IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Continuous and Secure Evolution of Software Models

Security Rules

Chahrazed Boudjemila

IMT-atlantique engineering schools in Brest
P4S, IMT Atlantique

Contents

1 Security Rules

The security rules are constraints or guidelines that define, enforce, and validate security properties within and across models. These rules ensure that security requirements, such as confidentiality, integrity, and availability, are consistently represented and maintained throughout the system's life-cycle, from high-level design to implementation.

1.1 Establishing Security rules for Diverse Case Studies

In this section, we present a set of security rules tailored to four distinct case studies. These rules are designed to address the unique security challenges and requirements of each case.

1.1.1 iTrust System

- ***Introduction***

  - Electronic health record (EHR) systems present a tremendous challenge because people's medical records, which are transmitted and protected through those systems.

  - Key initiatives aimed at adopting EHRs and increasing the sharing of health information present important privacy issues for patients.

  - Williams Laurie launched iTrust Medical Application in 2005 at the University of North Caroline.The main aim of this project is to provide undergraduate software engineering students with a deep and complex system adapted to the reality that students can deal with while they work in the software industry. This project helps students understand the importance of security and privacy requirements [2].

  - iTrust is considered as a medical application for the management of electronic medical records, it gathers medical information of a patient from many

sources in order to provide a detailed summary of the patient's health status that will be useful for personnel health care.

- iTrust provides healthcare staff with dynamically determined information about a patient's chronic disease risk indicators [3].

- iTrust requirements are often derived from U.S. Department of Health and Social Services (HHS) use cases. [3, 2].

- ***Metamodels and Models used for iTrust system***

  Among all the possible aspects and models of the systems, our use case relies on four different models (Deployment model, Data model, BPMN model, Access Control model). We construct these models by relying on UMLsec, BPMN2, EMF access-control metamodel.

- ***iTrust Security Rules***

  To define the security rules, we based on the semantic of the different security annotations integrated in the different models. For iTrust we use the security annotations of UMLsec and secBPMN. At the outset of the document, we outline generic security rules applicable that are applicable to each pair of model types: Deployment, Data, BPMN, and Access Control models. Users can utilize these generic security rules, established at the metamodel level, and subsequently apply them to the iTrust model. The application of generic security rules to the iTrust case study relies on whether the elements within iTrust models satisfy the conditions outlined in the generic security rules.

Security Rules for BPMN model and Deployment model

- *SecurityRule-1 :* when two Pools in the BPMN model (that correspond to artifacts in the deployment model), communicate security-critical data and are deployed in different devices, the communication between the two devices must occur through an encrypted channel. This rule is added to the concept PoolArtifactCorrespondece.

- *SecurityRule-2 :* if the MessageFlow in the BPMN model has a security annotation, the CommunicationPath in the deployment model must also have a corresponding (i.e., semantically equivalent) security annotation and vice versa. This rule is added to the concept MessageFlowCommunicationCorrespondences.

- *SecurityRule-3 :* when the Pool in the BPMN model (that corresponds to artifact in the deployment model deployed in a device), contains a DataObject

that is associate to a “ConfidentialityDO”, “IntegrityDo” or “PrivacyDO” annotations. The dependency between the corresponding Artifact and other Artifact must be annotated with “Integrity” or “secrecy”.

- *SecurityRule-4 :* when the Pool in the BPMN model (that corresponds to artifacts in the deployment model), contains a Task annotated with “Integrity-Act”. The dependency between this Artifact and other Artifact must be annotated with “Integrity” or “Secrecy”.

- *SecurityRule-5 :* when two Pools in the BPMN model (that correspond to artifacts in the deployment model), Communicate with each other via MessageFlow that is linked to “IntegrityMF” , “ConfidentialityMF” or “Non-RepuMF”. The dependency between the artifacts in the Deployment model must be annotated with “Integrity” or “Secrecy”.

- *SecurityRule-6 :* when the Pool in the BPMN model (that corresponds to artifact in the deployment model), contains a Task annotated with “Integrity-Act” and preceded with log in task . The dependency between the corresponding Artifact and other Artifact must be annotated with “login”.

Security Rules for BPMN model and Data model

- *SecurityRule-1 :* when the Pool in the BPMN model (that corresponds to Class in the data model), Contains a task which is the source or target for DataObject that is linked to the security annotations. The Class must have security annotation “ critical” with tag “secrecy = DataObject/Attribute” or “Integrity = DataObject/Attribute”. This SecurityRule is attached to the concept PoolClassCorrespondece.

- *SecurityRule-2 :* when the Pool in the BPMN model (that corresponds to Class in the data model), Contains a DataObject or MessageFlow that are linked to the security annotations. The Class must contains the corresponding security annotation.

- *SecurityRule-3 :* when the Pool in the BPMN model (that corresponds to Class in the data model), Contains a task which is the source or target for MessageFlow that is linked to the security annotations. The Class must have security annotation “critical” with tag “secrecy = Task” or “Integrity = Task”. This SecurityRule is attached to the concept PoolClassCorrespondece.

- *SecurityRule-4:* when the Pool in the BPMN model (that corresponds to Class in the data model), Contains a task which is the source or target for

MessageFlow that is linked to the security annotations. The operation representing the task must have security annotation “abacRequire” with tag “right =Message/Attribute”. This SecurityRule is attached to the concept PoolClassCorrespondece.

- *SecurityRule-5 :* when two Pools in the BPMN model (that correspond to Classes in the data model), contains a DataObject that is linked to the security annotations. The Association between the classes corresponding to two Pools must be annotated with “ Integrity” or “Secrecy”. This SecurityRule is attached to the concept PoolClassCorrespondece.

- *SecurityRule-6 :* when two Pools in the BPMN model (that correspond to Classes in the data model), contains a MessageFlow that is linked to the security annotations. The Association between the classes corresponding to two Pools must be annotated with “ Integrity” or “Secrecy”. This SecurityRule is attached to the concept PoolClassCorrespondece.

- *SecurityRule-7 :* when the Operation in the data model (that corresponds to Task in the BPMN model), contains ”AbacRequire” annotation with the tag “role” and “right”. The tag “role” must correspond to the Pool that contains this Task. This SecurityRule is attached to the concept OperationTaskCorrespondences.

- *SecurityRule-8 :* when the Operation in the data model (that corresponds to Task in the BPMN model), contains ”AbacRequire” annotation . The Task in the BPMN Pool must be annotated IntegrityACT . This SecurityRule is attached to the concept OperationTaskCorrespondences.

- *SecurityRule-9 :* When the Operation in the data model (which corresponds to a Task in the BPMN model) belongs to a Class annotated as ”Critical,” then the Task must be preceded by the LogIn task.

Security Rules for Deployment model and Data model

- *SecurityRule-1 :* when Deployment model annotated with “secure dependency”. The data model must contain at least one one Class annotated “Critical”.

- *SecurityRule-2 :* when Data model annotated with annotated “secure Link”. The deployment model must contain at least one association annotated “Integrity” or ”Secrecy”.

- *SecurityRule-3 :* when two Classes in the Data model (that correspond to artifacts in the deployment model), Contain Association between them annotated “Secrecy” or “ Integrity”. The Association between the Corresponding Artifacts must be annotated “Secrecy” or “Integrity”. This SecurityRule is attached to the concept ClassArtifactCorrespondence.

- *SecurityRule-4 :* when a Class in the Data model (that corresponds to artifact in the deployment model deployed in device), contains security annotation “Critical”. The communication Path between the corresponding device must be encrypted. This SecurityRule is attached to the concept ClassArtifactCorrespondence.

- *SecurityRule-5 :* when a class in the data model (that correspond to artifact in the deployment model) annotated ”Critical”. the associations relating this artifact with other must to be annotated “Secrecy” or “Integrity” This SecurityRule is attached to the concept ClassArtifactCorrespondence.

Security Rules for Access control model and Data model

- *SecurityRule-1 :* each user in the defined data model must have an associated role in the Access Control model. This rule is added to the concept UserRoleCorrespondence.

- *SecurityRule-2 :* when the Operation in the Data model (that corresponds to Authorization in the Access Control model), contains”AbacRequire” annotation with the tag “role” and “right”. The tag “role” must contain the same Role of the Authorization in the Access Control Model. This SecurityRule is attached to the concept OperationAuthorisationCorrespondence.

- *SecurityRule-3 :* If a class in the data model inherits from the ”User” class (which corresponds to a role in the Access Control model), and if the authorization of this role corresponds to operations, then the association between this class and the ”User” class must be annotated with ”secrecy” or ”integrity”. This rule is incorporated into the concept of UserRoleCorrespondence.

1.1.2 Air Traffic Management (ATM) system

An Air Traffic Management (ATM) system is a coordinated infrastructure designed to manage and control air traffic in a country’s airspace, such as the system includes the control of both civil and military operations. It comprises a set of technologies, operating processes, and stakeholders (e.g., pilots, airport personnel, national

airspace managers, weather services, and radar operators) that monitor and guarantee the secure passage of aircraft from takeoff to landing. The system is considered complex as it interacts with various components, each performing critical tasks that treat sensitive information exchanged with the system.

Security Rules for BPMN model and Deployment model

- *SecurityRule-1 :* when two Pools in the BPMN model (that correspond to artifacts in the deployment model), communicate security-critical data and are deployed in different devices, the communication between the two devices must occur through an encrypted channel. This rule is added to the concept PoolArtifactCorrespondece.

- *SecurityRule-2 :* if the MessageFlow in the BPMN model has a security annotation, the CommunicationPath in the deployment model must also have a corresponding (i.e., semantically equivalent) security annotation and vice versa. This rule is added to the concept MessageFlowCommunicationCorrespondences.

- *SecurityRule-3 :* when the Pool in the BPMN model (that corresponds to artifact in the deployment model deployed in a device), contains a DataObject that is associate to a "ConfidentialityDO", "IntegrityDo" or "PrivacyDO" annotations. The dependency between the corresponding Artifact and other Artifact must be annotated with "Integrity" or "secrecy".

- *SecurityRule-4 :* when the Pool in the BPMN model (that corresponds to artifacts in the deployment model), contains a Task annotated with "IntegrityAct". The dependency between this Artifact and other Artifact must be annotated with "Integrity" or "Secrecy".

- *SecurityRule-5 :* when two Pools in the BPMN model (that correspond to artifacts in the deployment model), Communicate with each other via MessageFlow that is linked to "IntegrityMF" , "ConfidentialityMF" or "NonRepuMF". The dependency between the artifacts in the Deployment model must be annotated with "Integrity" or "Secrecy".

- *SecurityRule-6 :* when the Pool in the BPMN model (that corresponds to artifact in the deployment model), contains a Task annotated with "IntegrityAct" and preceded with log in task . The dependency between the corresponding Artifact and other Artifact must be annotated with "login".

Security Rules for BPMN model and Data model

- *SecurityRule-1 :* when the Pool in the BPMN model (that corresponds to Class in the data model), Contains a task which is the source or target for DataObject that is linked to the security annotations. The Class must have security annotation " critical" with tag "secrecy = DataObject/Attribute" or "Integrity = DataObject/Attribute". This SecurityRule is attached to the concept PoolClassCorrespondece.

- *SecurityRule-2 :* when the Pool in the BPMN model (that corresponds to Class in the data model), Contains a DataObject or MessageFlow that are linked to the security annotations. The Class must contains the corresponding security annotation.

- *SecurityRule-3 :* when the Pool in the BPMN model (that corresponds to Class in the data model), Contains a task which is the source or target for MessageFlow that is linked to the security annotations. The Class must have security annotation "critical" with tag "secrecy = Task" or "Integrity = Task". This SecurityRule is attached to the concept PoolClassCorrespondece.

- *SecurityRule-4:* when the Pool in the BPMN model (that corresponds to Class in the data model), Contains a task which is the source or target for MessageFlow that is linked to the security annotations. The operation representing the task must have security annotation "abacRequire" with tag "right =Message/Attribute". This SecurityRule is attached to the concept PoolClassCorrespondece.

- *SecurityRule-5 :* when two Pools in the BPMN model (that correspond to Classes in the data model), contains a DataObject that is linked to the security annotations. The Association between the classes corresponding to two Pools must be annotated with " Integrity" or "Secrecy". This SecurityRule is attached to the concept PoolClassCorrespondece.

- *SecurityRule-6 :* when two Pools in the BPMN model (that correspond to Classes in the data model), contains a MessageFlow that is linked to the security annotations. The Association between the classes corresponding to two Pools must be annotated with " Integrity" or "Secrecy". This SecurityRule is attached to the concept PoolClassCorrespondece.

- *SecurityRule-7 :* when the Operation in the data model (that corresponds to Task in the BPMN model), contains "AbacRequire" annotation with the tag "role" and "right". The tag "role" must correspond to the Pool that contains this Task. This SecurityRule is attached to the concept OperationTaskCorrespondences.

- *SecurityRule-8 :* when the Operation in the data model (that corresponds to Task in the BPMN model), contains ”AbacRequire” annotation . The Task in the BPMN Pool must be annotated IntegrityACT . This SecurityRule is attached to the concept OperationTaskCorrespondences.

- *SecurityRule-9 :* When the Operation in the data model (which corresponds to a Task in the BPMN model) belongs to a Class annotated as ”Critical,” then the Task must be preceded by the LogIn task.

Security Rules for Deployment model and Data model

- *SecurityRule-1 :* when Deployment model annotated with “secure dependency”. The data model must contain at least one one Class annotated “Critical”.

- *SecurityRule-2 :* when Data model annotated with annotated “secure Link”. The deployment model must contain at least one association annotated “Integrity” or ”Secrecy”.

- *SecurityRule-3 :* when two Classes in the Data model (that correspond to artifacts in the deployment model), Contain Association between them annotated “Secrecy” or “ Integrity”. The Association between the Corresponding Artifacts must be annotated “Secrecy” or “Integrity”. This SecurityRule is attached to the concept ClassArtifactCorrespondence.

- *SecurityRule-4 :* when a Class in the Data model (that corresponds to artifact in the deployment model deployed in device), contains security annotation “Critical”. The communication Path between the corresponding device must be encrypted. This SecurityRule is attached to the concept ClassArtifactCorrespondence.

- *SecurityRule-5 :* when a class in the data model (that correspond to artifact in the deployment model) annotated ”Critical”. the associations relating this artifact with other must to be annotated “Secrecy” or “Integrity” This SecurityRule is attached to the concept ClassArtifactCorrespondence.

1.1.3 Instant Messaging Service

Instant Messaging (IM) is a service that allows users to exchange messages instantly. It is a key component of digital communication, providing a quick and efficient means for individuals and groups to converse, share files, and collaborate. Instant Messaging Services are widely used in both personal and professional

settings, offering various features beyond simple text exchanges, including multimedia sharing, presence indicators, and integration with other services. This case study was previously used in [1] to explore how to tackle security issues at the design level, with a few modifications to add context to models. The following subsections provide a detailed explanation of this case study.

Security Rules for BPMN model and Data model

- *SecurityRule-1:* when the Pool in the BPMN model (that corresponds to Class in the data model), Contains a task which is the source or target for DataObject that is linked to the security annotations. The Class must have security annotation " critical". This securityRule is attached to the concept PoolClassCorrespondece.

- *SecurityRule-2:* when the Class in the data model (that corresponds to the Pool in the BPMN model), Contains a security annotation Critical. the pool must contain at one security annotation. This securityRule is attached to the concept PoolClassCorrespondece.

- *SecurityRule-3:* when dataObject in the BPMN model (that correspond to Class in the data model), contain a security annotation "ConfidentialityDo". The class is marked with the "Critical" annotation, and the attribute corresponding to the data is further tagged with "secrecy".

- *SecurityRule-4:* when the Operation in the data model (that corresponds to Task in the BPMN model), contains "abacRequire" annotation . The Task in the BPMN Pool must be annotated IntegrityACT . This SecurityRule is attached to the concept OperationTaskCorrespondences.

- *SecurityRule-5:* When the Operation in the data model (which corresponds to a Task in the BPMN model) belongs to a Class annotated as "Critical," then the Task must be preceded by the LogIn task.

- *SecurityRule-6:* when the Class in the data model (that corresponds to Pool in the BPMN model), Contains security annotation " critical". If the pool contains a task wihth security annotation, the task must be preceeded with LogIn Task. This securityRule is attached to the concept PoolClassCorrespondece

Security Rules for Deployment model and Data model

- *SecurityRule-1:* when data model annotated with "secure data". The data model must contain at least one one Class annotated "Critical".

- *SecurityRule-2 :* when Data model annotated with annotated “secure Link”. The deployment model must contain at least one association annotated “Integrity” or ”Secrecy”.

- *SecurityRule-3:* when two Classes in the Data model (that correspond to nodes in the deployment model), Contain Association between them annotated “secrecy” or “ integrity”. The communicatioNPath between the Corresponding nodes must be annotated “encrypted” or “LAN”. This SecurityRule is attached to the concept ClassNodeCorrespondence.

- *SecurityRule-4:* if the an association in the data model (corresponding to communicationPath un the deployement model model), contain an element with security annotation,the CommunicationPath between nodes in the deployment model must contains a corresponding security annotation. This rule is added to the concept AssociationCommunPathCorrespondences

Security Rules for BPMN model and Deployment model

- *SecurityRule-1 :* if the two pools in the BPMN model (corresponding to two Nodes model), while the Pool contain an element with security annotation, the CommunicationPath between nodes in the deployment model must contain a corresponding security annotation. This rule is added to the concept PoolNodeCorrespondences.

- *SecurityRule-2 :* when the Pool in the BPMN model (that corresponds to artifact in the deployment model deployed in a device), contains a DataObject that is associate to a “ConfidentialityDO”, “IntegrityDo” or “PrivacyDO” annotations. The dependency between the corresponding nodes must be annotated with “Integrity” or “secrecy”.

- *SecurityRule-3 :* when the Pool in the BPMN model (that corresponds to artifacts in the deployment model), contains a Task annotated with “Integrity-Act”. The dependency between this Artifact and other Artifact must be annotated with “Integrity” or “Secrecy”.

1.1.4 Holiday Booking System

- ***Introduction***

  The holiday booking process describes the process where The agency takes charge of booking a flight and hotel based on the client’s request. In this process, the travel agency receives an application form from the client. The latter gathers information from airlines and hotels based on the client’s request

requirements. Subsequently, the agency presents a proposal to the client. When the client receives the proposal, they can either accept it or refuse it. If he accepts the proposal, he must proceed with the payment through the bank. The banks confirm the payment to the agency, which in turn confirms the booking to the client. After analyzing the holiday booking system, they identified these non-functional requirements: attack harm detection, access control, integrity, non-repudiation, and confidentiality.

- ***Metamodels and Models used for Holiday Booking system***

  To describe the holiday booking system at different MDA levels, they have decided to use different models. The BPMN model is used at the CIM level to identify the needs and requirements of the system. They propose extensions to the BPMN meta-model that support the NFR listed above. Then, to present the system at the PIM and PSM level, they transform the BPMN model to a SOAML model with NFR. The outcome can be transformed into web services-specific elements such as XML Schema, WSDL, and WS-Policy.

- ***Holiday Booking Security Rules***

  1. Security Rules for SOAML model and BPMN model
     - *SecurityRule-1 :* when the Participant in the SOAML model have the security annotation Privacy (which correspond to a Pool in the BPMN), the Pool must be annotated should be annotated Privacy.
     - *SecurityRule-2 :* when the Participant in the SOAML model have the security annotation Privacy (which correspond to a Pool in the BPMN), the DataObject must be annotated Integrity.
     - *SecurityRule-3 :* when the Participant in the SOAML model have the security annotation access Control (which correspond to a Pool in the BPMN), must have compatible permissions.
     - *SecurityRule-4 :* when the Participant in the SOAML model have the security annotation access control (which correspond to a Pool in the BPMN), it is required that the participant has the identical name as the Pool.
     - *SecurityRule-5 :* when the Participant in the SOAML model have the security annotation Access Control (which correspond to a Pool in the BPMN), confirm that the task within the Pool in the BPMN model, which manipulates DataObject, must either represent or introduce an operation in Services.
     - *SecurityRule-6 :* when the Participant in the SOAML model have the security annotation Access Control (which correspond to a

Pool in the BPMN), the DataObject must be annotated Integrity and non-repudiation.

- *SecurityRule-7 :* when two Pools in the BPMN model (which correspond to two Participants in the SOAML model), transmit DataObject that is linked to Intgrity or non-repudiation security annotations,These two pools should correspond to a service contract in the SOAML model that connects the two participants.

2. Security Rules for SOAML model and WSDL model
   - *SecurityRule-1 :* when the service Interface in the SOAML (which corresponds to the Interface in the WSDL model), contains Access control security annotation, Every operation within the service interface corresponds to an operation in the interface of the WSDL model.
   - *SecurityRule-2 :* when a message in an operation in the WSDL model holds a correspondence with a DataObject in the BMPN model tagged with the integrity annotation, then, the binding parameter of the WSDL operation must be one with an encryption mechanism.

References

[1] Axelle Apvrille and Makan Pourzandi. 2005. Secure software development by example. *IEEE Security & Privacy* 3, 4 (2005), 10–17.

[2] Jane Cleland-Huang, Orlena Gotel, Andrea Zisman, and others. 2012. *Software and systems traceability*. Vol. 2. Springer.

[3] Andrew Meneely, Ben Smith, and Laurie Williams. 2012. Appendix B: iTrust electronic health care system case study. *Software and Systems Traceability* (2012), 425.