

Anforderungsprüfung — ASSUMPTION ANALYZER

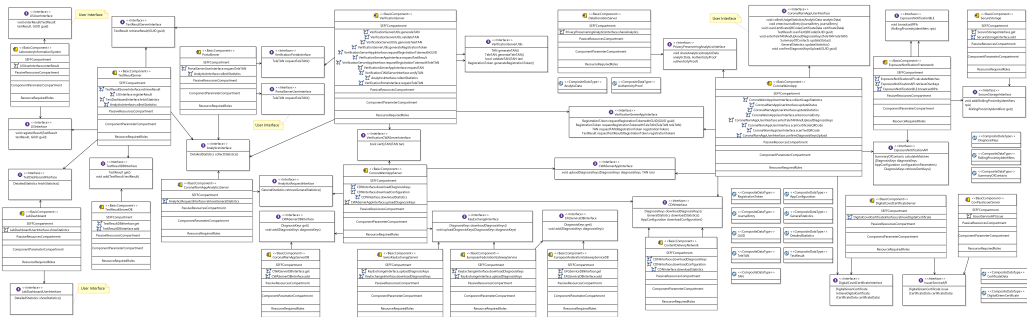
Betreuung: Sophie Corallo

Praktikum: Werkzeuge für Agile Modellierung

Tim Bächle | 18. September 2023



Motivation

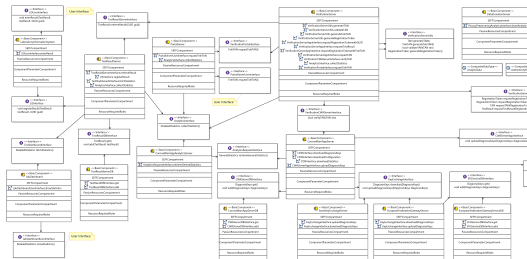


[2]

Motivation

Auf der einen Seite...

- Systeme werden tendenziell immer größer
- Sicherzustellen, dass große Systeme alle Anforderungen erfüllen ist schwierig
- Besonders Sicherheit ist ein wichtiger Aspekt
 - Regulatorisch
 - Stakeholder



[2]

Auf der einen Seite...

- Systeme werden tendenziell immer größer
- Sicherzustellen, dass große Systeme alle Anforderungen erfüllen ist schwierig
- Besonders Sicherheit ist ein wichtiger Aspekt
 - Regulatorisch
 - Stakeholder

Auf der anderen Seite...

- Schon die Architektur kann mit Sicherheitsanalysen analysiert werden
- Verschiedene Analysen betrachten unterschiedliche Sicherheitsaspekte
 - ABUNAI [1] betrachtet z.B. die Vertraulichkeit (Confidentiality)
- Die Nutzung mehrerer Analysen kann aufwendig sein
 - Installation, Nutzung, . . .

Auf der einen Seite...

- Systeme werden tendenziell immer größer
- Sicherzustellen, dass große Systeme alle Anforderungen erfüllen ist schwierig
- Besonders Sicherheit ist ein wichtiger Aspekt
 - Regulatorisch
 - Stakeholder

Auf der anderen Seite...

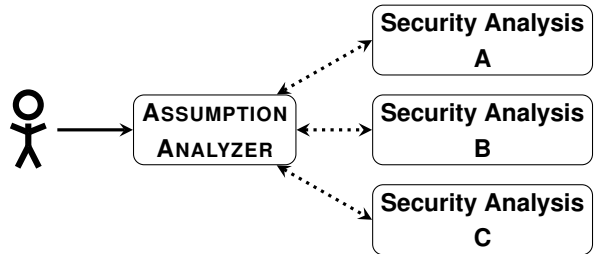
- Schon die Architektur kann mit Sicherheitsanalysen analysiert werden
- Verschiedene Analysen betrachten unterschiedliche Sicherheitsaspekte
 - ABUNAI [1] betrachtet z.B. die Vertraulichkeit (Confidentiality)
- Die Nutzung mehrerer Analysen kann aufwendig sein
 - Installation, Nutzung, . . .

⇒ Lässt sich das Auswerten mehrerer Sicherheitsanalysen einfacher gestalten?

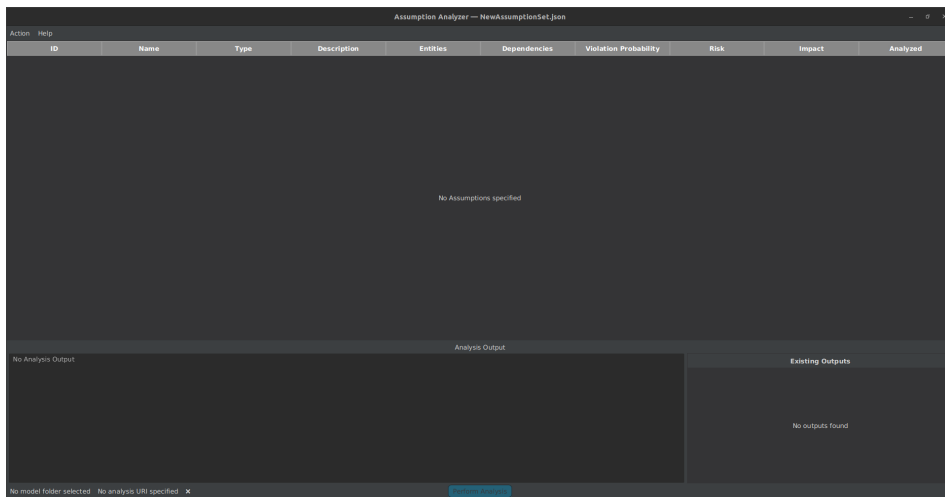
ASSUMPTION ANALYZER — Idee

Übergeordnete Ziele:

- Eine Anwendung
- Unterstützung diverser Sicherheitsanalysen
- Einfache Handhabung



ASSUMPTION ANALYZER — Anwendung



ASSUMPTION ANALYZER — Anwendung

Assumption Specification

Base Assumption

Dependencies on other Assumptions

☐ Resolve Uncertainty
☒ Introduce Uncertainty
☐ Analyzed

Node Constraints: IllegalDeploymentLocation
Data Constraints: ConfidentialDataNotExpected

Risk...

Violation probability...

Impact...

Affected Model Entities

ID	Name	Type	Model Views
_wqni4MP5Ee2NifGpaUwYsQ	IllegalDeploymentLocation		default.system
_YIPkQLm8Ee2dlMSi7oNVYQ	StoreTestResult	seff:ExternalCallAction	representations.aird
			default.usagemodel
			default.allocation

UsageModel Type: N/A Name: N/A Id: N/A

UsageScenario_UsageModel Type: N/A Name: HotlineRetrieveTeleTAN Id: _tyGHQLOKEe2o46d27a6tVQ

ScenarioBehaviour_UsageScenario Type: N/A Name: ScenarioBehaviour Id: _ztknMLOKEe2o46d27a6tVQ

UsageScenario_UsageModel Type: N/A Name: LabEntersTestResults Id: _FsTsULRJEE25KMRnMCaMfw

UsageScenario_UsageModel Type: N/A Name: LabRetrievesStatistics Id: _oj2UALRIEe25KMRnMCaMfw

ASSUMPTION ANALYZER — Anwendung

Assumption Analyzer — DemoConfig.json

ID	Name	Type	Description	Entities	Dependencies	Violation Probability	Risk	Impact	Analyzed
523a2cd-ebad-4df2-9e8d...	Base Assumption	Introduce Uncertainty	Nade Constraints: IllegalDeploymentLocation Data Constraints: ConfidentialDataNotExpected	_wgn4MP5Ee2NtKgaUwYQ _YIPkQLm8Ee2dRMSi7oNVYQ					false

Analysis Output

No Analysis Output

Existing Outputs

No outputs found

CoronaWarnApp_UncertaintyScenario2 http://localhost:2406/abunai ✓ [Perform Analysis](#)

ASSUMPTION ANALYZER — Anwendung

Assumption Analyzer — DemoConfig.json

ID	Name	Type	Description	Entities	Dependencies	Violation Probability	Risk	Impact	Analyzed
1523a2cd-ebad-4df2-9ebd...	Base Assumption	Introduce Uncertainty	Nade Constraints: LegalDeploymentLocation Data Constraints: ConfidentialDataNotExpected	_YpKQlMBE2dIMSI7oNVYQ _wqn4MPS5e2NiKPaUwYQ					true

Analysis Output

```

Did not find Impact set (2):
0: SEFFactionSequenceElement (Beginning requestTeleTAN, _fLwRILNXE2a46d27a6VQI)
  Calling SEFFactionSequenceElement / calling (GetTeleTAN, _V2aBLm2E2dIMSI7oNVYQ)
  SEFFactionSequenceElement (Beginning requestTeleTAN, _XDiwLmE2dIMSI7oNVYQ)
  Calling SEFFactionSequenceElement / calling (GenerateTeleTAN, _x_EoplmlE2dIMSI7oNVYQ)
  SEFFactionSequenceElement (Beginning generateTeleTAN, _puliobLG2e2Y3pKtbleM6Q)
  SEFFactionSequenceElement (GenerateTeleTAN, _mH5TOLmyE2dIMSI7oNVYQ)
  Calling SEFFactionSequenceElement / returning (GenerateTeleTAN, _x_EoplmlE2dIMSI7oNVYQ)
  SEFFactionSequenceElement (ReturnTeleTAN, _4VHrxLmE2dIMSI7oNVYQ)
  Calling SEFFactionSequenceElement / returning (GetTeleTAN, _V2aBLm2E2dIMSI7oNVYQ)
  SEFFactionSequenceElement (ReturnTeleTAN, _9wclm2E2dIMSI7oNVYQ)
  Calling SEFFactionSequenceElement / returning (RequestTeleTAN, _CarYBLRIE25KMRnMCaMfw)
  Calling SEFFactionSequenceElement / returning (StoreTestResult, _YpKQlMBE2dIMSI7oNVYQ)
  SEFFactionSequenceElement (Beginning add, _c5dMLNXE2a46d27a6VQI)
  Calling SEFFactionSequenceElement / returning (StoreTestResult, _YpKQlMBE2dIMSI7oNVYQ)
  Calling SEFFactionSequenceElement / returning (RegisterResult, _rctekLmE2dIMSI7oNVYQ)
  Calling SEFFactionSequenceElement / returning (EnterTestResults, _Ld5QLRJIE25KMRnMCaMfw)

Found 14 action sequences.
Confidentiality Violations:
0: SEFFactionSequenceElement (Beginning requestTeleTAN, _fLwRILNXE2a46d27a6VQI)
  Calling SEFFactionSequenceElement / calling (GetTeleTAN, _V2aBLm2E2dIMSI7oNVYQ)
  Calling SEFFactionSequenceElement / returning (GetTeleTAN, _V2aBLm2E2dIMSI7oNVYQ)
  SEFFactionSequenceElement (ReturnTeleTAN, _9wclm2E2dIMSI7oNVYQ)
  2: Calling SEFFactionSequenceElement / calling (StoreTestResult, _YpKQlMBE2dIMSI7oNVYQ)
  SEFFactionSequenceElement (Beginning add, _c5dMLNXE2a46d27a6VQI)
  
```

CoronaWarnApp_UncertaintyScenario2 http://localhost:2406/abunai ✓

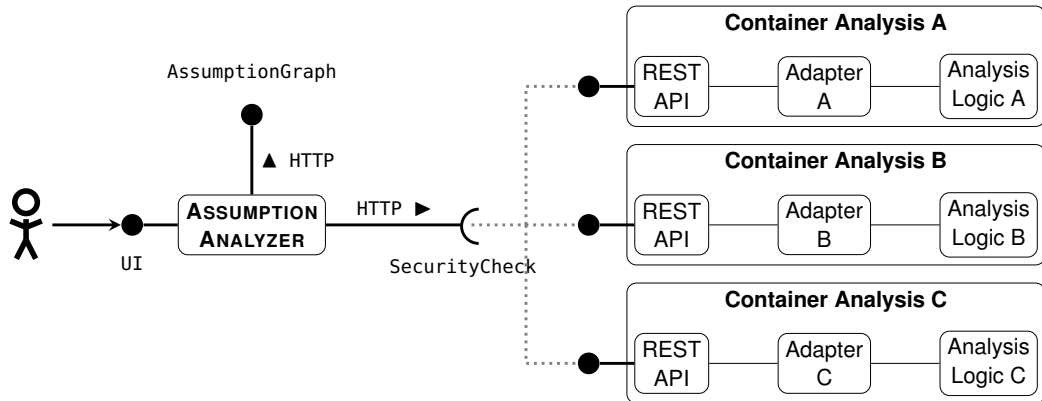
Perform Analysis

Analysis successfully executed.

Existing Outputs

- My Analysis Output #1
- My Analysis Output #2

ASSUMPTION ANALYZER — Architektur



Anbindung an Sicherheitsanalysen

Direkte Integration

- 💡 Integriere UI direkt in die einzelnen Analysen
- ⊕ Einfach
- ⊖ Schlechte Wartbarkeit
- ⊖ Eine Anwendung pro Analyse ⚡

Integration über CLI

- 💡 Statte die Analysen mit einem standardisierten CLI aus
- ⊕ Eine Anwendung für viele Analysen
- ⊖ Standardisierte CLI komplex
- ⊖ Hänge von absolutem Pfad der Analyse ab

Microservices

- 💡 Statte die Analysen mit einer REST-Schnittstelle aus
- ⊕ Eine Anwendung für viele Analysen
- ⊕ Vorteile einer Microservice Architektur
- ⊕ Containerisierung bietet sich an

Anbindung an Sicherheitsanalysen

Direkte Integration

- 💡 Integriere UI direkt in die einzelnen Analysen
- ⊕ Einfach
- ⊖ Schlechte Wartbarkeit
- ⊖ Eine Anwendung pro Analyse ⚡

Integration über CLI

- 💡 Statte die Analysen mit einem standardisierten CLI aus
- ⊕ Eine Anwendung für viele Analysen
- ⊖ Standardisierte CLI komplex
- ⊖ Hänge von absolutem Pfad der Analyse ab

Microservices

- 💡 Statte die Analysen mit einer REST-Schnittstelle aus
- ⊕ Eine Anwendung für viele Analysen
- ⊕ Vorteile einer Microservice Architektur
- ⊕ Containerisierung bietet sich an

Nutzerdaten — Ungespeicherte Änderungen

Boolean Flag

- 💡 Setzte Boolean Flag bei Änderung, Rücksetzen bei Speichervorgang
- ⊕ Einfach umzusetzen
- ⊖ Fehleranfällig: Evolution & Wartung
- ⊖ Muss bei Änderungen der Logik der Applikation angepasst werden

Vergleiche Serialisierung

- 💡 Vergleiche die Strings der JSON-Serialisierung
- ⊕ Sehr einfach umzusetzen
- ⊕ Unabhängig von Logik der Applikation
- ⊖ Fehleranfällig: Ungespeicherte Änderungen bei anderer Serialisierung?

Vergleiche Konfiguration

- 💡 Vergleiche Konfiguration der Anwendung mit der letzten gespeicherten
- ⊕ Robust
- ⊖ Benötige Mechanismus zum Klonen
- ⊖ Muss bei Änderungen der Konfiguration der Applikation angepasst werden

Nutzerdaten — Ungespeicherte Änderungen

Boolean Flag

- 💡 Setzte Boolean Flag bei Änderung, Rücksetzen bei Speichervorgang
- ⊕ Einfach umzusetzen
- ⊖ Fehleranfällig: Evolution & Wartung
- ⊖ Muss bei Änderungen der Logik der Applikation angepasst werden

Vergleiche Serialisierung

- 💡 Vergleiche die Strings der JSON-Serialisierung
- ⊕ Sehr einfach umzusetzen
- ⊕ Unabhängig von Logik der Applikation
- ⊖ Fehleranfällig: Ungespeicherte Änderungen bei anderer Serialisierung?

Vergleiche Konfiguration

- 💡 Vergleiche Konfiguration der Anwendung mit der letzten gespeicherten
- ⊕ Robust
- ⊖ Benötige Mechanismus zum Klonen
- ⊖ Muss bei Änderungen der Konfiguration der Applikation angepasst werden

Abunai Microservice

- Erwartet in aktueller Version Constraints in festem Format
- Potenzial, Constraints per NLP aus der Beschreibung der Assumption abzuleiten

Abunai Microservice

- Erwartet in aktueller Version Constraints in festem Format
- Potenzial, Constraints per NLP aus der Beschreibung der Assumption abzuleiten

Komplexe Abhängigkeiten

- Bisher nur direkte Abhängigkeiten zwischen Assumptions
- Potenzial, auch komplexe Abhängigkeiten (Verknüpfung mit OR, AND, etc.) einzuführen

Abunai Microservice

- Erwartet in aktueller Version Constraints in festem Format
- Potenzial, Constraints per NLP aus der Beschreibung der Assumption abzuleiten

Komplexe Abhängigkeiten

- Bisher nur direkte Abhängigkeiten zwischen Assumptions
- Potenzial, auch komplexe Abhängigkeiten (Verknüpfung mit OR, AND, etc.) einzuführen

Weitere Analysen

- Bisher nur Abunai unterstützt
- Weitere PCM-basierte Analysen lassen sich leicht hinzufügen

Vielen Dank für eure Aufmerksamkeit!

- [1] Sebastian Hahner. *Architecture-Based Uncertainty-Aware Confidentiality Analysis*. 2023. URL: <https://github.com/abunai-dev> (besucht am 23.08.2023).
- [2] Sebastian Hahner. *Case Study: Corona Warn App*. 2023. URL: <https://github.com/abunai-dev/CaseStudy-CoronaWarnApp> (besucht am 15.09.2023).