OWASP AppSensor, The Future of Application Security
OWASP AppSensor
The Future of Application Security

Dennis Groves, MSc

dennis.groves@owasp.org

February 17, 2013
Contents

Who am I?

Security Management

Security Operations

OWASP AppSensor

Bibliography
Who am I?

Security Management

Security Operations

OWASP AppSensor

Bibliography
About Me
What is my Bloodtype?

0
+POS+
"There are known knowns; there are things we know that we know. There are known unknowns; that is to say there are things that, we now know we don’t know. But there are also unknown unknowns – there are things we do not know we don’t know."
<table>
<thead>
<tr>
<th>Known Knowns</th>
<th>Unknown Knowns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known Unknowns</td>
<td>Unknown Unknowns</td>
</tr>
</tbody>
</table>
"It ain’t what you don’t know that gets you into trouble. It’s what you know for sure that just ain’t so.”
Who am I?

Security Management

Security Operations

OWASP AppSensor

Bibliography
A Risk Based Approach

Risk

The probable frequency and probable magnitude of future loss

\[
Risk = P(Impact)
\]  

(1)
A Brief History of Risk

\[ \text{Risk} = P(\text{Impact} \ast \text{Vulnerability}) \]  \hspace{1cm} (2)
A Brief History of Risk

\begin{align*}
Risk &= P(Impact \ast Vulnerability) \quad (2) \\
Risk &= Impact \ast Vulnerability \ast Threat \quad (3)
\end{align*}
A Brief History of Risk

\[ Risk = P(Impact \ast Vulnerability) \] 
\[ (2) \]

\[ Risk = Impact \ast Vulnerability \ast Threat \] 
\[ (3) \]

\[ Risk = P(Impact \ast Vulnerability \ast Threat) \] 
\[ (4) \]
A Brief History of Risk

\[
Risk = P(Impact \times Vulnerability) \quad (2)
\]

\[
Risk = Impact \times Vulnerability \times Threat \quad (3)
\]

\[
Risk = P(Impact \times Vulnerability \times Threat) \quad (4)
\]

\[
Risk = \frac{Impact \times Vulnerability \times Threat}{Countermeasures} \quad (5)
\]
A Brief History of Risk

\[ Risk = P(Impact \ast Vulnerability) \] (2)

\[ Risk = Impact \ast Vulnerability \ast Threat \] (3)

\[ Risk = P(Impact \ast Vulnerability \ast Threat) \] (4)

\[ Risk = \frac{Impact \ast Vulnerability \ast Threat}{Countermeasures} \] (5)

\[ Risk = Impact \ast \frac{P(Threat) \ast P(Vulnerability)}{Countermeasures} \] (6)
Risk Treatments

- Tolerate: Do nothing.
Risk Treatments

- Tolerate: Do nothing.
- Transfer: Outsource the risk.
Risk Treatments

- **Tolerate:** Do nothing.
- **Transfer:** Outsource the risk.
- **Terminate:** Eliminate the asset.
Risk Treatments

- Tolerate: Do nothing.
- Transfer: Outsource the risk.
- Terminate: Eliminate the asset.
- Treat: Reduce the risk.
Risk Reduction Methods

- Reduce the probability of a threat.
Risk Reduction Methods

- Reduce the probability of a threat.
- Reduce the probability of a vulnerability.
Risk Reduction Methods

- Reduce the probability of a threat.
- Reduce the probability of a vulnerability.
- Reduce the impact of an event?
Who am I?

Security Management

Security Operations

OWASP AppSensor

Bibliography
Theorem

Protection time must be greater than or equal to detection time plus reaction time.

$$P_t \geq D_t + R_t$$ (7)
Who am I?

Security Management

Security Operations

OWASP AppSensor

Bibliography
Moving Detection & Reaction into the Application
This is a high-level overview of the concept and why it is different.
Michael Coates, Colin Watson, John Melton Ryan Barnett, Simon Bennetts, Marc Chisinevski, Robert Chonjnacki, August Detlefsen, Sean Fay, Randy Janida, Alex Lauerman, Manuel Arredondo, Bob Maier, Craig Munson, Giri Nambari, Abdul Rauf, Jay Reynolds, Eric Sheridan, John Steven, Alex Thissen, Don Thomas, Kevin Wall, Mehmet Yilmaz, Jim Manico, Dinis Cruz, myself and many, many others...
Conventional Defensive Measures

- Perimeter Defence
Conventional Defensive Measures

- Perimeter Defence
- Cryptographic Communications
Conventional Defensive Measures

- Perimeter Defence
- Cryptographic Communications
- Anti-Virus (AV)
Conventional Defensive Measures

- Perimeter Defence
- Cryptographic Communications
- Anti-Virus (AV)
- Intrusion Detection/Prevention Systems (IDS/IPS)
Perimeter Defence

- Packet Filters
Perimeter Defence

- Packet Filters
- Firewalls
Perimeter Defence

- Packet Filters
- Firewalls
- Application Layer (WAF)
SSL 1.0 - 2.0 - 3.0
Cryptographic Communications

- SSL 1.0 - 2.0 - 3.0
- TLS 1.0 - 1.1 - 1.2
The system is already compromised!
The system is already compromised!

\[ P_t \geq D_t + R_t \]
Anti-Virus

- The system is already compromised!

\[ P_t \geq D_t + R_t \] (8)

- Anti-Virus is the same as giving up. ;)

Anti-Virus
Intrusion Detection/Prevention Systems

- Host Based - Tripwire etc.
Intrusion Detection/Prevention Systems

- Host Based - Tripwire etc..
- Network Based - Snort etc.
Intrusion Detection/Prevention Systems

- Host Based - Tripwire etc..
- Network Based - Snort etc..
- Application Based - OWASP AppSensor
Application Defensive Measures

- Attack-Aware Detection
Application Defensive Measures

- Attack-Aware Detection
- Normal and Malicious Behavior
Application Defensive Measures

- Attack-Aware Detection
- Normal and Malicious Behavior
- Evasion and Unknown Attacks
## AppSensor Detection Points

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>RE</td>
<td>Request Exceptions</td>
</tr>
<tr>
<td></td>
<td>AE</td>
<td>Authentication Exceptions</td>
</tr>
<tr>
<td></td>
<td>SE</td>
<td>Session Exceptions</td>
</tr>
<tr>
<td></td>
<td>ACE</td>
<td>Access Control Exceptions</td>
</tr>
<tr>
<td></td>
<td>IE</td>
<td>Input Exceptions</td>
</tr>
<tr>
<td></td>
<td>EE</td>
<td>Encoding Exceptions</td>
</tr>
<tr>
<td></td>
<td>CIE</td>
<td>Command Injection Exceptions</td>
</tr>
<tr>
<td></td>
<td>FIO</td>
<td>File IO Exceptions</td>
</tr>
<tr>
<td></td>
<td>HT</td>
<td>Honey Trap</td>
</tr>
<tr>
<td>Behavioural</td>
<td>UTE</td>
<td>User Trend Exceptions</td>
</tr>
<tr>
<td></td>
<td>STE</td>
<td>System Trend Exceptions</td>
</tr>
<tr>
<td></td>
<td>RP</td>
<td>Reputation</td>
</tr>
</tbody>
</table>
### AppSensor Rich Response

<table>
<thead>
<tr>
<th>Response Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Change</td>
<td>Full stack trace of error messages logged&lt;br&gt;Record DNS data on user’s IP address</td>
</tr>
<tr>
<td>Account Logout</td>
<td>Session terminated and user redirected&lt;br&gt;Session terminated only (no redirect)</td>
</tr>
<tr>
<td>Account Lockout</td>
<td>User account locked permanently&lt;br&gt;One user’s IP address range blocked</td>
</tr>
<tr>
<td>Application Disabled</td>
<td>Website shut down and replaced with static page&lt;br&gt;Application taken offline</td>
</tr>
</tbody>
</table>
This is the set of chapters that is of interest to Management. Why do they want an OWASP AppSensor and what is the set of actions they need to put in place to instantiate the OWASP AppSensor.
Design

This is the set of chapters that is of interest to Software Architects. What are the various requirements for an OWASP AppSensor and what the design trade-offs in different deployment configurations of the OWASP AppSensor.
This is the set of chapters that is of interest to Software Engineers (Developers). What is required for a developer to develop an OWASP AppSensor. Additionally, I imagine this is also about how to test the code to verify that it manages the exceptions as required
This is the set of chapters that is of interest to Operations. How do you deploy, tune and configure the OWASP AppSensor?
Future AppSensor Developments

- AppSensor-core
Future AppSensor Developments

- AppSensor-core
- AppSensor-ws-soap
Future AppSensor Developments

- AppSensor-core
- AppSensor-ws-soap
- AppSensor-ws-rest
Future AppSensor Developments

- AppSensor-core
- AppSensor-ws-soap
- AppSensor-ws-rest
- AppSensor Handbook
How Can You Help?

- Join the Mailing List and Participate
- Help us develop reference implementations
- Tell your friends, and employers
Bibliography

Who am I?

Security Management

Security Operations

OWASP AppSensor

Bibliography
Thank You!

Please send feedback to dennis.groves@owasp.org

- What did you like most?
Thank You!

Please send feedback to dennis.groves@owasp.org

- What did you like most?
- What did you like least?
Thank You!

Please send feedback to dennis.groves@owasp.org

- What did you like most?
- What did you like least?
- What can be improved?