Partial state-of-the-art of model-driven security (MDS)

Nan MESSE
nan.messe@irit.fr
Keywords

- Model(-)based security
- Model(-)driven security
- Security/secure by design
- Threat modeling
- Risk analysis/assessment
Basic security-related concepts and their relations

Nan MESSE. Security by Design: An asset-based approach to bridge the gap between architects and security experts. 2021
Why MDS?

- Detect and prevent vulnerabilities early in the SDLC [1]
- Reduce maintenance cost [2,5]
- Better communication between security experts and domain experts [2,5]
- Design security at different levels of abstraction, while maintaining traceability between low-level and high-level concepts [2]
- Enable the application of formal methods [3,5]
- Bridge the gap between security requirement and design [5]

Challenges

- Its adoption in practice is not yet widespread [2]
- The evolution of the system and the evolution of the threat [2]
- Legacy systems [1]
- Lack of formality, automation, process-integration and evaluation [3]
- Security properties have to be considered in a special way since they are non-functional properties [6]
- The security of platform layer is not often considered [7]

Dimensions

- Composant
  - Cyber level
  - Platform level
    - Runtime environment
    - Physical level

- Hierarchy / Relation
  - Data
  - Human
  - Context

Fig. 1. Phases of the secure software development life cycle.

Requirements

- Introduce the security aspect (control) since the requirement phase [2]
- Support for formal threat specification and formal security analysis [3,7]
- Support for automated transformation from models to implementation code [3]
- Increase the degree of automation of tracing and refining security requirements into implemented security solutions [7]
- Support different layers of the system [7]
- Allow compositional analyses (SoS) [7]
- Deal with both fully known parts and only partially known (or even unknown) parts of the system [7]
- The threat model should be extensible [7]
- The threat model should be strongly connected with system model [7]
- Deal with third-party code vulnerabilities [7]

Standards

- MITRE
  - CAPEC
  - CWE
  - CVE
  - CPE

- Common Criteria
- OWASP
- SQUARE Process
- NIST SP 800-160
Methodologies discussed in [3]

- **SecureUML**
  - Focus on access control constraints based on RBAC
  - Lack of support for formal analysis

- **UMLSec**
  - Address multiple security concerns (CIA)
  - Lack of automated transformation from models to implementation code

- **SECTET**
  - Secure web services by leveraging the OCL for specifying RBAC
  - Focus on generating security infrastructure (XACML), not all the source code

- **SECUREMDD**
  - Specific for developing secure smart card application

- **Secure data warehouses (DWs)**
  - Specific for developing secure DWs

---

Other Methodologies

Platform specificity of the selected approaches.

<table>
<thead>
<tr>
<th>Approach</th>
<th>General</th>
<th>PS</th>
<th>CPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecureUML (Basin, 2006)</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>UMLsec (Jürjens, 2005)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SECTET (Hafner et al., 2006)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ModelSec (Sánchez et al., 2009)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motii (2017)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security4UML (Neri et al., 2013)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISSEP (Ruiz et al., 2015)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SecureMDD (Moebius et al., 2009)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security-enhanced SPACE (Gunawan et al., 2011)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Neureiter et al. (2016)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DREMS (Levendovszky et al., 2014)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProCom (Saadatmand and Leveque, 2012)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wasicek et al. (2014)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Al Faruque et al. (2015)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eby et al. (2007)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SysML-Sec (Li et al., 2018)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEED (Vasilevskaya, 2015)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **SoSSec [4]**
  - Application domain: Systems-of-Systems (SoS)
- **TRADES [2]**
  - A domain specific language for security by design

---

Observations

- (a) Security concerns addressed by MDS
  - Confidentiality: 27%
  - Integrity: 9%
  - Availability: 12%
  - Authenticity: 10%
- (b) Aspect-Oriented Modeling vs. non-AOM
  - AOM: 13%
  - non-AOM: 87%
- (c) Code or Security Infrastructures generated?
  - Only Security Infra: 52%
  - Both generated: 48%
- (d) Transformations level
  - Endogenous: 20%
  - Exogenous: 80%
- (e) Transformations Automation
  - Manual: 10%
  - Semi-Auto: 7%
  - Automatic: 83%
- (f) Application Domains of MDS
  - IS/e-commerce: 16%
  - Data warehouses: 15%
  - Smart cards/embedded: 15%
  - Distributed System/SoA: 33%
  - Others: 27%

Observations

Table 6. This Author's geographic classification.

<table>
<thead>
<tr>
<th>Continent</th>
<th>Country</th>
<th>Authors Primary</th>
<th>Others</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td>Germany</td>
<td>16</td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>France</td>
<td>11</td>
<td>2</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Luxembourg</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Norway</td>
<td>3</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Netherlands</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Austria</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Sweden</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>UK</td>
<td>1</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Italy</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Hungary</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Belgium</td>
<td>1</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>North</td>
<td>USA</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>America</td>
<td>Canada</td>
<td>3</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Morocco</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Africa</td>
<td>Tunisia</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Asia</td>
<td>Malaysia</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Japan</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Bangladesh</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>India</td>
<td>2</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Pakistan</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Iran</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Australia</td>
<td>Australia</td>
<td>1</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>56</td>
<td>14</td>
<td>70</td>
</tr>
</tbody>
</table>
Community

KU Leuven, BELGIUM
Koen Yskout
Riccardo Scandariato
Wouter Joosen

Germany
Jan Jürjens
Johannes Geismann
Eric Bodden

SnT, University of Luxembourg
Phu H. Nguyen
Jacques Klein
Yves Le Traon
Observations

Figure 9. Classification of the application domain.

Figure 10. MDS approaches.

Figure 11. Security concerns distribution.

Potential research directions

- MDS approach (e.g. DSL) dealing with multiple security concerns [3]
- Evaluate MDS approaches with empirical studies or benchmarks [3]
- A common extensible threat model that is usable by all involved disciplines and stakeholders [7]
- Alignment of viewpoints from different system layers and the security layer
- The secure integration of third-party code into the system but also into the threat modeling approach [7]
- Common evaluation scenarios (EVITA project, CoCoMe, etc), with a list of weaknesses [7]
- Continuous integration of security requirement and security by design in DevSecOps
Conclusion

- MDS has resulted in a large number of publications, including general approaches and domain specific approaches.
- No systematic review on MDS after 2015 [6]
- More automated, formalized, towards DevSecOps!