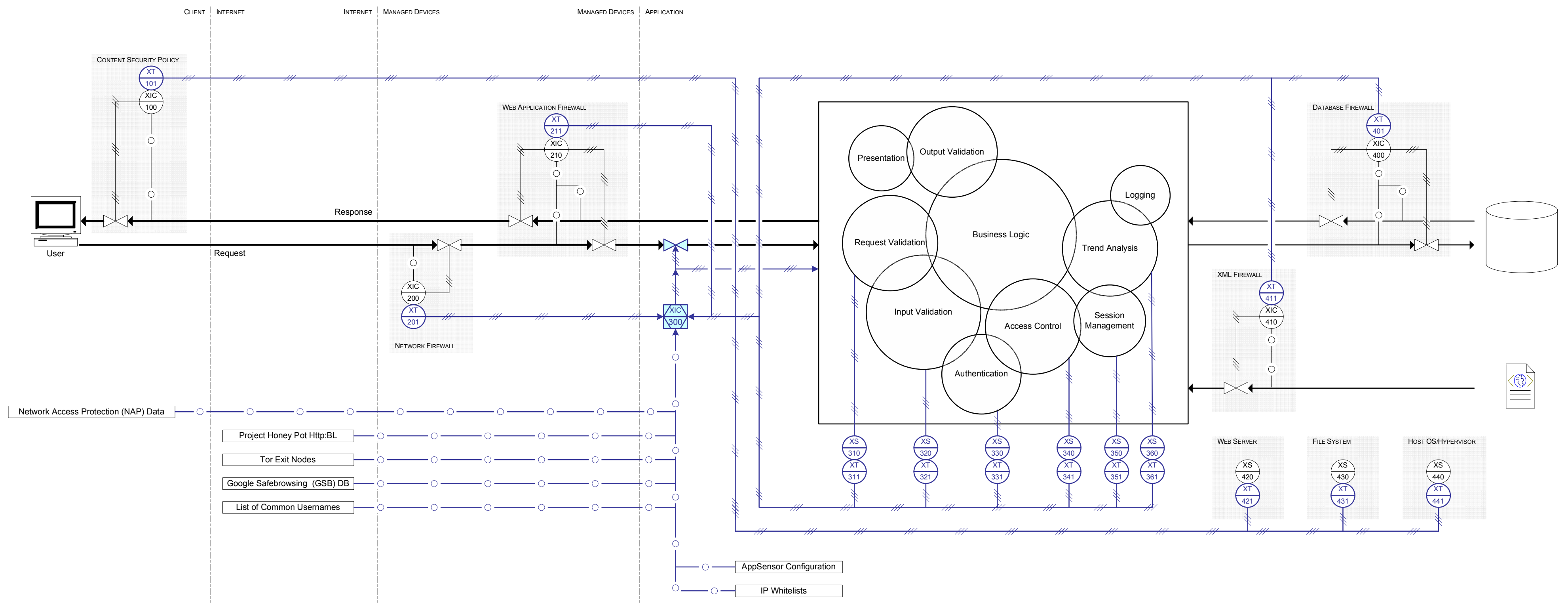
OWASP AppSensor Project

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



Key

X? nnn — Instrument, X=property being measured, ?=function C[ontroller], I[ndicator], S[ensor], T[ransmitter]

X? nnn — Computer Instrument

⋈ Control Point (e.g. restriction, prevention)

🟦 AppSensor Controller

□ Other AppSensor Component

■ Other Application Component

Application Data — Detection Signal — Control/Message Signal

Colin Watson

13 December 2009

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	-
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