Ontology Knowledge Bases of Security Vulnerabilities, Attacks & Defenses

PIs:

- Patrick Kamongi
- Mahadevan Gomathisankaran
- Krishna M. Kavi
Today’s Agenda

• Our WiPs Intro

• Our current work in progress

• Our key contributions
(OKB): our Ontology Knowledge Base

OKB-Attacks

OKB-Vulnerabilities

OKB-Defenses

Legend:
- Concepts
- Relationships

Relationships:
- hasMitigation
- isMitigationOf
- hasExploit
- hasCounterMeasure
- isExploitOf
- isCounterMeasureOf
(OKB-Vuln): Ontology Knowledge Base for Vulnerability modeling

- OKB-Vulnerabilities
  - hasSubClass CVSS Metric
  - hasSubClass IT Product

CVSS Metric
- hasSubClass Vulnerability
  - hasDataTypeProperties
  - hasObjectProperties

IT Product
- hasSubClass Vulnerability
  - hasDataTypeProperties
  - hasObjectProperties

Vulnerability
- hasSubClass CVSS Metric
  - hasCVEID
  - hasDescription
  - CVSSMetricValues
  - hasScore
  - hasIntegrityImpact
  - hasConfidentialityImpact
  - hasAvailabilityImpact
  - hasAuthentication
  - hasAccessVector
  - hasAccessComplexity
  - CVSSMetricsOf
(OKB-Attacks): Ontology Knowledge Base for Attacks modeling

OKB-Attacks

Attacks

hasSubClass

hasDataTypeProperties

hasAuthor

hasCVEID

hasDate

hasDescription

hasFile

hasID

hasPlatform

hasPort

hasType

hasObjectProperties
(OKB-Defenses): Ontology Knowledge Base for Defenses modeling

OKB-Defenses

Mitigation

hasSubClass

Countermeasure

hasSubClass

hasDataTypeProperties

hasObjectProperties

hasCveName

hasOrganization

hasStatement

hasObjectProperties
Why use ontologies to conceptualize our security information?
Why use ontologies approach instead of taxonomies for modeling security information as it has been done in the past?
What is the key point of using security ontology knowledge bases for Vulnerability Assessment work for any given Cloud Settings?
What motivated us to generate our security Ontology Knowledge Base (OKB) using feeds from only three of our named OKBs of Vulnerabilities, Attacks and Defenses?
References


4. Web Ontology Language (OWL), http://www.w3.org/TR/owl-ref/
Thank You!