Fehlermodelle der Fehlertoleranz für die Einbruchstoleranz

Timo Warns* · Wilhelm Hasselbring

Carl von Ossietzky Universität Oldenburg,
Abteilung Software Engineering
{timo.warns,hasselbring}@informatik.uni-oldenburg.de

Zusammenfassung

Die Einbruchstoleranz ist ein Ansatz zur Entwicklung sicherer System, bei dem die Konzepte und Techniken der Fehlertoleranz genutzt werden. Die Idee der Fehlertoleranz, dass ein System Fehler zur Laufzeit toleriert, wird auf Einbrüche in Komponenten eines Systems übertragen, um zu verhindern, dass solche Einbrüche Schaden am Gesamtsystem verursachen.
Die Entwicklung und Analyse von Protokollen der Fehlertoleranz erfordert Fehlermodelle für Annahmen über potentielle Ausfälle der beteiligten Komponenten. Dieses Papier gibt einen Überblick wie diese Modelle für die Einbruchstoleranz angepasst werden, um so Protokolle der Fehlertoleranz auf die Einbruchstoleranz zu übertragen. Im Einzelnen werden das AVI-Modell als Erweiterung der Beeinträchtigungskette und die allgemeinen hybriden Widersacherstrukturen für die Modellierung von ungerichtet abhängigen Ausfällen vorgestellt.

1 Einleitung

Sicherheitsanforderungen an ein System können auf unterschiedliche Art und Weise erfüllt werden. Eine Möglichkeit besteht darin, die Entstehung von Sicherheitslücken durch den systematischen Einsatz von Entwicklungsprozessen und -methoden zu verhindern. Zusätzlich müssen Sicherheitslücken, die während der Entwicklung oder zur Laufzeit erkannt werden, beseitigt werden. Eine weitere Möglichkeit ist, Techniken wie z.B. Firewalls einzusetzen, um zur Laufzeit zu verhindern, dass Angriffe Sicherheitslücken erreichen, die ausgenutzt werden sollen. Diese Möglichkeiten sind aber nur selten ausreichend, Einbrüche in ein System komplett zu verhindern. Es müssen also zusätzliche Maßnahmen ergriffen werden, die Sicherheit eines Systems zu gewährleisten, auch wenn Einbrüche stattfinden.

Sicherheit soll hier im Sinne des englischen Begriffs *Security* verstanden werden, also als Vermeidung von unerwünschten Folgen durch beabsichtigte und unberechtigte Handlungen. Wir folgen dem Verständnis von Avižienis u. a. [1], dass sich Sicherheit als Systemeigenschaft aus den Eigenschaften *Verfügbarkeit*, *Integrität* und *Vertraulichkeit* zusammensetzt.

Dobson und Randell [2] zeigen Parallelen zwischen der Entwicklung zuverlässiger und sicherer Systeme. Auch für zuverlässige Systeme können nicht alle Fehlerursachen verhindert

* Diese Arbeit wurde durch das Graduiertenkolleg GRK 1076/1 der Deutschen Forschungsgemeinschaft (DFG) unterstützt.

und beseitigt werden. Es werden daher Konzepte und Techniken der Fehlertoleranz eingesetzt, um Ausfälle von Komponenten zur Laufzeit zu tolerieren. Dafür ist in einem System Redundanz notwendig, z.B. durch zusätzliche Hardware- oder Software-Komponenten. Der Ansatz der Einbruchstoleranz verfolgt die Idee von Dobson und Randell [2] und vermeidet in Analogie zur Fehlertoleranz die Verletzung von Sicherheitanforderungen trotz der Anwesenheit von Einbrüchen.

Der Begriff der Einbruchstoleranz wurde zuerst von Fraga und Powell [5] für ein verteiltes Dateisystem verwendet, das die Vertraulichkeit, die Integrität und die Verfügbarkeit von Dateien sicher stellt. Dateien werden dafür in Fragmente geteilt, repliziert und über die Knoten des verteilten Systems verteilt (*fragmentation-redundancy-scattering*). Um die Vertraulichkeit sicherzustellen, werden die einzelnen Fragmente so angelegt, dass ein einzelnes Fragment keine signifikanten Informationen bzgl. der Ursprungsdatei hat. In den letzten Jahren haben insbesondere die Projekte *MAFTIA*[1] und *OASIS*[2] Protokolle und Architekturen der Einbruchstoleranz untersucht und damit zu einer weiteren Verbreitung des Ansatzes beigetragen.

Die Einbruchstoleranz nutzt Konzepte und Techniken der Fehlertoleranz und kombiniert sie mit Ansätzen zur Entwicklung sicherer Systeme. Der neue Kontext für die Fehlertoleranz erfordert eine Anpassung der zugrunde liegenden Fehlermodelle bzgl. böswillig beabsichtigter und voneinander abhängiger Ausfälle. Das Ziel dieses Papiers ist es, einen Überblick zu geben, wie Fehlermodelle der Fehlertoleranz für die Einbruchstoleranz angepasst werden. Insbesondere wird dabei auf die Beeinträchtigungskette und globale Annahmen über Komponentenausfälle eingegangen.

Das Papier ist wie folgt aufgebaut. Abschnitt 2 beschreibt ein Beispielszenario, in dem *Agreement*-Protokolle der Fehlertoleranz eingesetzt werden, um die Verfügbarkeit und Integrität eines Verzeichnisdienstes einer Public-Key-Infrastruktur abzusichern. Abschnitt 3 beschreibt die Beeinträchtigungskette der Fehlertoleranz, die Fehlerursachen, Fehler und Ausfälle zueinander in Verbindung setzt. Abschnitt 4 beschreibt die Anpassung der Beeinträchtigungskette durch das AVI-Modell. Abschnitt 5 stellt die Schwellwert-Annahme der Fehlertoleranz vor, mit der stochastisch unabhängige Ausfälle von Komponenten modelliert werden. Abschnitt 6 stellt die allgemeinen hybriden Widersacherstrukturen vor, mit denen sich ungerichtet abhängige Ausfälle modellieren lassen.

2 Beispiel: Verzeichnisdienst einer PKI

Am Beispiel einer *Public-Key-Infrastruktur* (PKI) veranschaulichen wir den Ansatz der Einbruchstoleranz. Eine PKI ist ein zentralisiertes System zur Ausstellung, Verteilung und Überprüfung digitaler Zertifikate. Digitale Zertifikate werden für die Absicherung elektronischer Kommunikation durch asymmetrische Verschlüsselung und digitale Unterschriften benötigt. Mit der Annahme, dass die PKI vertrauenswürdig ist, schenken Benutzer den darüber verbreiteten Zertifikaten hohes Vertrauen. Daher müssen an eine PKI hohe Sicherheitsanforderungen gestellt werden.

Neben anderen Komponenten umfasst eine PKI einen Verzeichnisdienst, der die Suche

[1] http://www.maftia.org/
[2] http://www.tolerantsystems.org/

und das Herunterladen von bereits ausgestellten Zertifikaten ermöglicht. Mit Hilfe einer *Certification* und *Registration Authority* werden für Benutzer Zertifikate ausgestellt, die über den Verzeichnisdienst verfügbar gemacht werden. Möchte ein Benutzer z.B. ein Dokument für einen Empfänger verschlüsseln, benötigt er dessen Zertifikat, das er über den Verzeichnisdienst erhält. Erhält ein Benutzer ein digital signiertes Dokument, benötigt er das Zertifikat des Absenders, das er ebenfalls über den Verzeichnisdienst erhält.

Die Sicherheit des Gesamtsystems wird insbesondere durch die Verfügbarkeit und Integrität des Verzeichnisdienstes beeinflusst. Wenn der Verzeichnisdienst nicht verfügbar ist, haben Benutzer keinen Zugriff auf Zertifikate der PKI. Sie können dann nur gegen ihnen bereits bekannte Zertifikate Unterschriften prüfen bzw. Kommunikation verschlüsseln. Gelingt es einem Widersacher Zertifikate zu verfälschen oder zu löschen, ist der Benutzer nicht mehr in der Lage, Kommunikation zum gewünschten Empfänger zu verschlüsseln bzw. Unterschriften zu prüfen.

Für derartige Anforderungen gibt es verschiedene Ansätze in der Fehlertoleranz. Eine Möglichkeit ist, den Verzeichnisdienst zu replizieren, das heißt ihn mehrfach vorzuhalten, wie in Abb. 1 gezeigt. Um die Sicherheit des Verzeichnisdienstes zu bewahren, müssen Benutzeranfragen auf mehrere Replikate abgebildet und koordiniert werden. Ansonsten würde ein Einbruch in ein einzelnes Replikat ausreichen, verfälschte Zertifikate an Benutzer dieses Replikats zu schicken. Lamport u. a. [10] beschreiben ein Protokoll zum *Byzantinischem Agreement*, das benutzt werden kann, um eine Abstimmung der Replikate über Antworten auf Benutzeranfragen umzusetzen. Beim Byzantinischen Agreement schlagen die beteiligten Komponenten Werte vor und müssen sich auf einen Wert einigen, auch wenn einige Komponenten ausgefallen sind. In unserem Beispiel können die Replikate entsprechende Protokolle nutzen, um Antworten auf Benutzeranfragen vorzuschlagen und sich auf eine korrekte Antwort zu einigen. Das ermöglicht es, ein korrektes Zertifikat zu liefern, auch wenn in einzelne Replikate eingebrochen wurde.

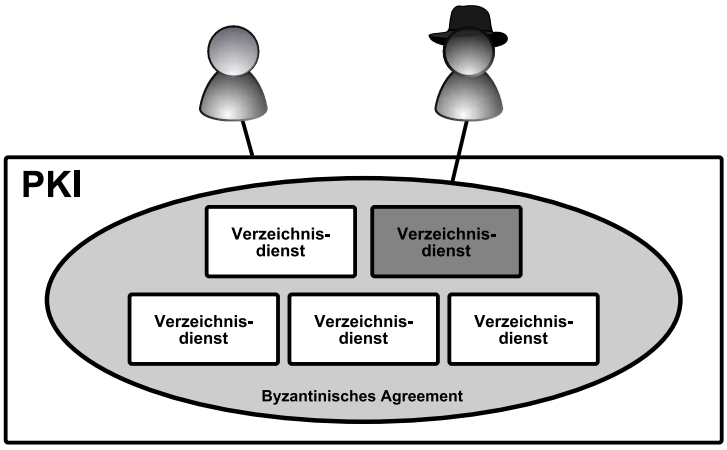

Abbildung 1: PKI mit repliziertem Verzeichnisdienst. Die PKI umfasst neben anderen Komponenten fünf Replikate des Verzeichnisdienstes. Ein Widersacher hat durch einen Einbruch ein Replikat unter seine Kontrolle gebracht. Das Byzantinische Agreement ermöglicht es Benutzern, die PKI zu nutzen, auch wenn ein Replikate kompromittiert ist.

3 Beeinträchtigungskette

Ansätze zur Fehlertoleranz können nach verschiedenen Strategien vorgehen, um Ausfälle eines Systems zu vermeiden. Laprie [11] stellt u.a. die Strategie *Fehlererkennung und -behebung* vor, bei der Fehler im System erkannt und behoben werden, um Ausfälle zu verhindern. Wesentlich ist dabei die Unterscheidung von Beeinträchtigungen nach *Fehlerursache* (engl. „fault“), *Fehler* (engl. „error“) und *Ausfall* (engl. „failure“). Diese bilden zusammen eine Kette, wie in Abb. 2 dargestellt.

Avižienis u. a. [1] erläutert, dass ein Ausfall als Ereignis verstanden wird, das auftritt, wenn ein Dienst, der von einem System erbracht wird, von einem korrekten Dienst abweicht. Ein Ausfall tritt also auf, wenn ein Dienst seine Spezifikation verletzt. Ein Fehler wird als Abweichung eines Systemzustands vom korrekten Systemzustand aufgefasst. Eine solche Abweichung kann zu einem Ausfall führen, wenn er die Erbringung eines Dienstes beeinflusst, also an die Systemgrenze dringt. Eine Fehlerursache wird als Mangel eines Systems gesehen, der einen Fehler ermöglicht. Die Aktivierung eines Fehlers ist implizit im Übergang von der Fehlerursache zum Fehler enthalten.

In einem Hardware-System wird z.B. ein defekter Speicherbaustein als Fehlerursache verstanden. Solange der defekte Baustein nicht benutzt wird, liegt noch kein Fehler vor. Der Fehler wird aktiviert, wenn der Baustein bei der Benutzung des Systems einen falschen Systemzustand verursacht. Beeinflusst dieser Zustand Ergebnisse, die von außerhalb des Systems sichtbar sind, liegt ein Ausfall vor.

Sicherheitsanforderungen an ein System werden in dessen Spezifikation definiert. Der Begriff des Ausfalls bildet damit auch die Verletzung von Sicherheitsanforderungen ab, da eine solche Verletzung auch die Systemspezifikation verletzt. Die Begriff des Ausfalls lässt sich damit auch auf die Einbruchstoleranz übertragen.

Eine solche Übertragung gelingt allerdings nicht für den Fehlerbegriff. Probleme der Fehlertoleranz, wie z.B. *Broadcast* zur Verteilung von Nachrichten, werden über Systemzustände spezifiziert, so dass die Definition von Fehlern über Zustände dort sinnvoll ist. Für die Eigenschaft der Vertraulichkeit bereitet dies allerdings Probleme. Die Vertraulichkeit kann verletzt werden, ohne dass in einem System Zustandsänderungen auftreten. Dies kann z.B. durch verdeckte Kanäle geschehen, die ungewollte Informationsflüsse aus dem System führen. Insbesondere werden Probleme der Fehlertoleranz in Form von *Safety*- und *Liveness*-Bedingungen über Zustände spezifiziert, die Lamport [9] eingeführt hat. McLean [13] zeigt, dass Informationsflüsse nicht über Safety- und Liveness-Bedingungen spezifiziert werden können. Es ist Gegenstand der Forschung, wie der Fehlerbegriff für die Vertraulichkeit angepasst werden muss. Da sich die Fehlertoleranz schon mit den Eigenschaften Verfügbarkeit und Integrität beschäftigt, bereiten diese weniger Probleme.

Für eine geeignete Anpassung des Fehlerbegriffs ist das Verständnis von Fehlerursachen

Abbildung 2: Beeinträchtigungskette der Fehlertoleranz. Eine Fehlerursache ermöglicht einen Fehler in einem System. Wenn ein Fehler an die Systemgrenze dringt, tritt ein Ausfall auf.

auch für die Einbruchstoleranz geeignet, da für eine Verletzung von Sicherheitsanforderungen Ursachen im System vorhanden sein müssen. Die Fehlertoleranz beschäftigt sich nach klassischem Verständnis allerdings mit unbeabsichtigten Fehlerursachen. Das ist historisch damit zu begründen, dass die Wurzeln der Fehlertoleranz in der Hardware-Entwicklung liegen, bei der Fehler durch Alterungserscheinungen und Verschleiß verursacht wurden. Im Bereich der Sicherheit trifft man allerdings auf böswillig beabsichtigte Bedrohungen durch einen Angreifer. Der folgende Abschnitt stellt das AVI-Modell vor, das diese Lücke schließen soll.

4 AVI-Modell

Veríssimo u. a. [14] führen das *Angriff-Verwundbarkeit-Einbruch*-Modell (engl. „Attack-Vulnerability-Intrusion“, AVI-Modell) als Erweiterung der Beeinträchtigungskette ein, um auch böswillig beabsichtigte Bedrohungen durch einen Angreifer der Fehlertoleranz zugänglich zu machen. Wie in Abb. 3 dargestellt, spalten sie die Fehlerursache in Verwundbarkeit, Angriff und Einbruch auf:

- Eine Verwundbarkeit ist eine Fehlerursache in einem Rechen- oder Kommunikationssystem, die mit böswilliger Absicht ausgenutzt werden kann.
- Ein Angriff ist eine böswillig beabsichtigte Fehlerursache, mit der eine Verwundbarkeit ausgenutzt wird.
- Ein Einbruch ist eine böswillig beabsichtigte Fehlerursache, die sich aus einem erfolgreichen Angriff auf eine Verwundbarkeit ergibt und während der Erbringung eines Dienstes auftritt.

Die Begriffe lassen sich am Beispiel der PKI für eine *Denial-of-Service* Bedrohung durch einen Pufferüberlauf veranschaulichen. Eine Verwundbarkeit ist z.B. ein Fehler in der Implementierung des Verzeichnisdienstes, wie eine Zuweisung von zu wenig Speicher für Eingabedaten. Ein Aufruf des Dienstes mit absichtlich zu großen Eingabedaten ist ein Angriff auf diese Sicherheitslücke. Wird der Aufruf nicht durch andere Techniken, wie z.B. eine Firewall, abgefangen, kommt es zu einem Einbruch. Da der entstehende Pufferüberlauf einen Teil des Speicherinhalts des Dienstes überschreibt, liegt ein Fehler vor. Dieser Fehler kann zu einem Absturz und damit zu einem Ausfall des Dienstes führen.

Das AVI-Modell versucht, die Bedrohungen der Sicherheit auf Beeinträchtigungen der Fehlertoleranz abzubilden, um so Einbrüche als Fehlerursachen mit bekannten Strategien

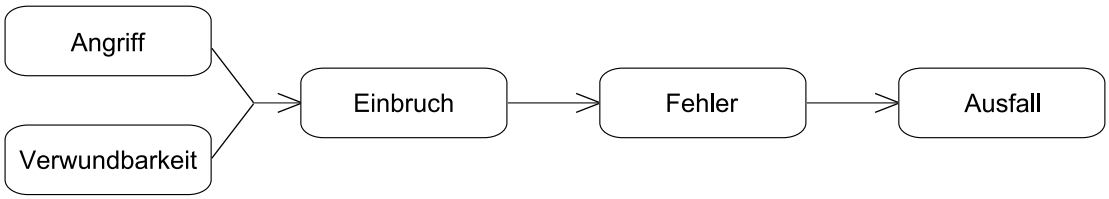

Abbildung 3: AVI-Modell von [14]. Gegenüber der klassischen Beeinträchtigungskette wurde die Fehlerursache in Angriff, Verwundbarkeit und Einbruch aufgespalten. Die Ausnutzung einer Verwundbarkeit durch einen Angriff führt zu einem Einbruch. Ein Einbruch kann einen Fehler im System verursachen.

tolerieren zu können. Das AVI-Modell ist aus Sicht der Fehlertoleranz attraktiv, da es nur geringe Differenzen zur klassischen Beeinträchtigungskette aufweist. Allerdings bestehen noch offene Fragen bzgl. der Tragfähigkeit für die weitere Entwicklung der Einbruchstoleranz.

Nach dem AVI-Modell nutzt ein Angriff eine Verwundbarkeit im System aus und führt einen Einbruch herbei. Damit wurde die Aktivierung einer Fehlerursache explizit in die Beeinträchtigungskette aufgenommen. In Analogie zum klassischen Modell müsste ein Einbruch bereits ein Fehler im System sein, wird aber als Fehlerursache verstanden. Eine offene Frage bzgl. des Modells ist, wie mit Beeinträchtigungen umzugehen ist, die im klassischen Modell als Fehler modelliert wurden, aber nun als Fehlerursache verstanden werden.

Das AVI-Modell nimmt keine Anpassung des Fehlerbegriffs bzgl. Vertraulichkeit vor. Da eine Verletzung der Vertraulichkeit nicht unbedingt einen Fehler benötigt, müsste schon die Ausnutzung einer Verwundbarkeit zu einem Ausfall führen können. Da ein solcher Übergang nicht vorgesehen ist, bleibt die offene Frage, wie mit Verletzungen von Vertraulichkeit umzugehen ist.

5 Schwellwertannahme

Für die Entwicklung und Analyse von Protokollen der Fehlertoleranz werden Annahmen über die Art und die Menge von Ausfällen von Komponenten benötigt. Im schlimmsten Fall hat ein Widersacher nach einem erfolgreichen Einbruch in eine Komponente die volle Kontrolle über die Komponente. Er kann dann für die Komponente beliebiges Verhalten hervorrufen, z.B. Anfragen falsch beantworten lassen. Daher werden für die Einbruchstoleranz meist *Byzantinische Ausfälle* angenommen. Ein Ausfall wird nach Lamport u. a. [10] als Byzantinischer Ausfall bezeichnet, wenn keinerlei Einschränkungen für den Ausfall angenommen werden. Eine andere Art des Ausfalls ist der *Absturz*, bei dem eine betroffene Komponente anhält, also nicht mehr auf Anfragen reagiert bzw. selbst Anfragen verschickt.

In der Fehlertoleranz wird bzgl. der Menge der ausgefallenen Komponenten meist die t von n Schwellwertannahme gemacht. Sie drückt aus, dass ein System aus n Komponenten besteht und davon bis zu t gleichzeitig ausfallen können. Protokolle werden darauf hin optimiert, dass sie mindestens t Ausfälle als Schwellwert tolerieren können. Bietet eine Komponente z.B. statische Informationen an, deren Verfügbarkeit sichergestellt werden soll, kann diese Komponente repliziert werden. Bei n Replikaten können dann bis zu $t = n-1$ gleichzeitige Abstürze toleriert werden, da nur eine einzelne Komponente notwendig ist, um auf die Information zuzugreifen.

Lamport u. a. [10] haben für synchrone Systeme unter der Schwellwertannahme gezeigt, dass das Byzantinische Agreement nur dann umgesetzt werden kann, wenn $n > 3t$ gilt. Für das Beispiel des Verzeichnisdienstes einer PKI gilt daher, dass mindestens sieben Replikate benötigt werden, um Einbrüche in zwei Replikate tolerieren zu können. Die in Abb. 1 gezeigten fünf Replikate können nur einen Einbruch tolerieren.

Bei der Schwellwertannahme legt man sich also auf eine Art von Ausfall fest, z.B. auf Byzantinische Ausfälle. Für die Protokolle der Fehlertoleranz ist die Annahme der By-

zantinischen Ausfälle eine starke Einschränkung. Es ergeben sich schlechtere Schranken in Bezug auf die Anzahl an Ausfällen, die toleriert werden können. Gleichzeitig kann die Annahme der Byzantinischen Ausfälle für die Einbruchstoleranz unnötig pessimistisch sein, da ein Widersacher nicht unbedingt beliebiges Verhalten hervorrufen kann. Daher werden auch hybride Modelle eingesetzt, mit denen unterschiedliche Arten von Ausfällen spezifiziert werden können.

Keidar und Marzullo [7] erläutern vier Probleme, die implizit in der t von n Annahme enthalten sind:

- Alle Arten von Ausfall sind gleich wahrscheinlich.
- Die Wahrscheinlichkeit eines Komponentenausfalls während ein Protokoll abläuft ist unabhängig von der Laufzeit des Protokolls.
- Alle Komponenten, die ausfallen können, haben die gleiche Ausfallwahrscheinlichkeit.
- Ausfallwahrscheinlichkeiten von verschiedenen Komponenten sind voneinander unabhängig.

Für die Einbruchstoleranz stellen insbesondere die letzten beiden Punkte Herausforderungen dar. In Bezug auf die Sicherheit haben Systeme häufig Eigenschaften in Analogie zum schwächsten Glied einer Kette. Das bedeutet, dass die Sicherheit eines Systems bei einem Einbruch in die schwächste Komponente verletzt wird, vergleichbar mit dem Reißen einer Kette beim Bruch des schwächsten Gliedes. Ein Widersacher wird sich auf die unsicherste Komponente, also auf das schwächste Glied, konzentrieren. Deren Ausfallwahrscheinlichkeit ist dann höher als die anderer Komponenten. Die implizite Annahme gleicher Wahrscheinlichkeiten ist damit nicht valide.

Komponenten stehen in unterschiedlichen Vertrauensbeziehungen zueinander. Eine Komponente, die einer anderen ein hohes Maß an Vertrauen schenkt, überprüft deren Antworten bzw. Anfragen kaum, da sie sie für vertrauenswürdig hält. Umgekehrt muss eine Komponente, die einer anderen nicht vertraut, deren Antworten und Anfragen sehr genau überprüfen. Wenn ein Widersacher in eine Komponente einbricht, der ein hohes Maß an Vertrauen geschenkt wird, kann es für ihn einfacher werden, in andere Komponenten einzubrechen. Zum Beispiel schenken Clients eines Client-Server-Systems den Servern häufig ein hohes Maß an Vertrauen, dass sie die angeforderten Dienste korrekt erbringen. Dieser Umstand kann es einem Widersacher nach einem Einbruch in den Server erleichtern, in die Clients einzubrechen. Damit ist die Ausfallwahrscheinlichkeit der Clients stark abhängig von der der Server. Die Annahme der unabhängigen Ausfälle gilt also nicht.

Häufig haben Komponenten gemeinsame Verwundbarkeiten, z.B. wenn sie auf der gleichen Plattform betrieben werden, die eine Verwundbarkeit hat. In diesem Fall sind die Ausfallwahrscheinlichkeiten der Komponenten stark voneinander abhängig, da sie bei einer Ausnutzung der gemeinsamen Verwundbarkeit zusammen ausfallen.

Verschiedene Modelle wurden vorgeschlagen, um die Probleme der Schwellwertannahme zu lösen. In Abschnitt 6 stellen wir das Modell der allgemeinen hybriden Widersacherstrukturen vor, das hybride Annahmen und abhängige Ausfälle berücksichtigt.

6 Widersacherstrukturen

Der Schwellwertannahme liegt die Annahme zugrunde, dass Ausfälle von Komponenten stochastisch unabhängig voneinander sind. Diese Annahme ist für die Einbruchstoleranz kaum haltbar und muss daher angepasst werden. Fitzi und Maurer [4] haben das Modell der *allgemeinen Widersacherstrukturen* (engl. „general adversary structures“) eingeführt, mit dem ungerichtet abhängige Ausfälle modelliert werden können. Vergleichbare Modelle sind die *fehleranfälligen Systeme* (engl. „fail-prone systems“) von Malkhi und Reiter [12] und die *Kern- und Überlebend-Mengen* (engl. „cores and survivor sets“) von Junqueira und Marzullo [6].

Fitzi u. a. [3] und Kursawe und Freiling [8] greifen die Widersacherstrukturen auf und erweitern sie um hybride Annahmen. Formal sind die *allgemeinen hybriden Widersacherstrukturen* wie folgt definiert. Sei Π die Menge aller beteiligten Komponenten. Eine *Widersacherklasse* $C = (B, C) \subseteq \Pi \times \Pi$ modelliert zwei Menge von Komponenten, die gemeinsam ausfallen können. Die beiden Mengen B und C dienen zur Modellierung der Art des Ausfalls der beteiligten Komponenten. Von den Komponenten in B wird angenommen, dass sie Byzantinisch ausfallen. Die Komponenten in C fallen nach Annahme mit einem Absturz aus. Eine Widersacherklasse $\mathcal{C} = (B', C')$ ist in einer Widersacherklasse $\mathcal{C} = (B, C)$ enthalten, wenn B' eine Teilmenge von B und C' eine Teilmenge von C ist. Eine *Widersacherstruktur* $\mathcal{Z}$ ist dann eine monotone Menge von Widersacherklassen, d.h. wenn eine Klasse C in $\mathcal{Z}$ ist, sind auch alle Klassen in $\mathcal{Z}$, die in C enthalten sind. Protokolle zur Einbruchstoleranz müssen daraufhin optimiert werden, dass sie Ausfälle, die mit einer Widersacherstruktur beschrieben werden, tolerieren können. Da in einer Klasse Komponenten erfasst werden, die gemeinsam ausfallen können, wird die Modellierung (ungerichtet) abhängiger Ausfälle möglich.

Schranken bzgl. der Fehlertoleranz werden für die hybriden Widersacherstrukturen in Form des $Q^{(m,n)}$ Prädikats angegeben (für $m \geq n$). Dabei erfüllt eine Widersacherstruktur $\mathcal{Z}$ das $Q^{(m,n)}$ Prädikat genau dann, wenn für alle Widersacherklassen $(B_1, C_1), \ldots, (B_m, C_m) \in \mathcal{Z}$ gilt, dass $B_1 \cup \ldots \cup B_m \cup C_1 \ldots C_n \neq \Pi$. Das heißt das m byzantinische Ausfallmengen und n Absturz-Ausfallmengen von m Widersacherklassen nicht die Menge aller Komponenten überdecken dürfen. Fitzi u. a. [3] haben gezeigt, dass eine Widersacherstruktur das Prädikat $Q^{(3,2)}$ erfüllen muss, damit das Byzantinische Agreement für die Struktur umgesetzt werden kann.

Wir veranschaulichen die Widersacherstrukturen am Beispiel des Verzeichnisdienstes einer PKI. Die Replikate des Dienstes werden auf Servern eingesetzt, die bestimmte Betriebssysteme benutzen, wie in Abb. 4 dargestellt. Wenn mehrere Replikate auf Servern mit dem gleichen Betriebssystem eingesetzt werden, kann es zu abhängigen Ausfällen kommen. Ein Widersacher kann z.B. eine Sicherheitslücke in dem Betriebssystem nutzen und so auf beiden Servern in den Verzeichnisdienst einbrechen. Das dargestellte Beispiel kann mit der Widersacherstruktur

$$\mathcal{Z} = \{(\{v_1, v_2\}, \{\}), (\{v_1\}, \{\}), (\{v_2\}, \{\}), (\{v_3\}, \{\}), (\{v_4\}, \{\}), (\{v_5\}, \{\}), (\{\}, \{\})\}$$

modelliert werden. Es können also gar kein Verzeichnisdienst ausfallen, jeder Verzeichnisdienst kann für sich alleine Byzantinisch ausfallen oder v_1 und v_2 fallen zusammen Byzantinisch aus. Um das Beispiel einfach zu halten, verzichten wir hier auf die Modellie-

rung von Ausfällen durch Absturz. Da die angegebene Struktur das $Q^{(3,2)}$ Prädikat erfüllt, ist die Umsetzung des Byzantinischem Agreement in diesem Szenario möglich. Unter der Schwellwertannahme kann hingegen nur der Ausfall einer Komponente toleriert werden.

Das Modell hat mehrere Vorteile gegenüber der klassischen t von n Annahme. Mit der Widersacherklasse als Tupel für Abstürze und Byzantinische Ausfälle handelt es sich um ein hybrides Modell, das realistischer ist als die reine Annahme von Byzantinischen Ausfälle. Außerdem berücksichtigen die Klassen gemeinsame Ausfälle von Komponenten.

Ein Nachteil der Widersacherstrukturen ist, dass sie nur ungerichtet abhängige Ausfallwahrscheinlichkeiten berücksichtigen. Realistischer sind aber gerichtete Abhängigkeiten, wie am Beispiel eines Client-Server-Systems deutlich wird. Die Wahrscheinlichkeit, dass ein Client ausfällt, kann stark von der Wahrscheinlichkeit eines Serverausfalls abhängen, da der Client vom Server abhängt und ihm in einem hohen Maße vertraut. Umgekehrt hängt die Ausfallwahrscheinlichkeit des Servers kaum von der der Clients ab, da der Server den Clients nur wenig vertraut und deren Anfragen genau überprüft, bevor er den angefragten Dienst erbringt.

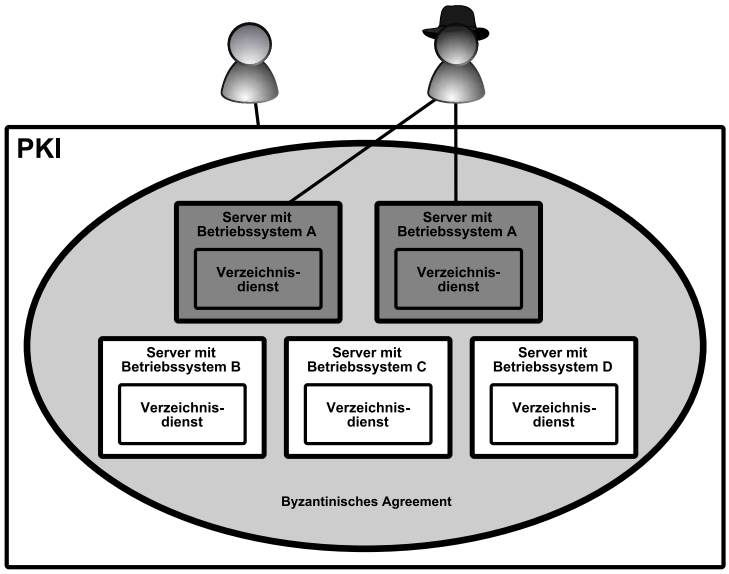

Abbildung 4: PKI-Beispiel für Widersacherstrukturen. Zwei der fünf Replikate des Verzeichnisdienstes liegen auf Servern mit dem gleichen Betriebssystem. Findet ein Widersacher eine Lücke in diesem Betriebssystem, kann er in beide Replikate einbrechen.

7 Fazit

In diesem Papier haben wir einen Überblick über Fehlermodelle der Fehlertoleranz gegeben und dargestellt, wie sie sich auf den Bereich der Einbruchstoleranz übertragen lassen. Dabei wurden das AVI-Modell als Erweiterung der Beeinträchtigungskette und die allgemeinen hybriden Widersacherstrukturen als Ersatz für die t von n Annahme vorgestellt. Das AVI-Modell ist gut mit der klassischen Beeinträchtigungskette vereinbar, lässt aber einige wesentliche Probleme bzgl. der Eigenschaft der Vertraulichkeit offen. Die Wider-

sacherstrukturen stellen eine große Verbesserung gegenüber der t von n Annahme dar, gehen aber nicht auf gerichtet abhängige Ausfälle ein.

Verschiedene Ansatzpunkte für zukünftige Forschung wurden aufgezeigt. Der derzeitige Fehlerbegriff ist für die Vertraulichkeit als Sicherheitseigenschaft nicht geeignet und muss für die Einbruchstoleranz angepasst werden. Aktuelle Modelle berücksichtigen nur ungerichtete Abhängigkeiten zwischen den Ausfällen von Komponenten und reduzieren hybride Annahmen auf Abstürze und Byzantinische Ausfälle. Es ist noch offen, wie gerichtete Abhängigkeiten in realistischeren Modellen berücksichtigt werden können. Neben Abstürzen und Byzantinischen Ausfällen müssen auch andere Arten des Ausfalls, wie die Verletzung von Zeitschranken, berücksichtigt werden.

Mit der Anpassung von Modellen muss auch die Anpassung von Protokollen erfolgen, um die Ziele der Einbruchstoleranz umzusetzen. Zur Zeit halten sich die Modelle noch eng an ihre Ursprünge aus der Fehlertoleranz, damit Konzepte und Techniken nahtlos übertragen werden können. Die Einbruchstoleranz steht vor der Herausforderung, notwendige größere Anpassungen vorzunehmen und dafür neue Protokolle zu entwickeln.

Literatur

[1] Avižienis, A. ; Laprie, J. C. ; Randell, B. ; Landwehr, C. E.: Basic Concepts and Taxonomy of Dependable and Secure Computing. In: *IEEE Transactions on Dependable and Secure Computing* 1 (2004), Nr. 1, S. 11–33

[2] Dobson, J. E. ; Randell, B.: Building Reliable Secure Computing Systems out of Unreliable Insecure Components. In: *Proceedings of IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, 1986, S. 187–193

[3] Fitzi, M. ; Hirt, M. ; Maurer, U. M.: General Adversaries in Unconditional Multiparty Computation. In: Lam, K.-Y. (Hrsg.) ; Okamoto, E. (Hrsg.) ; Xing, C. (Hrsg.): *Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT '99)* Bd. 1716 von Lecture Notes in Computer Science, Springer-Verlag, 1999, S. 232–246

[4] Fitzi, M. ; Maurer, U. M.: Efficient Byzantine Agreement Secure Against General Adversaries. In: Kutten, S. (Hrsg.): *Proceedings of the 12th International Symposium on Distributed Computing (DISC '98)* Bd. 1499 von Lecture Notes in Computer Science, Springer-Verlag, 1998, S. 134–148

[5] Fraga, J. ; Powell, D.: A Fault and Intrusion-Tolerant File System. In: Grimson, J. (Hrsg.) ; Kugler, H.-J. (Hrsg.): *Proceedings of the 3rd IFIP International Conference on Computer Security*, Elsevier Science, 1985, S. 203–218

[6] Junqueira, F. P. ; Marzullo, K.: Designing Algorithms for Dependent Process Failures. In: Schiper, A. (Hrsg.) ; Shvartsman, A. A. (Hrsg.) ; Weatherspoon, H. (Hrsg.) ; Zhao, B. Y. (Hrsg.): *Future Directions in Distributed Computing* Bd. 2584 von Lecture Notes in Computer Science, Springer-Verlag, 2003, S. 24–28

[7] Keidar, I. ; Marzullo, K.: The Need for Realistic Failure Models in Protocol Design. In: *Proceedings of 4th Information Survivability Workshop (ISW 2001/2002)*, 2001

[8] Kursawe, K. ; Freiling, F. C.: Byzantine Fault Tolerance on General Hybrid Adversary Structures / RWTH Aachen. 2005 (AIB-2005-09). – Forschungsbericht. Technischer Bericht

[9] Lamport, L.: Proving the Correctness of Multiprocess Programs. In: *IEEE Transactions on Software Engineering* 3 (1977), März, Nr. 2, S. 125–143

[10] Lamport, L. ; Shostak, R. ; Pease, M.: The Byzantine Generals Problem. In: *ACM Transactions on Programming Languages and Systems* 4 (1982), Juli, Nr. 3, S. 382–401

[11] Laprie, J. C. (Hrsg.): *Dependability: Basic Concepts and Terminology.* Springer-Verlag, 1992

[12] Malkhi, D. ; Reiter, M.: Byzantine Quorum Systems. In: *Proceedings of the 29th Annual ACM symposium on Theory of Computing (STOC '97)*, ACM Press, 1997, S. 569–578

[13] McLean, J.: A General Theory of Composition for Trace Sets Closed under Selective Interleaving Functions. In: *Proceedings of the 1994 IEEE Symposium on Security and Privacy (SP '94)*, IEEE Computer Society Press, 1994, S. 79–95

[14] Veríssimo, P. E. ; Neves, N. F. ; Correia, M. P.: Intrusion-Tolerant Architectures: Concepts and Design. In: Lemos, R. (Hrsg.) ; Gacek, C. (Hrsg.) ; Romanovsky, A. (Hrsg.): *Architecting Dependable Systems* Bd. 2677 von Lecture Notes in Computer Science. Springer-Verlag, 2003, S. 3–36