# Sicherheit in Verteilten Systemen

## Exposé

*Des Studienganges Informatik an der Dualen Hochschule Baden-Württemberg in Stuttgart am Campus Horb*

Von

Benita Dietrich und Paul Finkbeiner

| | |
|---|---|
| Matrikelnummern, Kurs | 2827561, 5804452, INF2018 |
| Fach | Software Engineering |
| Betreuer / Dozent | Prof. Dr. Antonius van Hoof |

# Motivation

In der Vergangenheit kam es bei großen Unternehmen wie Facebook, Microsoft, Visa- und MasterCard zum Teil mehrmals zu einer Entwendung von Kundendaten. Durch Attacken wie Buffer Overflows, Viren oder andere Angriffsvektoren werden Maschinen und Benutzer auf der ganzen Welt bedroht. Die Entwicklung des Internets legte ein besonderes Augenmerk auf den Bereich der Netzwerksicherheit. Trotz vieler Bemühungen von IT-Sicherheitsexperten und dem vorhanden sein leistungsfähiger Sicherheitsprotokolle und kryptografischen Modulen kann ein vollständig sicheres System immer noch nicht gewährleistet werden. Oftmals ist in dem Zusammenhang mit Daten Leaks nicht unbedingt die Kommunikation zwischen Client und Server, sondern die eigentliche Software am Datenverlust maßgeblich beteiligt. Die Gründe für das Schreiben unsicherer Software liegen oftmals an der mangelnden Wahrnehmung von Fehlern seitens der Softwareentwickler oder der mangelnden Verwendung von konkreten Mustern (Patterns) zur Lösung von Sicherheitsproblemen. In der Software Entwicklung wird oftmals durch Frameworks bereits zur Entwicklungszeit die Möglichkeit mitgeliefert bestimmte Sicherheitsmechanismen zu verwenden. Der Entwickler hat die Aufgabe diese verstehen und richtig einsetzten zu können. Ein deutlicher Trend ist momentan im Autonomisierungsbereich zu beobachten. Mit dem steigenden Einsatz von Software in z.B. Haushaltsgeräten wird sich das Thema Sicherheit noch verschärfen. Kernziel der Ausarbeitung ist unter anderem das Aufzeigen der Zusammenhänge zwischen Sicherheitsaspekten in der Infrastruktur der Software und anderer Bereiche mit einem Fokus auf die verteilten Systeme. Der Sachverhalt wird am Beispiel von heutzutage weit verbreiteten elektronischen Zahlungsmitten aufgezeigt.

# Fragestellung

Im Rahmen der Arbeit soll die zentrale Frage “Wie können verteilte Systeme sicher gestaltet und implementiert werden?” beantwortet werden.

Zunächst sollen die Begriffe Sicherheit und verteilte Systeme definiert werden, um einen ersten Einblick in das Thema zu bieten. Hinführen soll die Einführung auf die Beantwortung der Frage, was vor wem im System geschützt werden muss. Auf dieser Basis kann beschrieben werden, was es für Angriffe auf verteilte Systeme gibt. Welche Sicherheitslücken können von Angreifern ausgenutzt werden? Weiterhin sollen Anforderungen an verteilte Systeme abgeleitet und konkret definiert werden. Welche Sicherheitsdienste werden benötigt, um diese Anforderungen umzusetzen? Neben einer allgemeinen Definition dieser Dienste soll auch ein konkreter Vergleich mit der tatsächlichen Praxis erfolgen. Wie erfolgt die Sicherstellung eines sicheren Systems in der Praxis? Für den Vergleich kann ein Beispiel herangezogen werden. Um zu zeigen, dass das theoretisch erläuterte funktioniert, soll ein Prototyp entwickelt werden. Der Prototyp soll abstrakt einige Sicherheitsdienste implementieren und so das zuvor erklärte demonstrieren. Zur Umsetzung der Prototypen sollen geeignete Technologien und Architekturen gesucht und evaluiert werden, sodass der beste und einfachste Ansatz ausgewählt wird.

# Methoden

Als Methode zur Einarbeitung in das Thema und zur Definierung der Angriffe, Sicherheitslücken und Sicherheitsdienste ist eine umfassende Literaturrecherche mit wissenschaftlichen Quellen notwendig. Aus dem erarbeiteten Wissen können dann in Eigenarbeit die Anforderungen an die verteilten Systeme herausgearbeitet werden.

Um anschließend die praktische Implementierung und Verwendung der Sicherheitsdienste beurteilen zu können, sollen gewählte beispielhafte verteilte Systeme untersucht werden. Sofern verfügbar, bietet sich neben einem Einblick in die Architektur, auch einen Einblick in den Code an.

Zuletzt soll gemeinsam ein abstraktes Beispiel für die Demonstrierung des Einsatzes der Sicherheitsdienste gesucht werden. Hierfür muss mittels Literaturrecherche neben einer geeigneten Technologie auch die konkrete Umsetzungsvariante entschieden werden. Das Beispiel soll als ein Prototyp entwickelt werden und vorführen, wie verteilte Systeme sicher gestaltet werden können.

# Ausblick (Fazit)

Die Betrachtung verschiedener Sicherheitsaspekte im Zusammenhang mit elektronischen Zahlungsmitteln gab einen detaillierten Überblick über die präferierte Technologie und Implementierungsverfahren. Die Auswirkungen von fehlerhaften Implementierungen und Lücken im Bereich der Netzwerksicherheit stellten dabei die Negativbeispiele dar. Viele der genannten Themen setzten ein Grundwissen von sicherheitstechnischen Systemen voraus, die im Zuge der Ausarbeitung ebenfalls erläutert wurden.

Mithilfe der eigenen Implementierung war in geringem Umfang eine Re-Konturierung des Sachverhaltes möglich. Die Implementierung eines Prototyps lieferte wichtige Kenntnisse, die bei dem Verständnis von komplexen Sachverhalten halfen.

Die In der Arbeit ermittelten Sachkenntnisse sollen, die notwenigen Bestandteile zur Umsetzung eines sicheren verteilten Systems liefern.

# Gliederungsentwurf

1. **Einleitung**
   - **1.1. Einführung in verteilte Systeme (1 Seite)**
     Eine kurze Einführung, die verteilte Systeme definiert und die Merkmale nennt
   - **1.2. Sicherheit (1 Seite)**
     Definierung des Begriffes Sicherheit in Bezug auf die verteilten Systeme. Was muss vor wem im System geschützt werden?
2. **Sicherheitslücken**
   - **2.1. Angriffe (2 Seiten)**
     Beschreibung und Klassifizierung möglicher Angriffe und welche Systemlücken genutzt werden können
   - **2.2. Anforderungen an verteilte Systeme (1 Seite)**
     Aus vorherigem Kapitel abgeleitete Anforderungen an die verteilten Systeme, um Sicherheit zu garantieren und Angriffe zu verhindern.
3. **Sicherheitsdienste**
   Erläuterung der verschiedenen Sicherheitsdienste, die ein verteiltes System nutzt. (1 Seite zu jedem Punkt)
   - **3.1. Vertraulichkeit**
   - **3.2. Authentifizierung**
   - **3.3. Integrität**
   - **3.4. Nicht-Anfechtbarkeit**
   - **3.5. Zugriffsteuerung/ Autorisierung**
   - **3.6. Verfügbarkeit**
4. **Sicherheit verteilter Systeme in der Praxis (4 Seiten)**
   Beschreibung, wie die Sicherheitsdienste in der Praxis umgesetzt werden. Hier soll Bezug auf ein praxisnahes Beispiel genommen werden
5. **Implementierung (2 - 3 Seiten)**
   Das im vorherigen Kapitel erklärte Beispiel soll in abstrakter Weise als ein Prototyp implementiert werden.
6. **Fazit (1 Seite)**

# Zeitplan

Der anliegende Projektplan ist in Kalenderwochen eingeteilt, um zur Bearbeitung des Projektes flexibler zu sein. Die Einteilung der einzelnen Themen ist bislang noch nicht konkretisiert.

| Aufgaben | Verantwortlich | Start | Ende | Tage | Status | KW40 | KW41 | KW42 | KW43 | KW44 | KW45 | KW46 | KW47 | KW48 | KW49 | KW50 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Projektbeginn** | | | | | | | | | | | | | | | | |
| Projektthema finden | Paul & Benita | 29.9 | 6.10 | 14 | Abgeschlossen | | | | | | | | | | | |
| **Vorarbeiten** | | | | | | | | | | | | | | | | |
| Exposé erstellen | Paul & Benita | 2.9 | 2.9 | 14 | In Bearbeitung | | | | | | | | | | | |
| **Bearbeitungsphase** | | | | | | | | | | | | | | | | |
| Einleitung | Paul & Benita | | | 7 | Nicht begonnen | | | | | | | | | | | |
| Sicherheitslücken | Paul & Benita | | | 14 | Nicht begonnen | | | | | | | | | | | |
| Sicherheitsdienste | Paul & Benita | | | 14 | Nicht begonnen | | | | | | | | | | | |
| Sicherheit verteilter Systeme i.d.P | Paul & Benita | | | 14 | Nicht begonnen | | | | | | | | | | | |
| Implementierung | Paul & Benita | | | 14 | Nicht begonnen | | | | | | | | | | | |
| Fazit | Paul & Benita | | | 14 | Nicht begonnen | | | | | | | | | | | |
| Ausblick | Paul & Benita | | | 14 | Nicht begonnen | | | | | | | | | | | |
| **Entwicklung** | | | | | | | | | | | | | | | | |
| Technische Anforderungen | Paul & Benita | | | 7 | Nicht begonnen | | | | | | | | | | | |
| Datenbank-Entwicklung | Paul & Benita | | | 14 | Nicht begonnen | | | | | | | | | | | |
| API-Entwicklung | Paul & Benita | | | 14 | Nicht begonnen | | | | | | | | | | | |
| Benutzeroberfläche Kunde | Paul & Benita | | | 14 | Nicht begonnen | | | | | | | | | | | |
| Tests | Paul & Benita | | | 14 | Nicht begonnen | | | | | | | | | | | |
| Abschluss Entwicklung | Paul & Benita | | | 14 | Nicht begonnen | | | | | | | | | | | |
| **Abschluss** | | | | | | | | | | | | | | | | |
| Überarbeitung der Arbeit | Paul & Benita | | | 14 | Nicht begonnen | | | | | | | | | | | |
| Erstellung der Präsentation | Paul & Benita | | | 14 | Nicht begonnen | | | | | | | | | | | |
| Abgabe | Paul & Benita | | | 1 | Nicht begonnen | | | | | | | | | | | |
| Präsentation | Paul & Benita | | | 1 | Nicht begonnen | | | | | | | | | | | |