Open Web Application Security Project (OWASP)

AppSensor - Response Actions

V0.9 - 3rd August 2011

Colin Watson
Based on original ideas by Michael Coates and with contributions from John Melton, Ryan Barnett and Don Thomas.

Responses

The AppSensor book v1.1 identified response actions: "Security Violation Message", "Account Logout", "Account Lockout" and "Administrator Notification". "Function Disabled" and "Application Disabled" are also mentioned.

Further discussion of new detection points and alternative responses on the project's mailing list has broadened the range of response actions. The responses are all defensive, rather than offensive, but may be categorised by whether the user is aware of any changes, whether process are altered but may still be completed, or whether other changes are made to the process to alter its functionality or disable it.

"Security Violation Message" might be seen as a user notification and has been renamed. Thus if we include messages sent to other systems (e.g. SIEM, network firewall) we have three types of notification: user, administrator and other.

Table 1: AppSensor Responses
Listed by category, then alphabetically by ID

Category		Response	
Type	Description	ID	Description
Silent	User unaware of application's response	ASR-A	Logging Change
		ASR-B	Administrator Notification
		ASR-C	Other Notification
		ASR-N	Proxy
Passive	Changes to user experience but nothing denied	ASR-D	User Status Change
		ASR-E	User Notification
		ASR-F	Timing Change
Active	Application functionality reduced for user(s)	ASR-G	Process Terminated
		ASR-H	Function Amended
		ASR-I	Function Disabled
		ASR-J	Account Logout
		ASR-K	Account Lockout
		ASR-L	Application Disabled
Intrusive	User's environment altered	ASR-M	Collect Data from User

Additionally, ASR-P means “No Response”, and ASR-Q to Z are undefined. Examples are shown in the following table.

Table 2: Examples for each AppSensor Response
Listed alphabetically by ID

Response ID	Description	Examples
ASR-A	Logging Change	Capture sanitised request headers and response bodies Full stack trace of error messages logged Record DNS data on user's IP address Security logging level changed to include 'informational' messages
ASR-B	Administrator Notification	Email alert sent to everyone in the administration team SMS alert sent to the on-call administrator Visual indicator on application monitoring dashboard Audible alarm in control room
ASR-C	Other Notification	Broadcast event to SIEM Signal sent to upstream network firewall, application firewall (e.g. XML, web) or load balancer Alert sent to fraud protection department Record added to server event log Event highlighted in daily management report Email alert t sent to staff member's manager Proactive entry added to customer support system
ASR-D	User Status Change	Internal trustworthiness scoring about the user changed Reduce payment transfer limit before additional out-of-band verification is required Reduce maximum file size limit for each file upload by the forum user Increase data validation strictness for all form submissions by this citizen Reduce number of failed authentication attempts allowed before the user's account is locked (ASR-K below)
ASR-E	User Notification	On-screen message about mandatory form fields On-screen message about data validation issues Message sent by email to the registered email address to inform them their password has been changed
ASR-F	Timing Change	Extend response time for each failed authentication attempt File upload process duration extended artificially Add fixed time delay into every response Order flagged for manual checking Goods despatch put on hold (e.g. despatch status changed)
ASR-G	Process Terminated	Discard data, display message and force user to begin business process from start Redirection of an unauthenticated user to the log-in page Redirection to home page Display other content (i.e. terminate process but display the output of some other page without redirect) Redirection to a page on another website
ASR-H	Function Amended	Limit on feature usage rate imposed Reduce number of times/day the user can submit a review Additional registration validation steps Additional anti-automation measures (e.g. out-of-band verification activated, CAPTCHA introduced) Static rather than dynamic content returned Additional validation requirements for delivery address Watermarks added to pages, images and other content
ASR-I	Function Disabled	'Add friend' feature inactivated 'Recommend to a colleague' feature links removed and disabled Document library search disabled Prevent new site registrations Web service inactivated Content syndication stopped Automated Direct Debit system turned off and manual form offered instead
ASR-J	Account Logout	Session terminated and user redirected to logged-out message page Session terminated only (no redirect)
ASR-K	Account Lockout	User account locked for 10 minutes User account locked permanently until an Administrator resets it One user's IP address range blocked Unauthenticated user's session terminated
ASR-L	Application Disabled	Website shut down and replaced with temporary static page Application taken offline
ASR-M	Collect Data from User	Deploy additional browser fingerprinting using JavaScript in responses Deploy a Java applet to collect remote IP address Deploy JavaScript to collect information about the user's network
ASR-N	Proxy	Requests from the user invisibly passed through to a hardened system Request are proxied to a special honeypot system which closely mimics or has identical user functionality
ASR-P	No Response	A detection point fired, but the threshold for any other response has not been reached

Classifications

All the current responses are generally reactive responses—they are the result of some user activity identified by the AppSensor detection points. Where the user's status is altered, time delays are introduced or the function amended (ASR-D, ASD-F and ASR-H), these may also be considered pro-active actions to control against future attacks.

The following table shows classifications based on purpose (logging, notifying,disrupting and blocking), whether the target of the response is an individual user, more than one or the all users of the system, and whether the response action is instantaneous only (e.g. alert email to administrator), occurs for a finite duration (e.g. temporary account lock-out) or might be considered relatively permanent from the application's point of view (e.g. permanent lock-out, application disabled).

Table 3: Some AppSensor Response Action Classifications
Listed alphabetically by ID

● indicates 'always' and ○ 'sometimes'

Response		Classification								
		Purpose				Target User		Response Duration		
ID	Description	Logging	Notifying	Disrupting	Blocking	One	All	Instantaneous	Period	Permanent
ASR-A	Logging Change	●				●	○	○	○	
ASR-B	Administrator Notification	●	●			●	●	●		
ASR-C	Other Notification	●	●			●		●		
ASR-D	User Status Change	●				●			●	
ASR-E	User Notification	●	●	●		●		●		
ASR-F	Timing Change	●		●		●	○	○	○	
ASR-G	Process Terminated	●	○	●		●		●		
ASR-H	Function Amended	●	○	●	●	●	○		●	○
ASR-I	Function Disabled	●	○	●	●	●	○		●	○
ASR-J	Account Logout	●	○	●	●	●		●		
ASR-K	Account Lockout	●	○	●	●	●			●	○
ASR-L	Application Disabled	●	○	●	●		●			●
ASR-M	Collect Data from User	●				●			●	
ASR-N	Proxy	●				●	○		●	○

Other classifications may be more suitable in other circumstances.

Classifications are not applicable for ASR-P (No Response).

Severity

The ranking of severity is highly dependent upon the business impact, and thus this is organisation dependent. For example taking one application offline may be more critical to the business than another.

Severity may be based on a scale of 0 (emergency), 1 (alert), ... to 7(debug) like that used in the Syslog Protocol:

> RFC 5424, The Syslog Protocol, IETF, March 2009
> http://tools.ietf.org/html/rfc5424

The severity levels used by an application are application and organisation-specific, but one idea is illustrated below

Table 4: Possible Application Severity Levels

Code	Syslog Message Severity	Application Equivalent
0	Emergency: system is unusable	Application unavailable for all users
1	Alert: action must be taken immediately	Function unavailable for all users
2	Critical: critical conditions	Function or application unavailable to a single user
3	Error: error conditions	Other security events (not included in codes 0, 1, 2 or 4)
4	Warning: warning conditions	A security event but user allowed to continue
5	Notice: normal but significant condition	Normal, but special, expected user event
6	Informational: informational messages	Normal expected user behaviour
7	Debug: debug-level messages	Greater granularity for above

These can then be used to provide an approximate severity rating for AppSensor responses. The logging and notifying types of response need to be tailored to the particular event.

Table 5: Guide to AppSensor Response Severity Levels
Listed alphabetically by ID

Response ID	Description	Severity Level(s)	Notes
ASR-A	Logging Change	0 - 4	Specific response may be more urgent/greater for higher severity level
ASR-B	Administrator Notification	0 - 5	(notes as for ASR-A)
ASR-C	Other Notification	0 - 3	(notes as for ASR-A)
ASR-D	User Status Change	3	
ASR-E	User Notification	0 - 4	(notes as for ASR-A)
ASR-F	Timing Change	4	
ASR-G	Process Terminated	4	
ASR-H	Function Amended	3	
ASR-I	Function Disabled	1 or 2	Depending whether all users are affected, or just a single user
ASR-J	Account Logout	3	
ASR-K	Account Lockout	2	
ASR-L	Application Disabled	0	
ASR-M	Collect Data from User	4	
ASR-N	Proxy	1 or 2	(notes as for ASR-I)
ASR-P	No Response	4	

Further information

OWASP AppSensor project

- Home page
  http://www.owasp.org/index.php/Category:OWASP_AppSensor_Project
- Detection points
  http://www.owasp.org/index.php/AppSensor_DetectionPoints

Mailing lists

- General project matters
  https://lists.owasp.org/mailman/listinfo/owasp-appsensor-project
- Code development
  https://lists.owasp.org/mailman/listinfo/owasp-appsensor-dev

Licensing