUE TO PCI DSS

talk by angelo.maragna@gmail.com 2ndAngyel

THE PRESENTER

Angelo Maragna
Italian, 38y old, currently working at Net World Sports Ltd in Wrexham as a **Magento Developer**
Coder since 1988 and professional developer since 2003.

Experience in:

- PHP development
- Windows server systems administration (from design to implementation, management and support)
- Windows and linux Web server administration
- ERP and CRM implementations (italian ERPS, vTiger CRM)
- Door to door sales
- Freelance company websites developer (from sales, to graphic design, development and customer training)

Studying now for the CISSP certification.

Security, what a big subject…

This presentation wants to shed some light on the information security domain applied to our day to day work and to tickle magento developers and devops with platform design concepts and tenets about security. The extensive field of information security is a so wide argument that a whole week wouldn't be enough to satisfactory cover it. The following content have been extracted from PCI DSS and CISSP documentation.

Angelo Maragna

What THE TALK ?!?

1. PCI DSS
2. General concepts about security
3. Security in software development
4. Security in production environments
5. Magento and security

1. PCI DSS

1. Payment Card Industry Data Security Standards

- **What is PCI DSS?**
  (Document library on pcisecuritystandards.org)

- **To whom does it concern?**

1. Payment Card Industry Data Security Standards

- **When do you have to comply?**

  Always, just understand how many VISA or Mastercard transactions you "process" per year:

  Merchant Level 1 • More than 6M/year

  Merchant Level 2 • From 1 to 6 M/year

  Merchant Level 3 • From 20k to 6M/year e-commerce

  Merchant Level 4 • < 20k by ecommerce and <1M in general

- **What does it practically mean?**

10 PRINT “CIAO”

20 GOTO 10

2. GENERAL CONCEPTS ABOUT SECURITY

2. General concepts about security

- Security governance principles

Website is offline No cached version of this page is available.

Retry for a live version

Error 524

Ray ID: 1ef072edc42f07df • 2015-05-31 06:00:27 UTC

A timeout occurred

You
Browser
Working

Los Angeles
CloudFlare
Working

Host
Error

2. General concepts about security

- Security governance principles
- Policies, standards, guidelines and procedures

2. General concepts about security

- Security governance principles
- Policies, standards, guidelines, and procedures
- Security vulnerabilities, threats and safeguards

3. SECURITY IN SW DEVELOPMENT

3. SECURITY IN SOFTWARE DEVELOPMENT

- System development lifecycle
- Skilled reviewers
- Security experience

3. SECURITY IN SOFTWARE DEVELOPMENT

System development lifecycle

- Conceptual definition
- Functional requirements determination
- Control specifications development
- Design review
- Code review meetings
- User acceptance testing review
- Maintenance and change management

3. SECURITY IN SOFTWARE DEVELOPMENT

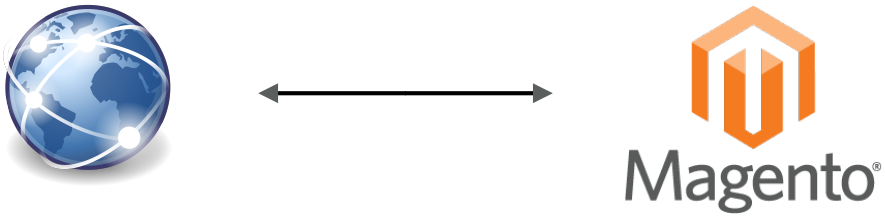
Skilled reviewers / Train yourself / Security experience

- The OWASP organisation (Manchester meeting next thursday)
- Secure coding best practices (PDF)
- Developer guide (https://github.com/OWASP/DevGuide)
- Insecure web application WebGoat (docker)

4. SECURITY IN PRODUCTION ENVIRONMENTS

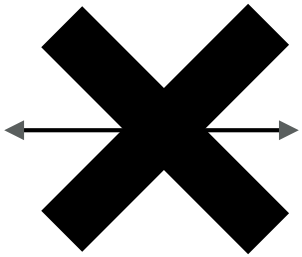
4. Security in production environments

- Layering
- Separation of duties and network segmentation
- Development, testing, staging and production
- Platform hardening



4. Security in production environments

- Layering
- Separation of duties and network segmentation
- Development, testing, staging and production
- Platform hardening



4. Security in production environments

- Layering
- Separation of duties and network segmentation
- Development, testing, staging and production
- Platform hardening

4. Security in production environments

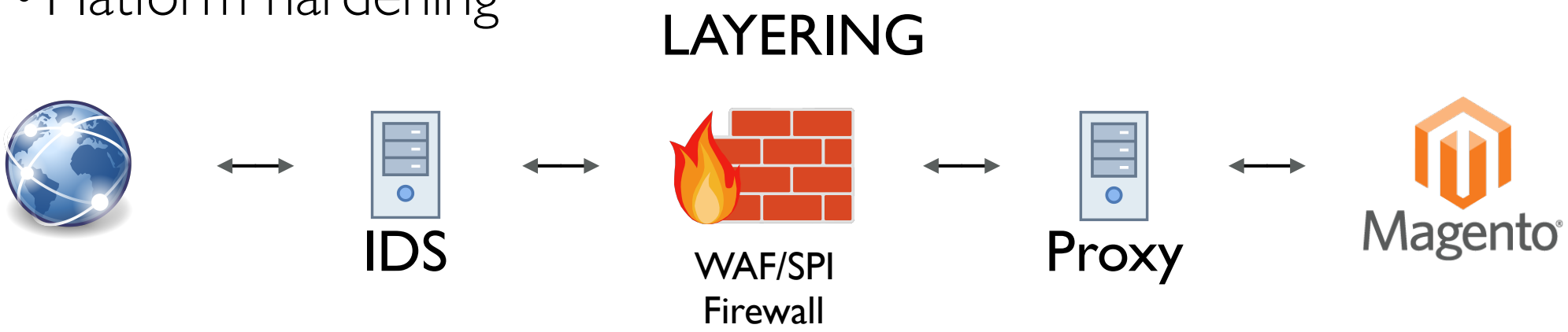
- Layering
- Separation of duties and network segmentation
- Development, testing, staging and production
- Platform hardening

4. Security in production environments

- Layering
- Separation of duties and network segmentation
- Development, testing, staging and production
- Platform hardening

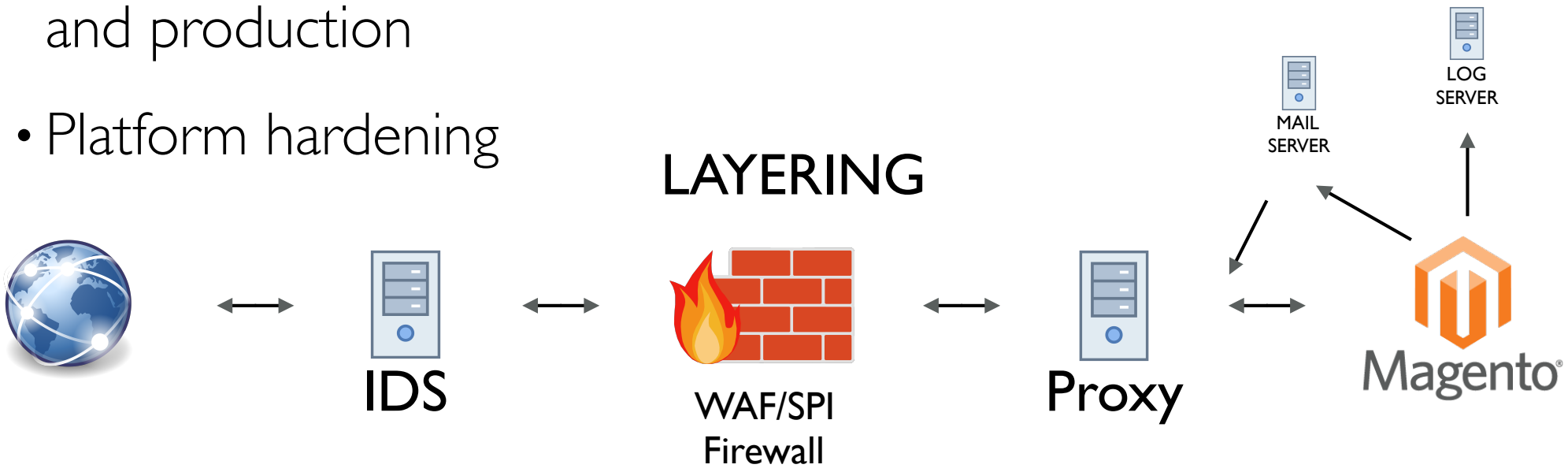
4. Security in production environments

- Layering
- Separation of duties and network segmentation
- Development, testing, staging and production
- Platform hardening



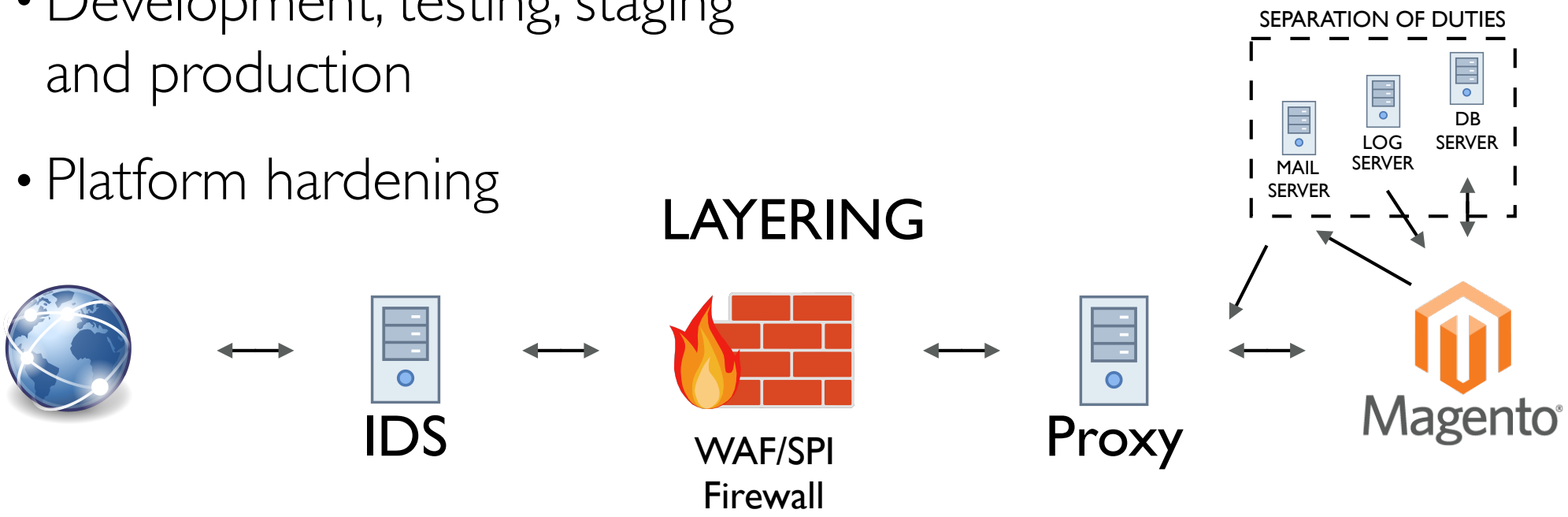
4. Security in production environments

- Layering
- Separation of duties and network segmentation
- Development, testing, staging and production
- Platform hardening



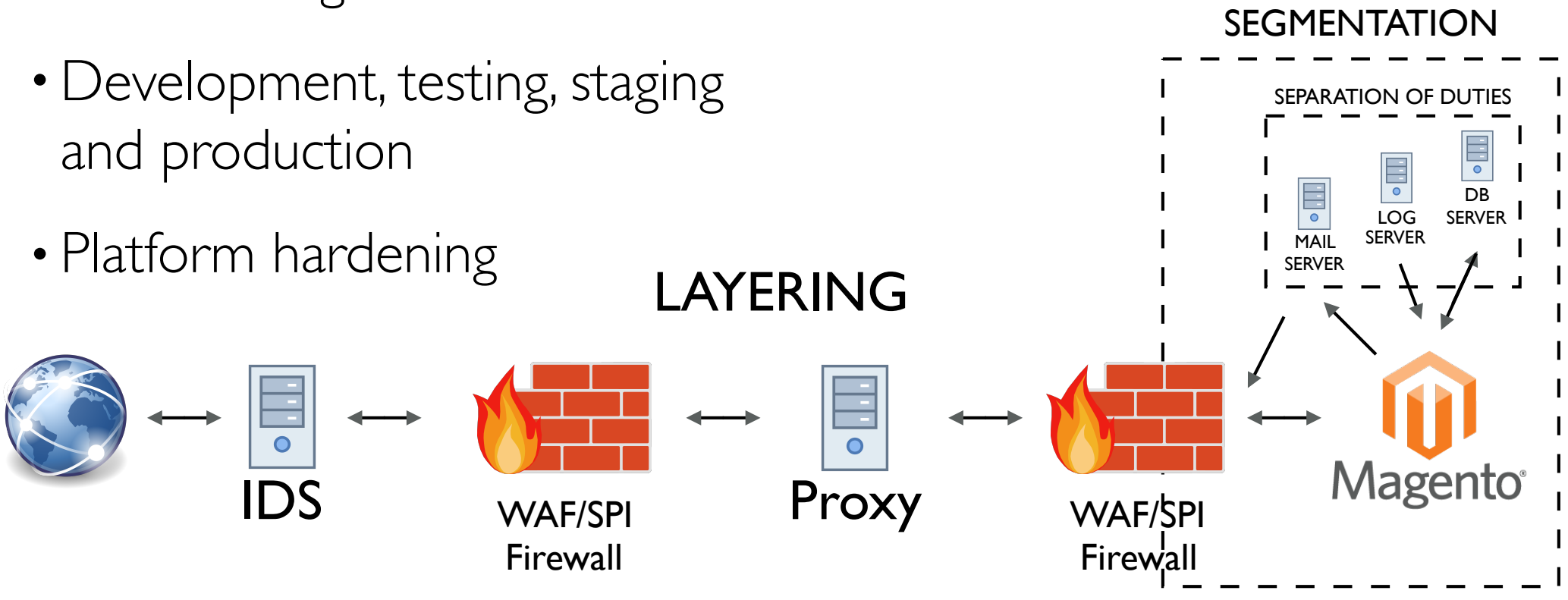
4. Security in production environments

- Layering
- Separation of duties and network segmentation
- Development, testing, staging and production
- Platform hardening



4. Security in production environments

- Layering
- Separation of duties and network segmentation
- Development, testing, staging and production
- Platform hardening



5. MAGENTO AND SECURITY

5. Magento and security

- Coding
- Editors and administrators authorisation
- Encrypting communications
- Cardholder data process types
- Logging
- Encrypted extensions

"DILIGENCE IS THE MOTHER OF GOOD LUCK"

–Benjamin Franklin

slides available on github.com/angelomaragna/magento-security

THANKS

– Angelo Maragna

slides available on github.com/angelomaragna/magento-security