Architectural Scoring – Internal Notes

This document describes internal process used to perform the architectural scoring aspects of RABET-V.

# Enumeration

First, look at registered technology vendor’s submission for any architectural artifacts. These can be used to build the diagrams.

The construction of RABET-V diagrams is based on top-down elaboration. This means we start with the highest level components, and work our way down to the most specific.

Only two elements can appear directly on a RABET-V Diagram, «SecurityEnclave» (trust zones) and Security Services. Security Services aren’t considered to “belong” to any component of the vendor’s solution. Trust Zones can contain additional subsystems or components.

Each RABET-V diagram should address an aspect of the overall architecture. No single diagram can adequately describe an entire system. A separate diagram should be created for each trust zone, and if necessary, each solution space component.

**Note**

A solution space component is one that is provided by the vendor and is the responsibility of the vendor to protect. Most, but not all components fall into this category. Only solution space components are subject to scorable security services.

The diagrams should always show the trust zone (notated with a [«SecurityEnclave»](https://docs.nomagic.com/display/UAFP190/Security+Enclave) stereotype) each component belongs to. Place ports on the left-hand side components if it is their defining diagram (i.e. the diagram that defines the trust boundary).

Each security service should have at least one outgoing «protect» dependency to a port, interface or component. Additionally, each «protect» dependency should point to the highest level component possible. For example, if a firewall protects the entire trust zone, the target of the «protect» dependency should be the trust zone itself. This minimizes the number of arrows required on a given diagram.

Below is a breakdown noting where «protect» dependencies should be applied:

* At Component Level
  + If the entire component is protected by a security service
* At port
  + If the entire port is secured across all interfaces
* At interface
  + If only a particular interface is protected

# Scoring

The RABET-V diagrams provide a means to score the architecture, once at each service service’s point of use. A stereotype «ScorableElement» is used to hold tags for each criterion in the SSAM rubric (except *depth* which is scored outside of MagicDraw).

**Tip**

A table called Scoring Instrument – Subsystem Level provides all the scorable points on a single table, and is recommended for this task.

For each criterion in the rubric, there is space to score the architecture as well as space to provide notes about the score. The notes aren’t strictly necessary but may be helpful in defending scores that are less than perfect.

# Exempting Components

Certain components may not require mitigations from all ten security control families, this is an exception to the rule, but does happen. Examples include components that are several degrees removed from the exposing port (e.g. databases), as well as components that are primarily, but not totally, secured by someone other than the RTP (e.g. a PaaS or SaaS component provided by a cloud vendor). Exempted components can be indicated by applying the «ExemptedComponent» stereotype. Each component can be exempted on a security control family by security control family basis. For example, all security services may be required except one (e.g. injection protection). These notations will appear in the excel exports.

**Note**

It is possible that over time certain common “profiles” will be developed for components such that components with the same characteristics will be exempted in the same way.

# Composite Security Services

Composite security services, much like regular services, can be drawn on RABET-V diagrams. It is recommended to draw a separate defining diagram for the composite security service as many composites contain three or more components. Represent the composing components as regular UML components. Remember that these components do not provide a security service on their own. The composite service is also a security service and is the only component that should appear on a diagram containing solution space components. Scoring occurs like others, at their point of use. Reliability metrics should roll up to the composing service (i.e. the composite’s Reliability score should factor in the reliability of its composed parts).

# Building the Report

Reports are generated via the Document Modeling feature of MagicDraw. This generates a DocBook file which can be used to generate HTML or PDF reports. A default report template comes with the RABET-V Template, but note that diagrams that you develop must be manually added to this template. In later iterations, a macro can be developed to automate this step.

# Exporting

## Exporting Scores

Use the “Scoring Instrument – Subsystem Level”. Make sure the Scope includes all the subsystems for the product.

## Exporting Gaps

* Run Analyze -> Validation -> Validate
* Run the RABET-V Validation Suite
* Double check the validation scope
* Run the validations
* When the Validation Results panel opens, click the export button.

# Appendix: RABET-V Metamodel

## ExemptedComponent

A component that has received an exemption from receiving mitigations from one more security control families.

| **Tag** | **Multiplicity** | **Type** | **Tag Description** |
| --- | --- | --- | --- |
| AuthenticationReason | 0..1 | String | Reason why the component should be exempted from providing mitigations in the Authentication security control family. |
| AuthorizationReason | 0..1 | String | Reason why the component should be exempted from providing mitigations in the Authorization security control family. |
| BoundaryProtectionReason | 0..1 | String | Reason why the component should be exempted from providing mitigations in the Boundary Protection security control family. |
| DataConfidentialityIntegrityReason | 0..1 | String | Reason why the component should be exempted from providing mitigations in the Data Confidentiality and Integrity security control family. |
| InjectionPreventionReason | 0..1 | String | Reason why the component should be exempted from providing mitigations in the Injection Prevention security control family. |
| LoggingAlertingReason | 0..1 | String | Reason why the component should be exempted from providing mitigations in the Logging/Alerting security control family. |
| SecretManagementReason | 0..1 | String | Reason why the component should be exempted from providing mitigations in the Secret Management security control family. |
| SystemAvailabilityReason | 0..1 | String | Reason why the component should be exempted from providing mitigations in the System Availibility security control family. |
| SystemIntegrityReason | 0..1 | String | Reason why the component should be exempted from providing mitigations in the System Integrity security control family. |
| UserSessionReason | 0..1 | String | Reason why the component should be exempted from providing mitigations in the User Session security control family. |

## protect

A dependency that asserts that a security service is required to protect an component.

| **Tag** | **Multiplicity** | **Type** | **Tag Description** |
| --- | --- | --- | --- |
| EffectiveControls | 0..\* | Requirement |  |

## RABET V Model

An architecture description of a product in the RABET-V Program. The architecture description covers the entire scope of a submitted product at a particular release.

| **Tag** | **Multiplicity** | **Type** | **Tag Description** |
| --- | --- | --- | --- |
| Product Version |  |  |  |
| Registered Technology Vendor | 1 | String |  |

## ScorableElement

An element that is subject to scoring using the SSAM rubric.

| **Tag** | **Multiplicity** | **Type** | **Tag Description** |
| --- | --- | --- | --- |
| Central Configuration | 1 | [CompletenessScale](#_d0a680a6c973974bcff2c58413da4df6) | Measures whether the component’s configuration is centrally managed by the provider |
| Central Configuration Notes | 0..1 | String | Any general notes regarding the components configuration. |
| Change Management | 1 | [CompletenessScale](#_d0a680a6c973974bcff2c58413da4df6) | The component’s configuration is under full change management with attribution. |
| Change Management Notes | 0..1 | String | Notes justifying score for change management. |
| Isolation | 1 | [LevelScale](#_f1c5423c1903d17d56f872646cbdd9cb) | Measures whether access to the security service component is mediated through a central software component. |
| Isolation Notes | 0..1 | String | Notes justifying score for isolation. |
| Modularity | 1 | [LevelScale](#_f1c5423c1903d17d56f872646cbdd9cb) | Measures whether the component is segregated from other components at the system level and dedicated to providing its security service. |
| Modularity Notes | 0..1 | String | Notes justifying score for modularity. |
| Services Provided | 1..\* | [SecurityServiceType](#_4aa0f8bda125c45db7737f7c1793d5b0) | List of the security control families that the component provides. |

## SecurityService

Mechanisms used to provide confidentiality, integrity authentication, source authentication and/or support non-repudiation of information.

| **Tag** | **Multiplicity** | **Type** | **Tag Description** |
| --- | --- | --- | --- |
| Deployment Type | 1 | [SecurityServiceDeploymentType](#_86ca075e1807ec5fd1f85be96ad25dd9) | The method in which the components of the security service are deployed. |
| Deployment Type Notes | 0..1 | String | Notes about the deployment of the security service. |
| Reliability | 1 | [LevelScale](#_f1c5423c1903d17d56f872646cbdd9cb) | Measures whether the component (or the substantial logic thereof) is provided by a reputable party and actively maintained. |
| ReliabilityNotes | 0..1 | String | Notes justifying score for reliability. |

## SolutionSpace

A component that contains substantial amounts of the vendor's intellectual property. Indicates that the component should be scored.

## ThirdParty

A component produced by a party other than the Registered Technology Provider.

| **Tag** | **Multiplicity** | **Type** | **Tag Description** |
| --- | --- | --- | --- |
| Vendor | 0..1 | String | Name of the vendor of the component. |

## VersionedComponent

A component with a version number.

| **Tag** | **Multiplicity** | **Type** | **Tag Description** |
| --- | --- | --- | --- |
| Version | 0..1 | String | Version number of the component (e.g. 1.1.2) |

## Enumeration CompletenessScale

| **Value** | **Value Description** |
| --- | --- |
| none |  |
| partial |  |
| complete |  |

## Enumeration LevelScale

| **Value** | **Value Description** |
| --- | --- |
| 0 |  |
| 1 |  |
| 2 |  |
| 3 |  |
| na |  |

## Enumeration SecurityServiceDeploymentType

| **Value** | **Value Description** |
| --- | --- |
| composite |  |
| transparent |  |

## Enumeration SecurityServiceType

| **Value** | **Value Description** |
| --- | --- |
| Authentication |  |
| Authorization |  |
| Boundary Protection |  |
| Injection Prevention |  |
| Logging Alerting |  |
| Secret Management |  |
| System Integrity |  |
| User Session |  |
| Data Confidentiality and Integrity |  |
| System Availability |  |