Knowledge Building and Sharing: A Metamodel for Guided Research, Learning, and Application

Kimberly Zeitz & Chris Frisina

Client: Randy Marchany
Director of the VT IT Security Lab
Prior Research Contact: Noha El Sherbiny

Blacksburg
May 6, 2013
CS6604
Motivation

• Clarify scattered field concepts
• Guide decision making
• Knowledge sharing and reuse
• Teaching and learning
• Uniform knowledge format for use and comparison
Metamodel

What is it?

- Schema for data
- Construction and organization of domain concepts
- Frames, rules, and constraints for formatting and sharing knowledge

How was it developed?

- Motivations and envisioned contributions
- Uniform Format for use with envisioned Digital Library System
- Preservation & Expansion
Metamodel

Utilization

– Organization of research for sharing knowledge

– Applications:
  • Industry application to needs
  • Academic course material organization for teachers and learning tool for students

– Stakeholders Model
Stakeholders

Practitioner
- Adds Domain Knowledge and Experience
- Provided with Case Specific Knowledge Catered Towards Needs
- Provided with Study Materials and Subject Mappings
- Adds Feedback for System Usage

Researcher
- Adds Research Findings and Artifacts
- Provided with Relevant Knowledge and Studies Past and Present
- Provided with Organizational Tool for Coursework

Learner

Teacher
- Adds Domain Resources and Course Materials
Metamodel

• Validation
  – Proof of Concept
  – Security domain concept overview
  – Preliminary Modeling with Co-occurrence Graph
  – Selected four sub areas
  – MOSAIC: Model of Securing Application Information Confidentiality
  – Further evaluation to be discussed later
## Sample Format

<table>
<thead>
<tr>
<th>Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area:</td>
</tr>
<tr>
<td>Keywords:</td>
</tr>
<tr>
<td>Pros:</td>
</tr>
<tr>
<td>-</td>
</tr>
<tr>
<td>Cons:</td>
</tr>
<tr>
<td>-</td>
</tr>
<tr>
<td>Links:</td>
</tr>
<tr>
<td>Artifacts</td>
</tr>
<tr>
<td>Usage Scenario</td>
</tr>
<tr>
<td>Examples</td>
</tr>
<tr>
<td>Studies</td>
</tr>
</tbody>
</table>
Proof of Concept

• MOSAIC: Model of Securing Application Information Confidentiality

• Scenario: Sarah has been assigned to assess the security vulnerabilities of the company's internal digital library system and propose solutions
Metamodel Information Flow

**Motivation**
- Expert Knowledge

**Metamodell Development**
- MOSAIC Guided Decision Flow
- Sample Format
  - Name:
  - Area:
  - Keywords:
  - Proc:
  - Con:
  - Link:
  - Artifacts
  - User Scenario
  - Examples
  - Studies

**Proof of Concept**
- Domain link
  - Access Controls
  - Threat Modeling
  - Data Classification

**Evaluation**
- Pertinent Information
  - AC
  - DC
  - TM
  - PIR
# Threat Modeling: Asset-centric Perspective

**Name:** Asset-centric Perspective  
**Area:** Security/MOSAIC/Threat Modeling  
**Keywords:** Threat Modeling, security

**Pros:**
- “Non-experts can typically contribute by identifying assets to focus on” - Adam Shostack  
- Helps identify things attackers want or things you want to protect.  
  - Adam Shostack

**Cons:**
- “Only experts used to structuring their thinking around assets typically benefit from this type.” - Adam Shostack.  
- No direct line from assets to threats or security steps - Adam Shostack

**Links:**
- Artifacts  
- Usage Scenario  
- Examples  
- Studies
## Threat Modeling: Attacker-centric Perspective

**Name:** Attacker-centric Perspective  
**Area:** Security/MOSAIC/Threat Modeling  
**Keywords:** Threat Modeling, security  

**Pros:**
- Generally helpful for experts, gathering less-technical input, and prioritizing efforts. -Adam Shostack  
- Useful for creating attacker personas to focus on human centered possibilities -Adam Shostack  
- Can aid in keeping track of expert knowledge gathered from experience -Adam Shostack  
- Help to make threats “real” with a who and why element -Adam Shostack

**Cons:**
- Hard to translate to what the threats mean for system security -Adam Shostack.  
- Has a tendency to evoke “no one would ever do that” when you humanize an attack -Adam Shostack  
- Can be swayed by bias of creators of personas and scenarios -Adam Shostack

**Links:**  
Artifactsc  
Usage Scenario  
Examples  
Studies
# Threat Modeling: System-centric Perspective

**Name:** System-centric Perspective  
**Area:** Security/MOSAIC/Threat Modeling  
**Keywords:** Threat Modeling, security

**Pros:**

+ Considered the “best” structured threat modeling approach - Adam Shostack  
+ Unique to the existing or envisioned software or system - Adam Shostack  
+ Can utilize existing software modeling documentation such as architecture, UML diagrams, or APIs if they are available - Adam Shostack  
+ Builds off of a common system understanding - Adam Shostack  
+ Shows the accumulating complexity of projects - Adam Shostack

**Cons:**

- You have to hope that those involved, such as developers, understand the assets and potential attackers - Adam Shostack.

**Links:**

- [Artifacts](#)  
- [Usage Scenario](#)  
- [Examples](#)  
- [Studies](#)
Evaluation

• Can conduct an IRB approved study
• Domain expert will organize course materials
• Students in class learn two units of equal difficulty
  • Unit 1: Standard text and resources
  • Unit 2: Our metamodel
• Look at student feedback and assess progress such as through student presentations or grades
Conclusion

• Metamodel for information sharing, collaboration, and learning
• Lookup and collaboration tool for researchers
• Reference and learning tool for practitioners
• Organization and modeling tool for teachers
• Learning and studying tool for students
• Need:
  – Digital Library for access and contributions
  – User participation both adding and receiving
Questions?
References

Metamodel


Access Controls


Threat Modeling

References

Data Classification


Private Information Retrieval