A systematic review on security in Process-Aware Information Systems

Marlon Müller

Garching bei München, May, 22nd 2024

Motivation

Security in Process-Aware Information Systems (PAIS) gained increased attention in recent research.

Fast releases of new literature makes it hard to overlook current state of the art.

Research Questions

Q1: What does security in PAIS mean?

Q2: Which security controls are currently utilized in PAIS?

Q3: What are the challenges of current security research in PAIS?

Q1: What does security in PAIS mean?

No common definition across current literature, definitions are often focused on specific aspects

Most common definition is the protection of CIA-properties with relations to Authorization and Access Control

Q2: Which security controls are currently utilized in PAIS

Identification of 12 security controls that could be clustered in 5 categories

Shows that a rich set of security methods exists

Most current literature focused on Access Control Models (61 papers) and Service-Oriented Architectures (SOA) Applications (40 papers)

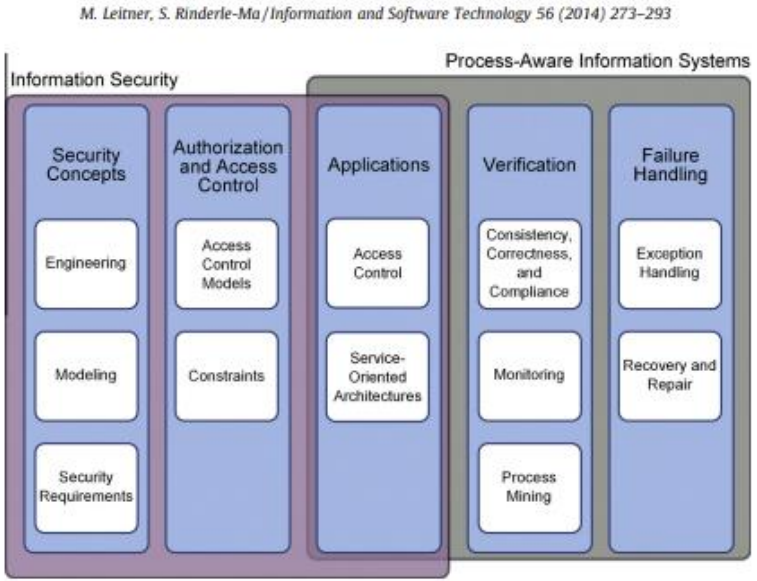


Fig. 5. Categorization of existing security controls in PAIS.

Q3: What are the challenges of current security research in PAIS?

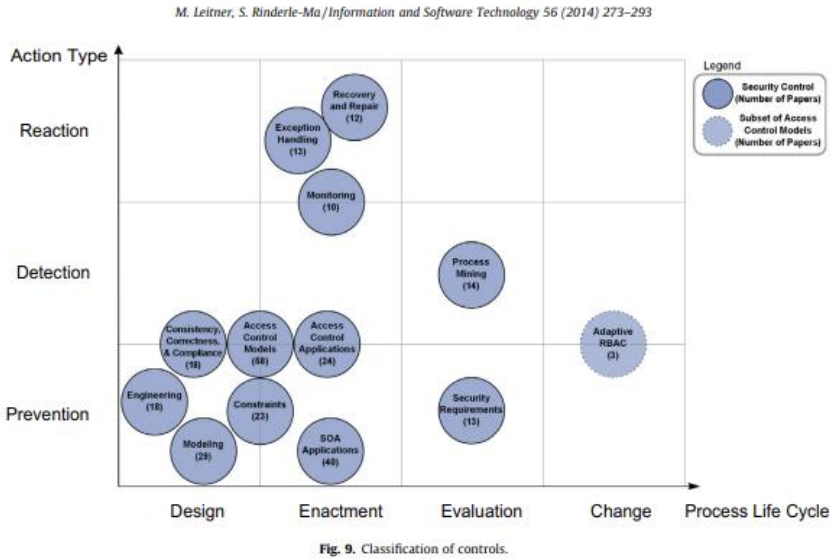


Fig. 9. Classification of controls.

Q3.1: Is security enforced in every phase of the process lifecycle?

- Most literature in Enactment (51%), fewest in Change (1%)
- For holistic approach all phases should be considered
- Due to emerging importance also topics with many publications should be further researched

Q3.2: Which types of security controls are utilized in PAIS?

- Prevention (63%), Detection (23%) and Reaction (11%)
- Most literature in Prevention/Design and Prevention/Enactment

But: some literature could have been excluded due to filter for security **AND** PAIS related papers

Q3: What are the challenges of current security research in PAIS?

- Agreement on terminology and controls
- Consistency with related fields and concepts
  - Take existing standards into consideration
- Measurement
  - Adapt existing measurements and metrics into PAIS security research
- Testing
  - Analyze which existing techniques could be adapted for PAIS
- Evaluation
  - How can security assessment be conducted at design or run time?
- Detection controls
  - How can intrusion detection be conducted during run time?
- Reaction controls
  - Research should more focus on human factors and how to react to attacks
- Human orientation
  - Humans are a big factor (social engineering), but current research focuses on technical aspects of security

My approach to update the survey

Concentrate on research published between 2013 and today.

Evaluate how the focus of research might have shifted between security controls (Q2), the process lifecycle (Q3.1) and the action types (Q3.2).

Analyze if the research challenges carved out in Q3 have been addressed in current research.

Which security controls in PAIS were researched since 2013?

Which parts of the process lifecycle and which action types are researched?

What are challenges of current security research in PAIS in comparison to 2012?

Review protocol

Use IEEExplore and Google Scholar as resources

Business Process	Security
Workflow	Access Control
Process-Aware	Authorization
	Constraints

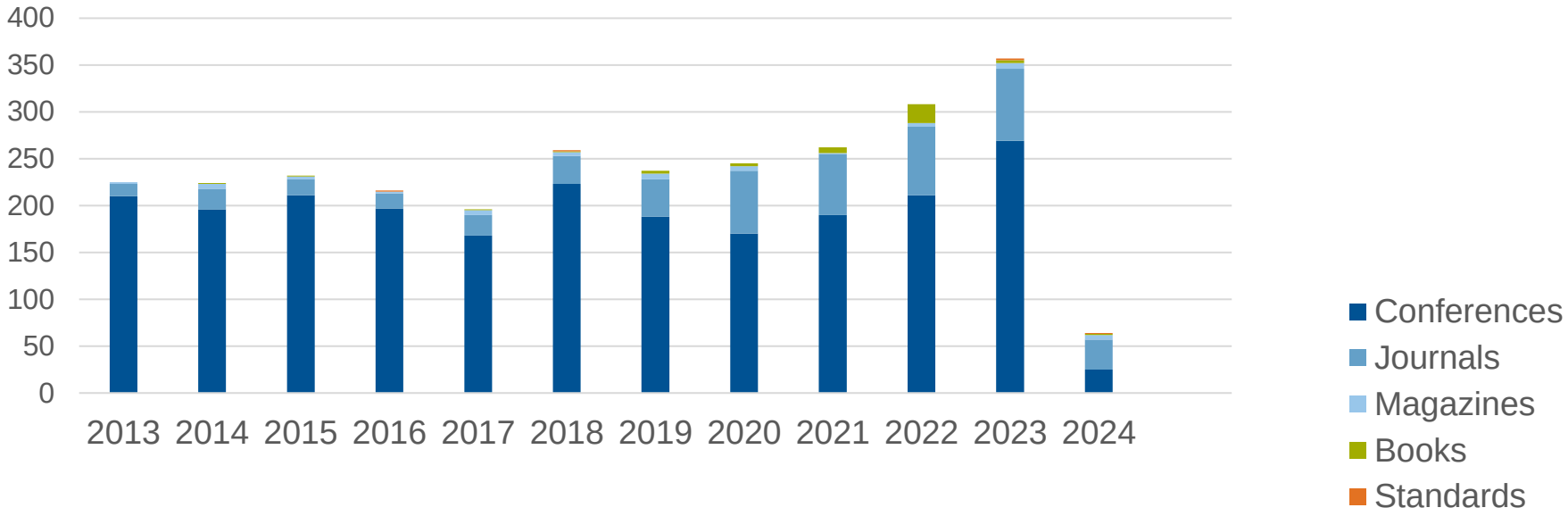
Check keywords, title and abstract for relation to security **AND** PAIS.

Categorize results after filtering for relevant papers.

Detailed evaluation only for the most cited papers.

Results

In total ~2.800 (unfiltered) results



How to categorize results

Can be briefly categorized with 4 metrics:

1. What security control is researched?
2. Where in the process lifecycle is the security control located?
3. To what action type does the security control belong?
4. Which research challenges are addressed by the paper?

Metric 2 und 3 should be the same for most of the already researched security controls and should only be necessary if new security controls where developed.