Information Security Knowledge Sharing

Do we have to reinvent the security wheel at every organization?

Dr. Stefan Fenz

Vienna University of Technology

Xylem Technologies

Background

Numerous brilliant information security knowledge sources.

ISO IEC

enisa
European Network
and Information
Security Agency

NIST National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

CSA cloud security alliance℠

Bundesamt
für Sicherheit in der
Informationstechnik

Challenges

- InfoSec knowledge sources are fragmented, not machine-readable and difficult to share because of the broad range of InfoSec domains.

- The development of an effective and efficient information security program requires the involvement of stakeholders such as end-users and senior management.

- Only a few individuals per organization keep deeper knowledge about the final information security program.

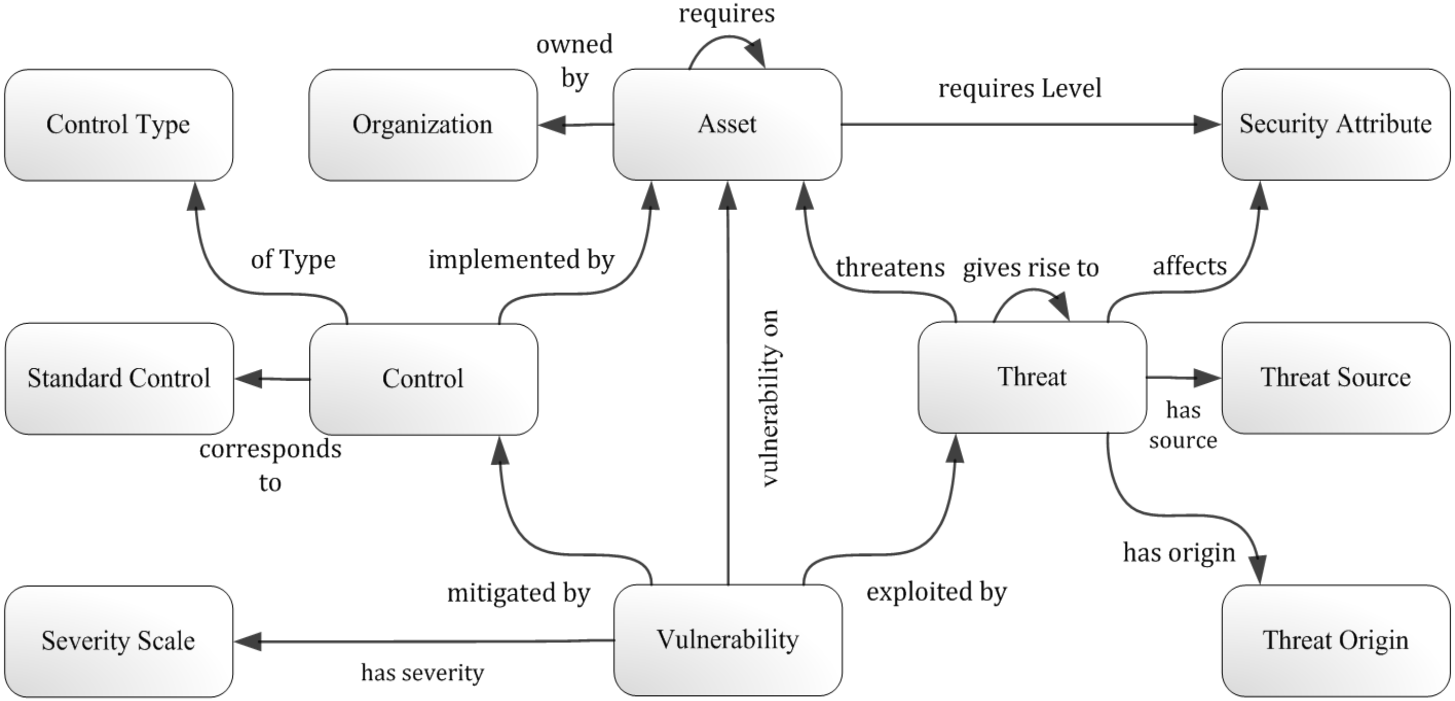
Challenges

- As a result we reinvent the security wheel at every organization and invest too much time in gathering, understanding and applying InfoSec knowledge.

To address these problems we aim at a unified and machine-readable information security knowledge sharing approach, enabling users to collaboratively understand and extend the knowledge body.

The knowledge base

- Knowledge is stored in an OWL ontology
- Content
  - Threats, Vulnerabilities, Controls, Standard Controls (ISO, GSHB, etc.)



Example: Fire threat

- threat_canBeConsequenceOf_threat: UntrainedStaffMember
- threat_givesRiseTo_threat: Smoke
- threat_exploits_vulnerability: NoFireExtinguisher
- vulnerability_mitigatedBy_control: FireExtinguisherControl
- Implementation Rule: Section AND asset_contains_asset SOME FireExtinguisher
- control_correspondsTo_standardControl: A.9.1.4 Protecting against external and environmental threats

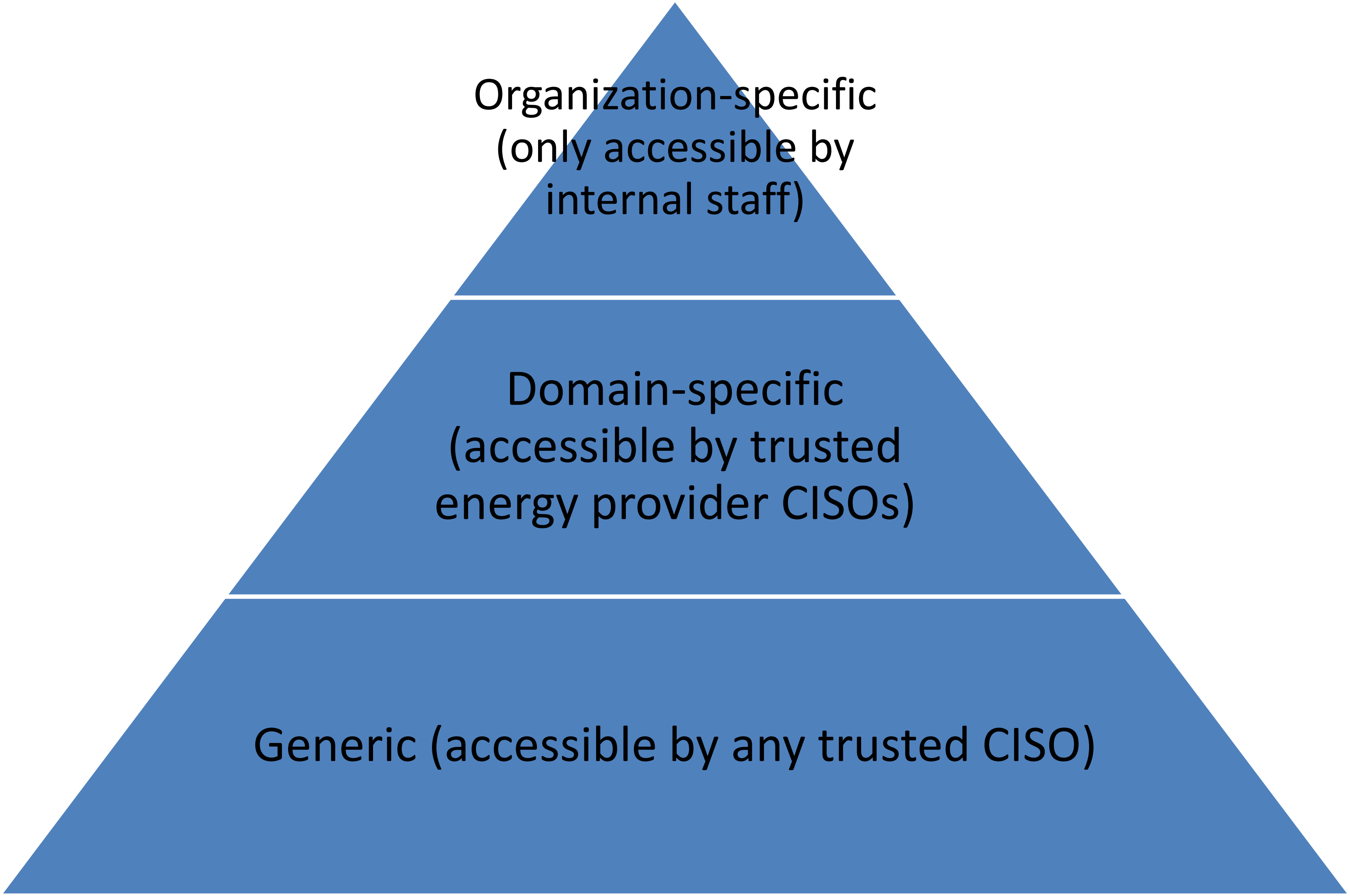
What is the benefit?

- Knowledge is machine-readable, based on common standards and thus we are able to…
  - do reasoning to create new facts based on existing facts (e.g., based on the fact that a fire extinguisher is located in a certain room the machine infers that certain controls are fulfilled)
  - Easily integrate the knowledge base with other knowledge sources (ontology import functionality)
  - Use standard editors, reasoners and storage solutions
  - Store the knowledge independent of the language
  - Use existing APIs to reuse the knowledge for risk and compliance management tools

Collaboration

- The knowledge base is not restricted to a certain organization.
- By a web-based editor knowledge is shared on a global level
- Three layers
  - Generic InfoSec knowledge: common threats (e.g., flood) and vulnerabilities
  - Domain-specific knowledge (e.g., vulnerabilities specific to wind power stations in the context of the energy production domain)
  - Organization-specific knowledge (e.g., vulnerabilities in legacy systems which are used by the own organization)

Collaboration

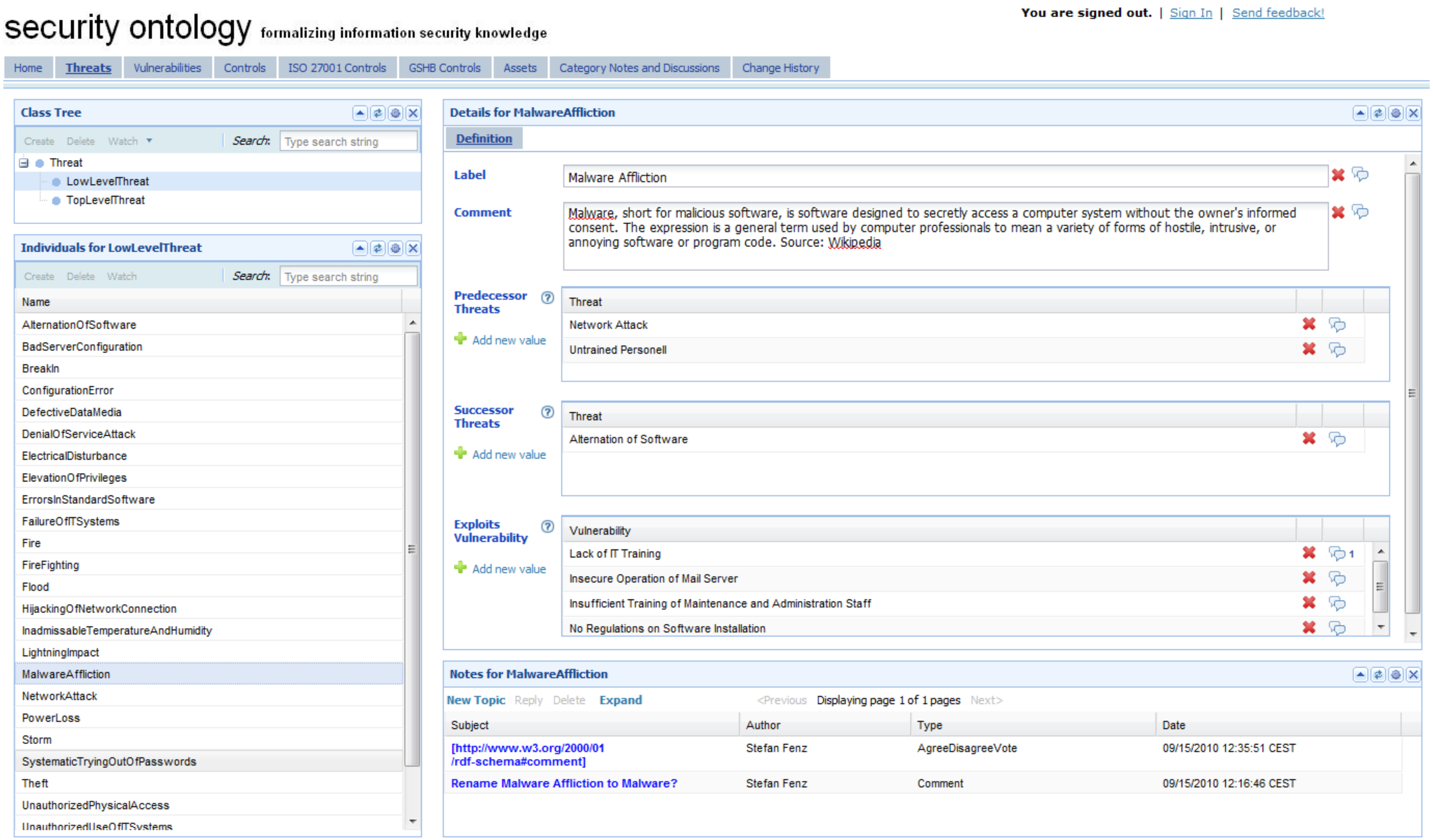


Organization-specific (only accessible by internal staff)

Domain-specific (accessible by trusted energy provider CISOs)

Generic (accessible by any trusted CISO)

Prototype



security ontology formalizing information security knowledge

You are signed out. | Sign In | Send feedback!

Class Tree

- Threat
  - LowLevelThreat
  - TopLevelThreat

Individuals for LowLevelThreat

Name
AlternationOfSoftware
BadServerConfiguration
BreakIn
ConfigurationError
DefectiveDataMedia
DenialOfServiceAttack
ElectricalDisturbance
ElevationOfPrivileges
ErrorsInStandardSoftware
FailureOfITSystems
Fire
FireFighting
Flood
HijackingOfNetworkConnection
InadmissableTemperatureAndHumidity
LightningImpact
MalwareAffliction
NetworkAttack
PowerLoss
Storm
SystematicTryingOutOfPasswords
Theft
UnauthorizedPhysicalAccess
UnauthorizedUseOfITSystems

Details for MalwareAffliction

Definition

Label: Malware Affliction

Comment: Malware, short for malicious software, is software designed to secretly access a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Source: Wikipedia

Predecessor Threats

Threat
Network Attack
Untrained Personell

Successor Threats

Threat
Alternation of Software

Exploits Vulnerability

Vulnerability	
Lack of IT Training	1
Insecure Operation of Mail Server	
Insufficient Training of Maintenance and Administration Staff	
No Regulations on Software Installation	

Notes for MalwareAffliction

New Topic Reply Delete Expand
<Previous Displaying page 1 of 1 pages Next>

Subject	Author	Type	Date
[http://www.w3.org/2000/01/rdf-schema#comment]	Stefan Fenz	AgreeDisagreeVote	09/15/2010 12:35:51 CEST
Rename Malware Affliction to Malware?	Stefan Fenz	Comment	09/15/2010 12:16:46 CEST

Collaboration benefits

- Share the knowledge maintenance effort with other trusted organizations
- Reduce the costs and increase the quality of knowledge management by decentralizing it to the relevant stakeholders
- Efficiently reuse collected knowledge in risk and compliance management activities (download functionality)
- Empower the organization to help itself and to reduce the need for costly external support

Next steps

- Establishment of a core user group in a certain domain (e.g., smart grid security)
- Definition of real-world requirements for the described knowledge sharing portal (done by the core group)
- Design and implementation of an extended prototype to address the requirements
- Attraction of additional users to join the initiative by demonstrating the business value which has been realized at the core group members.

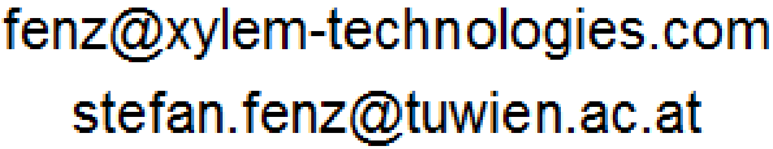
- Goal: reach critical mass to enable significant distribution of the knowledge sharing initiative and to increase the return for each participant

ENISA and Policy Context

- WPK 1.1: Identifying evolving threats, risks and challenges
  - Collaborative tool for knowledge exchange
- WPK 3.3: Regular cooperation among NIS communities

- Collaborative European approach to Network and Information security (Council Resolution 18/12/2009)
  - Quality of information handling
  - Raise awareness, good practices, and guidance

Contact



fenz@xylem-technologies.com
stefan.fenz@tuwien.ac.at