Hausarbeit

des Studiengangs Informationstechnik

der Dualen Hochschule Baden-Württemberg Mannheim

Sicherheit und Fehlermodelle von verteilten Systemen

Julian Fuchs, Marius Bröcker, Sebastian Wallat

November 10, 2020

Bearbeitungszeitraum:	24.10.2020-27.11.2020
Matrikelnummer, Kurs:	1708267, TINF18-IT1
Vorlesung:	Verteilte Systeme

Eidesstattliche Erklärung

Wir versichern hiermit, dass wir diese Hausarbeit mit dem Thema: "Sicherheit und Fehlermodelle von verteilten Systemen" selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt haben.

Datum, Ort

Unterschrift

Zusammenfassung

Thema

Contents

List of Figures

Abkürzungsverzeichnis

DLR **D**eutsches Zentrum für **L**uft- und **R**aumfahrt

1 Einführung

Ein wichtiger Aspekt verteilter Systeme (vS) ist das erhöhte Sicherheits- und Schutzbedürfnis dieser. Dies ergibt sich aus ihrem offenen Aufbau, sowie der netzwerkgestützten Kommunikation zwischen den einzelnen Teilsystemen. Aus diesem Grund besitzen verteilte Systeme eine viel zahl verschiedenster Angriffsvektoren. Besonders im Kontext von kritischer Infrastruktur (KRITIS) und verschiedenen Branchen wie etwa Banken und E-Commerce müssen Sicherheit und Datenschutz als essentielle Bestandteile des Gesamtsysteme angesehen werden.
Um eine möglichst große Zahl an möglichen Sicherheitsproblemen zu eliminieren ist es notwendig schon während der ersten Planungsphasen die sicherheitsrelevanten Aspekte mit in die Überlegungen einzubeziehen. So können eventuelle Schwachstellen möglichst früh identifiziert und entsprechende Gegenmaßnamen in das System integriert werden. Wichtig hierbei ist das alle Schutzmaßnamen kontinuierlich im gesamten System implementiert werden, da schon eine einziger Mangel innerhalb einer Komponente zur Kompromittierung des Gesamtsystems führen kann.
Um allen Sicherheits- und Datenschutz relevanten Anforderungen modernen IT Systeme zu entsprechen sind eine viel zahl verschiedenster Mechanismen und Sub-Komponenten zu betrachten. Die wichtigsten dieser sollen im weiteren Verlauf dieser Arbeit näher beleuchtet werden, hierzu zählen unter anderem:

- Kryptoverfahren
- Authentisierung
- Autorisierung
- Arten von Fehlern und Störungen, sowie deren korrekte Behandlung

2 Sicherheit

2.1 Schutzziele

An dieser Stelle lohnt es sich kurz auf die Grundlagen der Informationssicherheit IT-Sicherheit einzugehen.

"Als Informationssicherheit bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden (technischen oder nicht-technischen) Systemen, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken."[[1]]
"IT-Sicherheit ist ein Teil der Informationssicherheit. In Abgrenzung zur IT-Sicherheit umfasst die Informationssicherheit neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch noch die Sicherheit von nicht elektronisch verarbeiteten Informationen."[[1]]

Somit lässt sich festhalten, das die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität die oberste Priorität aller Sicherheitstechnischen Überlegungen darstellen sollten. Im folgenden sollen diese drei Schutzziele weiter erläutert werden:

- Vertraulichkeit: Verhinderung von jeglichen unautorisierter Informationsgewinn (Abgreifen von vertraulichen Daten)
- Integrität: Verhinderung von unabsichtlicher bzw. unautorisierter Modifizierung von Daten. (Falls eine Datenveränderung nicht komplett unterbunden werden kann, so muss zumindest gewährleistet werden, dass diese vom System bemerkt wird)
- Verfügbarkeit: Es muss verhinder werden, dass autorisierte Subjekte von unautorisierten Zugriffen in der Nutzung ihrer Berechtigungen beeinträchtigt werden.

2.2 Angriffsvektoren

Ziel eines möglichen Angreifers ist es, eines der im vorherigen Kapitel erläuterten Schutzziele zu verletzen. Hierbei kann ein bestimmter Angriff (Vektor) durchaus mehrere Schutzziele kompromittieren. Im folgenden sollen einige mögliche Angriffsmöglichkeiten beispielhaft aufgeführt werden.

- Man-in-the-Middle(MITM): Vertraulichkeit
- Trojaner (z.B. Emotet/Trickbot): Integrität
- Denial of Service (Dos/DDos): Verfügbarkeit
- SQL-Injection: Vertraulichkeit, Integrität

2.3 Schutzmaßnahmen

2.3.1 Verschlüsselung

2.3.2 Authentisierung

2.3.3 Autorisierung

3 Fehlermodelle

3.1 Anforderungen

3.2 Arten von Fehlern und Störungen

3.3 Fehlerbehebung

Bibliography

[1] P. D. K. Bayreuther, "It-sicherheit, einführung and grundlage," 2020.

[2] A. Schill and T. Springer, "Verteilte systeme," *eXamen-press*, 2012.