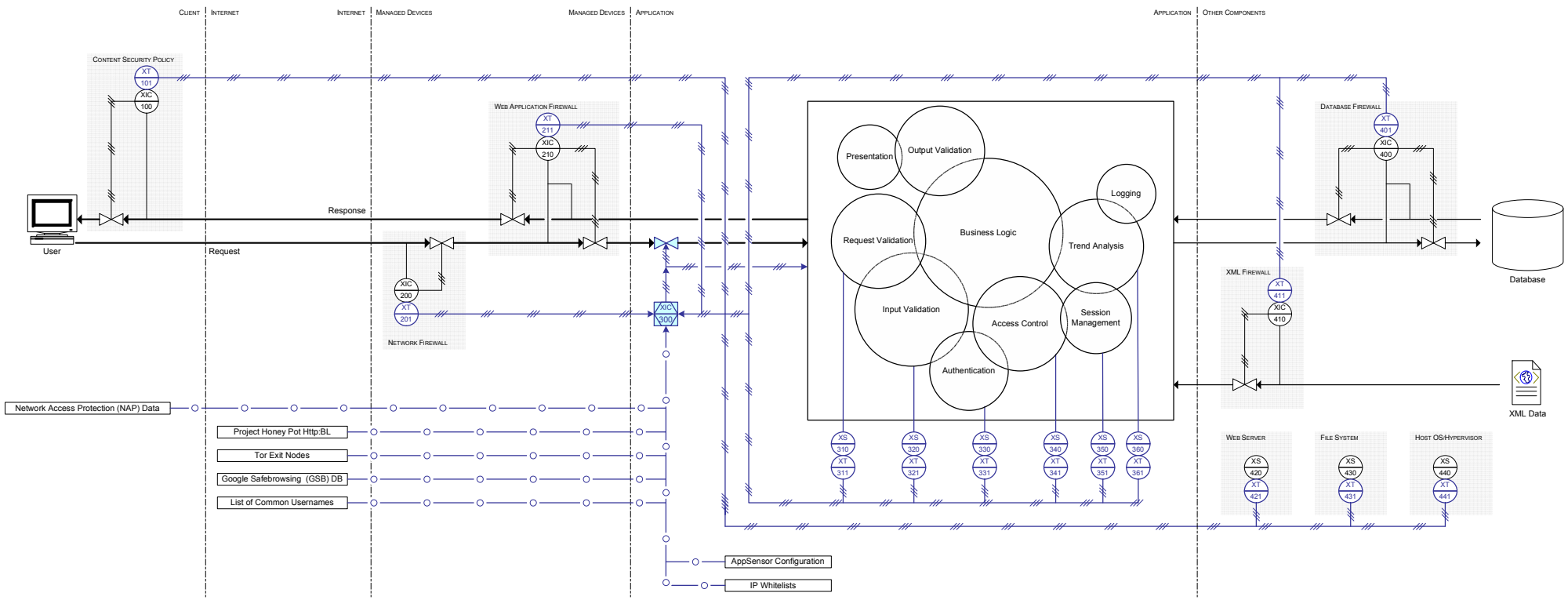
OWASP AppSensor Project

Schematic arrangement of example sensors, in the style of a process piping and instrumentation diagram (P&ID)



Key

- Instrument, X=property being measured, ?=function C[ontroller], I[ndicator], S[ensor], T[ransmitter]
- Computer Instrument
- Control Point (e.g. restriction, prevention)
- AppSensor Controller
- Other AppSensor Component
- Other Application Component
- Application Data
- Information Feed
- Control/Message Signal
- Network Boundary

ID	Description	Method
100	Content security policy (CSP) enforcement by browser	-
101	Transmission of CSP violations back to host	XML Report via HTTP POST
200	Network firewall enforcing rules	-
201	Transmission of firewall violations to AppSensor	E.g. logs or HTTP POST
210	Web application firewall detecting/enforcing rules	-
211	Transmission of results to AppSensor	E.g. logs, HTTP header or HTTP POST
300	AppSensor controller	-
310	Request validation sensor	RE1-4
311	Transmission	-
320	Input, encoding, injection and file IO sensor	IE1-2, EE1-2, CIE1-4, FIO1-2
321	Transmission	-
330	Authentication sensor	AE1-11
331	Transmission	-
340	Access control sensor	ACE1-4
341	Transmission	-

ID	Description	Method
350	Session management sensor	SE1-6
351	Transmission	-
360	Behaviour sensor	UT1-4, STE1-3
361	Transmission	-
400	Database firewall detecting/enforcing rules	-
401	Transmission of results to AppSensor	E.g. logs or HTTP POST
410	XML feed firewall detecting/enforcing rules	-
411	Transmission of results to AppSensor	E.g. logs or HTTP POST
420	Web server monitoring	E.g. HTTP request log file analysis
421	Transmission of results to AppSensor	E.g. logs
430	File system monitoring	E.g. file integrity, disk usage
431	Transmission of results to AppSensor	E.g. logs or HTTP POST
440	Host operating system/hypervisor monitoring	E.g. system logs, host IDS, anti-malware
441	Transmission of results to AppSensor	E.g. logs

Created for the OWASP AppSensor Project by Colin Watson, Watson Hall Ltd, http://www.watsonhall.com

Version 1.3 (14 December 2009)

OWASP AppSensor Project

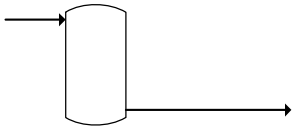
Notes on use of P&ID

Introduction to the symbolisation

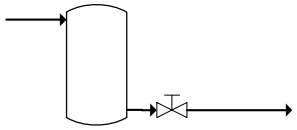
Piping and instrumentation diagrams (P&IDs) are a medium-scale view of the components of a physical process such as a batch or continuous chemical manufacturing plant. The OWASP AppSensor Project's concept of sensors embedded through a web application gave the idea of laying out an application system in the style of process diagram with its associated vessels (hardware and software assets), pipes (data flows) and instrumentation (monitoring and controls). A couple of examples will help explain P&IDs and how this has been translated into the web application world.

Example A: Process diagram

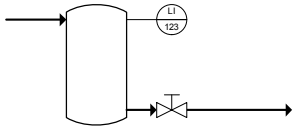
1. A vessel with an input and output pipe might be represented like this:



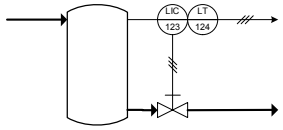
2. It may have a valve on the outlet to control the discharge:



3. We show a level (L) gauge that has a local display/indicator (I) like this, and give it an identity “123”:



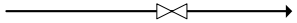
4. This could be converted into a controller (C) of the valve and also transmit (T) the level data further away (e.g. a control room):



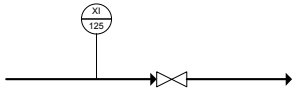
Example B: Web application diagram

1. In this case, we can look at a single application data flow or connection:

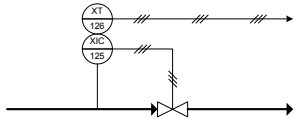
2. We could show a security control point in a similar way to the valve - this could be used to alter or block the data flow:



3. We could monitor some general characteristic (X) and provide a display indicator (I) with its own identity “125”:



4. This could be converted into a controller (C) of the data flow and also transmit (T) the characteristic information elsewhere:



The control point in example B might be something like a firewall inspecting the traffic against a set of rules, or a routine validating the POST data submitted from a form, depending upon the granularity of the diagram.

Further reading and inspiration

1. OWASP AppSensor Project, http://www.owasp.org/index.php/Category:OWASP_AppSensor_Project

2. Chemical Engineering Drawing Symbols, D.G. Austin, George Godwin Limited, London, ISBN 0-7114-3318-6 or John Wiley & Sons Inc, New York, ISBN 0-470-26601-5

3. How to Read P&IDs, Control Engineering Online, Reed Business Information, http://www.controleng.com/article/275616-How_to_read_P_IDs.php

4. Piping and Instrumentation Diagram, Wikipedia, http://en.wikipedia.org/wiki/Piping_and_instrumentation_diagram