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?

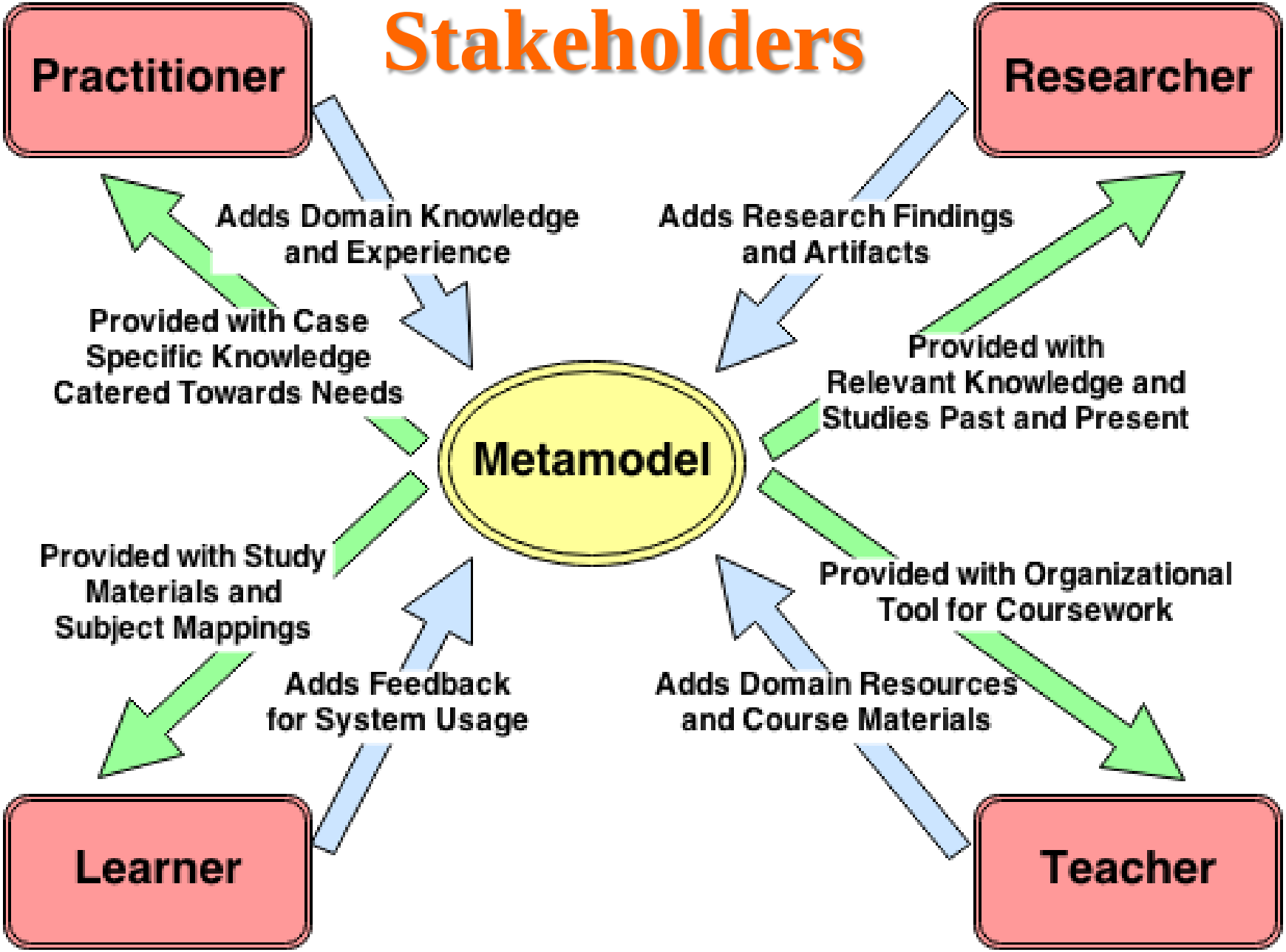
- Motivations and envisioned contributions
- Uniform Format for use with envisioned Digital Library System
- Preservation & Expansion

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



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

Metamodel Format

Sample Format

Name:
Area:
Keywords:
Pros:
+
Cons:
-
Links:
Artifacts
Usage Scenario
Examples
Studies

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

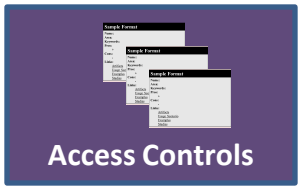
Metamodel Information Flow

Expert Knowledge

Sample Format

Name:
Area:
Keywords:
Pros:
+
Cons:
-
Links:
Artifacts
Usage Scenario
Examples
Studies

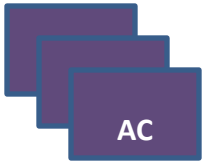
Domain link

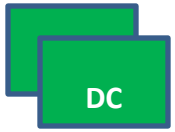


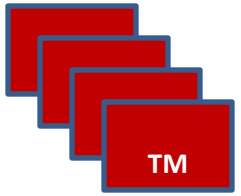
User Criteria

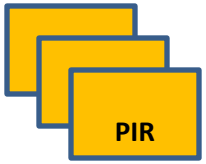
MOSAIC Guided Decision Flow

Pertinent Information

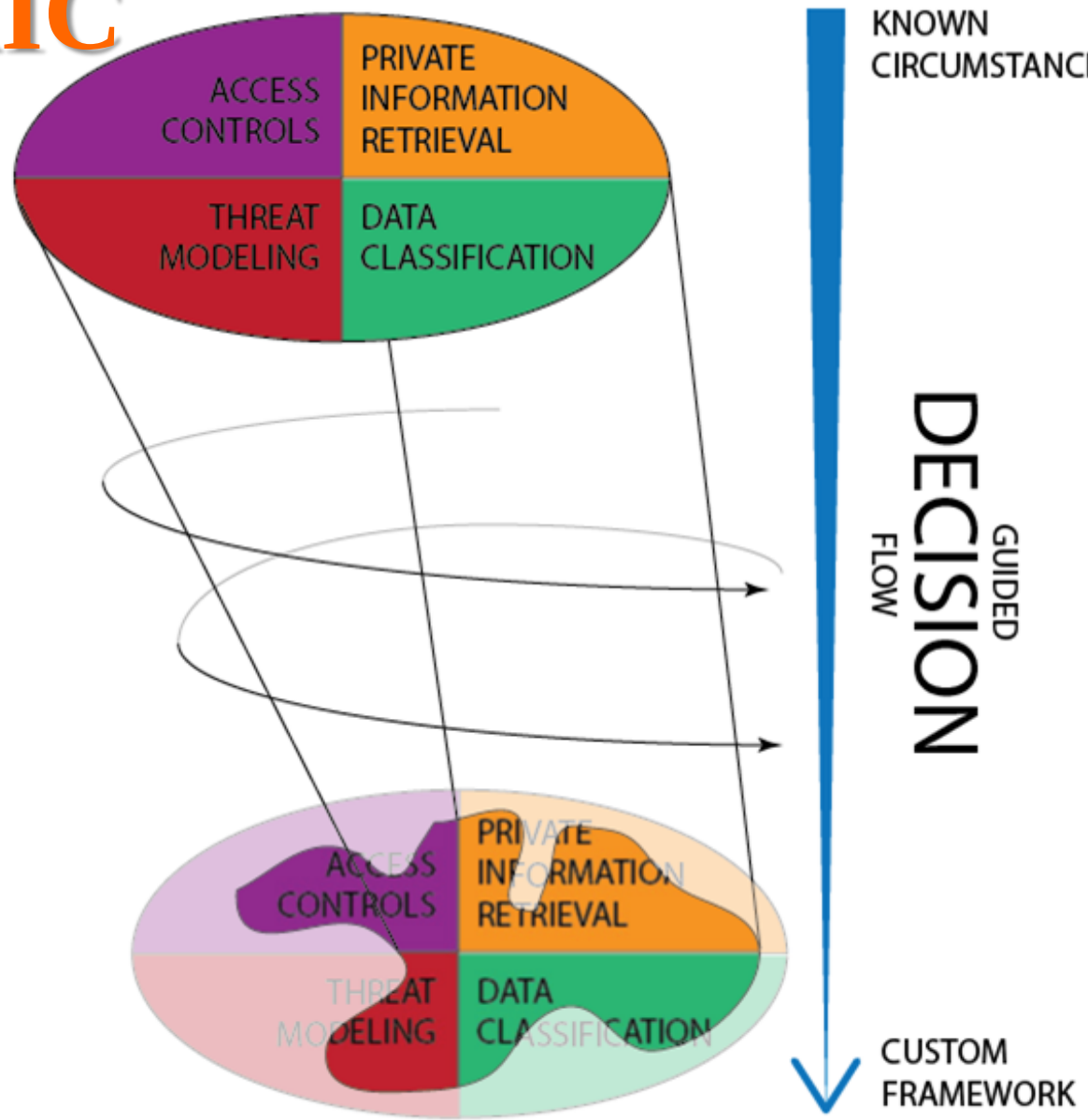








MOSAIC


ACCESS CONTROLS
PRIVATE INFORMATION RETRIEVAL
THREAT MODELING
DATA CLASSIFICATION
KNOWN CIRCUMSTANCES
GUIDED DECISION FLOW
CUSTOM FRAMEWORK

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:

Artifacts
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 — Metamodel Development Phase

- J. Heaney, G. Dolsen, and J. Page. An environment for security model development. In Systems Integration '90. Proceedings of the First International Conference on Systems Integration, pages 320-329. IEEE Comput. Soc. Press, 1990.
- J. Bau and J. C. Mitchell. Security Modeling and Analysis. IEEE Security & Privacy Magazine, 9(3):18-25, May 2011.
- D. S. McCrickard. Making Claims: Knowledge Design, Capture, and Sharing in HCI (Synthesis Lectures on Human-Centered Informatics). Morgan & Claypool Publishers, 2012.
- M. A. Goncalves, E. A. Fox, L. T. Watson, and N. A. Kipp. Streams, structures, spaces, scenarios, societies (5s): A formal model for digital libraries. ACM Trans. Inf. Syst., 22(2):270-312, Apr. 2004.

Access Controls — Proof of Concept Phase

- M. Ion, G. Russello, and B. Crispo, “Enforcing Multi-user Access Policies to Encrypted Cloud Databases,” in *2011 IEEE International Symposium on Policies for Distributed Systems and Networks*, 2011, pp. 175–177.
- N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3):614-634, 2001.
- K. Ren, W. Lou, K. Kim, and R. Deng. A Novel Privacy Preserving Authentication and Access Control Scheme for Pervasive Computing Environments. IEEE Transactions on Vehicular Technology. 55(4):1373-1384, July 2006.
- R. Sandhu, E. Coynek, H. L. Feinstein, and C. E. Youman, “Role-Based Access Control Models,” *IEEE Comput.*, pp. 38–47, 1996.
- N. Adam, V. Atluri, E. Bertino, and E. Ferrari, “A content-based authorization model for digital libraries,” *IEEE Trans. Knowl. Data Eng.*, vol. 14, no. 2, pp. 296–315, 2002.

Threat Modeling — Proof of Concept Phase

- A. Shostack. Threat Modeling: Designing for Security. Wiley, 2014.

References

Data Classification — Proof of Concept Phase

- S. Wiseman. Control of confidentiality in databases. Computers & Security, 9(6):529-537, Oct. 1990.
- Jun Zhang, Li-Jun Yun, and Zheng Zhou. Research of BLP and Biba dynamic union model based on check domain. In 2008 International Conference on Machine Learning and Cybernetics, volume 7, pages 3679-3683. IEEE, July 2008.
- X. Ma, Y. Huang, and D. Li. A Security Model Based on Lattice. In 2010 International Conference on Electrical and Control Engineering, pages 4958-4961. IEEE, June 2010.
- Q. Huang and C. Shen. A new MLS mandatory policy combining secrecy and integrity implemented in highly classified secure level OS. In Proceedings 7th International Conference on Signal Processing, 2004. Proceedings ICSP '04. 2004., volume 3, pages 2409-2412. IEEE, 2004.
- Y. Shen and L. Xiong. Lattice Based BLP Extended Model. In 2009 Second International Conference on Future Information Technology and Management Engineering, pages 309-312. IEEE, Dec. 2009.
- Yihe Liu and Xingshu Chen. A new information security model based on BLP model and BIBA model. In Proceedings 7th International Conference on Signal Processing, 2004. Proceedings. ICSP '04. 2004., volume 3, pages 2643-2646. IEEE, 2004.
- S. Wiseman. Control of confidentiality in databases. Computers & Security, 9(6):529-537, Oct. 1990.

Private Information Retrieval — Proof of Concept Phase

- A. Beresford and F. Stajano. Location privacy in pervasive computing. IEEE Pervasive Computing, 2(1):46-55, Jan. 2003.
- B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, “Private information retrieval,” J. ACM, vol. 45, no. 6, pp. 965–981, Nov. 1998.
- C. Devet, I. Goldberg, and N. Heninger. Optimally robust private information retrieval. In Proceedings of the 21st USENIX Conference on Security Symposium, Security'12, pages 13-13, Berkeley, CA, USA, 2012. USENIX Association.
- P. Mittal, F. Olumon, C. Troncoso, N. Borisov, and I. Goldberg. PIR-Tor: Scalable Anonymous Communication Using Private Information Retrieval. USENIX Security Symposium, 2011.