

MOSAIC:

Model of Securing Application Information Confidentiality

Kimberly Zeitz & Chris Frisina

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

Blacksburg
March 6, 2013
CS6604

Background

Motivation

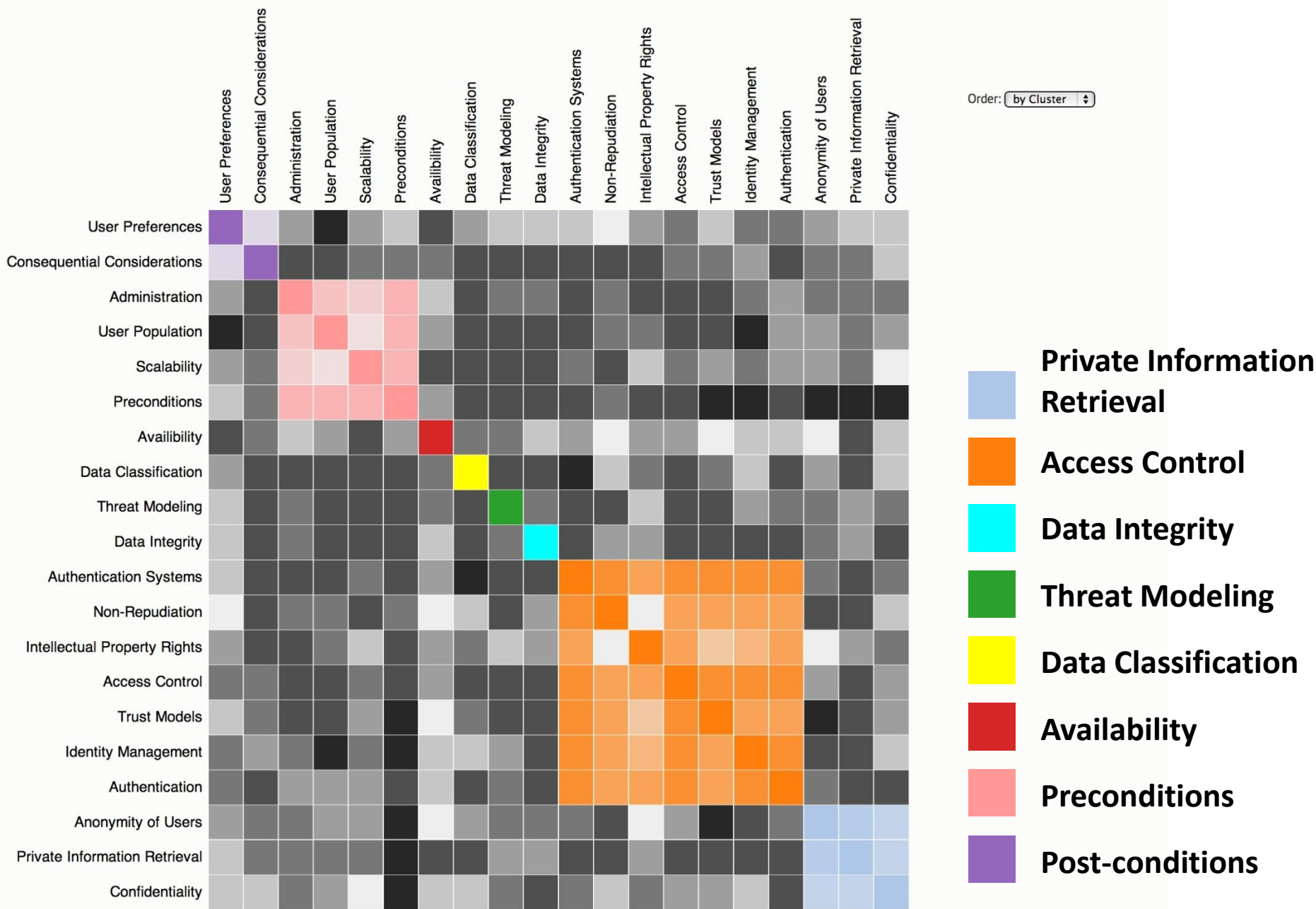
- Clarify scattered security concepts
- Guide decision making
- Comprehensive tailored security framework
- Breakdown of decisions based on security concern areas

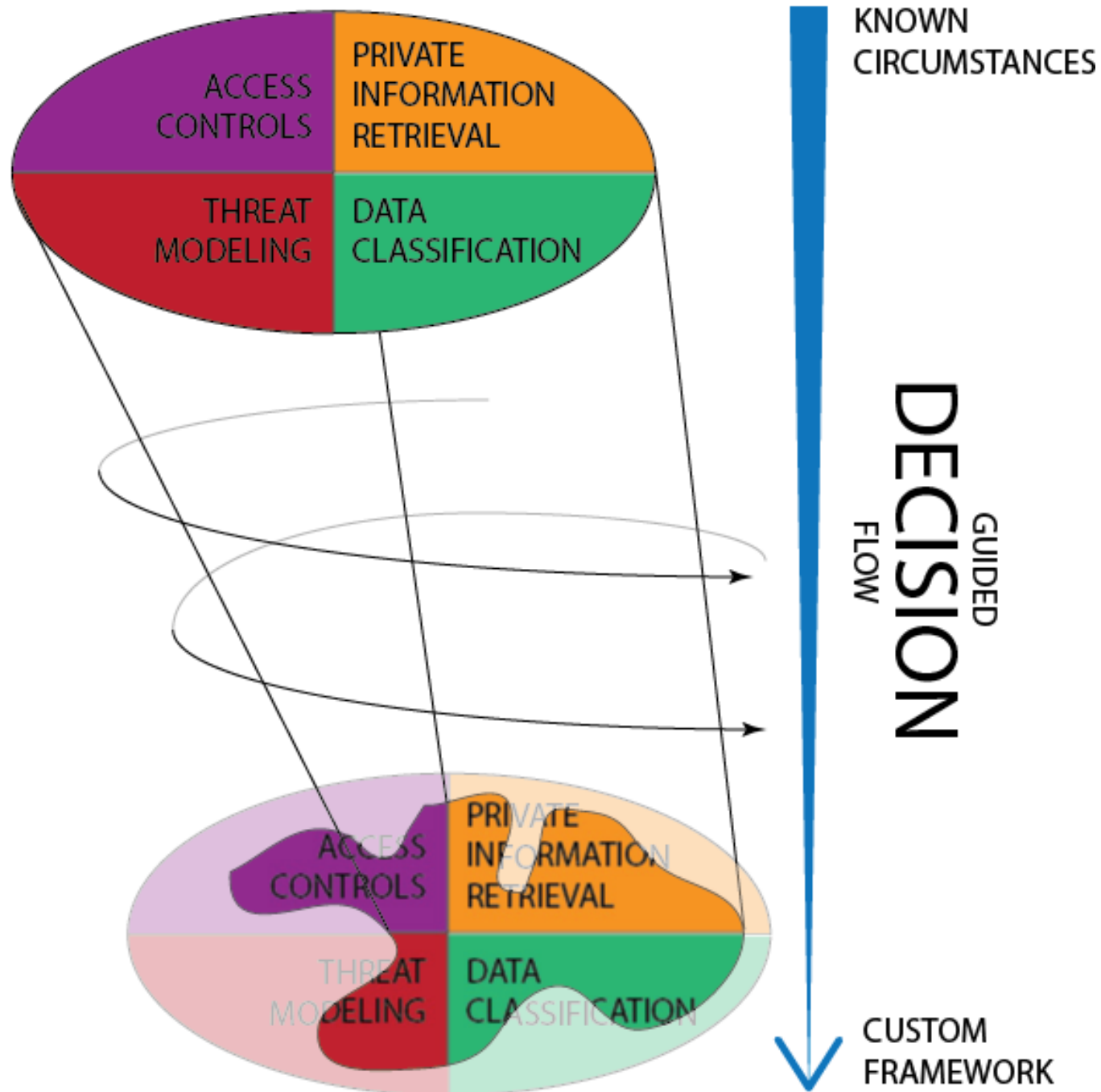
[illegible]

Order: **by Strength**



Security Co-occurrences





(Content) CBAC

(Role) RBAC

(Task) TBAC

(Team) TMAC

Access Control List

Capability List

**Access
Controls**

**Private
Information
Retrieval**

Pseudonyms

Database Replication

Secret Handshakes

Onion Routing

**Threat
Modeling**

**Data
Classification**

**Biba for Data
Integrity**

Write-down read up

**BLP [Bell-LaPadula]
for Confidentiality**

Write-up read down

Attacker-centric

System-centric

Asset-centric

Remaining Work

- Justification for classification system
- Detail current methodologies
 - Pros & Cons
 - Relevant Situations
- Present the decisions and solutions in a usable and concise manner

Questions?

References

Access Controls

- [1] N. R. 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.
- [2] A. Adams and M. A. Sasse, “Users are not the enemy,” *Commun. ACM*, vol. 42, no. 12, pp. 40–46, Dec. 1999.
- [3] R. Butler, C. Kesselman, J. Volmer, S. Tuecke, I. Foster, D. Engert, and V. Welch, “A national-scale authentication infrastructure,” *Computer (Long. Beach. Calif.)*, vol. 33, no. 12, pp. 60–66, 2000.
- [4] J.-W. Byun, E. Bertino, and N. Li, “Purpose based access control of complex data for privacy protection,” in *Proceedings of the tenth ACM symposium on Access control models and technologies - SACMAT '05*, 2005, p. 102.
- [5] 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.
- [6] N. K. Ratha, J. H. Connell, and R. M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.
- [7] K. Ren, W. Lou, K. Kim, and R. Deng, “A Novel Privacy Preserving Authentication and Access Control Scheme for Pervasive Computing Environments,” *IEEE Trans. Veh. Technol.*, vol. 55, no. 4, pp. 1373–1384, Jul. 2006.
- [8] R. Sandhu, E. Coynek, H. L. Feinstein, and C. E. Youman, “Role-Based Access Control Models,” *IEEE Comput.*, pp. 38–47, 1996.

Data Classification

- [1] A. F. Karr, J. Lee, A. Sanil, J. Hernandez, S. Karimi, and K. Litwin, “Disseminating Information but Protecting Confidentiality,” *IEEE Comput.*, vol. 34, no. 2, pp. 36–37, 2001.
- [2] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, “Location-based trust for mobile user-generated content,” in *Proceedings of the 9th workshop on Mobile computing systems and applications - HotMobile '08*, 2008, p. 60.
- [3] S. Wiseman, “Control of confidentiality in databases,” *Comput. Secur.*, vol. 9, no. 6, pp. 529–537, Oct. 1990.

References

Private Information Retrieval

- [1] D. Asonov, “Private Information Retrieval: An Overview of Current Trends,” 2001.
- [2] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, “Private information retrieval,” J. ACM, vol. 45, no. 6, pp. 965–981, Nov. 1998.
- [3] C. Devet, I. Goldberg, and N. Heninger, “Optimally Robust Private Information Retrieval,” Secur. Proc. 21st USENIX Conf. Secur. Symp.
- [4] P. Mittal, F. Olumofin, C. Troncoso, N. Borisov, and I. Goldberg, “PIR-Tor: Scalable Anonymous Communication Using Private Information Retrieval,” USENIX Secur. Symp., 2011.
- [5] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, “The new Casper: query processing for location services without compromising privacy,” VLDB, pp. 763–774, Sep. 2006.
- [6] P. Neuhaus, “privacy and confidentiality in digital reference,” Ref. User Serv. Q., vol. 43, no. 1, pp. 26–36, 2003.
- [7] B. Sattarzadeh, M. Asadpour, and R. Jalili, “Improved User Identity Confidentiality for UMTS Mobile Networks,” in Fourth European Conference on Universal Multiservice Networks (ECUMN’07), 2007, pp. 401–409.
- [8] G. Tsudik and S. Xu, “Privacy Enhancing Technologies,” in Privacy Enhancing Technologies, vol. 4258, G. Danezis and P. Golle, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 295–315.

Threat Modeling

- [1] A. Adams and M. A. Sasse, “Users are not the enemy,” Commun. ACM, vol. 42, no. 12, pp. 40–46, Dec. 1999.
- [2] S. Saha, D. Bhattacharyya, T. Kim, and S. K. Bandyopadhyay, “Model Based Threat and Vulnerability Analysis of E-Governance Systems,” Int. J. u- e- Serv. Sci. Technol., vol. 3, no. 2, 2010.
- [3] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.