Ambient Software Engineering Group (ASEG)

- Software Security Vulnerabilities Analysis Project -

Sultan S. Alqahtani, Ellis E. Eghan, Jurgen Rilling

The Problem

Are popular APIs free of security vulnerabilities?

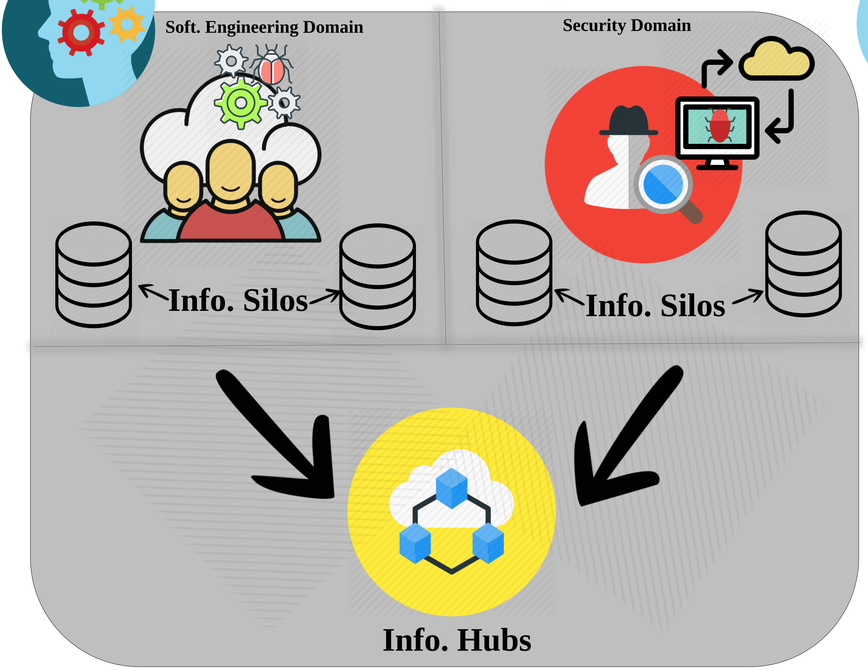
The Approach

Security Vulnerability Analysis Framework (SV-AF)

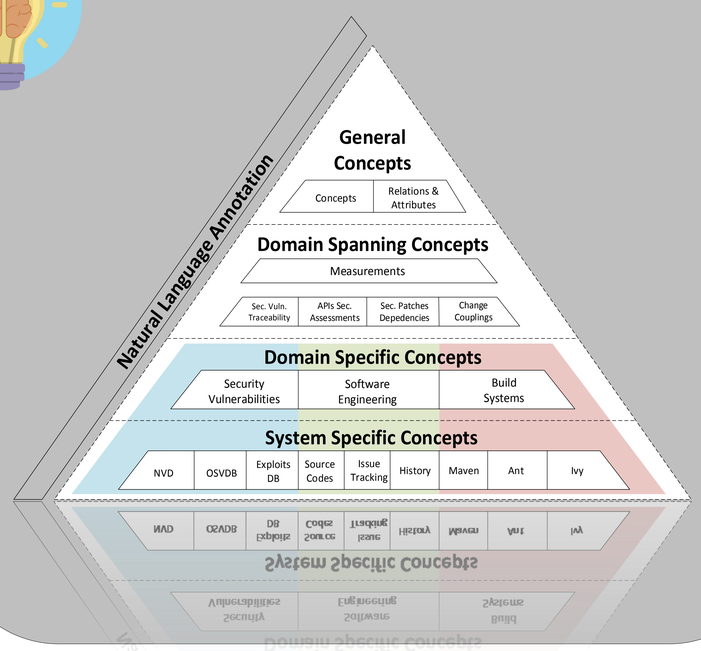
The Solution

Semantic Global Problem Scanner (SE-GPS)

SV-AF context & goals



SV-AF method



SV-AF results

Results: The studies also show that not only 750 projects in Maven affected are directly by known vulnerabilities, but also due to transitive dependencies, an additional 415604 Maven projects are potentially affected by these vulnerabilities.

Data Size	SV-AF w=0.1			OWASP		
	Precision	Recall	F1-score	Precision	Recall	F1-score
500	0.88	0.68	0.77	0.81	0.26	0.40

ID	Component Name	# Vulner-abilities	CVE-IDs	Number of dependent components based on transitivity level (L)		
				L1	L2	L3
P1	Wss4j 1.6.16	2	CVE-2015-0227 CVE-2014-3623	336	639	73
P2	Httpclient 4.1	2	CVE-2011-1498 CVE-2014-3577	685	4961	41326
P3	Derby 10.1.1.0	3	CVE-2005-4849 CVE-2006-7216 CVE-2006-7217	385	37999	66147
P4	Hibernate-validator 4.1.0.Final	1	CVE-2014-3558	3805	39295	128109
P5	Openjpa 1.1.0	1	CVE-2013-1768	74	49460	141303

Sultan S. Alqahtani, Ellis E. Eghan, Juergen Rilling, Tracing known security vulnerabilities in software repositories – A Semantic Web enabled modeling approach, Science of Computer Programming, Available online 4 February 2016, ISSN 0167-6423, http://dx.doi.org/10.1016/j.scico.2016.01.005. 28 pp. IPF: 0.71

UNIVERSITÉ Concordia UNIVERSITY