Running order

Guide v2.0
• Preamble
• Overview
• Illustrative case studies
• Making it happen
• Demonstration implementations
• Model dashboards
• Reference materials

This presentation
• Timeline
• Terminology
• Architectures
• Detection points
• Live demo
• Responses
• Case studies
• Media
• Q&A
AppSensor Guide v2.0 timeline
AppSensor Guide v2.0 release timeline

- May 1: End final review
- May 2: Project co-leaders informed
- May 3: A very busy day
- May 4: v2.0 created
- May 5: Project wiki updated
- May 6: Other contributors informed
- May 7: Announced to project list
- May 8: v2.0.1 created
- May 9: Source files uploaded
- May 10: Tonight!
Terminology

Symbol Key
- Events
- Detection Points
- Event Manager
- Reporting Client
- Responses
- Event Analysis Engine
- Event Store
- Attack Store
Part IV: Demonstration Implementations

- Seven examples
# Chapter 20:
Web Services (AppSensor WS)

<table>
<thead>
<tr>
<th>Client</th>
<th>Network</th>
<th>Perimeter Network Devices</th>
<th>Web/Application Tier (Web Services)</th>
<th>Data Tier (Data Store)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(e.g. web browser, mobile device/app, another application)</td>
<td>(e.g. internet, VPN, internal network)</td>
<td>(e.g. routers, network firewalls, load balancers)</td>
<td>(e.g. web servers, application servers, applications as services)</td>
<td>(e.g. database servers)</td>
</tr>
</tbody>
</table>

## Symbol Key
- **Events**
- Detection Points
- Event Manager
- Reporting Client
- Responses
- Event Analysis Engine
- Event Store
- Attack Store
# Chapter 21: Fully Integrated (AppSensor Core)

<table>
<thead>
<tr>
<th>Client (e.g. web browser, mobile device/app, another application)</th>
<th>Network (e.g. internet, VPN, internal network)</th>
<th>Perimeter Network Devices (e.g. routers, network firewalls, load balancers)</th>
<th>Web/Application (e.g. web servers, application servers, application)</th>
<th>Data Tier (e.g. database servers)</th>
</tr>
</thead>
</table>

![Diagram of integrated systems](image)

## Symbol Key
- **Events**
- **Detection Points**
- **Event Manager**
- **Reporting Client**
- **Responses**
- **Event Analysis Engine**
- **Event Store**
- **Attack Store**
Chapter 22: Light Touch Retrofit

| Client (e.g. web browser, mobile device/ app, another application) | Network (e.g. internet, VPN, internal network) | Perimeter Network Devices (e.g. routers, network firewalls, load balancers) | Web/Application Tier (e.g. web servers, application servers, application, applications as service) | Data Tier (e.g. database servers) |

Host (e.g. operating system, host firewall, services, file system)

**Symbol Key**
- EVENTS
- DETECTION POINTS
- EVENT MANAGER
- REPORTING CLIENT
- RESPONSES
- EVENT ANALYSIS ENGINE
- EVENT STORE
- ATTACK STORE
# Chapter 23: Ensnare for Ruby

<table>
<thead>
<tr>
<th>Client</th>
<th>Network</th>
<th>Perimeter Network Devices</th>
<th>Web/Application</th>
<th>Data Tier</th>
</tr>
</thead>
<tbody>
<tr>
<td>(e.g. web browser, mobile device/app, another application)</td>
<td>(e.g. internet, VPN, internal network)</td>
<td>(e.g. routers, network firewalls, load balancers)</td>
<td>(e.g. web servers, application servers, application)</td>
<td>(e.g. database servers)</td>
</tr>
</tbody>
</table>

**Symbol Key**
- **Events**
- **Detection Points**
- **Event Manager**
- **Reporting Client**
- **Responses**
- **Event Analysis Engine**
- **Event Store**
- **Attack Store**
Chapter 24: Invocation of AppSensor Code Using Jni4Net

<table>
<thead>
<tr>
<th>Client (e.g. web browser, mobile device/app, another application)</th>
<th>Network (e.g. internet, VPN, internal network)</th>
<th>Perimeter Network Devices (e.g. routers, network firewalls, load balancers)</th>
<th>Web/Application Tier (e.g. web servers, application servers, .Net application, AppSensor WS)</th>
<th>Data Tier (e.g. database servers)</th>
</tr>
</thead>
</table>

![Diagram showing network flow and interactions between different tiers and components]

**Symbol Key:***
- EVENTS
- DETECTION POINTS
- EVENT MANAGER
- REPORTING CLIENT
- RESPONSES
- EVENT ANALYSIS ENGINE
- EVENT STORE
- ATTACK STORE
# Chapter 25: Using an External Log Management System

<table>
<thead>
<tr>
<th>Client (e.g. web browser, mobile device/app, desktop application, another application)</th>
<th>Network (e.g. internet, VPN, internal network)</th>
<th>Perimeter Network Devices (e.g. routers, network firewalls, load balancers)</th>
<th>Web/Application Tier (e.g. web servers, application servers, application)</th>
<th>Data Tier (e.g. database servers)</th>
</tr>
</thead>
</table>

![Diagram]

**Symbol Key**
- Events
- Detection Points
- Event Manager
- Reporting Client
- Responses
- Event Analysis Engine
- Event Store
- Attack Store

Logging aggregation and event management
Chapter 26: Leveraging a Web Application Firewall

<table>
<thead>
<tr>
<th>Client</th>
<th>Network</th>
<th>Perimeter Network Devices</th>
<th>Web Application Firewall</th>
<th>Web/Application Tier (e.g. web servers, application servers, applications)</th>
<th>Data Tier (e.g. database servers)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(e.g. web browser, mobile device/app, another application)</td>
<td>(e.g. internet, VPN, internal network)</td>
<td>(e.g. routers, network firewalls, load balancers)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Symbol Key*

- **Events**
- **Detection Points**
- **Event Manager**
- **Reporting Client**
- **Responses**
- **Event Analysis Engine**
- **Event Store**
- **Attack Store**

*Diagram Illustration*

- **Host** (e.g. operating system, services, file system)
- **Console**
Detecting malicious use
Human error

- Unacceptable
  - Reject
- Acceptable
  - Ask for Re-entry
  - Accept but Sanitize
  - Accept
Inhuman behaviour

Unacceptable

Form RADIO BUTTON element item value is not a positive, non zero integer

Form TEXT element account code is a string, but is the wrong format

Form TEXT element phone number value contains a hyphen character

Acceptable

Form TEXT element password value has trailing white space
Inhuman behaviour in a different context

- Form TEXT element phone number value contains a hyphen character
- Form TEXT element account code is a string, but is the wrong format
- Form RADIO BUTTON element item value is not a positive, non-zero integer
- Form TEXT element password value has trailing white space
Live demo

- A hotel lift

* Welcome to the Hotel Lift Control Program menu *

15:13:52 hrs on Wednesday 14 May 2014

Choices available to you
F  - Go to floor "n"
    As a guest you have access to accommodation floors 3, 4 & 5 and the roof terrace on 8
M  - Display this menu again
A  - Alarm
X  - Finished

AppSensor: CIE1=0 / ACE1=0 / ACE3=0 / HT3=0
[FLOOR 0] Type selection (e.g. F5) and press ENTER: 4
[FLOOR 0] Sorry, I do not understand that, please try again

AppSensor: CIE1=0 / ACE1=0 / ACE3=1 / HT3=0
[FLOOR 0] Type selection (e.g. F5) and press ENTER: F4
[FLOOR 0] Going to floor 4...
[FLOOR 4] Arrived at floor 4

AppSensor: CIE1=0 / ACE1=0 / ACE3=1 / HT3=0
[FLOOR 4] Type selection (e.g. F5) and press ENTER: F7
[FLOOR 4] Sorry, cannot go there

AppSensor: CIE1=0 / ACE1=1 / ACE3=1 / HT3=0
[FLOOR 4] Type selection (e.g. F5) and press ENTER:
The six “best” detection point types

- Authorization failures
  (e.g. resource or action requested with insufficient privileges)

- Client-side input validation bypass
  (e.g. data format mismatch or missing mandatory values)

- Whitelist input validation failures
  (e.g. invalid data type or data length/range)

- Authentication failures
  (e.g. password change failures, re-authentication failure)

- Blatant code injection attack
  (e.g. common SQL injection strings)

- High rate of function use
  (e.g. requests/pages/views/windows per 5 minutes)
### Response types

<table>
<thead>
<tr>
<th>Category</th>
<th>Type</th>
<th>Description</th>
<th>Response ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silent</td>
<td>User</td>
<td>unaware of application's response</td>
<td>ASR-A</td>
<td>Logging Change</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ASR-B</td>
<td>Administrator Notification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ASR-C</td>
<td>Other Notification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ASR-N</td>
<td>Proxy</td>
</tr>
<tr>
<td>Passive</td>
<td>Changes</td>
<td>to user experience but nothing denied</td>
<td>ASR-D</td>
<td>User Status Change</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ASR-E</td>
<td>User Notification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ASR-F</td>
<td>Timing Change</td>
</tr>
<tr>
<td>Active</td>
<td>Application functionality reduced for user(s)</td>
<td>ASR-G</td>
<td>Process Terminated</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ASR-H</td>
<td>Function Amended</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ASR-I</td>
<td>Function Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ASR-J</td>
<td>Account Logout</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ASR-K</td>
<td>Account Lockout</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ASR-L</td>
<td>Application Disabled</td>
</tr>
<tr>
<td>Intrusive</td>
<td>User</td>
<td>environment altered</td>
<td>ASR-M</td>
<td>Collect Data from User</td>
</tr>
</tbody>
</table>
What does your attacker dashboard look like?

Not AppSensor:
Detection, analysis and response all completed

With AppSensor:

AppSensor Dashboards > Supplier Portal
Detection, analysis and response all completed

With AppSensor:

[Image of AppSensor Dashboard showing a notification]

12:26:03 **Mr Joey Smith** attempted to access an account belonging to someone else.
Detection, analysis and response all completed

With AppSensor:

12:26:03 **Mr Joey Smith** attempted to access an account belonging to someone else.

Transactional functionality has been disabled for this user.
Event notified to CRM (ID 509578). Fraud flag set in CRM.
Part II:
Illustrative Case Studies

- Chapter 5: Case Study of a Rapidly Deployed Web Application
- Chapter 6: Case Study of a Magazine’s Mobile App
- Chapter 7: Case Study of a Smart Grid Consumer Meter
- Chapter 8: Case Study of a Financial Market Trading System
- Chapter 9: Case Study of a B2C Ecommerce Website
- Chapter 10: Case Study of B2B Web Services
- Chapter 11: Case Study of a Document Management System
- Chapter 12: Case Study of a Credit Union’s Online Banking
# Case Study: Credit Union’s Online Banking 1/2

| **Background** | A credit union is redeveloping its online banking systems. It has mature software development practices where security is considered at many stages of the development lifecycle, and has made a significant investment in infrastructure protection. In the redevelopment the credit union wants to take the opportunity to build in advanced attack impact-minimizing techniques to protect the web applications. The primary concerns are customers whose own computers have been compromised by malware (e.g. Citadel, KINS, SpyEye, Zeus), and secondly other fraudulent activity. The credit union maintains data flow diagrams for each business process and has identified all the state-changing steps deemed to be higher risk. This has been complemented by an analysis of known web security incidents from other banks in order to define placement of detection points that can feed event information into an existing fraud prevention analysis engine, developed by the credit union’s statisticians and actuaries, but which currently lacks the user and context specific information available from the online customer systems. |
| **Objectives** | 1. Detect early signs of attacks  
2. React in order to minimize the impact of the attack. |
Case Study: Credit Union’s Online Banking 1/2

Detection points

<table>
<thead>
<tr>
<th>Area</th>
<th>ID Scope</th>
<th>Detection Description</th>
<th>AppSensor Refs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td>- Every request</td>
<td>Usage of a process step</td>
<td>UT1</td>
</tr>
<tr>
<td></td>
<td>- Every request</td>
<td>Per-request token integrity check</td>
<td>IE4</td>
</tr>
<tr>
<td></td>
<td>- Every request</td>
<td>Known trojanized browser attack</td>
<td>IE3</td>
</tr>
<tr>
<td>Reputation</td>
<td>- Every request</td>
<td>Address, IP and card blacklists</td>
<td>RP2</td>
</tr>
<tr>
<td></td>
<td>- Each session</td>
<td>Customer profiling</td>
<td>RP2</td>
</tr>
<tr>
<td></td>
<td>- Each session</td>
<td>Third party fraud scoring</td>
<td>RP2</td>
</tr>
</tbody>
</table>

The events are sent to the centralized fraud analysis engine that uses a highly customized stochastic model to identify malicious behavior. In this case, the events recorded are not only misuse, but also per-user usage patterns.

Response actions and thresholds

<table>
<thead>
<tr>
<th>ID (from above)</th>
<th>Threshold</th>
<th>Response Description</th>
<th>AppSensor Refs</th>
</tr>
</thead>
<tbody>
<tr>
<td>(All)</td>
<td>(Probabilistic)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proceed</td>
<td></td>
<td>Proceed</td>
<td>ASR-P</td>
</tr>
<tr>
<td>Proceed but track</td>
<td></td>
<td>Proceed but track</td>
<td>ASR-A, ASR-D</td>
</tr>
<tr>
<td>Prevent</td>
<td></td>
<td>Prevent transaction</td>
<td>ASR-G</td>
</tr>
<tr>
<td>transaction</td>
<td></td>
<td>Log user out</td>
<td>ASR-J</td>
</tr>
<tr>
<td>Flag</td>
<td></td>
<td>Flag for further investigation</td>
<td>ASR-C</td>
</tr>
<tr>
<td>Redirect</td>
<td></td>
<td>Redirect to free AV</td>
<td>ASR-E</td>
</tr>
</tbody>
</table>
Case Study: Credit Union’s Online Banking 1/2

Detection points

Request detection points are numerous and are of two main types; these are complemented by reputational data from other internal and external anti-fraud systems.

<table>
<thead>
<tr>
<th>Area</th>
<th>ID</th>
<th>Scope</th>
<th>Detection Description</th>
<th>AppSensor Refs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td>-</td>
<td>Every request</td>
<td>Usage of a process step</td>
<td>UT1</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>Every request</td>
<td>Per-request token integrity check</td>
<td>IE4</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>Every request</td>
<td>Known trojanized browser attack</td>
<td>IE3</td>
</tr>
<tr>
<td>Reputation</td>
<td>-</td>
<td>Every request</td>
<td>Address, IP and card blacklists</td>
<td>RP2</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>Each session</td>
<td>Customer profiling</td>
<td>RP2</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>Each session</td>
<td>Third party fraud scoring</td>
<td>RP2</td>
</tr>
</tbody>
</table>

The events are sent to the centralized fraud analysis engine that uses a highly customized stochastic model to identify malicious behavior. In this case, the events recorded are not only misuse, but also per-user usage patterns.

Response actions and thresholds

The response action is determined in real time at each and every detection point activation whether to allow the process to continue, or to perform some other action.

<table>
<thead>
<tr>
<th>ID (from above)</th>
<th>Threshold</th>
<th>Response Description</th>
<th>AppSensor Refs</th>
</tr>
</thead>
<tbody>
<tr>
<td>(All)</td>
<td>(Probabilistic)</td>
<td>Proceed</td>
<td>ASR-P</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Proceed but track</td>
<td>ASR-A, ASR-D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prevent transaction</td>
<td>ASR-G</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Log user out</td>
<td>ASR-J</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flag for further investigation</td>
<td>ASR-C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Redirect customer to free AV</td>
<td>ASR-E</td>
</tr>
</tbody>
</table>
Where to obtain the new guide
In your machine

- **AppSensor Guide v2.0, May 2014**
  - PDF
  - DOC
  - Source materials
    https://4ed64fe7f7e3f627b8d0-bc104063a9fe564c2d8a75b1e218477a.ssl.cf2.rackcdn.com/appsensor-guide-2v0-owasp.zip

- **Article in CrossTalk Magazine, September 2011**
AppSensor Guide
By OWASP Foundation
View this Author's Spotlight

Paperback, 203 Pages ★★★★★ (2 Ratings)

List Price: £8.55
Price: £5.13
You Save: £3.42 (40%)
Ships in 3–5 business days

The AppSensor Project defines a conceptual technology-agnostic framework and methodology that offers guidance to implement intrusion detection and automated response into software applications. This OWASP guide describes the concept, how to make it happen, and includes illustrative case studies, demonstration implementations and full reference materials.
In your hand
“In your hand” thank you

- OWASP Project Reboot Initiative 2012 (Eoin Keary)
  https://www.owasp.org/index.php/Projects_Reboot_2012

- AppSensor reboot application

  - $5,000
    - Pay for any design costs in creating a front cover for the book (10%)
    - Fund the printing (and delivery) of 250 copies of the book, which can be used by project participants as prizes or giveaways during AppSensor presentations at OWASP chapter meetings, OWASP conferences and related events (60%)
    - Pay for the layout and printing of flyers to promote the project and book in conference bags (30%)
Thank you to the guide's creators

Version 2.0
Lead Author

Colin Watson

Co-Authors

Dennis Groves    John Melton

Other Contributors, Editors and Reviewers

Josh Amishav-Zlatin    Ryan Barnett    Michael Coates    Craig Munson    Jay Reynolds

Version 1
Author

Michael Coates
### Thank you to the project's contributors

<table>
<thead>
<tr>
<th>Name</th>
<th>Name</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Josh Amishav-Zlatin</td>
<td>Erlend Oftedal</td>
<td>Craig Munson</td>
</tr>
<tr>
<td>Ryan Barnett</td>
<td>Sean Fay</td>
<td>Giri Nambari</td>
</tr>
<tr>
<td>Simon Bennetts</td>
<td>Dennis Groves</td>
<td>Jay Reynolds</td>
</tr>
<tr>
<td>Joe Bernik</td>
<td>Randy Janida</td>
<td>Chris Schmidt</td>
</tr>
<tr>
<td>Rex Booth</td>
<td>Chetan Karande</td>
<td>Sahil Shah</td>
</tr>
<tr>
<td>Luke Briner</td>
<td>Eoin Keary</td>
<td>Eric Sheridan</td>
</tr>
<tr>
<td>Rauf Butt</td>
<td>Alex Lauerman</td>
<td>John Steven</td>
</tr>
<tr>
<td>Fabio Cerullo</td>
<td>Junior Lazuardi</td>
<td>Alex Thissen</td>
</tr>
<tr>
<td>Marc Chisinevski</td>
<td>Jason Li</td>
<td>Don Thomas</td>
</tr>
<tr>
<td>Robert Chojnacki</td>
<td>Manuel López Arredondo</td>
<td>Christopher Tidball</td>
</tr>
<tr>
<td>Michael Coates</td>
<td>Bob Maier</td>
<td>Kevin W Wall</td>
</tr>
<tr>
<td>Dinis Cruz</td>
<td>Jim Manico</td>
<td>Colin Watson</td>
</tr>
<tr>
<td>August Detlefsen</td>
<td>Sherif Mansour Farag</td>
<td>Mehmet Yilmaz</td>
</tr>
<tr>
<td>Ryan Dewhurst</td>
<td>John Melton</td>
<td></td>
</tr>
</tbody>
</table>
Thank you, the audience

- Use the concept
- Tweet and blog about the AppSensor Project and the new guide
- Create a Lulu.com account
  - Rate the guide
  - Review it

@AppSensor

https://www.owasp.org/index.php/AppSensor
Take aways

- Don't ever offer to write a book
- Every AppSensor instance is different
- AppSensor can be as simple or complex as you choose
Your speaker

Colin Watson

Watson Hall Ltd

https://www.watsonhall.com
colin@watsonhall.com
020 7183 3710