OWASP AppSensor
In Theory, In Practice and In Print

AppSec Research 2013, Hamburg, Germany, 23rd August 2013

Colin Watson, Watson Hall Ltd

Dennis Groves, Desago Ltd

OWASP
The Open Web Application Security Project

About ~~Us~~ Me

- ## Colin Watson

  colin.watson@owasp.org @clerkendweller

  Founder of Watson Hall Ltd, based in London, where his work involves the management of application risk, designing defensive measures, building security & privacy in to systems development and keeping abreast of relevant international legislation and standards. He holds a BSc in Chemical Engineering from Heriot-Watt University in Edinburgh, and an MSc in Computation from the University of Oxford.

- ## Dennis Groves

  dennis.groves@owasp.org @degroves

  Co-founder of OWASP and a well known thought leader in application security who's work focuses on multidisciplinary approaches to information security risk management. He holds an MSc in Information Security from Royal Holloway, University of London.

Universal Security Strategy

- If you can try to prevent bad guys getting to you
- If you cannot
  - try to detect and react before it succeeds
  - try to detect whether you've been compromised
- If you've been compromised
  - do incident response and clean up

Risk Treatments

OWASP
The Open Web Application Security Project

- Tolerate: Do nothing
- Transfer: Outsource the risk
- Terminate: Eliminate the asset
- Treat: Reduce the risk

Risk Reduction Methods

OWASP
The Open Web Application Security Project

- Reducing the risk (treatment) is the most common strategy used today
  - Reduce the probability of a threat
  - Reduce the probability of a vulnerability
- Risk optimisation is rarely practiced, but is a highly effective method
  - Reduce the impact of an event

Conventional Defensive Measures

- Perimeter defence
  - Packet Filters
  - Firewalls
  - Application layer (WAFs, filters, guards)
- Cryptographic communications
- Anti-Virus (AV)
- Network and host Intrusion Detection/Prevention Systems (IDS/IPS)

Intrusion Detection/Prevention Systems

OWASP
The Open Web Application Security Project

- IDS/IPS
  - Host based – OSSEC, Tripwire, etc
  - Network based – Snort, etc
  - Application based - OWASP AppSensor.

OWASP AppSensor

- Moving detection & reaction into the application

Application Defensive Measures

- Attack-aware detection
- Normal and malicious behavior
- Real-time response
- Evasion
- Unknown attacks

Resilient Software

OWASP
The Open Web Application Security Project

„Software Assurance goals promote the security and resilience of software across the development, acquisition, and operational lifecycle; as such, SwA is scoped to address trustworthiness, dependability (correct and predictable execution), conformance, and survivability.“

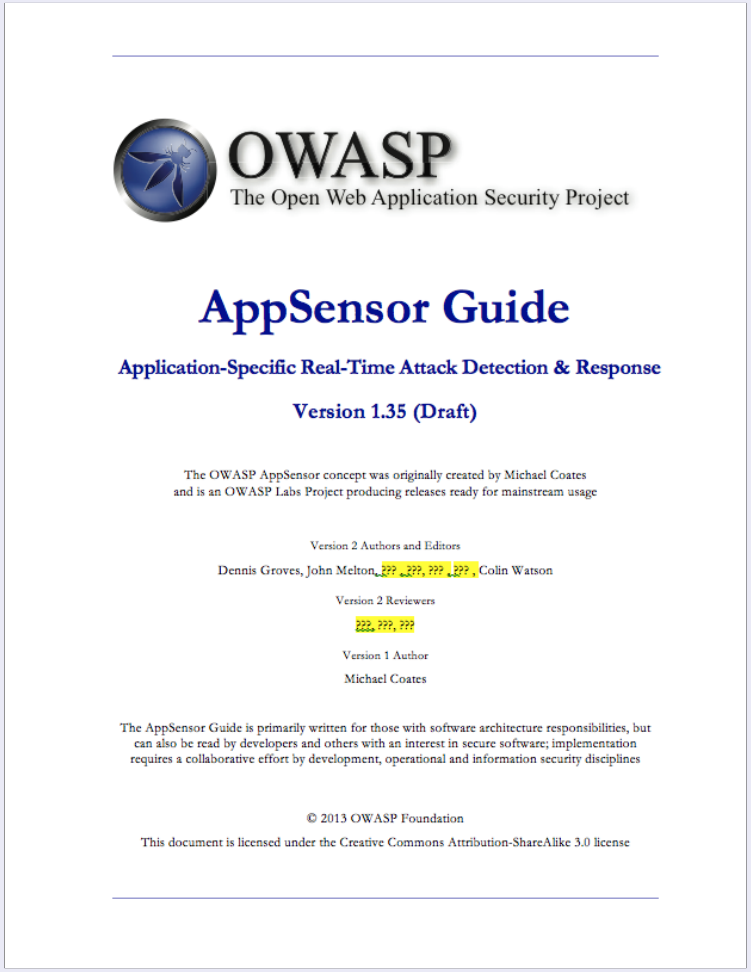
„The resilient software of the future will require cyber defenses that are proactive, not reactive. Moreover, these defenses, as appropriate, need to marshal automated collective action to protect, detect, respond, and recover our cyber assets. They will categorize cyber attacks and provide a set of future cyber ecosystem capabilities to mitigate those attacks.“

AppSensor Guide v2

OWASP
The Open Web Application Security Project

In numbers

- 150 pages
- 41 tables
- 27 figures
- 24 chapters
- 7 case studies
- 6 demonstration implementations



OWASP
The Open Web Application Security Project

AppSensor Guide

Application-Specific Real-Time Attack Detection & Response

Version 1.35 (Draft)

The OWASP AppSensor concept was originally created by Michael Coates
and is an OWASP Labs Project producing releases ready for mainstream usage

Version 2 Authors and Editors

Dennis Groves, John Melton, ???, ???, ???, ???, Colin Watson

Version 2 Reviewers

???, ???, ???

Version 1 Author

Michael Coates

The AppSensor Guide is primarily written for those with software architecture responsibilities, but can also be read by developers and others with an interest in secure software; implementation requires a collaborative effort by development, operational and information security disciplines

© 2013 OWASP Foundation

This document is licensed under the Creative Commons Attribution-ShareAlike 3.0 license

Practical Deployment 1

OWASP
The Open Web Application Security Project

Illustrative case studies

- Rapidly deployed web application
- Magazine's mobile app
- **Smart grid consumer meter**
- Financial market trading system
- B2B E-commerce website
- B2B web services
- Document management system

Gas and electricity smart meters are beginning to replace traditional meters and allow remote usage monitoring, configuration and can offer some benefits to both the supplier and consumer. Remote connectivity may use an embedded SIM card to connect with a mobile network provider, or in the case of broadband-connected home, utilize the existing WiFi connection. Customers often have concerns about privacy, confidentiality of data, difficulties in changing their supplier and health due to the use of mobile phone and WiFi technology.

Mobile technicians connect to smart meters using an infrared optical port which is more reliable in the many different locations that the meters can be installed in. The technicians use security codes to authenticate and then may alter the configuration or collect information. The long highly-random security codes could be identified by brute force and dictionary attacks.

The same functionality is also available remotely, but the optical port is much more exposed.

1. Identify attacks against authentication functions

Practical Deployment 2

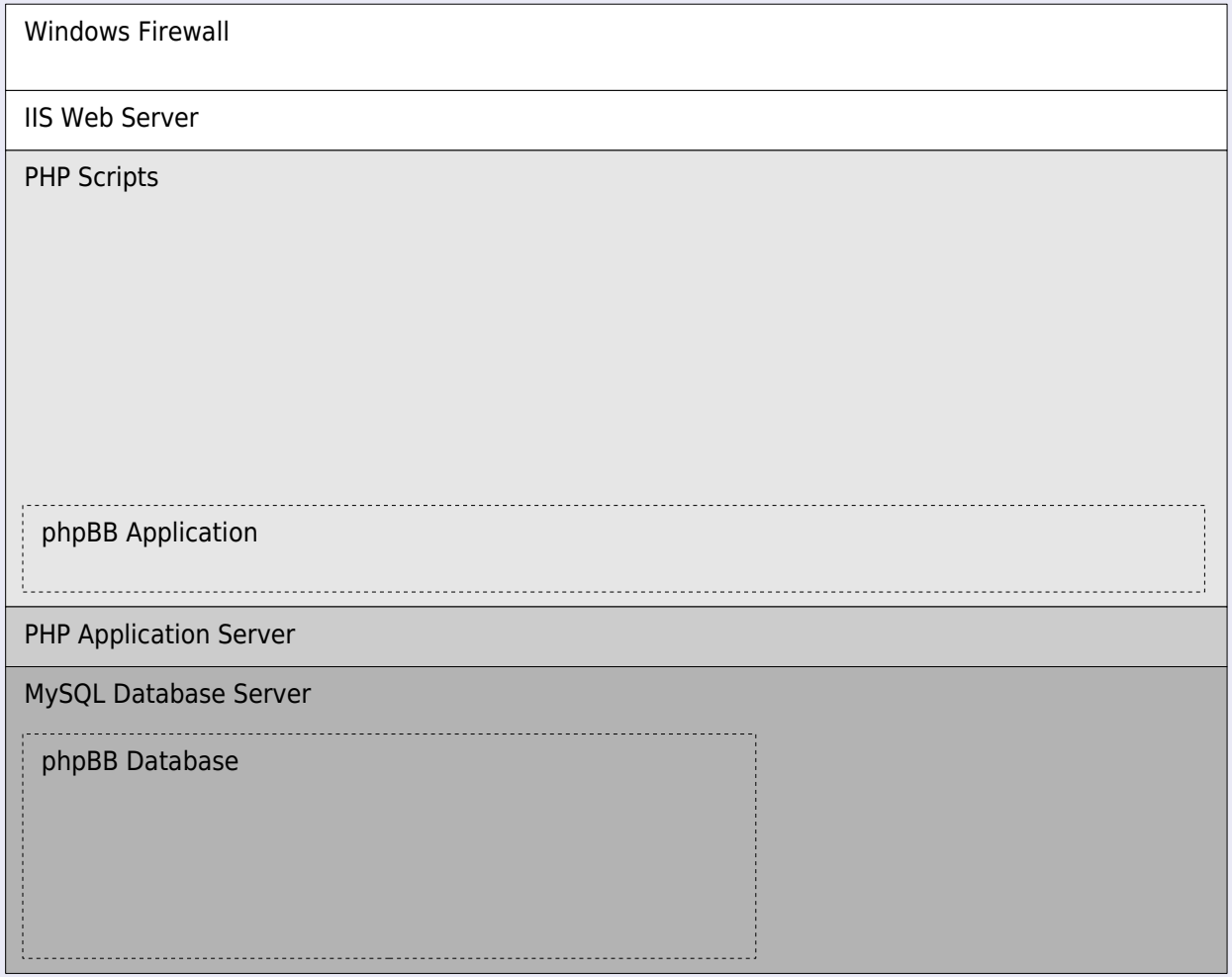
Demonstration implementations

- Web services (AppSensor WS)
- Fully integrated (AppSensor Core)
- Light touch retrofit
- Invocation using Jni4Net
- Using an external log management system
- Leveraging a web application firewall

Format for each

- Introduction
- Description
- AppSensor scope
- Source code
- Implemenation
- Considerations
- Related implementations

Example: Light Touch Retrofit



Detection and Event Analysis

OWASP
The Open Web Application Security Project

Windows Firewall

IIS Web Server

PHP Scripts

New custom code

- Violation of Blacklist
- Multiple Usernames
- Large Number File Uploads
- Force Browsing
- Violation of Whitelist
- Multiple Passwords
- Honey Trap Data / Resource
- High Rate Posts

Event Manager

Event Analysis Engine

phpBB Application

PHP Application Server

MySQL Database Server

phpBB Database

New custom tables

Event Store

Attack Store

Respond

OWASP
The Open Web Application Security Project

Windows Firewall
Disable Application for a Single User

IIS Web Server

PHP Scripts

New custom code

* Violation of Blacklist
* Multiple Usernames
* Large Number File Uploads
* Force Browsing
* Violation of Whitelist
* Multiple Passwords
* Honey Trap Data / Resource
* High Rate Posts

Event Manager

Event Analysis Engine

phpBB Application

PHP Application Server

MySQL Database Server

phpBB Database

Disable Posts by a Single User

New custom tables

Event Store

Attack Store

Do More

OWASP
The Open Web Application Security Project

Windows Firewall
Disable Application for a Single User

IIS Web Server

PHP Scripts

New custom code

* Violation of Blacklist
* Multiple Usernames
* Large Number File Uploads
* Force Browsing
* Violation of Whitelist
* Multiple Passwords
* Honey Trap Data / Resource
* High Rate Posts

Event Manager
Event Analysis Engine
Honeypot Event Analysis

phpBB Application

PHP Application Server

MySQL Database Server

phpBB Database
Disable Posts by a Single User

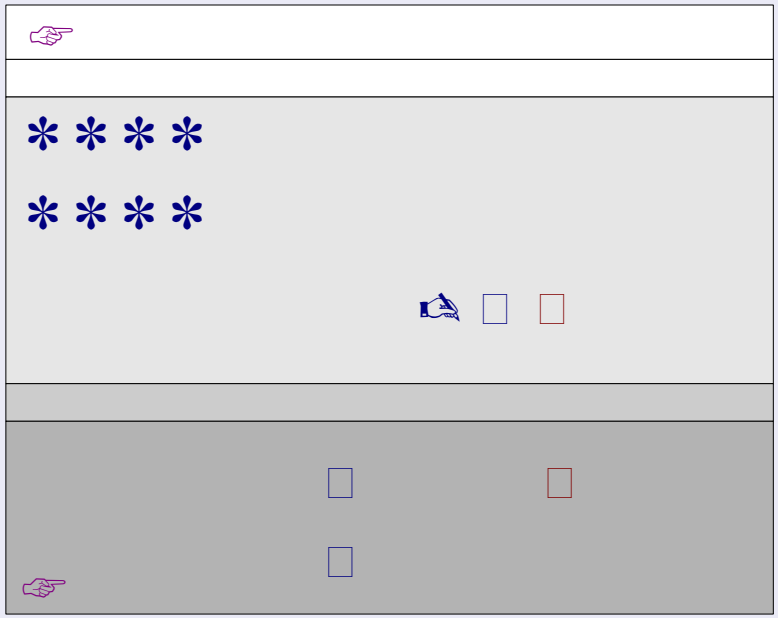
New custom tables
Event Store
Attack Store

Honeypot Logging

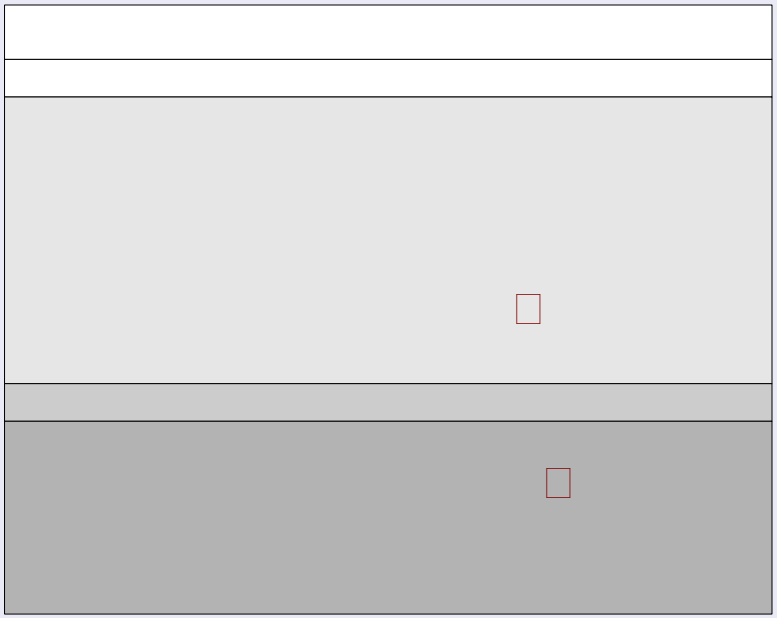
Currently Running

OWASP
The Open Web Application Security Project

A: With AppSensor



B: Without



Project Contributors

OWASP
The Open Web Application Security Project

Ryan Barnett
Simon Bennetts
Joe Bernik
Rex Booth
Luke Briner
Rauf Butt
Fabio Cerullo
Marc Chisinevski
Robert Chojnacki
Michael Coates
Dinis Cruz
August Detlefsen
Ryan Dewhurst
Sean Fay
Dennis Groves
Randy Janida
Eoin Keary
Alex Lauerman
Jason Li
Manuel López Arredondo
Bob Maier
Jim Manico
John Melton
Craig Munson
Giri Nambari
Jay Reynolds
Chris Schmidt
Sahil Shah
Eric Sheridan
John Steven
Alex Thissen
Don Thomas
Pål Thomassen
Kevin W Wall
Colin Watson
Mehmet Yilmaz

Forward Plan

OWASP
The Open Web Application Security Project

2013

- Book finalisation and publication
  - DoHS design funding?
  - OWASP Reboot funding
- Completion on honeypot trial
- OWASP Cheat Sheet Series
  - Active Defense Cheat Sheet
- OWASP Code Review Guide
  - Review for active defense
- OWASP Testing Guide
  - Business logic tests?

Beyond

- Standalone engine
- Reporting interface

Project Resources

- Project home page
  https://www.owasp.org/index.php/OWASP_AppSensor_Project
- Mailing lists
  - Project
    https://lists.owasp.org/mailman/listinfo/owasp-appsensor-project
  - Development
    https://lists.owasp.org/mailman/listinfo/owasp-appsensor-dev
- Resilient software
  https://buildsecurityin.us-cert.gov/swa/topics/resilient-software
- CrossTalk Journal
  http://www.crosstalkonline.org/storage/issue-archives/2011/201109/201109-Watson.pdf
- Example detection points
  https://www.owasp.org/index.php/AppSensor_DetectionPoints
- Example responses
  https://www.owasp.org/index.php/AppSensor_ResponseActions
- Book v1.1 (2008)
  http://www.lulu.com/shop/owasp-foundation/owasp-appsensor/paperback/product-4520003.html
- Book ~~v2~~ v1.35 (2013)
  https://www.owasp.org/index.php/File:Owasp-appensor-guide-v2.doc
- High Interaction Honeypot Analysis Toolkit (HIHAT)
  http://hihat.sourceforge.net/s

Q&A

- Comments
- Questions

- Feedback
  - What did you like most?
  - What did you like least?
  - What can be improved?
- Contribute to project

Presentation

OWASP
The Open Web Application Security Project

- https://www.owasp.org/index.php/File:Appseceu2013-appsensor.odp
- AppSecEU website