

Advanced Patterns And Frameworks

Zusammenfassung & Notizen

Hochschule für Technik Rapperswil

Frühjahressemester 2013

Autoren Manuel Alabor (MAL)
URL <http://swissmanu.github.com/hsr-apf-2013/patterns.pdf>
Build 22. April 2013, 17:44

Inhaltsverzeichnis

1.	Access Control Models	3
1.1.	Authorization	3
1.2.	Role Based Access Control	5
1.3.	Multilevel Security	7
1.4.	Reference Monitor	10
1.5.	Role Rights Definition	12
2.	Identification & Authentication	15
2.1.	Einführung	15
2.2.	I&A Requirements	16
3.	System Access Control Architecture	20
3.1.	Access Control Requirements	20
3.2.	Single Access Point	22
3.3.	Check Point	24
3.4.	Security Session	25
4.	Firewall Architectures	29
4.1.	Packet Filter Firewall	29
4.2.	Proxy Based Firewall	32
4.3.	Stateful Firewall	33
5.	Secure Internet Applications	36
5.1.	Information Obscurity	36
5.2.	Secure Channels	38
A.	Abbildungen, Tabellen & Quellcodes	42
B.	Literatur	44
C.	Glossar	45
D.	Workshops	46

Kapitel 1 **Access Control Models**

1.1. Authorization

Das Authorization Pattern beschreibt auf einfache Art und Weise die Zugriffsberechtigungen eines Subjekts auf ein bestimmtes Objekt. Es spezifiziert zudem die Art des erlaubten Zugriffes (Lesend, schreibend etc.)

Kontext

Jegliche Umgebungen in denen der Zugriff auf enthaltene Objekte kontrolliert werden muss.

Problem

In einer kontrollierten Umgebung muss sichergestellt werden, dass nur berechtigte Subjekte auf entsprechende Objekte zugreifen können. Es stellt sich also die Herausforderung, diese Information losgelöst von den eigentlichen Objekten abzulegen. Dabei soll aber eine gewisse Flexibilität bei der Definition von Berechtigungen, Objekten und Subjekten erhalten bleiben.

Des weiteren sollen diese Informationen so einfach wie möglich im Nachhinein änderbar sein.

Lösung

Strukturell fällt die Lösung zum Authorization Pattern relativ simpel aus:

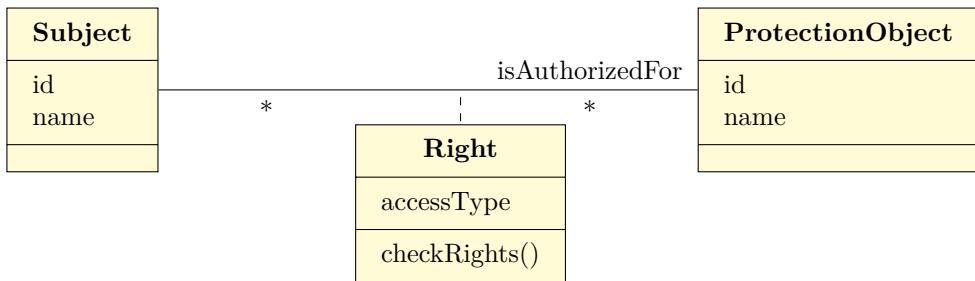


Abbildung 1.1.: Authorization Klassendiagramm

- Subject beschreibt jegliche Aspekte des zu berechtigenden Subjekts
- Das ProtectionObject ist das zu schützende Objekte
- Right enthält alle Informationen, wie Subject auf ProtectionObject zugreifen darf/-kann

Erweiterungen

Die vorgestellte Struktur kann um komplexere Aspekte erweitert werden. So kann bspw. mittels einem "Copy"-Flag eine Stellvertretung eines Subjektes durch ein anderes ermöglicht werden. Weiter ist die Verwendung eines Prädikats denkbar, welches eine Regel mit zusätzlicher "Intelligenz" austatten kann (-> "Darf nur zugreifen wenn Zeit innerhalb Arbeitszeit")

Diese Anpassungen können direkt auf dem Rights-Objekt modelliert werden.

Vor- & Nachteile

- Durch seine Offen- und Allgemeinheit kann dieses Pattern auf jegliche Umgebung appliziert werden (Filesysteme, Organisationsstrukturen, Zugangskontrollen etc.)
- In der beschriebenen Form sind administrative Aufgaben (Änderung der Zugriffsrechte) nicht gesondert definiert. Für bessere Sicherheit ist dies jedoch von Vorteil
- Für viele Subjekte/Objekte müssen entsprechend viele Berechtigungsregeln erfasst und auch verwaltet werden
- Viele Regeln machen die Verwaltung für einen Administrator zu einer heiklen Aufgabe (Verkettung von Berechtigungen etc.)

Beispielanwendungen

- Dateisysteme
- Firewalls greifen teilweise auf dieses Pattern zurück, um Regeln für den analysierten Traffic zu modellieren

Mögliche Prüfungsfragen

- *Macht es Sinn, auch verbietende Regeln zu erfassen?*

Möglich wäre dies bestimmt, im Normalfall verkompliziert dies jedoch das Sicherheitskonzept auf allen Ebenen: Die Administration wird undurchsichtiger, die Überprüfung/Durchsetzung der Regeln wird komplexer und es besteht die Möglichkeit, dass sich ein Subjekt komplett "ausschliessen" kann. (vgl. Windows Filesystem)

1.2. Role Based Access Control

Diese Pattern basiert stark auf dem Authorization Pattern und versucht dessen Nachteile durch einen zusätzlichen Abstraktionslayer auszugleichen. Das "Role Based Access Control" Pattern definiert Berechtigungen nicht direkt auf Stufe der Subjekte, sondern versucht diese in Gruppen (Aufgabenbereiche, Kaderposition, Arbeitsort etc.) einzuteilen und anschliessend auf dieser Ebene quasi übergeordnet zu berechtigen.

Kontext

Eine Umgebung mit vielen Objekten und Subjekten. Deren Berechtigungen ändern häufig. Zudem ist damit zu rechnen dass eben so oft neue Subjekte und Objekte hinzukommen oder wieder wegfallen.

Problem

Die Rechteverwaltung in dem beschriebenen Kontext generiert einen hohen administrativen Aufwand. Um die Anzahl individueller Berechtigungen zu minimieren soll versucht werden, alle Subjekte in Gruppen einzuteilen. Die Einteilung basiert darauf, dass Subjekte mit ähnlichen Aufgaben zumeist auch ähnliche oder identische Berechtigungen benötigen. Trotzdem sollen die Berechtigungen weiterhin präzise abgebildet werden können ("Need to know").

Lösung

Organisationen bieten normalerweise bereits mehr oder weniger wohldefinierte Gruppenstrukturen (Abteilungen, Aufgabenbereiche). Ein gutes Sicherheitskonzept sollte bestrebt sein, dass jedes Subjekt genau auf die Objekte Zugriff hat, mit welchen es täglich arbeitet (wiederum "Need to know").

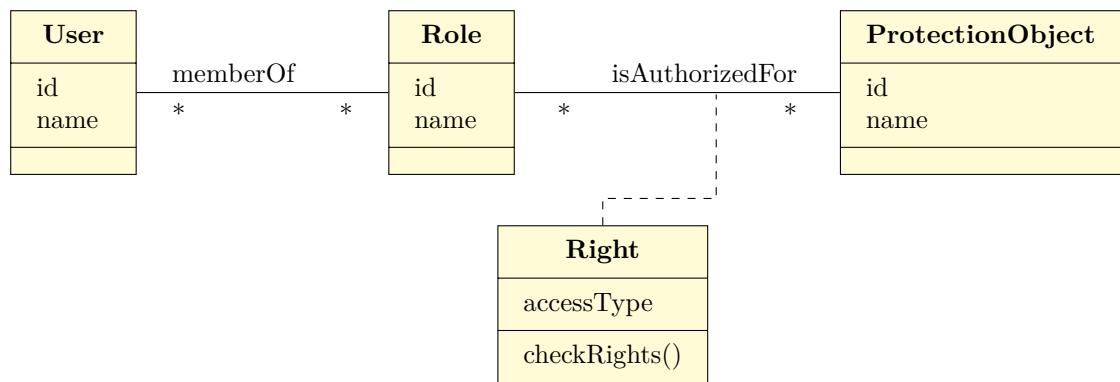


Abbildung 1.2.: Basic Role Based Access Control Klassendiagramm

Im Vergleich zum Authorization Pattern kommt lediglich ein neues Element hinzu: Die Role fasst mehrere User (Subjekte) zu einer Menge zusammen und berechtigt sie über Right für ein spezifisches ProtectionObject.

Erweiterungen

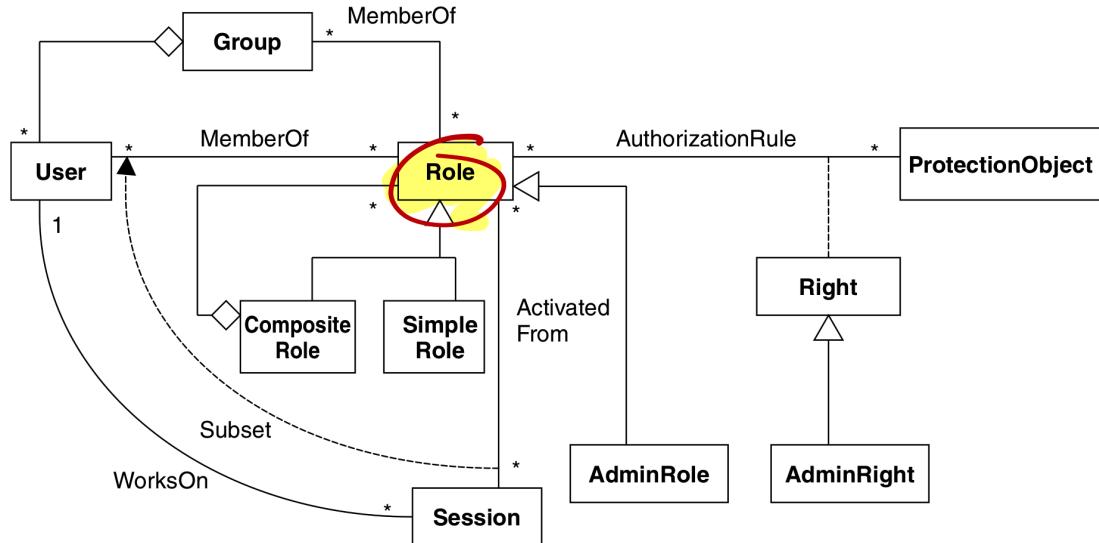


Abbildung 1.3.: RBAC mit Composite, Admins & Abstract Session

Composite Pattern

Statt einer simplen Assoziation zwischen User und Role könnte auch mit dem Composite-Pattern gearbeitet werden, um diese Abhängigkeit zu modellieren.

Administration

Wie ebenfalls bereits im Authorization-Pattern erwähnt kann auch dieses Modell zielgerichtet um Administrations-Elemente erweitert werden. Auf diese Weise kann zusätzliche Klarheit im System geschaffen werden, wer genau für was zuständig ist.

Abstract Session

Um die Möglichkeiten auf die Spitze zu treiben, sei hier auch das Abstract Session Pattern erwähnt: Die Abhängigkeit einer Session kann so direkt ins Security Modell "miteinmodelliert" werden.

Vor- & Nachteile

- Die Zusammenfassung zu Gruppen ermöglicht eine vereinfachte Administration der gesamthaft vorhandenen Berechtigungen
- Veränderungen in der realen Organisationsstruktur (Neuzugänge, Abgänge, Jobwechsel etc.) können einfacher auf das Sicherheitskonzept abgebildet werden
- Ein Subjekt kann durch mehrere Sessions verschiedene Funktionen auf einmal wahrnehmen
- Theoretisch können Gruppen wiederum in Gruppen zusammengefasst werden (Yay, even more complexity...)
- Konzeptionelle Komplexität nimmt durch die neuen Elemente wiederum zu!

Beispielanwendungen

- Windows 2000 Rights Management (Group Policies)

Mögliche Prüfungsfragen

- *Ein Subjekt hat die Rollen "Personalabteilung" und "USB Datenaustausch" zugewiesen. Wie kann verhindert werden, dass das Subjekt Personalinformationen auf einen USB-Stick speichern kann?*

Durch die Implementierung des *Abstract Session* Patterns kann das Subjekt gezwungen werden, sich jeweils nur mit einer bestimmten Rolle am System anzumelden. So hat es jeweils entweder nur auf die Personaldaten zugriff oder kann nur Dateien mit einem USB-Stick austauschen.

wackeliges Beispiel ;-)

1.3. Multilevel Security

Oft sollen Informationen in verschiedene Sicherheitskategorien eingesortiert werden: Ein Unternehmen möchte bspw. nicht, dass der neue Praktikant auf strategisch wichtige

Informationen aus dem Verwaltungsrat-Meeting zugreifen kann. Das *Multi Level Security* Pattern beschreibt wie Informationen klassifiziert werden können.

Es definiert hierzu *Policies* welche Subjekten *Clearances* für bestimmte *Sensitivity Levels* erteilt.

Kontext

Sicherheitskritische Informationen resp. deren Verwahrung erfordert erhöhten Aufwand im Sicherheitskonzept.

Problem

Es gibt es unterschiedlich sensitive Informationen. Ein Subjekt soll entsprechend seiner Stellung innerhalb der Organisationsstruktur Zugriff auf kritische oder weniger kritische Informationen Zugriff erhalten.

Dabei soll ein Maximum an Flexibilität für das Verändern von Parametern bestehen:

- Ein Subjekt soll so einfach wie möglich einer anderen Stufe in der Organisation zugewiesen werden können
- Die Sensitivität einer Information muss so einfach wie möglich angepasst werden können

Lösung

Jeder Information wird ein *Sensitivity Level* zugewiesen. *Policies* definieren, welche Subjekte aus der Organisationsstruktur auf welche *Sensitivity Levels* Zugriff erhalten.

Policies werden von *Trusted Processes* erstellt und verwaltet. Sie werden gem. dem Bell-LaPadula Sicherheitsmodell[wika] umgesetzt/überprüft:

1. *No-Read-Up*
Niedriger eingestufte Subjekte dürfen keine Informationen höher eingestufter Subjekte lesen
2. *No-Write-Down*
Höher eingestufte Subjekte dürfen keine Informationen in Ressourcen tiefer eingestufter Subjekte schreiben (Informationsweitergabe!)
3. *Zugriffsmatrix*
Matrix, welche Zugriffsberechtigungen von Subjekten auf Ressourcen festlegt

Die Korrektheit der *Policies* wiederum wird über das Biba-Modell[wikb] (der Umgehung des Bell-LaPadula Konzepts) sichergestellt:

1. *No-Read-Down*
Höher eingestufte Subjekte dürfen keine Informationen tiefer eingestufter Subjekte lesen

2. No-Write-Up

Tiefer eingestufte Stubjekte dürfen nicht in Informationen höher eingestufter Subjekte schreiben

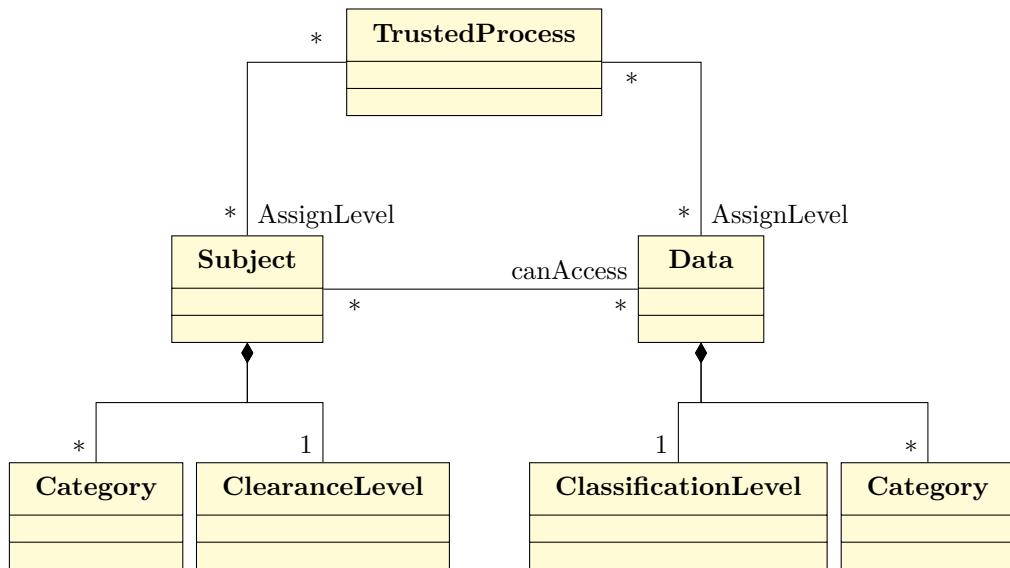


Abbildung 1.4.: Multilevel Security Klassendiagramm

Vorteile

- Welcher Benutzer welche Berechtigung erhalten soll kann relativ einfach am Organigramm einer Organisation abgeleitet werden.
- Durch die Modellierung der *Trusted Processes* trennt dieses Pattern strikt zwischen Administration und tatsächliche Umsetzung Sicherheitsregeln.

Nachteile

- Bei der Umsetzung dieses Patterns sollte darauf geachtet werden, dass normierte Bezeichnungen für die entsprechenden Sensitivity und Clearance Levels verwendet wird (-> Glossar)
- Der *Trusted Process* ist eine kritische Stelle im System.
“Aber wer wird über die Wächter selbst wachen?”
- Daten als auch Benutzer müssen optimalerweise in hierarchische Berechtigungstrukturen eingeteilt werden können. Dementsprechend kann dieses Pattern nur schwer auf alltägliche Systeme übertragen werden. (vgl. Militär)

- Nur weil ein Subjekt mit einer hohen Sicherheitsklassifizierung ausgestattet wurde, muss dies nicht bedeuten, dass keine Informationen nach Aussen getragen werden. Beispiel: Banker telefoniert im Zug lautstark und gibt sensible Kundeninformationen preis.

Erweiterungen

Das Rollenkonzept von 1.2 Role Based Access Control kann mit diesem Pattern problemlos komponiert werden: Dabei werden die *Clearance Levels* einfach auf die Gruppen statt direkt auf die Benutzer zugewiesen.

Beispielanwendungen

- Militärisches IT-System
- Datenbanksysteme (bspw. Oracle)
- Betriebssysteme (bspw. HP Virtual Vault: HP Unix Abkömmling, proprietär)

1.4. Reference Monitor

aka Policy Enforcement Point

Das *Reference Monitor* Pattern beschreibt eine abstrakte Vorghensweise, wie definierte Sicherheitsvorschriften um- und vorallem durchgesetzt werden können.

Kontext

Ein IT-System, in welchem Subjekte (Benutzer als auch technische Prozesse) auf diverse Ressourcen zugreifen möchten.

Problem

Die vorangegangenen Patterns beschrieben bis anhin lediglich, *wie* Sicherheitsrichtlinien modelliert und definiert werden können. Regeln nur zu definieren kommt einem weglassen dieser gleich. Wir benötigen also eine Möglichkeit, die aufgestellten Regeln auch effektiv durchzusetzen und zu überwachen.

Beim definieren eines möglichen Mechanismus soll darauf geachtet werden, dass dieser so abstrakt wie möglich und dadurch auf verschiedenste Architekturen sowie auf alle Ebenen eines Systems appliziert werden kann.

Lösung

Folgendes Klassendiagramm zeigt den Ansatz des abstrakten *Reference Monitors*, inkl. einer konkreten Implementierung dessen. Die Collection aus *Authorization Rules* ist konkret mit einer ACL vergleichbar.

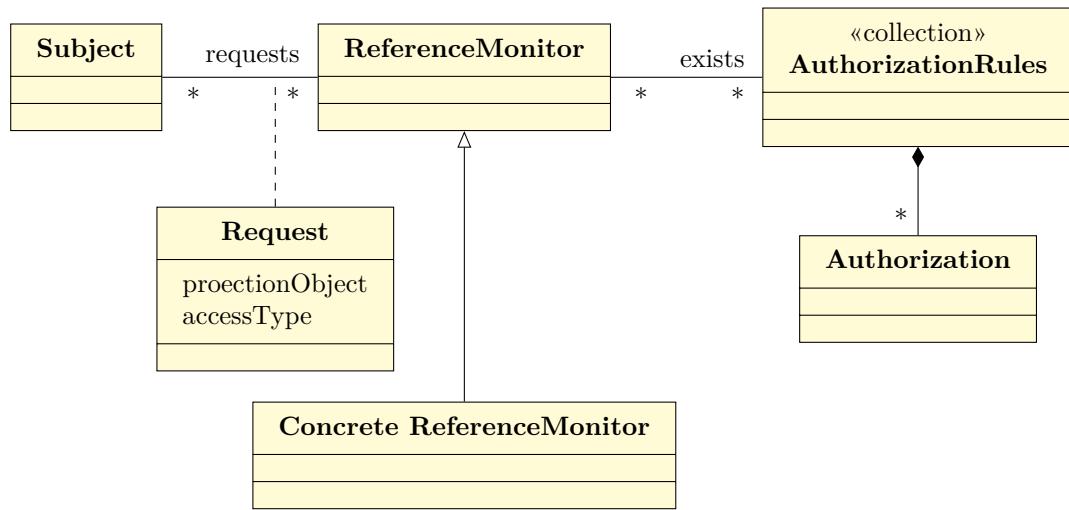


Abbildung 1.5.: Reference Monitor - Klassendiagramm

Die effektive Überprüfung, ob ein Subjekt für den Zugriff berechtigt ist, ist denkbar einfach: Jeder Zugriff auf eine Resource (ein Protection Object) wird durch den Reference Monitor geführt. Dieser prüft, ob eine entsprechende Zugriffsregel vorhanden ist und gewährt ggf. den Zugriff.

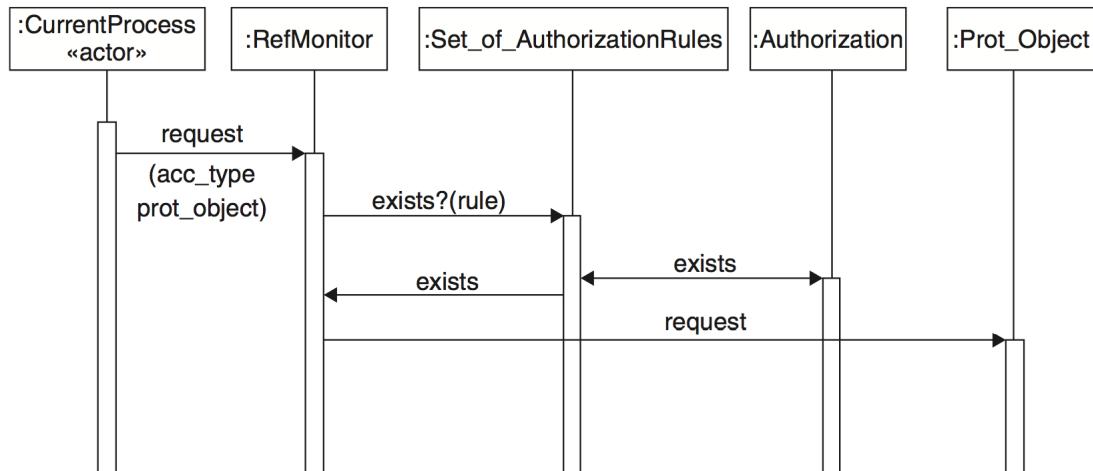


Abbildung 1.6.: Reference Monitor - Sequenzdiagramm [Sch+06]

Dieses Vorgehen leitet vom *Interceptor* Pattern ab, und findet an vielen anderen Orten Verwendung (JEE Servlet Filter usw.)

Vor- & Nachteile

- Wenn sichergestellt werden kann, dass alle *Requests* überprüft werden können, so ist eine maximale Befriedigung der Sicherheitsanforderungen gewährt.
- Jede Resource benötigt ihre eigene Implementierung eines *Reference Monitors*; Ein *Request* auf eine Datei muss evtl. anders behandelt werden als ein *Request* auf eine spezifische Datenbanktabelle.
- Die Prüfung vieler *Requests* kann bei hoher Systemlast zum Performancerisiko führen. Dementsprechend sollte die Logik zur Sicherheitsprüfung auch so einfach/- schlank wie möglich gehalten werden.

Beispielanwendungen

- Datenbanksysteme
- Betriebssysteme (bspw. Windows 2000 ff. verwendet eine ACL für NTFS Berechtigungen)

1.5. Role Rights Definition

Beim Definieren von Sicherheitsrichtlinien spielt das *Least Privilege* oder auch das *Need to know* Prinzip eine fundamentale Rolle: Jedes Subjekt soll gerade so viele Berechtigungen erhalten, damit es seine Aufgaben ungehindert erledigen kann.

Das *Role Rights Definition* Pattern beschreibt einen systematischen Ansatz, wie aus vorhandenen *Requirements Engineering* Artefakten *Need to Know*-konforme Sicherheitsregeln gewonnen werden können

Kontext

Eine relativ komplexe Ansammlung von Rollen soll mit passenden Berechtigungen ausgestattet werden.

Problem

Role Based Access Control wird in vielen Systemen als grundlegendes Sicherheitkonzept verwendet. Wie im Abschnitt 1.2 erwähnt ist die Definition von Berechtigungskonzepten bei umfangreichen System (und grosser Anzahl an Aufgabenbereichen) mit beträchtlichem Aufwand verbunden.

Zudem überlässt *Role Based Access Control* es komplett dem Implementator, aufgrund von welchen Informationen Gruppen resp. deren Berechtigungen zusammengestellt werden.

Wie können wir *Role Based Access Control* mit Sicherheitsrichtlinien füttern, welche folgende Punkte befriedigen?

- Rollen sollen Aufgabenbereichen in der Organisationsstruktur entsprechen

- Rechte sollen so erteilt werden, dass sie dem *Need to know* Prinzip genügen
- Weiterhin soll die Anpassung bestehender Rollen und Rechten so einfach wie möglich bleiben
- Die Definition von Rechten und Rollen soll unabhängig von einer effektiven Implementierung des Systems bleiben

Lösung

Die Idee ist denkbar einfach: Ein (hoffentlich bestehendes) Use Case Model und die damit verbundenen Sequenzdiagramme werden dazu verwendet, alle von *Role Based Access Controls* benötigten Elemente zu erfassen:

- Ein *Actor* entspricht einer *Role*
- Jegliche *Objects* entsprechen einem potentiellen *ProtectionObject*
- Jede *Operation* welche ein *Actor* auf einem *Object* ausführt, ist ein potentielles *Right* einer *Role*
- Eine *Use Case Exception* bestimmt das Verhalten im Falle einer Verletzung einer Sicherheitsrichtlinie

Vorteile

- Sicherheitsrichtlinien können, bei entsprechendem Projektvorgehen, bereits sehr früh definiert und erkannt werden.
- Wird ein “*model driven*”-Ansatz für die Softwareentwicklung gewählt, können Sicherheitsrichtlinien im optimalsten Fall “einfach” aus den bestehenden Requirements Artefakten generiert werden
- *Role Rights Definition* erstellt “perfekte” Sicherheitsrichtlinien für *RBAC*
- Sind alle Use Cases modelliert, und das System kann auf diese Weise komplett abgebildet werden, so ist ein Maximum an Sicherheit garantiert
- Verändert sich die Funktionalität (sprich die Use Cases) des Systems (neuer Release etc.), so können auch die damit verbundenen Änderungen im Sicherheitskonzept problemlos abgebildet werden.
- *Role Rights Definition* bleibt komplett implementationsneutral

Nachteile

- Ohne ausführliches, durchgehendes und kompetentes Requirements Engineering hat dieses Pattern so gut wie keinen Nutzen

Mögliche Prüfungsfragen

- Für welches Pattern ist der “Output” von Role Rights Definition bestens geeignet? Warum?

Role Rights Definition analysiert Use Cases und extrahiert daraus aufgaben- und funktionsbezogene Zugriffsberechtigungen für alle vorhandenen *Actors*.

Diese Regeln entsprechen dem *Need to know* Prinzip: Jeder *Actor* kann genau das tun/sehen, was er zu Ausübung seiner Aufgaben tun/sehen können muss.

Damit sind eben diese Regeln optimal für die Verwendung im *RBAC* Pattern geeignet.

- Warum reicht es nicht aus, lediglich das Use Case Model zur Gewinnung von Roles und Rights zu analysieren?

Die Sequenzdiagramme geben detaillierte Auskunft darüber, zu welchem Zeitpunkt welcher *Actor* welches *Right* für welches explizite *Protection Object* benötigt. Ohne diese Informationen ergibt sich ein unvollständiges Gesamtbild.

Kapitel 2 Identification & Authentication

2.1. Einführung

“Identification & Authentication” (I&A) fasst folgende zwei Schritte zusammen:

1. Feststellen der Identität eines Subjektes sowie Verbindung zu einer im System abgelegten ID herstellen (Identification)
2. Mittels einem Authenticator¹ prüfen, ob Subjekt wirklich für die ermittelte ID berechtigt ist (Authentication)

Für dieses grundlegende Schema gibt es zwei verschiedene Varianten:

1. Ein Subjekt wird mit einer eindeutigen Identität in Verbindung gebracht (Individual I&A)
2. Ein Subjekt wird lediglich auf die Zugehörigkeit zu einer Gruppe geprüft (Group I&A)
Beispiel: Wache prüft jede Person an der Pforte, ob er einen Mitarbeiterbadge bei sich trägt.

Um I&A einsetzen zu können ist eine Reihe weiterer (aktiver und passiver) Komponenten nötig:

- *Subjektregistrierung*: Ein Subjekt muss initial registriert werden, damit es später wieder identifiziert und authentifiziert werden kann
- *Sessionmanagement*: Schlagwort Single-Sign-On
- *Gesicherte Systemkomponenten, “Using function”*: Komponenten, welche I&A aufrufen und dessen Output verwenden (z.B. Patterns aus dem Kapitel 1)

¹ Als Authenticator gilt z.B. ein Passwort, Hardwaretoken, Streichliste usw.

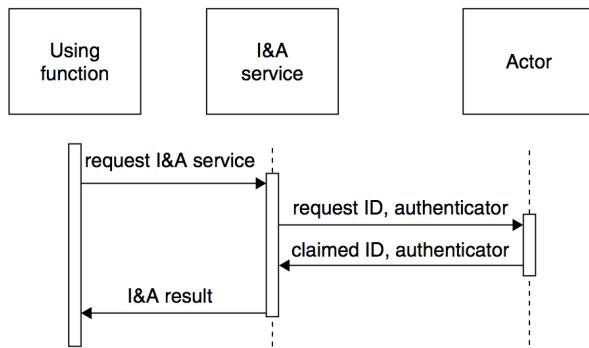


Abbildung 2.1.: Generischer Ansatz von I&A “Using functions” [Sch+06]

Mögliche Prüfungsfragen

- *Was ist ein Authenticator?*

Nachdem ein Subjekt mit einer im System abgelegten Identität in Verbindung gebracht wurde, wird der Authenticator verwendet, um sicherzustellen, dass das Subjekt auch wirklich das Subjekt ist, für welches es sicht ausgibt.

Beispiel: Nach Eingabe des Benutzernamens wird das Passwort als Authenticator verwendet.

- *Welche grundlegenden Typen von I&A unterscheidet man?*

Individual und Group Identification & Authentication

2.2. I&A Requirements

Muss ein I&A Service etabliert werden, hilft das I&A Requirements Pattern mit seinen generischen Requirementsvorlagen bei der Analyse eines bestehenden oder zu konzipierenden Systems.

Dabei werden nicht nur sicherheitsrelevante Faktoren berücksichtigt. Aspekte wie Kosteneffektivität oder Benutzerzufriedenheit und -Akzeptanz fließen ebenso in die Analyse mit ein.

Kontext

Eine Organisation oder ein Projekt konzipiert die Verwendung von I&A. Das Pattern unterstützt die Analyse jeglicher Situationen, in welchen sowohl Identification als auch Authorization notwendig ist.

Problem

Der Natur nach können Anforderungen oftmals im Konflikt zueinander stehen. Insbesondere im Bereich der I&A können hohe Sicherheitsanforderungen nicht mit dem tiefen Projektbudget vereinbar sein.

Wie können nun aber eben diese Anforderungen auf die aktuelle Situation angepasst miteinander in Einklang gebracht werden?

Lösung

Das I&A Requirements Pattern definiert folgende Vorgehensweise:

1. *Requirements Specification*

Generische Requirementsvorlagen im Systemdesign-Prozess aufgreifen und auf eigene Situation anpassen

2. *Prioritization Process*

Die Menge an angepassten, generischen Requirements wird nun gem. der aktuellen Situation priorisiert

Generische Requirementsvorlagen

Anforderung	Erläuterung
Accurately Detect Imposters	Requests von unberechtigten Actors sollen als solche erkannt werden.
Accurately Recognize Legitimate Actors	Korrekte Requests an den Service sollen auch als solche erkannt werden.

Tabelle 2.1.: I&A Requirements: Funktionale Anforderungen

Die beiden funktionalen Anforderungen stehen praktisch immer in gegenseitiger Wechselwirkung: Werden mehr Requests als *Falsch* klassifiziert, erwischt man automatisch auch mehr Requests, welche eigentlich *Richtig* gewesen wären.

Anforderung	Erläuterung
Minimize Mismatch with user Characteristics	Unterschiedliche Wissenstände, Umgebungseinflüsse (Standort ...) usw. von Actors sollen zu so wenigen wie möglichen Fehlinterpretationen von Service Requests führen.
Minimize Time and Effort to Use	Bspw. Zeitaufwand für mehrmaliges eintippen des Passworts soll verhindert werden
Minimize Risks to User Safety	Beispiel: Retina Scanner muss mit Gasmaske funktionieren; dies steht im Konflikt mit der Genauigkeit der Re却esterkennung
Minimize Costs of Per-user Setup	
Minimize Changes Needed to Existing System Infrastr.	Soll der I&A Service in ein bestehendes System integriert werden, sollen die anfallenden Änderungen in der bestehenden Infrastruktur ggf. minimiert werden
Minimize Costs of Maintenance, Management & Overhead	
Protect I&A Service and Assets	Wie wichtig ist der Schutz des I&A Services und er zu schützenden Objekte?

Tabelle 2.2.: I&A Requirements: Nichtfunktionale Anforderungen

Analogie: Anlagestrategie im Finanzsektor

Es können nie alle Anforderung gleich gut abgedeckt werden. Wie bei einer Anlagestrategie (Dreieck *Liquidität, Sicherheit, Rentabilität*) müssen alle Anforderungen analysiert und auf die eigene Situation/Präferenzen zugeschnitten werden.

Vorteile

- Eine ausführliche Domain- und Anforderungsanalyse wird gefördert.
- Die vorliegenden Requirementsvorlagen fördern die ausführliche Auseinandersetzung mit den verschiedensten Einflüssen auf I&A.
- Als angenehmen Nebeneffekt erhält man eine umfangreiche Dokumentation über die I&A Aspekte des Systems.

Nachteile

- Der Aufwand zur Umsetzung dieses Patterns kann tendenziell sehr Resourcenintensiv sein (Anforderungsanalyse, Priorisierung etc. etc.)
- Die vielen Ausprägungen der einzelnen Anforderungen können leicht in einem Over-Engineering enden. Diese Gefahr kann jedoch durch pragmatische Herangehensweise (Verwendung als Guidelines) minimiert werden

- Da eine umfangreiche Dokumentation als Resultat des Patterns entsteht, besteht natürlich auch die Gefahr, dass diese im Laufe der Zeit nicht mehr aktualisiert wird.

Mögliche Prüfungsfragen

- *Gibt es ein I&A Patentrezept?*

Nein. Jedes System kommt mit seinen eigenen, spezifischen Anforderungen an I&A. Aus diesem Grund kann und sollte das I&A Requirements Pattern nur als Guideline/Vorlage zu eigenen spezifischen Implementierungen verwendet werden.

Kapitel 3 **System Access Control Architecture**

3.1. Access Control Requirements

Das Pattern Access Control Requirements ist sehr mit dem aus I&A bekannten Pattern "I&A Requirements" zu vergleichen.

Statt Anforderungen für I&A zu definieren und zu erarbeiten, stellt "Access Control Requirements" eine Sammlung von allgemein gültigen Anforderungsschablonen zur Verfügung, welche das spezifizieren eine Massgeschneiderten Zugriffskontrolle ermöglichen.

Kontext

Eine Organisation oder ein Projekt konzipiert die Verwendung von Access Controls.

Problem

Der Natur nach können Anforderungen oftmals im Konflikt zueinander stehen. Insbesondere im Bereich von Access Control können hohe Sicherheitsanforderungen nicht mit dem tiefen Projektbudget vereinbar sein.

Wie können nun aber eben diese Anforderungen auf die aktuelle Situation angepasst miteinander in Einklang gebracht werden?

Lösung

Das Access Control Requirements Pattern definiert folgende Vorgehensweise:

1. *Requirements Specification*

Generische Requirementsvorlagen im Systemdesign-Prozess aufgreifen und auf eigene Situation anpassen

2. *Prioritization Process*

Die Menge an angepassten, generischen Requirements wird nun gem. der aktuellen Situation priorisiert

Generische Requirementsvorlagen

Folgende Anforderungen gilt es im Rahmen dieses Patterns zu analysieren und lösungsgerecht auszubalancieren:

Anforderung	Erläuterung
Deny unauthorized access	Unberechtigten Subjekten soll der Zutritt zu schützenswerten Objekten verwehrt werden
Permit authorized access	

Tabelle 3.1.: Access Control Requirements Requirements: Funktionale Anforderungen

Anforderung	Erläuterung
Limit the damage when unauthorized access is permitted	Kann ein unbefugtes Subjekt trotzdem Zugang zum System erhalten, soll der entstehende Schaden so klein wie möglich sein. Dies führt möglicherweise zu erneuten Sicherheitsprüfungen und erschwert für berechtigte Subjekte die alltägliche Nutzung des gesicherten Systems.
Limit the blockage when authorized access is denied	Wird ein grundsätzlich berechtigtes Subjekt abgewiesen, so sollen die Auswirkungen für dieses so klein wie möglich sein (Produktivität etc.)
Minimize burden of access control	Die Zugriffskontrolle soll nicht zur Bürde werden. Schlagworte wie Performance, Reaktionszeit usw. sind hier von grosser Bedeutung.
Support desired authorization policies	Meet the requirements ;-)
Make access control service flexible	Die Zugriffskontrolle soll nach Möglichkeit schnell anpassbar sein. Beispiel: Nach Terroranschlag erhöhte Sicherheitsstufe für zwei Monate, anschliessend wieder gewohntes Dispositiv.

Tabelle 3.2.: Access Control Requirements: Nichtfunktionale Anforderungen

Vorteile

- Eine ausführliche Domain- und Anforderungsanalyse wird gefördert.
- Die vorliegenden Requirementsvorlagen fördern die ausführliche Auseinandersetzung mit den verschiedensten Einflüsse auf Access Control.
- Als angenehmen Nebeneffekt erhält man eine umfangreiche Dokumentation über den Access Control Aspekt des Systems.

Nachteile

- Der Aufwand zur Umsetzung dieses Patterns kann tendenziell sehr Resourcenintensiv sein (Anforderungsanalyse, Priorisierung etc. etc.)

- Die vielen Ausprägungen der einzelnen Anforderungen können leicht in einem Over-Engineering enden. Diese Gefahr kann jedoch durch pragmatische Herangehensweise (Verwendung als Guidelines) minimiert werden
- Da eine umfangreiche Dokumentation als Resultat des Patterns entsteht, besteht natürlich auch die Gefahr, dass diese im Laufe der Zeit nicht mehr aktualisiert wird.

Mögliche Prüfungsfragen

- *Gibt es ein Access Control Patentrezept?*

Nein. Jedes System kommt mit seinen eigenen, spezifischen Anforderungen an Access Control. Aus diesem Grund kann und sollte das Access Control Requirements Pattern nur als Guideline/Vorlage zu eigenen spezifischen Implementierungen verwendet werden.

3.2. Single Access Point

Der Single Access Point definiert einen klaren Zugangspunkt zu einem System. Die so entstehende Schnittstelle kann dazu verwendet werden, effektive Sicherheitsrichtlinien praktisch umzusetzen.

Kontext

Subjekten soll Zugang zu einem System gewährt werden. Die Subjekte sollen bevor sie Zugang erhalten geprüft werden. Das System soll vor Beschädigung und Missbrauch geschützt werden.

Problem

Gewährt man Subjekten Zugang zu den Komponenten eines Systems, ist deren Integrität automatisch in Gefahr.

Nun könnte man den Zugang zu jeder Komponente im System gesondert überprüfen. Dies macht im Bezug auf Performance und/oder Accessability meistens weniger Sinn (Subjekte wollen nicht mehrfach ein Passwort eingeben müssen oder sich wiederholt von einem Security-Mitarbeiter abchecken lassen müssen).

Weiter führt die wiederholte Implementierung der Sicherheitsrichtlinien unweigerlich zu höheren Kosten. Sei dies im Bereich der späteren Wartung oder bei Initialaufwänden. Erschwerend kommt im Bezug auf die Kosten hinzu, dass die meisten Komponenten im System nicht 1:1 miteinander vergleichbar sind und so evtl. nicht unbedingt gleich geschützt werden können.

Lösung

Es wird ein Single Access Point (“ein einziger Zugangspunkt”) definiert, welcher die Sicherheitsrichtlinien umsetzen kann und welcher jegliche Subjekte, welche Zugang zum System erhalten wollen passieren müssen.

Dieser Single Access Point muss prominent platziert sein. Kann ein Subjekt ihn nicht finden, wird dieses kaum glücklich über die Sicherheitsmaßnahme sein.

Hat ein Subjekt den Single Access Point passiert, kann es sich im System frei bewegen.

Ist eine feinere Steuerung für den Zugriff auf Komponenten gewünscht, können Komponenten im System wiederum einen Single Access Point implementieren und so den Zugang zu sich selber prüfen.

Durch die Definition des Single Access Points definiert man auch eine Grenze, welche das System schützt. Es ist dabei wichtig nicht zu vergessen, dass entsprechender Aufwand nötig ist diese Grenze zu schützen/aufrecht zu erhalten (Bsp. Bau des Gitters um ein Areal, setzen der Firewall-Einstellungen etc.). Denn mit dieser Grenze steht und fällt die Sicherheitswirkung dieses Patterns.

Somit besteht die Umsetzung des Single Access Point Patterns aus folgenden Punkten:

1. Sicherheitsrichtlinien definieren
2. Single Access Point definieren (prominente Stelle etc.)
3. Effektive Prüfung der Sicherheitsrichtlinien umsetzen (Single Access Point kann auch einfach nur für Auditing/Logging verwendet werden)
4. Initialisierung des Systems (Session aufsetzen usw.)
5. Grenzen des Systems schützen (fortlaufend)

Vorteile

- Ein einziger Zugangspunkt zum System vereinfacht die Komplexität und verbessert die User Experience
- Es muss keine wiederholte Implementierung der gleichen Sicherheitsprüfung umgesetzt werden
- Das Single Access Point Pattern kann auf verschiedensten Abstraktionsebenen umgesetzt werden
- Die interne Komplexität eines Systems kann möglicherweise vereinfacht werden, da der Sicherheitsaspekt “zentral” umgesetzt wird

Nachteile

- Verfehlt ein Subjekt den Zugangspunkt, kann das System für ihn als nutzlos betrachtet werden

- Single Access Point <=> Single Point of Failure: Beim Ausfall des Zugangspunktes kann möglicherweise das gesamte System nicht mehr verwendet werden
- Der Zugangskontrolle muss vertraut werden können (erhöhter Aufwand für Lohn eines Wachmanns oder Schutzmassnahmen gegen Hacker etc.)
- Die Grenze des Systems ist und bleibt die schwächste Stelle im Sicherheitsdispositiv

Reallife Beispiele

- Anmeldescreens verschiedenster Betriebssysteme
- Eingangskontrolle an einem Openair Festival
Prominenz des Eingangs ist wichtig, da die Besucher sonst den Eingang nicht finden und vor den Absperrungen randalieren ;)
- Freizeitpark
Nach einmaligem Bezahlen am Eingang hat man Zutritt zu allen Attraktionen (abgesehen von den Größenkontrollen bei den Achterbahnen). Ein Shuttlebus vom Parkplatz zum Eingang erleichtert es dem Besucher, den Eingang zu finden.
- Nachtclub
Nach der Kontrolle beim Securitypersonal hat man freien Zugang zu allen Bars. Möchte man in den VIP-Bereich, ist eine weitere Kontrolle durch das Securitypersonal nötig (Eingeladen? Reserviert? Genug Bargeld? ;-))
Beispiel einer schlechten Systemgrenze: Der Notausgang kann auch verwendet werden, um sich Zutritt zu verschaffen

Mögliche Prüfungsfragen

- *Nennen Sie ein Beispiel ausserhalb der IT-Welt, welche das Single Access Point Pattern umsetzen*
Siehe "Reallife Beispiele"

3.3. Check Point

Kontext

Problem

Lösung

Vorteile

-

Nachteile

-

Mögliche Prüfungsfragen

- ?

3.4. Security Session

Wurde ein Subjekt einmal identifiziert und authentifiziert, sollen die dadurch erlangten Informationen wenn möglich nicht erneut abgefragt resp. erfragt werden müssen.

Mit der *Security Session* werden Informationen zur Identität und dem Aufenthalt eines Subjektes in einem System generalisiert gespeichert. Zudem werden diese Informationen entsprechenden Systemkomponenten zugänglich gemacht.

Kontext

Subjekt spezifische Informationen sollen zwischen den Komponenten eines gesicherten Systems ausgetauscht werden können.

Problem

Subjekte haben im seltensten Fall Zugriff auf ein komplettes System, welches sie mit anderen Subjekten teilen.

Oft wird unter Verwendung von *Identification & Authentication* Patterns die Identität eines Subjektes festgestellt. Mittels den kennengelernten *Access Control Models* wird anschliessend sichergestellt, dass jedes Subjekt nur auf Funktionen oder Ressourcen zugriff hat, für welche es auch berechtigt ist.

Beim *Single Access Point* und *Check Point* wurde aufgezeigt, dass die zentralisierte Identifizierung und Authentifizierung für ein gut entworfenes System viele Vorteile mit sich bringt: Jede Systemkomponente kann sich fortan auf ihre Kernkompetenzen fokussieren und muss sich nicht auch noch um sicherheitsrelevante Aspekte kümmern.

Oftmals sollen Systemkomponenten in einem globalen Kontext übergreifend Informationen (bspw. den Namen eines Subjektes) ablegen und austauschen können. Wie kann nun aber sichergestellt werden, dass sich auf ein spezifisches Subjekt bezogene Informationen nicht mit denen anderer Subjekte vermischen?

Weiter sollen die Aktivitäten eines Subjektes innerhalb des Systems "als Ganzes" verfolgt werden können: Befindet sich ein Subjekt bereits im System? War es für eine gewisse Zeit inaktiv oder war es aktiv im System? Hat es das System verlassen?

Lösung

Es wird ein *Session* Objekt eingeführt. Das Session Objekt enthält zum einen sicherheitsrelevante Informationen (quasi seinen "Ausweis" während dem Aufenthalt im System) und bietet den Systemkomponenten zusätzlich die Möglichkeit, beliebige Informationen zu einem Subjekt abzuspeichern.

Das Session Objekt wird nach erfolgreichem Anmelden im System (optimalerweise bspw. am Check Point) initialisiert. Meistens wird es da mit gewissen Standardwerten befüllt: Zugriffsberechtigungen um wiederholte Abfragen in der Datenbank zu vermeiden, Benutzerprofil usw.

Im Hintergrund kann ein *Manager* verwendet werden, um alle aktuellen Sessions zu überwachen. Er kann z.B. sicherstellen dass inaktive Sessions nach einer gewissen Zeit sich automatisch wieder am System frisch anmelden müssen.

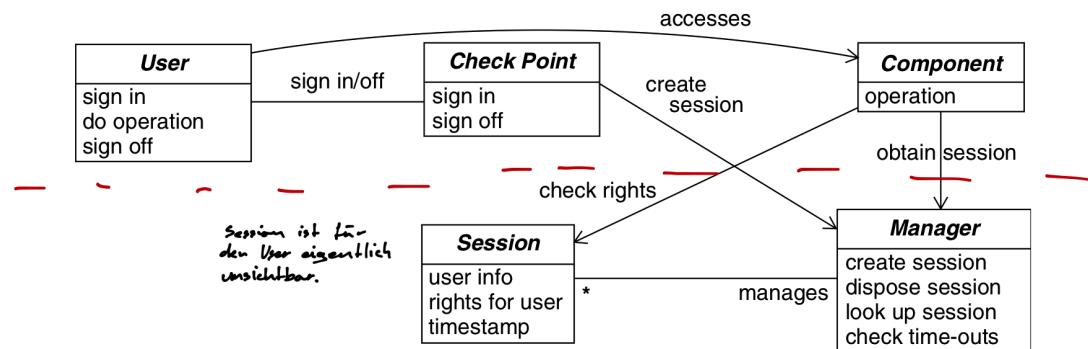


Abbildung 3.1.: Security Session: Schematischer Aufbau [Sch+06]

Damit ein Subjekte wiederkehrend mit seinem Session Objekt in Verbindung gebracht werden kann, wird eine Session ID nach aussen publiziert. Dabei ist zu beachten, dass diese für Aussenstehende keine Rückschlüsse auf tatsächliche Inhalte des Session Objektes zulassen.

Das Sequenzdiagramm in Abbildung 3.2 zeigt ein Session Objekt von seiner Erstellung bis hin zu der Zerstörung sobald das Subjekt das System verlässt.

Implementierung

1. Session Objekt einführen (klar definierte Schnittstelle zur Speicherung von Informationen (Key/Value Pairs, ...))
2. Einführung eines Session Managers zur Verwaltung der Session Objekte (Zugriff auf Session Objekte mittels Session ID's usw.)
3. Session Timeouts und die nötig werdenden Aktionen (erneut Anmelden usw.) definieren
4. Dem Subjekt ermöglichen, sich an einer Session an- und abzumelden (you don't say ;)

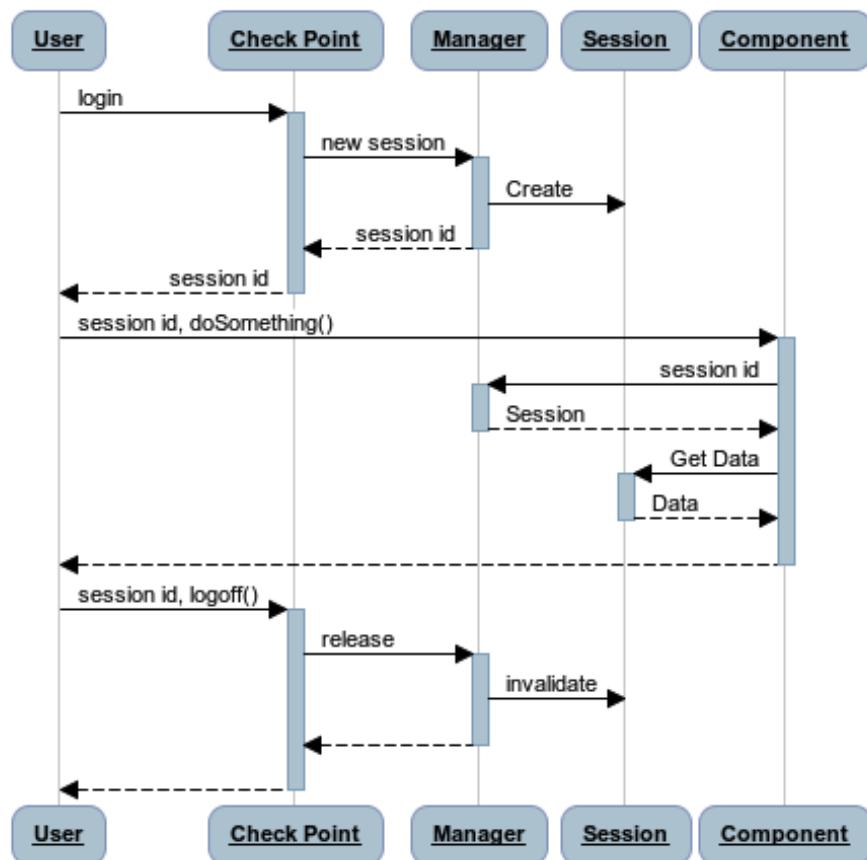


Abbildung 3.2.: Security Session: Interaktion der verschiedenen Akteure

Vorteile

- Klar definierter und zentraler Standort für jegliche Informationen zu einem Subjekt welches sich im System befindet
- Komponenten können sich auf ihre Kernfunktionalitäten konzentrieren

Nachteile

- Die Verfügbarkeit eines zentralen, globalen Objektes ermuntert möglicherweise zu unschönen Programmietechniken
- Eine Überladung des Session Objektes mit grossen Datenmengen führt zu schlechter Systemperformance
- Schlecht gewählte Session ID's lassen möglicherweise Rückschlüsse auf den tatsächlichen Inhalt des Session Objekts

Reallife Beispiele

- Jegliche Webapplikationen welche ein Benutzerauthentifizierung benötigen greifen auf die Security Session zurück, um einen Stateful-Kontext über das eigentliche Zustandslose Medium HTTP zu erzeugen.
- Beispiel aus Bachelorarbeit *Alexandre Joly, Michael Weibel & Manuel Alabor*: Wird eine Webapplikation auf mehreren CPU-Kernen ausgeführt, kommt es durch Verwendung eines In-Memory-Storages für die Session-Objekte ggf. zu Problemen, da beim Neustart eines Kerns resp. beim Neustart der gesamten Applikation die Sessions verloren gehen. Abhilfe schafft die Auslagerung der Session Objekte wie persistente Datenbanken.

Mögliche Prüfungsfragen

- *Wann wird eine Security Session erzeugt?*
Nach erfolgreicher Authentifizierung eines Subjektes. Dies kann bspw. vom Check Point initiiert werden. Optimalerweise würde dieser die Session jedoch nicht selber erzeugen, sondern den Session Manager damit betrauen.

Kapitel 4 Firewall Architectures

4.1. Packet Filter Firewall

Werden verschiedene Computernetzwerke miteinander verbunden, entstehen unweigerlich Sicherheitsrisiken. In einem Netzverbund ist es nicht immer wünschenswert, dass Besucher aus einem (fremden) Netz Zugriff auf alle Ressourcen im eigenen Netz erhalten.

Mit der *Packet Filter Firewall* kann ein- und ausgehender IP-basierter Datenverkehr analysiert und mit entsprechenden Regeln gefiltert werden.

Kontext

Das eigene Computernetzwerk wird mit verschiedensten anderen Netzen verbunden. Jedes dieser Netze besitzt unterschiedliche “Levels of Trust”.

Als kleinsten gemeinsamen Nenner läuft jegliche Kommunikation in diesen Netzen über das Internet Protocol (IP). Die dadurch entstehenden Datenpakete können aufgrund der Informationen in deren Header analysiert werden.

Problem

Hosts in fremden Netzen sind potentielle Angreifer auf Ressourcen in unserem Netz. Gibt es eine Möglichkeit, diese Hosts zu erkennen und den von ihnen ausgehenden Netzwerkverkehr bestmöglich zu blockieren?

Folgende Faktoren spielen dabei eine wichtige Rolle:

- Eine komplette Abschottung des eigenen Netzes ist keine Option: Kommunikation ist ein wichtiger Bestandteil des “Daily Business”.
- Für den Benutzer soll die Sicherheitsmaßnahme transparent sein und keinen zusätzlichen Aufwand bedeuten (Login etc.)
- Der umzusetzende Mechanismus soll flexibel auf Änderungen anpassbar sein und die organisatorischen Sicherheitsrichtlinien so präzis wie möglich abbilden.
- Die Lösung soll so wenig Leistung wie möglich benötigen

Lösung

Die *Packet Filter Firewall* analysiert ein- und ausgehenden Netzwerkverkehr. Dabei wird jedes einzelne IP-Paket auf den Inhalt in seinem Header betrachtet und mit einem Set von definierten Regeln geprüft.

Diese Regeln bestehen im Normalfall aus einer Kombination von Ports und IP-Adressen oder IP-Adress-Bereichen. Dabei kann eine Regel sowohl Zugriff gewähren als auch verbieten.

Auf diese Weise können sehr komplexe Sicherheitsdispositive gebildet und geprüft werden. Um aber auch bei komplexeren Regelsets eine optimale Performance zu erzielen ist die Reihenfolge der Regeln von grösster Bedeutung.

Beispiel: Prüfung eingehendes IP-Paket

1. Ein fremder Host möchte auf eine Ressource im eigenen Netz zugreifen.
2. Die *Packet Filter Firewall* sucht anhand der Quell-IP-Adresse sowie des Ziel-IP-Adresse und -Ports nach einer passenden Regel
3. Wird eine passende Regel gefunden, wird das Paket entsprechend zugelassen (oder verworfen, falls die Regel dies so definiert)
4. Wird keine passende Regel gefunden, kommt eine Standard-Regel zum Zuge. Möchte man hohe Sicherheit gewährleisten, besagt diese meistens, dass das Paket verworfen werden soll.

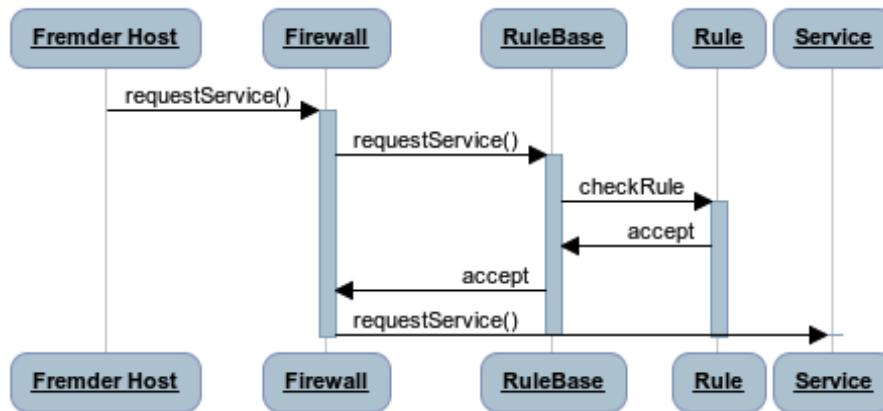


Abbildung 4.1.: Packet Filter Firewall Sequenzdiagramm

Der Akteur *RuleBase* bietet minimale Verwaltungsfunktionen (CRUD) für Firewall-Regeln.

Vorteile

- Die Firewall filter für den Benutzer transparent jeglichen Netzwerkverkehr
- Da die Firewall jedes IP-Paket beim empfangen oder senden einmal “in den Händen” hat, ermöglicht die Firewall ein ausführliches Logging an den Schnittstellen zwischen verschiedenen Netzwerken.
- Eine *Packet Filter Firewall* verschlingt minimale Ressourcen/Leistung. Unter anderem da lediglich die strukturierten Header-Informationen eines IP-Pakets analysiert werden.

Nachteile

- Fälscht ein potentieller Angreifer seine IP-Adresse, kann dies die *Packet Filter Firewall* nicht erkennen und versagt in dieser Situation.
- Die Leistungsfähigkeit der Firewall ist stark von der Reihenfolge der definierten Regeln abhängig. Beispiel: Möchte man einen kompletten IP-Adress-Bereich blockieren, macht es wenig Sinn, diesen am Ende der Regelliste zu platzieren und so alle feingranularen Regeln zuerst zu prüfen.
- Die *Packet Filter Firewall* kann keine Attacken auf Layern über IP erkennen. Da nur IP-Headers analysiert werden, können im IP-Payload problemlos schädliche Befehle/schädlicher Code enthalten sein.
- Natürlich kann die Firewall nur erfolgreich Netzwerkverkehr analysieren, welcher auch über diese geleitet wird. Es gilt also sicherzustellen, dass alle Wege in das zu schützende Netz über die Firewall(s) geleitet werden (Single Access Point)

Reallife Beispiele

- In einem Landwirtschaftsbetrieb ist jedes Tier (Netzwerkverkehr) mit einem RFID (IP-Header) ausgestattet. Will ein Tier in den Stall (zu schützendes Netz), wird es durch eine Schleuse (Firewall) geleitet. Anhand der Informationen auf dem RFID gelangt das Tier in den Stall, falls der Bauer dies vorneweg so erlaubt (Regeldefinition) hat. Darf das Tier den Stall nicht betreten, wird es wieder ins Freie geleitet.

Mögliche Prüfungsfragen

- *Was ist ausschlaggebend für die Performance einer (Packet Filter) Firewall?*
Die Optimierung der Reihenfolge der Firewall-Regeln.
- *Wie erreichen Sie ein Höchstmass an Sicherheit mit der Verwendung einer (Packet Filter) Firewall?*
Jeglicher Netzwerkverkehr muss über die Firewall geleitet werden. Weiter wird die

Standardregel für Behandlung von eingehendem Netzwerkverkehr so eingestellt, dass dieser verboten wird. Anschliessend müssen nur noch Regeln für den erlaubten Verkehr erstellt werden.

4.2. Proxy Based Firewall

Als Nachteil der “Packet Filter Firewall” wird erwähnt, dass lediglich der Inhalt des IP-Headers im Zuge der Überprüfung analysiert wird.

Die *Proxy Based Firewall* fügt der “Packet Filter Firewall” spezifische Applikations-Proxies hinzu, welche den ein- und ausgehenden Traffic überprüfen und ggf. an den internen, eigentlichen Dienst weiterleiten.

Der interne Dienst wird auf diese Weise für den externen Host komplett unsichtbar; er kommuniziert lediglich mit dem Proxy.

Kontext

Netzwerkverkehr soll auf der Ebene des Application-Layers gefiltert werden können (vgl. “Packet Filter Firewall” tut dies lediglich auf dem Network-Layer). Auf diese Weise soll sichergestellt werden, dass keine schädlichen Befehl/schädlicher Code ins eigene Netz hinein gelangt resp. aus dem eigenen Netz heraus gesendet werden kann (Würmer, Trojaner etc.).

Problem

Wie kann die “Packet Filter Firewall” so erweitert werden, dass nicht nur der IP-Header zur Filterung von Netzwerkverkehr verwendet werden kann? Wie kann auch der IP-Payload in die Filterung miteinbezogen werden?

Ergänzend zu den für die Packet Filter Firewall definierten Forces kommen folgende ergänzend hinzu:

- In unserem Netzwerk werden verschiedenste Dienste angeboten. Entsprechend Umfangreich muss auch das Wissen der Firewall über die jeweiligen Dienste sein.

Lösung

Die Firewall stellt für jeden zu schützenden Dienst einen Proxy zur Verfügung. Will ein fremder Host mit einem Dienst kommunizieren, kommuniziert er lediglich mit dem entsprechenden Proxy.

Aufgrund von definierten Regeln analysiert der Proxy den ein- oder ausgehenden Verkehr. Dabei bleibt es ihm frei überlassen ob er diesen weiterleiten, blockieren oder gar modifizieren will.

Vorteile

- Die *Proxy Based Firewall* kann Netzwerkverkehr auf Applikationsebene filtern. Sie kann dabei gezielt auf applikationsspezifische Eigenheiten eingehen und die Kommunikation ggf. sogar verändern.

Nachteile

- Für jeden Dienst wird eine konkrete Proxyimplementierung benötigt.
- Das Betreiben der Proxies sowie die genauere Analyse des kompletten IP-Pakets führt zu höheren Kosten sowie tendenziell höherem Performance Overhead.
- Erhöhte Komplexität aufgrund der zusätzlichen Sicherungsebene.

Reallife Beispiele

- NAT - Network Address Translation

Mögliche Prüfungsfragen

- Nennen Sie konkrete Anwendungen für die *Proxy Based Firewall*. Zugang zu bestimmten Internetseiten blockieren (HTTP Proxy), “Network Address Translation” um die interne Netzwerkstruktur zu verschleiern. Idee: Telnet-Proxy welcher gewisse Kommandos nicht zulässt.

4.3. Stateful Firewall

Mit der Proxy Based Firewall wurde bereits eine erweiterung der einfachen Packet Filter Firewall vorgestellt.

Die Stateful Firewall erweitert die Proxy Based Firewall. Dabei erhält sie die Möglichkeit, die verarbeitete Kommunikation nicht nur Paketweise zu bewerten und zu klassifizieren, sondern diese auch mit bereits vergangenen Kommunikationsvorgängen in Zusammenhang zu bringen.

Kontext

Um bessere Sicherheit bspw. gegen Denial of Service [wikc] zu gewährleisten, soll eine zustandslose Firewall die Möglichkeit erhalten, die untersuchten Pakete in einen höheren Zusammenhang bringen zu können.

Problem

Wie können eingehende Pakete nicht nur einzeln kontrolliert (vgl. Packet Filter Firewall) sondern auch miteinander in Verbindung gebracht werden?

Wie kann dieser Sachverhalt weiter dazu verwendet werden, eine höhere Sicherheit zu gewährleisten?

Lösung

Stellt ein Client eine Verbindung zur Firewall her, wird diese Verbindung in einer Liste/Tabelle zwischengespeichert und als *geöffnet* markiert.

Dies ermöglicht das optimierte überprüfen (oder eben gerade nicht-überprüfen) von weiteren eingehenden Paketen des selben Clients.

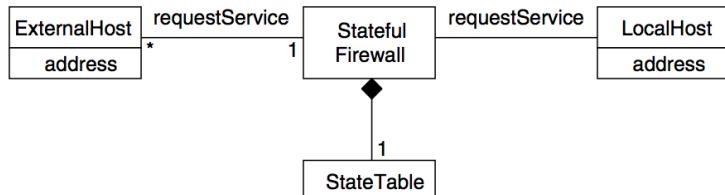


Abbildung 4.2.: Stateful Firewall: Schematischer Aufbau

Implementierung: Handling eines Requests

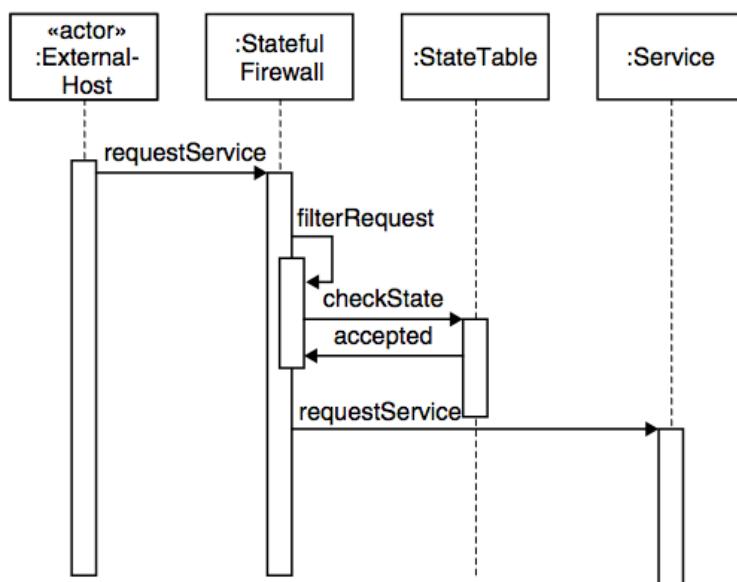


Abbildung 4.3.: Stateful Firewall: Ablauf [Sch+06]

1. Client (External Host) greift auf das System zu
2. Die Stateful Firewall prüft, ob die Verbindung zum Client bereits in der State Table vorhanden ist. Sollte dies der Fall sein, wird der Request weitergeleitet.
3. Existiert die Verbindung noch nicht in der State Table, wird der Request gem. der Packet Filter Firewall geprüft. Soll der Request zugelassen werden, wird die Ver-

bindung zum Client in die State Table eingetragen und der Request anschliessend weitergeleitet.

Neben einer Kombination mit einer Packet Filter Firewall ist auch eine Verwendung der Stateful Firewall mit der Proxy Based Firewall problemlos umsetzbar.

Vorteile

- In der einfachen Packet Filter Firewall-Kombination ist die Implementierung relativ kostengünstig und bietet einen guten Schutz
- Die Effizienz im Bezug auf den Sicherheitsaspekt der einfacheren Firewall Patterns kann durch die neuen Zustandsinformationen gesteigert werden
- Für neue Attacktypen müssen lediglich neue Vergleichsalgorithmen/Regeln implementiert werden

Nachteile

- Mit dem Wissen über die Existenz einer State Table kann theoretisch eine Attacke speziell zur Überlastung der Firewall geplant werden
- Es können nur Attacken erkannt werden, für welche auch entsprechende Erkennungsalgorithmen vorhanden sind (Firmwareupgrades nötig?)

Mögliche Prüfungsfragen

- *Ist eine Stateful Firewall ein eigenständiges Pattern?*
Nein, es erweitert mindestens das Packet Filter Firewall Pattern.

Kapitel 5 **Secure Internet Applications**

5.1. Information Obscurity

Grundsätzlich ist anzunehmen dass jedes System irgendwann einer Attacke nachgibt. Das Information Obscurity Pattern stellt sicher, dass sensible Daten auch innerhalb des geschützten Systems bei einem möglichen ungewollten Zugriff weiter geschützt sind.

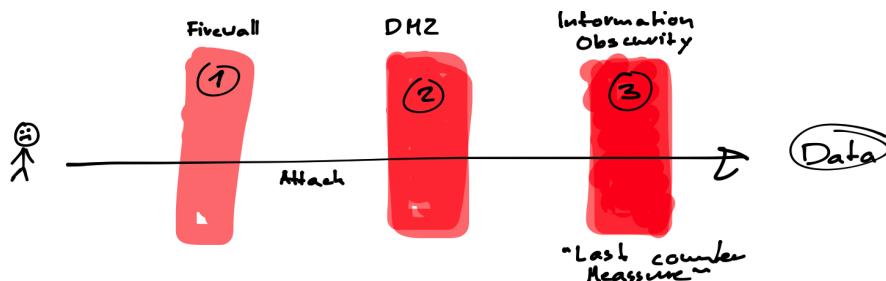


Abbildung 5.1.: Information Obscurity als letzte Sicherheitsmaßnahme

Kontext

Ein Internet Server-System (Webserver, Applikationsserver, Datenbankbackend etc.) tauscht zwischen den einzelnen Komponenten Informationen aus. Das System an sich ist bereits nach Außen geschützt.

Problem

Wie kann sichergestellt werden, dass sensitive Informationen welche zwischen den einzelnen Systemkomponenten ausgetauscht wird und evtl. innerhalb von diesen abgelegt ist beim Zugriff von Unbefugten weiterhin geschützt sind?

- Es gilt abzuwägen welche Informationen überhaupt besonders geschützt werden sollen. Nicht jede Information ist hoch sensitiv und rechtfertigt die nötige Leistung zur Ver- und Entschlüsselung.
- Zu einer Ver- und Entschlüsselung sind entsprechende kryptographische Schlüssel notwendig. Diese gilt es wiederum entsprechend zu sichern.

Lösung

Nachdem alle vorhandenen Informationsarten klassifiziert wurden, werden die als sensitiv bewerteten mittels passender Verschlüsselungsmechanismen zusätzlich gesichert.

Folgende Komponenten sind beim Information Obscurity Pattern beteiligt:

- Ein *Key* zur Ver- und Entschlüsselung der Informationen
- Ein *Key Store* welcher die sichere Aufbewahrung und Herausgabe der Keys gewährleistet
- Eine *Kryptographiekomponente* welche die eigentliche Arbeit übernimmt

Nicht zu vergessen ist natürlich die eigentliche Anwendungskomponente welche über die Kryptographiekomponente auf die verschlüsselten Informationen zugreift. Weiter sollte der Key Store über eine *Protected Location* verfügen, in welcher er die Keys vor unbefugtem Zugriff geschützt (USB-Stick etc.) aufbewahren kann.

Ergänzungen

- Es ist nicht immer nötig, dass verschlüsselte Informationen entschlüsselt werden müssen, um auf deren Inhalt schliessen zu können.
Beispiel: Passworthashes werden mit dem Hash der Benutzereingabe verglichen
- Jeder Schutz für sensitive Daten ist zwecklos, wenn bspw. der Webserver über einen Cache verfügt welcher alle gerenderten HTML-Informationen unverschlüsselt zwischenspeichert. Es gilt also jede Komponenten im System einem genauen Audit zu unterziehen.
- Der Sicherung von Konfigurationsinformationen (Keys) sollte besondere Aufmerksamkeit geschenkt werden: Oft können diese ohne es zu bemerken kopiert werden und somit die Information Obscurity Massnahmen nutzlos machen.
- Information Obscurity muss nicht zwingend mit einer Verschlüsselung im eigentlichen Sinne zusammenhängen: Bspw. kann man durch generische Bezeichnungen für Server (Sv1, Sv2 usw. statt Dataserver, Keyserver usw.) bereits dem potentiellen Eindringling bereits einen Stein in den Weg legen und dem eigenen Sicherheitsteam einen Zeitvorteil verschaffen.
- Wie so oft ist auch bei Information Obscurity die Balance zwischen Nutzen, Kosten und Performance zu finden.

Vorteile

- Sollte ein Angreifer in das gesicherte System gelangen, bietet Information Obscurity ein weitere Schicht an zusätzlicher Sicherheit für sensitive Informationen
- Da im optimalen Fall nicht alle Informationen mittels Information Obscurity geschützt werden, halten sich Performanceeinbussen in vertretbaren Grenzen.

Nachteile

- Die Performance kann tendenziell leiden wenn zu viele Informationen durch einen Ver- und Entschlüsselungsprozess geschleust werden müssen
- Die Komplexität des Systems erhöht sich, was wiederum Auswirkungen auf Wartbarkeit usw. hat.
- Komponenten welche von der Information Obscurity betroffen sind werden tendenziell aufwändiger und teurer in der Entwicklung.

Reallife Beispiele

- Verschiedenste OpenSource Projekte legen keine Klartext-Passwort in der Benutzerdatenbank ab sondern lediglich einen Hash (z.B. MD5) von diesem. Beim Login wird vom eingegebenen Passwort ebenfalls ein Hash erstellt und mit dem in der Datenbank hinterlegten verglichen.
- Beim Einbruch ins PlayStation Network von Sony (Online Gameing Platform für die Sony PlayStation Konsolen) wurden zig tausende Kreditkarteninformationen abgerufen und anschliessend auf dem Schwarzmarkt verkauft. Entsprechende Information Obscurity Massnahmen für eben diese Informationen hätten evtl. grösseren (Image-) Schaden eingrenzen können.

Mögliche Prüfungsfragen

- *Welche Informationen sollten durch Information Obscurity geschützt werden?*
Dies kann nicht generell beantwortet werden. Jedes System, jede Situation bedarf einer spezifischen Analyse und Klassifizierung der vorliegenden Informationen. Grundsätzlich sind aber für ein Unternehmen geschäftskritische Daten (seien diese operationeller oder aber auch rufbezogener Natur) tangiert.

5.2. Secure Channels

Kommunikation über Netzwerke/das Internet können und werden abgefangen und gesehen. Gibt es eine Möglichkeit, diese Netze zu verwenden und trotzdem eine sichere Punkt zu Punkt Verbindung zu gewährleisten?

Kontext

Das System soll Informationen zu Clients in einem Netzwerk/dem Internet senden und von diesen empfangen können. Dabei sollen sensitive Informationen verschlüsselt resp. für fremde Augen abgeschirmt ausgetauscht werden können. Sensitive Informationen haben dabei einen geringen Anteil an der gesamten ausgetauschten Kommunikation.

Problem

Wie können sensitive Informationen auf einem öffentlichen Netzwerk gesichert übertragen werden?

Wichtige Faktoren sind dabei:

- Die meiste Kommunikation bedarf keiner Sicherheitsmassnahmen. Sensitive Informationen müssen jedoch gesichert übertragen werden können, sobald sie das/die gesicherten Systeme verlassen.
- Verschlüsselung von Daten benötigt mehr Leistung
- Die verschlüsselte Kommunikation soll auch mit Unbekannten Partnern möglich sein; es soll dementsprechend nicht notwendig sein, spezialisierte Software oder Hardware zu installieren (Client und/oder Server)

Lösung

Sollen sensitive Informationen ausgetauscht werden ist ein Secure Channel, ein sicherer Kanal zu erstellen, welcher die entsprechenden Informationen verschlüsselt.

Für "normal" klassifizierte Informationen soll weiterhin der standardmässige Kommunikationskanal verwendet werden.

Dabei hängen die einzelnen Komponenten wie folgend beschrieben voneinander ab:

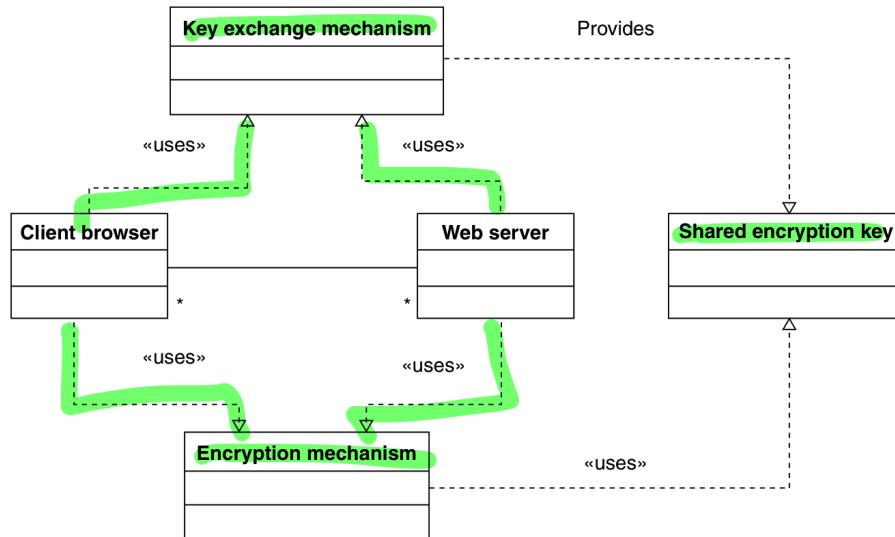


Abbildung 5.2.: Komponenten des Secure Channels Patterns [Sch+06]

- Der *Web server* stellt die eigentlichen Informationen bereit und kann mit dem *Client browser* über einen universalen *Key exchange mechanism* Schlüssel zur gesicherten Kommunikation aushandeln.

- Der *Client browser* verfügt ebenfalls über den universellen *Key exchange mechanism* über welchen er mit dem *Web server* das Setup einer gesicherten Verbindung durchführen kann.
- Sowohl der Client browser als auch der Web server können auf einen *Encryption mechanism* zugreifen, welcher sie befähigt, mittels dem ausgehandelten *Shared encryption key* einen Secure Channel einzurichten.

Beispiel: Secure Socket Layer (SSL)

Ein heute täglich verwendetes Beispiel bietet SSL. Alle gängigen Browser und Web Server Implementation ermöglichen den verschlüsselten Datenaustausch via dem Secure Socket Layer Protokolls.

Beim Erstellen eines Secure Channels wird dabei zuerst immer ein sogenannter *Session Key* ausgetauscht, welcher zur symmetrischen Verschlüsselung von Nachrichten verwendet werden kann:

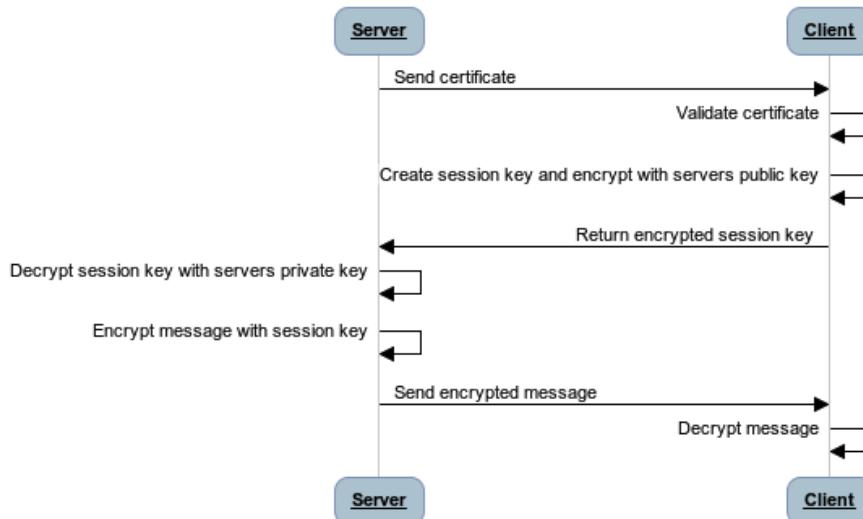


Abbildung 5.3.: Aushandeln eines Session Keys zur sicheren Kommunikation via SSL

Dabei fällt auf, dass zur Ermittlung des Session Keys eine asymmetrische Verschlüsselung zur Anwendung kommt. Diese benötigt mehr Leistung und kommt aus diesem Grund anschliessend nicht mehr zur Verwendung.

Der Session Key kann mitten in einer aktiven Verbindung ausgewechselt werden. So erschwert man potentiellen Angreifern zusätzlich das dechiffrieren der Nachrichten.

Ergänzungen

- Die Verwendung eines Load Balancers und mehreren Web Servern erschwert die Verwendung eines Secure Channels: Nach dem Aufbauen einer Verbindung zum

einen Web Server muss der Load Balancer nicht gezwungenermassen bei einem nächsten Request wieder auf den selben Web Server weiterleiten.

Um dieses Problem zu umgehen kann ein Load Balancer eine Verbindung an einen spezifischen Web Server "pinnen", solange die entsprechende SSL aktiv ist.

Vorteile

- Die Sicherheit von übertragenen Informationen ist gewährleistet. Sie können auf dem Weg zu ihrem eigentlichen Ziel nicht gelesen werden.
- Es ist keine spezifische Software/Hardware notwendig; SSL wird von allen aktuellen Browsern unterstützt.
- Durch den Key exchange mechanism ist es möglich, dass sich eigentlich unbekannte Partner einen Secure Channel aufbauen können.
- Normale, ungesicherte Kommunikation wird nicht beeinträchtigt.

Nachteile

- Die Verwendung eines Secure Channels benötigt an beiden Enden mehr Leistung.
- Verschiedene Massnahmen um ein System skalierbar zu machen (Load Balancing) verkomplizieren die Verwendung eines Secure Channels
- Erhöhte Wartungskosten, evtl. sogar höhere Anschaffungskosten für Serverhardware um zusätzliche Leistung stellen zu können.

Mögliche Prüfungsfragen

- *Warum verwendet nur der Key exchange mechanism eine asynchrone Verschlüsselung?*
Asynchrone Kryptographie Methoden sind aufwändiger zu berechnen. Aus diesem Grund wird lediglich der Session Key für den Secure Channel über diese sicherere Verschlüsselungsmethode übertragen.
Der Session Key wird während dem Aufrechterhalten des Secure Channels beliebig ausgetauscht um so ebenfalls eine hohe Sicherheit zu gewährleisten.

Anhang A **Abbildungen, Tabellen & Quellcodes**

Abbildungsverzeichnis

1.1. Authorization Klassendiagramm	4
1.2. Basic Role Based Access Control Klassendiagramm	6
1.3. RBAC mit Composite, Admins & Abstract Session	6
1.4. Multilevel Security Klassendiagramm	9
1.5. Reference Monitor - Klassendiagramm	11
1.6. Reference Monitor - Sequenzdiagramm [Sch+06]	11
2.1. Generischer Ansatz von I&A “Using functions” [Sch+06]	16
3.1. Security Session: Schematischer Aufbau [Sch+06]	26
3.2. Security Session: Interaktion der verschiedenen Akteure	27
4.1. Packet Filter Firewall Sequenzdiagramm	30
4.2. Stateful Firewall: Schematischer Aufbau	34
4.3. Stateful Firewall: Ablauf [Sch+06]	34
5.1. Information Obscurity als letzte Sicherheitsmaßnahme	36
5.2. Komponenten des Secure Channels Patterns [Sch+06]	39
5.3. Aushandeln eines Session Keys zur sicheren Kommunikation via SSL	40

Tabellenverzeichnis

2.1. I&A Requirements: Funktionale Anforderungen	17
2.2. I&A Requirements: Nichtfunktionale Anforderungen	18
3.1. Access Control Requirements Requirements: Funktionale Anforderungen . .	21
3.2. Access Control Requirements: Nichtfunktionale Anforderungen	21

Quellcodeverzeichnis

Anhang B Literatur

- [Sch+06] Markus Schumacher u. a. *Security Patterns - Integrating Security and Systems Engineering*. 1. Aufl. John Wiley & Sons, Ltd, 2006. ISBN: 978-0-470-85884-4.
- [wika] wikipedia.org. *Bell-LaPadula-Sicherheitsmodell*. URL: <http://de.wikipedia.org/wiki/Bell-LaPadula-Sicherheitsmodell> (besucht am 03.03.2013).
- [wikb] wikipedia.org. *Biba-Modell*. URL: <http://de.wikipedia.org/wiki/Biba-Modell> (besucht am 03.03.2013).
- [wikc] wikipedia.org. *Denial Of Service*. URL: http://de.wikipedia.org/wiki/Denial_of_Service (besucht am 14.04.2013).

Anhang C **Glossar**

ACL

Access Control List; eine Liste mit Zugriffsregeln für eine bestimmte Resource. 10

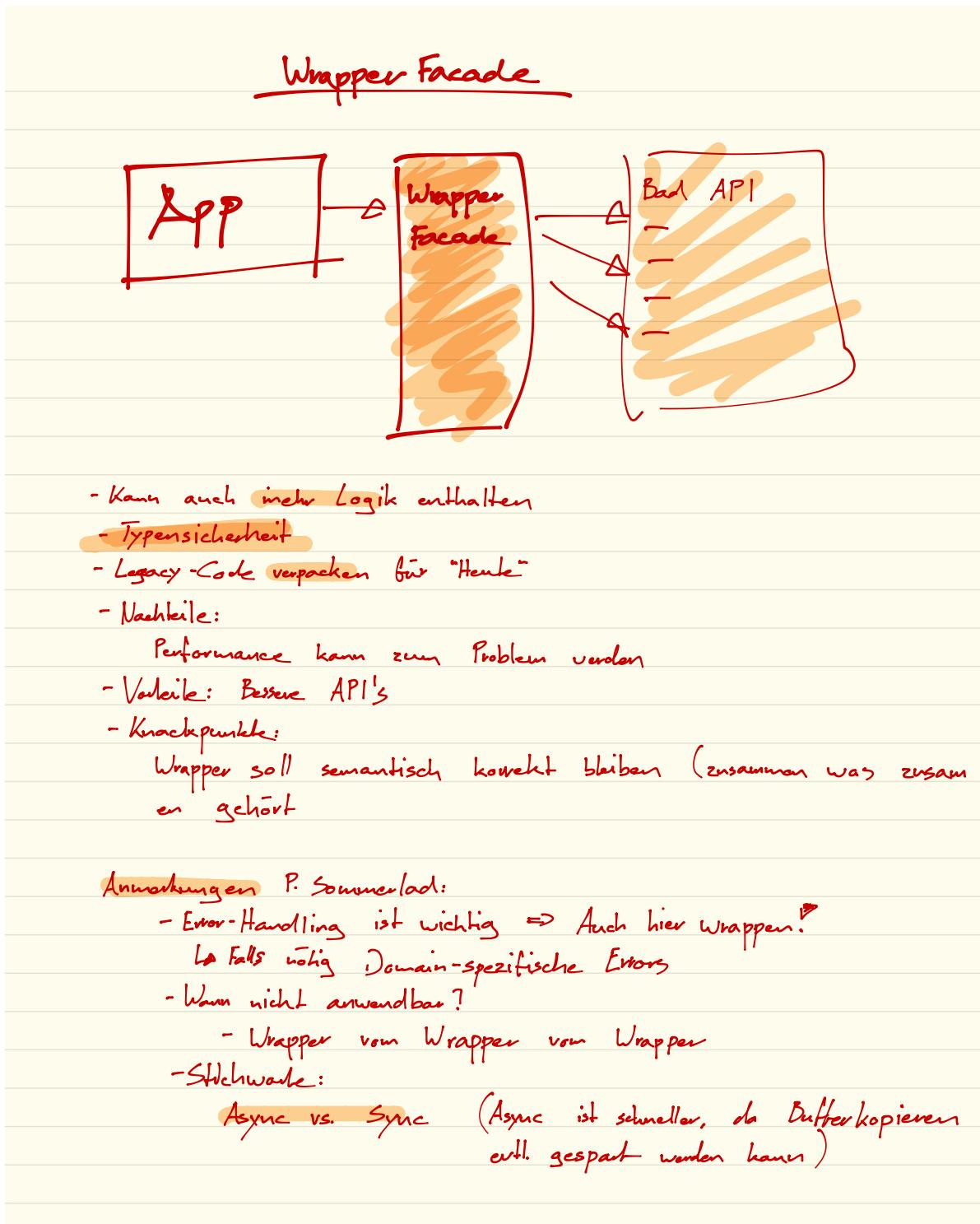
CRUD

CRUD steht als Abkürzung für *Create, Read, Update and Delete* und ist damit ein Synonym für die grundlegenden Mutationsoperationen von Informationen.. 30

RBAC

Role Based Access Control; Siehe Abschnitt 1.2. 13, 14

Anhang D **Workshops**



Fault Tolerant Systems

Introduction: Zusammenhang Fault, Error & Failure

Fault: Bug, Ursache

Error: Zustand

Failure Effektives Problem

↳ Zu vermeidendes Problem

- Failure definieren sich im Normalfall durch Abweichung von der Spec

- Unterschiedliche Faults können zu gleichen Errors/Failures führen

- Coverage: Wahrscheinlichkeit dass sich ein System innerhalb gegebener Zeit wieder erholen kann: Mean Time To Failure } Mean Time Between Failure
Mean Time To Recover

$$\hookrightarrow \text{Reliability: } e^{-\frac{t}{MTTF}}$$

- FIT: $\frac{\# \text{ Failures}}{1 \cdot 10^3 \text{ h}}$ ⇒ Failures in Time

⇒ Stichwort: Server-Zuverlässigkeit

Fail Silent: Bei Fehler übernimmt automatisch andere Komponente

Fail Consistency: Man muss herausfinden welche Systemkomponenten fehlerhaft sind

Malicious Failure: Man kann nicht einfach herausfinden welche Systeme fehlerhaft sind ⇒ Byzantinische Generäle zur Abstimmung

Architekturpatterns Fault Tolerance

12.03.2013

"Allgemeingültige" Patterns für gesamte Architekturen

Units of Mitigation

Problem: Fehler soll nicht gesamtes System beeinträchtigen
⇒ Beschränkung auf "Unit", bspw. try-catch-Block
⇒ Unitgröße ist essentiell (zu gross: simulös,
zu klein: Code-Aufwand)

Lösung: Aufteilen in Units, jede Unit enthält Logik für eigene Fehler

Beispiele für Units: → Funktionsgruppen

- try-catch, CPU-Cores, Threads, Layers, Interfaces

Fehler bleiben Unit-spezifisch ⇒ Erkennung & Behebung bleiben intern

Was passiert solange eine Unit mit Fehlerbehandlung beschäftigt ist?

- Abhilfe durch Redundanz (AKW-Kühlsystem)
- Queering

Correcting Audits

Begriffe: statische Daten: User ID, dynamische: Wechselkurs

Problem: Defekte Daten sollen so früh wie möglich erkannt und korrigiert werden. Werden solche Daten gefunden, wird geprüft, wie weit sich der Fehler evtl. schon ausgebreitet hat.

Lösung: Finden: Strukturelle Fehler; Zusammenhänge (Vorsch. Umrechnungen des selben Wertes), macht der Wert Sinn?

⇒ Datendesign für einfache Prüfung anlegen

Korrigieren: Direkt vom Programm

Repeat Finden, um Korrekturen zu prüfen

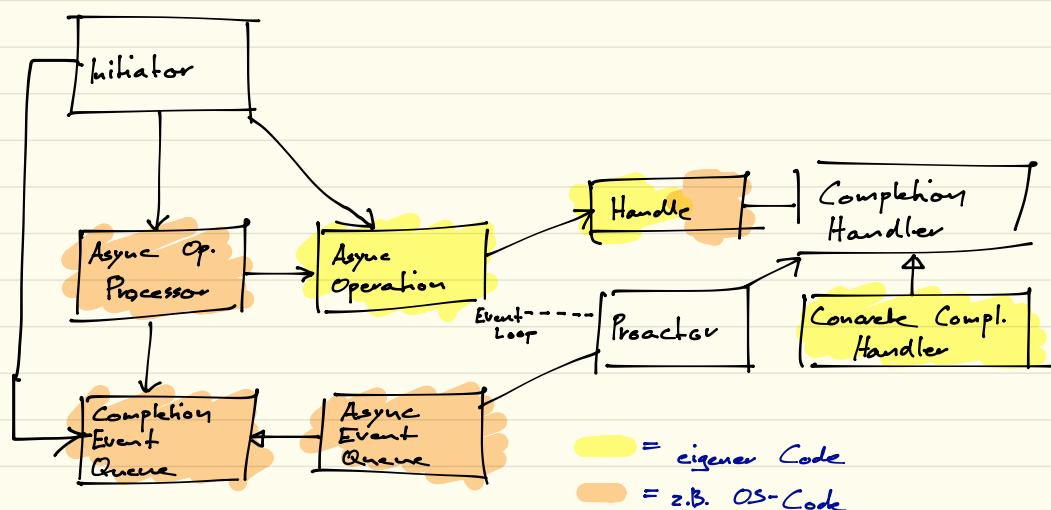
Escalation

Problem: Was passiert, wenn Fehler immer wieder auftritt?

Lösung: Fehler als externe Instanz nach aussen weitergeben

- bspw. Operator
- bspw. Fehlerbehandlungsdienst.

Proactor



⇒ NS Operation Queue? Warum "Proactor"? ⇒ Pattern arbeitet selbstständig eine Queue ab.

Vergleich Reactor: Reactor "antwortet sofort", Proactor entscheidet selber wann er welche gequeckten Operations ausführen soll
⇒ ermöglicht z.B. Priorisierung der Operations

Knackpunkte: Asynchrone Entwicklung vs. sequentiell

Vorteile:

- Parallelisierung I/O & Completion Handler
- Tendenziell robuster, da entkoppelt (Async hält)

(⇒ Warum Async I/O schneller? OS-näher)

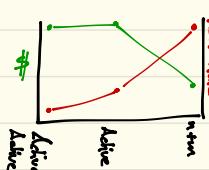
Fault Tolerant Systems: Redundancy

Redundanz sagt nicht, dass "Not-System" identisch sein muss... 13.03.2013

Typen

- ① Räumliche Redundanz (z.B. Hardware aufteilen etc)
- ② Zeitliche Red. (Berechnungen wiederholt ausführen)
- ③ Informatisch (Daten mehrmals abgelegt zum Vergleichen)
↳ z.B. Punkte speichern, dann Distanz berechnen

Räuml. Red.



• Aktiv-Aktiv Alle Redundanzen immer aktiv (Load Balancing...)

• Aktiv-Passiv Redundanz ist passiv, bis sie gebraucht wird (Notstrom)

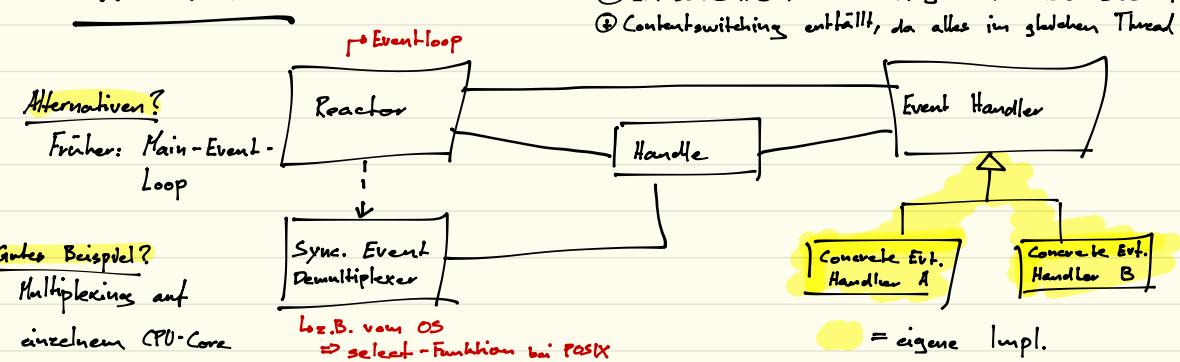
• n+m 5 aktiv, 3 passiv \Rightarrow Abwärmen, optimieren

Recovery Blocks Gleiche Aufgaben von verschiedenen Implementierungen ausführen lassen, Ergebnis vergleichen & bestes wählen
 \Rightarrow n-Version-Programming

Beispiel: Verschiedene Sort-Algos



Reactor



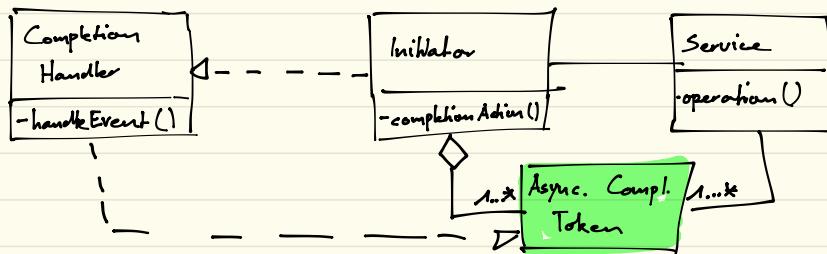
- ① Ein schlechter Handler kann ganzen Reactor blockieren
- ② Contextswitching entfällt, da alles im gleichen Thread

Command Processor vs Reactor
 Reactor looppt über registrierte Events, und führt entsprechende Handler aus
 Command Processor führt lediglich Code aus, ohne "Events"

Was tun gegen Freeze?
 Evtl. auslagern in eigene Threads

Asynchronous Completion Token

26.03.2013



Idee

Zustandsloses Dienst einfach mit einem Zustand verschen
Token kann "Alles" sein; Pointer, Wert, Funktion... ⇒ kann für Schabernack missbraucht werden

Token Passing

Ruft ein Service einen weiteren Service auf, kann das Token weitergereicht werden.

Beispiel

- HTTP-Cookie ist ein "ACT" ⇒ Verschlüsselung & Signieren
- Starbucks Card

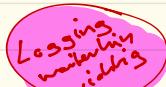
Minimize Human Intervention

Idee

Fehlerquelle "Mensch" minimieren

Situationen

- Mensch vergisst etwas zu tun ⇒ unterstützen



- Mensch versucht etwas unerlaubtes/unerwartetes zu tun

⇒ verhindern, dass Mensch unerwartetes tun kann (z.B. UI-Blocking während Verarbeitung)

Weiteres

- System soll versuchen, Fehler selber zu lösen (keine Popups, ...)
- Gut für unerfahrene Benutzer

Beispiel

Zur HB Blackout: Kabel wurde durchtrennt, Operator hat fälschlicherweise Reparatur eingeleitet, austausch von

Someone in Charge

Simple

Immer ist eine Komponente für den Fehler verantwortlich, resp. dessen Behebung ⇒ Falls nicht befähigt: Escalation
z.B. wichtig in verteilten Systemen