Zusammenfassender Abschlussbericht für das Gesamtvorhaben DoS-Resist-VPN

Michael Grey, Technische Universität Ilmenau
Markus Trapp, Technische Universität Ilmenau
Michael Roßberg, Technische Universität Ilmenau
Günter Schäfer, Technische Universität Ilmenau

Robin Schlögel, secunet Security Networks AG
Alexander Heinlein, secunet Security Networks AG

Zuwendungsempfänger 1	Technische Universität Ilmenau Postfach 10 05 65 98694 Ilmenau
Projektleitung	Prof. Dr.-Ing. Günter Schäfer
Förderkennzeichen	16BY1202A
Ausführende Stelle	Fachgebiet Telematik/Rechnernetze Institut für Praktische Informatik und Medieninformatik Fakultät für Informatik und Automatisierung Technische Universität Ilmenau
Förderperiode	März 2012 - Dezember 2014

Zuwendungsempfänger 2	secunet Security Networks Aktiengesellschaft Kronprinzenstrasse 30 45128 Essen
Projektleitung	Robin Schlögel
Förderkennzeichen	16BY1202B
Ausführende Stelle	secunet Security Networks AG Geschäftsbereich Hochsicherheit Ammonstraße 74 01067 Dresden
Förderperiode	März 2012 - Dezember 2014

1 Einleitung

Die Nutzung moderner Kommunikationstechnologien ermöglicht heutzutage den zügigen Austausch von Informationen zwischen verschiedenen Standorten von Firmen und Behörden. Gleichzeitig wird unsere Gesellschaft im Zuge dieser Entwicklung allerdings immer abhängiger von der korrekten Funktionsweise dieser Technologien. Gerade im Zusammenhang mit virtuellen privaten Netzwerken (VPN) treten dabei besondere Herausforderungen auf, da durch die vorgenommene Verschlüsselung illegitime Daten nicht von den jeweiligen Internet Service Providern (ISP) gefiltert werden können. Somit stellen bandbreitenerschöpfende Denial-of-Service (DoS)-Angriffe ein signifikantes Problem dar, wenn eine hohe Verfügbarkeit des VPN erwirkt werden soll.

Um diesem Problem zu begegnen, soll im Rahmen des Projektes *Sichere Autokonfiguration sabotageresistenter IPsec-Infrastrukturen* eine bestehende Autokonfigurationstechnologie für IPsec-virtuelle private Netzwerke (VPN), namens Secure OverLay for IPsec Discovery (SOLID), um Maßnahmen zur Erhöhung der Resistenz gegen DoS-Angriffe erweitert werden. Darüber hinaus ist es vorgesehen, die Integration in die „Sichere Inter-Netzwerk Architektur (SINA)“-Produktlinie der secunet Security Networks AG voranzutreiben, die Technologie beherrschbar und somit für einen breiten Einsatz nutzbar zu machen.

Insgesamt soll in dem Projekt eine neue Qualität sowohl der reaktiven als auch proaktiven Schutzmechanismen von IPsec-VPN gegen DoS-Angriffe erreicht werden. Damit wird zum einen der technologische Vorsprung der bereits erfolgreichen SINA-Plattform weiter ausgebaut werden und zum anderen Anwendern eine einfache Möglichkeit gegeben werden, auf diese Angriffe zu reagieren. Für die TU Ilmenau ergeben sich ferner Forschungsfragen von starkem aktuellem Interesse.

2 Kurzdarstellung

2.1 Aufgabenstellung

Als wesentliche Schwachstelle klassischer VPN bezüglich gezielter DoS-Angriffe sind die typischerweise verwendeten, zentralen Koordinatoren anzusehen, welche bereits implizit ein exponiertes Angriffsziel darstellen, da die Verfügbarkeit dieser Komponenten den Zustand des gesamten VPN beeinflusst. Im Vergleich zu konkurrierenden Ansätzen war das SOLID-Verfahren daher bereits im Vorfeld des DoS-Resist-Vorhabens als vergleichsweise resistent anzusehen. Aufgrund des verteilten Konstruktionsprinzips ist der Einfluss von DoS-Angriffen in der Regel auf wenige Knoten begrenzt, wodurch die Verfügbarkeit des Gesamtsystems nur begrenzt beeinträchtigt wird. Selbst im Zuge einer Partitionierung des Gesamtsystems können die verschiedenen Teile des VPN unabhängig voneinander weiterarbeiten.

Allerdings wurde das SOLID-Verfahren zunächst noch nicht gegenüber dynamischen Effekten bei Sabotageangriffen untersucht. Darüber hinaus war zu klären, ob eine zusätzliche Resistenz durch die explizite Konstruktion besonders angriffsresistenter VPN-Technologien erwirkt werden kann. Im Rahmen des Projektes sollten schließlich eine Reihe von konkreten Lösungen zur Steigerung der Resistenz gegenüber DoS-

Angriffen entworfen werden, welche den Vorsprung der SOLID-Technologie gegenüber dem Stand der Technik und Forschung weiter ausbauen. Darüber hinaus ergeben sich für das SOLID-Verfahren – auch aufgrund dessen signifikanter Komplexität – unmittelbare Fragestellungen der Implementierungssicherheit bezüglich des Einsatzes in sicherheitskritischen Umgebungen.

Dementsprechend wurden für dieses Vorhaben folgende Forschungsschwerpunkte definiert:

- *Angriffsresistente VPN-Topologien:* Aufgrund ihrer praktischen Bedeutung gelten VPN als exponierte Ziele für DoS-Angriffe. Die kaum mögliche Differenzierung zwischen Angriffsverkehr und gültigen Nutzdaten erschwert dabei auch den ISPs eine etwaige Reaktion auf entsprechende Angriffe. Insbesondere bezüglich ihrer Wirkung auf dezentrale Strukturen erfolgte allerdings bisher keine genauere Betrachtung von DoS-Angriffen. Dabei drängt sich besonders die Frage auf, inwiefern besonders angriffsresistente VPN-Topologien existieren und gegebenenfalls gefunden und konstruiert werden können.
- *Dynamische DoS-Angriffe:* Neben klassischen DoS- und DDoS-Angriffen werden in den nächsten Jahren auch komplexe dynamische Angriffsstrategien zunehmend eine Rolle spielen. Hierbei könnten gegebenenfalls gezielte Schwingungen in der Topologiekontrolle dezentraler Verfahren erzeugt werden oder – durch sogenannte gepulste Angriffe – mit vergleichsweise wenig Angriffsverkehr die Datenübertragung auf geschützten Verbindungen durch gezieltes Ausnutzen der TCP-Staukontrolle unterbunden werden.
- *Implementierungssicherheit:* Entsprechend der im Rahmen einer Produktisierung intendierten Referenzszenarien soll ein Einsatz des SOLID-Verfahrens auch in sicherheitskritischen Umgebungen ermöglicht werden. Das SOLID-Verfahren verwendet dabei letztlich zur Durchsetzung der Sicherheitsziele die IPsec-Protokollfamilie (weiterführende Informationen zu IPsec können beispielsweise [SR14] entnommen werden), wodurch das Schutzniveau im Vergleich zu manuell konfigurierten Ansätzen nicht geschwächt wird. In Anbetracht der komplexen Kontrollmechanismen des verteilten SOLID-Verfahrens ist eine sichere Implementierung dennoch als anspruchsvoll anzusehen. In Hinblick auf die angestrebte Verfügbarkeit des VPN wird dabei sowohl die Identifikation gefährdeter softwareseitiger Schnittstellen als auch eine komponentenweise Separierung der Implementierung angestrebt.

Im Hinblick auf eine konkrete praktische Weiterentwicklung des Verfahrens und einer Integration in die SINA Produktfamilie der secunet wurde die Konzentration darüber hinaus auf die folgenden Arbeitsschwerpunkte gelegt:

- *Anpassung am SINA-Produkt:* Der bereits vorhandene Prototyp erfordert trotz enger Abstimmung bei der Entwicklung einige Anpassungen für eine vollständige SINA-Integration. Davon sind insbesondere das Zertifikat-Management, die eingesetzte strongSwan-Version und die Firewall-Regeln betroffen. Hierbei sind die notwendigen Konfigurationsschnittstellen zu schaffen und Patches zu betroffenen Softwarekomponenten einpflegen. Teil dieser Arbeit stellt dabei auch die Anpassung von in der Forschung gewonnenem Code an die Sicherheits- und Qualitätsanforderungen der secunet dar.

- *Test und Leistungsverhalten:* Parallel zur Zeit, in der an der TU Ilmenau Optimierungen in Bezug auf Sicherheit und Effizienz erfolgen, sollen von Seiten der secunet umfangreiche Tests durchgeführt und das Leistungsverhalten näher untersucht werden. Nach Bearbeiten dieses Punktes soll eine Überführung in die kommerzielle Weiterentwicklung erfolgen.

2.2 Voraussetzungen, unter denen das Vorhaben durchgeführt wurde

Im Rahmen des DoS-Resist-VPN-Vorhabens konnte auf das SOLID-Verfahren zurückgegriffen werden, welches am Fachgebiet Telematik/Rechnernetze der Technischen Universität Ilmenau unter Begleitung der secunet Security Networks AG bereits seit 2007 entwickelt wird.

Mit der Sicheren Inter-Netzwerk Architektur (SINA) bietet die secunet Security Networks AG bereits seit 2002 sowohl national als auch international äußerst erfolgreich betreiber- und netzübergreifende IPsec-VPN-Produkte an.

Das im Rahmen der engen Zusammenarbeit entstandene SOLID-Verfahren und insbesondere der entstandene Prototyp auf Basis der SINA-Familie ermöglichte bereits zu Beginn des DoS-Resist-VPN-Vorhabens eine automatisierte Konfiguration und Verwaltung von IPsec-basierten VPN.

Dabei erlaubt SOLID die Organisation und Verwaltung sehr großer, komplexer und tief verschachtelter Strukturen, was nach wie vor als Alleinstellungsmerkmal anzusehen ist. Im Rahmen des BMBF-geförderten Vorhabens *Mobile IPsec-Infrastrukturen auf SINA-Basis* wurden bereits vor Beginn des DoS-Resist-VPN-Vorhabens eine Reihe von Lösungen zur Anbindung und Integration mobiler Teilnehmer entworfen, wodurch ein Vorsprung des SOLID-Verfahrens auch in dieser Domäne erwirkt werden konnte. Im Resultat hat die gemeinsam mit der secunet entwickelte Expertise bereits im Vorfeld des DoS-Resist-VPN-Vorhabens zu mehreren, teils gemeinsamen, Veröffentlichungen zum Themengebiet VPN-Autokonfiguration geführt. Darüber hinaus sind aus der Kooperation zwei europaweite Patente über das dem SOLID-Ansatz zugrundeliegende Prinzip hervorgegangen.

2.3 Planung und Ablauf des Vorhabens

2.3.1 TU Ilmenau

Insbesondere aufgrund der angespannten Arbeitsmarktsituation, aber auch durch veränderte Kundenanforderungen und eine zielgerichtete Konzentration auf die technische SOLID-SINA-Integration, sind zu Beginn der Förderperiode auf Seiten der TU Ilmenau zunächst nicht vorhergesehene Verzögerungen entstanden. Am Anfang des Projektes wurden daher verstärkt wissenschaftliche Hilfskräfte unter Anleitung mit dem Projekt vertrauter Mitarbeiter eingesetzt, um das Vorhaben unter diesen Voraussetzungen planmäßig beginnen zu können. Im November 2012 konnte mit Herrn Rothenberger ein Mitarbeiter für die Bearbeitung des Vorhabens gewonnen werden, welcher sich bereits zuvor ausführlich mit der Thematik DoS-resistenter Netzwerkinfrastrukturen auseinandersetzte. Seit Juli 2013 waren darüber hinaus mit Herrn Trapp und Herrn Grey zwei Mitarbeiter im Rahmen des Projektes beschäftigt, welche mit

dem SOLID-Verfahren vertraut sind und bereits im vorangegangenen *Mobil-SOLID-SINA*-Vorhaben erfolgreich gearbeitet haben. Durch diese Konstellation wurde ein schnelles Vorankommen gewährleistet.

Aus der anfänglichen Verzögerung ergab sich dennoch eine veränderte Zeit- und Kostensituation, wodurch die Beantragung einer kostenneutralen Verlängerung des Förderzeitraums notwendig wurde. Durch die Gewährung der kostenneutralen Verlängerung konnte der zunächst verzögerte Arbeitsstand bis zum Ende des Vorhabens vollständig aufgeholt werden. Bis zum Projektende wurden auf Seite der TU Ilmenau, gemäß AZA Kostenstelle 0811, insgesamt 52 Personenmonate für Beschäftigte TVöD/TV-L E 12 bis E 15 aufgewendet.

Der zeitliche Verlauf des Projektes ist in Abbildung 1 skizziert. Im Rahmen des Projektes konnten dabei alle Arbeitspakete wie geplant vollständig bearbeitet und abgeschlossen werden.

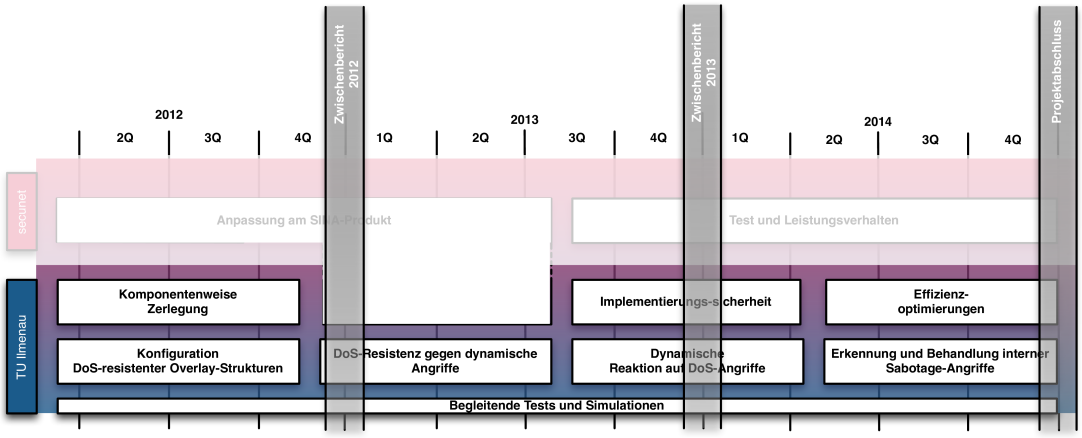

Abbildung 1: Überblick über den Projektablauf an der TU Ilmenau

2.3.2 secunet Security Networks AG

Auch die secunet Security Networks AG hatte im Rahmen des Projektes zunächst Schwierigkeiten die vorgesehenen Stellen zu besetzen. Aus diesem Grund wurde in den ersten Projektjahren noch keine Mittel abgerufen, sondern lediglich in Gesprächen mit der TU Ilmenau die Zielsetzungen verfeinert. Im Resultat der Bemühungen geeignete Kandidaten zu finden, konnte mit Herrn Alexander Heinlein zum 01.04.2013 bei der secunet ein neuer Mitarbeiter gewonnen werden. Herr Heinlein hat einen Masterabschluss von der TU Ilmenau, und hat sich in seinem Studium intensiv mit der IPsec-Autokonfiguration auseinander gesetzt. Herr Heinlein bearbeitete zunächst im Jahr 2013 vorrangig das Teilvorhaben Mobil-SOLID-SINA (Förderkennzeichen 16BY1000). Dieses Teilvorhaben wurde zum 31.12.2013 abgeschlossen, so dass Herr Heinlein mit Beginn des Jahres 2014 die Arbeitspakete des Vorhabens DoSResist-VPN bearbeitete. Hierbei ist zu erwähnen, dass das Mobil-SOLID-SINA Vorhaben thematisch mit dem DoSResist-Vorhaben verwandt war, so dass er durch die zuvorige Bearbeitung des Mobil-SOLID-SINA-Projektes gut auf das DoS-Resist-VPN-Vorhaben vorbereitet war.

Analog zur Situation an der TU Ilmenau konnte der verzögerte Arbeitsstand durch die Gewährung einer kostenneutralen Verlängerung bis Ende 2014 vollständig aufgeholt werden, wodurch schließlich alle inhaltlichen Ziele des Vorhabens erreicht wurden.

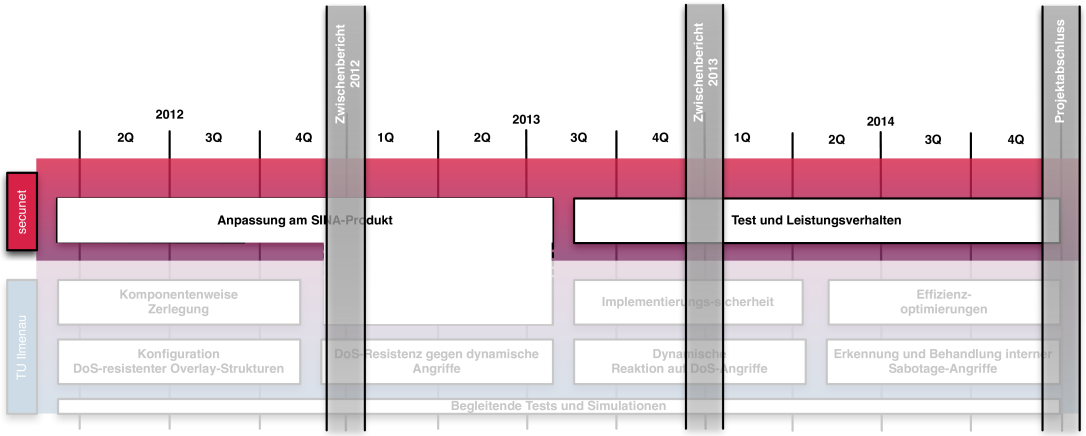

Abbildung 2: Überblick des Projektablaufs bei der secunet

2.4 Wissenschaftliche und technische Ausgangssituation

Der Umgang mit Denial-of-Service-Angriffen ist auch nach vielen Jahren großen Forschungsinteresses noch immer ein brisantes Thema, was bereits an einer Reihe von Vorfällen deutlich wird, welche mediale Aufmerksamkeit erfahren. Die Motivation hinter diesen Verfügbarkeitsangriffen ist dabei vielschichtig, häufig werden allerdings politische, wirtschaftliche oder schlicht finanzielle Interessen verfolgt [Les07, KK08, BFT11].

Die wenigen existierenden Gegenmaßnahmen unterliegen dabei typischerweise praktischen Einschränkungen. Dazu zählen beispielsweise Lösungsansätze, welche das Filtern von Angriffsverkehr durch ISPs vorsehen. Während das Filtern von Angriffsverkehr für typischen Datenverkehr in den öffentlichen Netzbereichen zumindest teilweise durchgesetzt werden kann, ist der Nutzdatenverkehr von VPNs aufgrund der hierbei eingesetzten Verschlüsselung nicht anhand typischer Kriterien von Angriffsverkehr zu unterscheiden.

In Verbindung mit dem Umstand, dass VPN großer Unternehmen und Behörden ein exponiertes Angriffsziel darstellen, ist die Ausgangssituation dementsprechend als ungünstig anzusehen. Die Auswirkungen von gezielten Angriffen auf die Ressourcen des Zielsystems können dabei in der Praxis noch vergleichsweise zufriedenstellend durch spezifische Gegenmaßnahmen eingeschränkt werden: Beispielsweise werden typischerweise SYN-Cookies verwendet, um die Anfälligkeit des TCP–Drei–Wege–Handshakes gegenüber sogenannten SYN-Flood-Angriffen eingesetzt. Demgegenüber stehen allerdings bandbreitenerschöpfende DoS-Angriffe, welchen bisher nicht mit geeigneten Gegenmaßnahmen gegenübergetreten werden kann.

Wie bereits erwähnt, verschärft sich dabei die Ausgangssituation in Anbetracht dynamischer bandbreitenerschöpfender Angriffe weiter. Hierbei können beispielsweise Besonderheiten der TCP-Staukontrollmechanismus ausgenutzt werden, um die Über-

tragung von Nutzdaten mit relativ wenig Angriffsverkehr – im Rahmen sogenannter Low-Rate DoS-Angriffe – vollständig zu unterdrücken.

Im Rahmen des Vorhabens konnte jedoch auf den SOLID-Ansatz zurückgegriffen werden, welcher bereits aufgrund der verteilten Konstruktion und der daraus resultierenden limitierten Exponiertheit der beteiligten Instanzen im Vergleich zu Konkurrenzverfahren eine vielversprechendere Ausgangssituation verspricht.

2.5 Zusammenarbeit mit anderen Stellen

Das DoS-Resist-VPN-Vorhaben wurde in enger Zusammenarbeit der secunet Security Networks AG und der TU Ilmenau bearbeitet. Im Rahmen des Vorhabens wurde sowohl in fachlichen Fragestellungen Rücksprache gehalten als auch innerhalb der Arbeitspakete gemeinsam nach Lösungen gesucht. Darüber hinaus wurde stets der Prozess der Produktisierung vorangetrieben, um den wirtschaftlichen Erfolg des SOLID-Verfahrens auf SINA-Basis mittel- und langfristig sicherzustellen.

Eine enge Zusammenarbeit mit externen Stellen gab es daneben nicht. Allerdings wurden Projektergebnisse mit einem großen Netzbetreiber, einem Telefoniehersteller und zwei Landesbehörden besprochen, um eine zukünftige Nutzbarkeit der enstandenen Technologie sicherzustellen.

3 Eingehende Darstellung

3.1 Verwendung der Zuwendung und des erzielten Ergebnisses im Einzelnen

Im Folgenden werden die im Rahmen des Vorhabens erzielten Ergebnisse vorgestellt. Der wissenschaftliche Fokus lag hierbei auf Forschungsfragen zu DoS-resistenten VPN-Strukturen, Umgang mit (komplexen) DoS-Angriffsstrategien und der Implementierungssicherheit des VPN-Verfahrens. Darüber hinaus lagen weitere Schwerpunkte auf vorbereitenden Maßnahmen der Integration von SOLID sowohl in das SINA Management-System als auch in die SINA L3 Box 3.9. Entsprechend der vorgesehenen Arbeitspakete wurden folgende Ergebnisse erzielt:

3.1.1 Komponentenweise Zerlegung

Auch heutzutage ist das Eindringen in Programme durch die Ausnutzung von Programmierfehlern (wie beispielsweise das Ermöglichen eines Buffer-Overflows) keine Seltenheit. So wurden über das Jahr 2012 durchschnittlich 70 Buffer-Overflow-Schwachstellen im Monat registriert und gemeldet [OSV14]. Daher sollte in diesem Arbeitspaket die Möglichkeit untersucht werden, die Auswirkung eines solchen Angriffs zu beschränken.

Ziel der komponentenweise Zerlegung ist die Einteilung des Prototyps in seine Privilegiengruppen und die Separierung aller Funktionen diesbezüglich. Dabei benötigt die Mehrzahl der Funktionen keine besonderen Rechte, jedoch gibt es auch Funktionen, die die Ausführung von Systemcalls realisieren (wie beispielsweise den Zugriff

auf das Dateisystem oder das Netzwerk). Diese benötigen für einen fehlerfreien Ablauf die jeweiligen Rechte, diese Systemfunktionen nutzen zu dürfen. Die aus der Separierung resultierenden Teilprozesse des ursprünglich monolithischen Prototyps können anschließend mit der für ihre Ausführung benötigten minimalen Rechtemenge gestartet werden. Daraus ergibt sich dann folgender Vorteil: Gelingt es einem Angreifer, die Kontrolle über einen Teilprozess zu übernehmen, ist er anschließend nur in der Lage, die (verminderten) Rechte dieses einen Teilprozesses zu missbrauchen. Im ursprünglichen, monolithischen Programm hätte er nach dem Eindringen über die selbe Softwareschwäche Zugriff auf alle Rechte des gesamten Programms erlangt. Eine beispielhafte Unterteilung, die verschiedene Rechtegruppen voneinander separiert, ist in Abbildung 3 dargestellt. Dort wird ein monolithischer Prozess in 6 Teilprozesse aufgeteilt: 5 Prozesse, denen jeweils die Rechte ihrer Rechtegruppe zugewiesen werden und 1 Prozess, der keine Rechte benötigt.

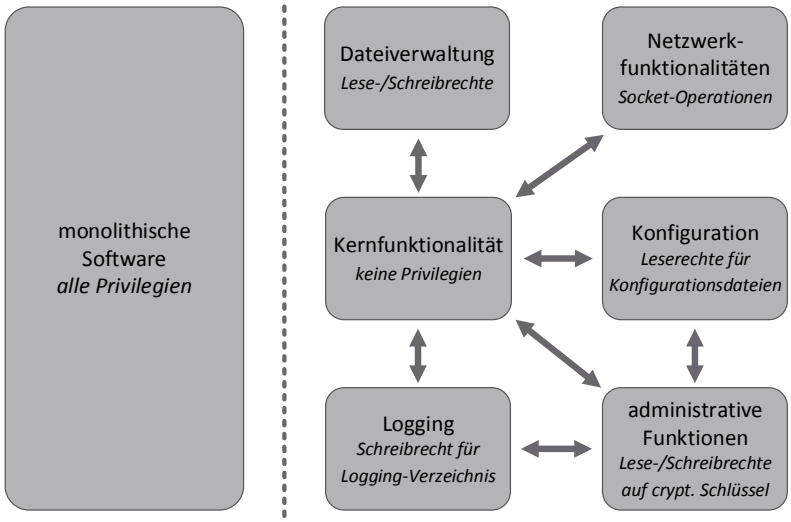

Abbildung 3: Mögliche Aufteilung einer monolithischen Software

Im Rahmen dieses Arbeitspaketes wurden Möglichkeiten und Grenzen der Automatisierung dieser Separierung untersucht. Diese Untersuchung wurde auf Grundlage der Callgraphen mehrerer Programme durchgeführt, aus denen die beinhalteten Funktionen und deren Systemaufrufe extrahiert werden konnten. Daraus ergab sich die Zuordnung von Funktion und benötigter Rechte. Bei der Aufteilung der Funktionen auf mehrere Teilprozesse muss auf mehrere Aspekte und deren Einflüsse auf Sicherheit und Performance geachtet werden.

- **Anzahl Privilegiengruppen:** Allgemein kann festgestellt werden, dass die Möglichkeiten des Angreifers nach einer erfolgreichen Kompromittierung stärker eingeschränkt werden können, wenn die Aufteilung der von einem Programm benötigten Privilegien in unterschiedliche Gruppen möglichst feingranular erfolgt. Daher scheint hier eine hohe Anzahl an Gruppen und daraus resultierend eine hohe Anzahl an Prozessen sinnvoll. Jedoch kann eine zu hohe Prozessanzahl zu Lasten der Performance und Handhabbarkeit gehen, da (Prozess-) Overhead und Synchronisierungaufwand steigen.

Des Weiteren müssen auch Grenzen der Separierbarkeit beachtet werden. So sind nicht alle Privilegien beliebig voneinander trennbar. Beispielsweise kann das Recht, einen Socket oder eine Datei zu öffnen, im Allgemeinen nicht von dem Recht auf diese zuzugreifen getrennt werden, da das entsprechende Handle dem öffnenden Prozess exklusiv zur Verfügung stehen kann. Sollen alle Privilegien, welche von der Software benötigt werden, automatisiert ermittelt werden, müssen ebenfalls Einschränkungen beachtet werden. So können manche Privilegien zur Übersetzungszeit nicht ermittelt bzw. genauer bestimmt werden, wenn beispielsweise Informationen darüber erst zur Laufzeit aus einer Konfigurationsdatei geladen oder durch Nutzereingaben spezifiziert werden.

- **Benötigte Interprozesskommunikation:** Durch die Trennung von Funktionen in mehrere Prozesse entfällt die Möglichkeit eines einfachen Funktionsaufrufs innerhalb eines Prozesses. Daher müssen Aufrufe, die über die Prozessgrenze hinaus gehen als Interprozesskommunikation (RPC) realisiert werden. Der dafür anfallende Overhead kann die Leistungsfähigkeit des Programms beeinträchtigen, weshalb darauf geachtet werden sollte, stark zusammenhängende Funktionen nicht unnötig zu separieren. Im Rahmen des aktuell eingereichten Artikels [TRS15] wurden Untersuchungen zum allgemeinen Einfluss von Interprozesskommunikation auf Netzwerkapplikationen durchgeführt, durch die gezeigt werden konnte, dass die Ausführungszeit solcher Anwendungen im Allgemeinen von deren Systemaufrufen (wie Festplatten- und Netzwerkzugriff) dominiert werden.
- **Separierungsgranularität:** Nicht nur die Aufteilung der Privilegien auf mehr oder weniger Prozesse und die damit einhergehende unterschiedliche Separierung der privilegierten Funktionen hat Einfluss auf den potenziellen Sicherheitsgewinn. Auch die Aufteilung der unprivilegierten Funktionen auf mehrere unprivilegierte Prozesse kann einen Einfluss haben. Dies ist exemplarisch in Abbildung 4 dargestellt. Hier gelingt es einem Angreifer durch eine verwundbare Funktion in einen Prozess einzudringen und anschließend beliebigen Code innerhalb dieses Prozesses auszuführen. Da der kompromittierte Prozess über keinerlei Rechte verfügt, kann der Angreifer keine Systemaufrufe, welche besondere Rechte benötigen würden, tätigen. Jedoch kann er Funktionsaufrufe mit von ihm spezifizierten Parametern durchführen. In Beispiel auf der linken Seite kann dadurch sowohl ein manipulierter Inhalt, als auch eine manipulierte Zieldatei an den Prozess zum Dateihandling weitergegeben werden. Dieser besitzt die Rechte zum Zugriff auf das Dateisystem und hat im Allgemeinen keine Möglichkeit, den eingehenden Aufruf auf seine Validität zu untersuchen. Auf der rechten Seite, wo der unprivilegierte Prozess beispielhaft ein weiteres Mal unterteilt wurde, kann der Angreifer nur den Inhalt als Parameter manipulieren, da die Zieldatei in dem Prozess bestimmt wird, in den der Angreifer nicht eindringen konnte. Dadurch kann das Einschleusen beliebigen Inhaltes in beliebige Dateien unterbunden werden.

Anhand dieser Kriterien wurde ein formales Modell als Optimierungsproblem zur besseren Verständlichkeit und Vergleichbarkeit entwickelt. Da die Bestimmung der exakten Lösung dieses NP-harten Problems nicht in annehmbarer Zeit möglich ist, wurde eine Heuristik zu deren Approximation entwickelt. Dadurch konnten unterschiedliche

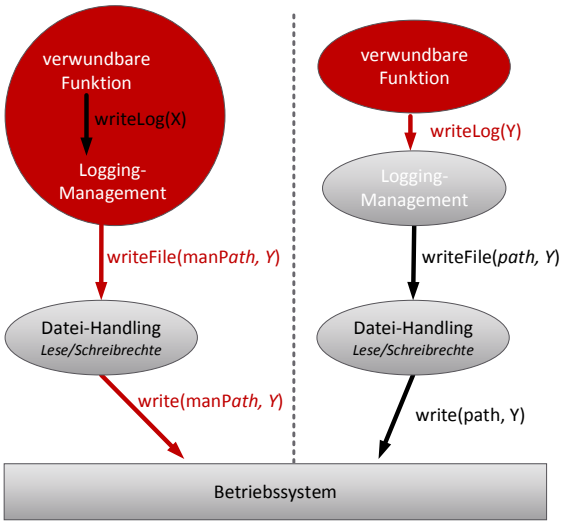

Abbildung 4: Angriffsmöglichkeiten bei unterschiedlichen Separationsgranularitäten

mögliche Separierungen einer Software unter Sicherheitsaspekten miteinander verglichen werden. Aus diesen Betrachtungen gewonnene Erkenntnisse werden in dem Artikel [TRS15] bei der Konferenz *IEEE Symposium on Computers and Communications* vorgestellt.

3.1.2 Konfiguration DoS-resistenter Overlay-Strukturen

Ein zunächst vorwiegend theoretisch orientierter Schwerpunkt des Vorhabens lag in der Suche nach besonders DoS-resistenten Overlay-Strukturen. Wesentliche Voraussetzung ist dabei der Umstand, dass im Zuge von DoS-Angriffen nicht nur einzelne Knoten, sondern gegebenenfalls durch entsprechende Beobachtung der Umgebung ganze Knotennachbarschaften ausfallen können. Diese Ausgangssituation ist anhand eines Beispiels in Abbildung 5 dargestellt. Dementsprechend wurde nach Graphstrukturen gesucht, welche zufriedenstellende Robustheitseigenschaften gegenüber dem Ausfall von Knotennachbarschaften aufweisen. Zunächst stand im Rahmen des

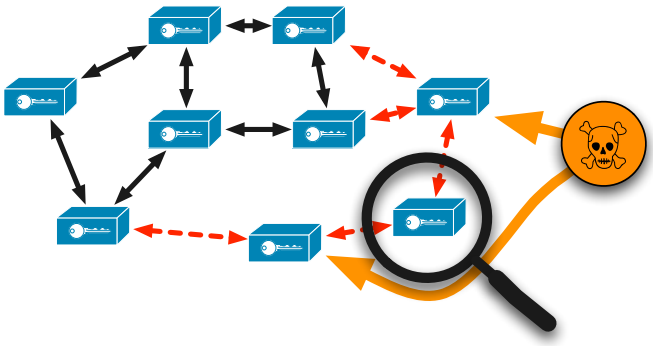

Abbildung 5: Auswirkungen der Beobachtung eines Knotens auf dessen Nachbarschaft

Arbeitspaketes der Entwurf eines geeigneten Angreifermodells im Mittelpunkt, wo-

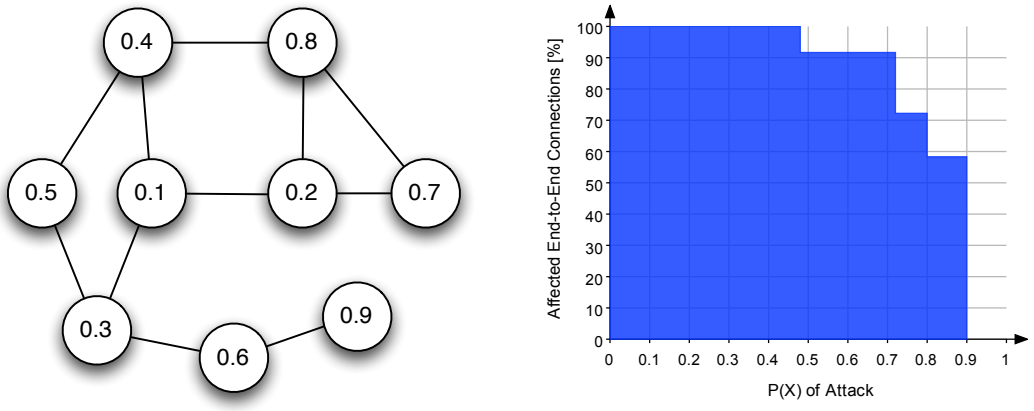

Abbildung 6: Ein beispielhaftes Overlay-Netzwerk mit Beobachtungswahrscheinlichkeiten (links) und der resultierende Einfluss eines optimalen DoS-Angreifers (rechts)

bei der Fokus – wie im Sicherheitsumfeld üblich – auf Worst-Case-Angriffe gelegt wurde. Daraus resultieren die folgenden Annahmen: Angreifer besitzen zum einen vollständiges Wissen über die im jeweiligen Szenario gegebene Topologie und können dementsprechend optimale Angriffe planen. Diese Voraussetzung ist durchaus haltbar, insbesondere wenn bedacht wird, dass eine solche Topologiesicht bereits nicht nur durch Kenntnis der zumeist deterministischen Konstruktionsalgorithmen sondern auch durch ausführliche Verkehrsflussanalyse erworben werden kann. Dabei wird deutlich, dass ein Beobachten des Netzwerkverkehrs eines bestimmten Knotens mit einem bestimmten Aufwand für einen möglichen Angreifer verbunden ist. Dieser Aufwand wird im Folgenden durch ein Kostenmaß repräsentiert. Unter Berücksichtigung des entworfenen Modells ergibt sich schließlich der optimale Angriff $D_{opt}(G, P_{min})$ bei einem Einsatz von $-\log P_{min}$ Kosten folgendermaßen:

$$D_{opt}(G, P_{min}) = max\left\{ D_G(X) \;\middle|\; X \subseteq V, \sum_{x \in X} \log p_x \geq \log P_{min} \right\}$$

Daraus kann schließlich die Verwundbarkeit gegenüber einem optimalen Angreifer bestimmt werden. Dazu wird prinzipiell die Fläche unter der Funktion $D_{opt}(G, P_{min})$ evaluiert, womit ein DoS-Effizienz-Index $E_{opt}(G)$ folgendermaßen definiert werden kann:

$$E_{opt}(G) = \int_0^1 D_{opt}(G, P_{min})\, \mathrm{d}P_{min}$$

Anhand von Abbildung 6 wird die Berechnung dieser Effizienz noch einmal illustriert. Dabei ist auf der linken Seite der Abbildung ein einfaches Overlay-Netzwerk dargestellt. Jeder Knoten ist hierbei mit einer Wahrscheinlichkeit für eine erfolgreiche Beobachtung annotiert. Wird schließlich entsprechend dem vorgestellten Modell ein optimaler Angriff durchgeführt, repräsentiert $D_{opt}(G, P_{min})$ die Anzahl verlorener Ende-zu-Ende-Verbindungen. Bei Betrachtung der zugehörigen Darstellung auf der rechten Seite wird schließlich deutlich, dass $E_{opt}(G)$ die Fläche unter der Funktion $D_{opt}(G, P_{min})$ reflektiert und als Maß für die Verwundbarkeit gegenüber dem optimalen Angreifer dient.

Im Rahmen des Vorhabens konnte des Weiteren gezeigt werden, dass das Finden dieser optimaler Attacken zumindest NP-schwer ist. Dies wurde durch eine Reduktion auf das Vertex-Cover-Problem gezeigt, wobei der entsprechende Beweis auf homogenen Beobachtungswahrscheinlichkeiten basiert. Allerdings muss davon ausgegangen werden, dass auch für große Netze optimale Angriffe approximiert werden können. Neben dem optimalen Angriff wurden natürlich auch weitere Angreifermodelle untersucht, wobei weiterführende Informationen der entstandenen Veröffentlichung [GRS14] entnommen werden können.

Anknüpfend an die gewonnen Erkenntnisse und unter Zuhilfenahme dieses Modells wurden schließlich im Rahmen des Arbeitspaketes verschiedene vielversprechende Graphstrukturen bezüglich deren Resistenz gegenüber bandbreitenerschöpfenden Angriffen untersucht. Dabei wurde offenbar, dass insbesondere Strukturen mit folgenden Eigenschaften eine hohe Resistenz aufweisen:

- Konstante, niedrige Knotengrade,
- eine große Taillenweite,
- geringe durchschnittliche Pfadlängen, und
- starke Homogenität bezüglich typischer Zentralitätsmetriken (bspw. Knotengrad und Betweenness- bzw. Closeness-Zentralität).

Ein Vergleich einer Auswahl von Graphstrukturen und bezüglich deren Verwundbarkeit bezüglich eines optimalen Angriffs ist in Abbildung 7 dargestellt. Unter anderem wird dabei deutlich, dass besonders die konstruierten Graphen mit hoher Taillenweite eine niedrige Verwundbarkeit aufweisen. Darüber hinaus wird deutlich, dass auch reguläre zufällige Graphen deutlich robuster sind als typischerweise in strukturierten Overlays konstruierte Graphen. In Bezug auf das zu realisierende Overlay-Routing weisen Butterfly-, De-Bruijn und Hypercube-Graphen dabei zunächst günstige Voraussetzungen auf, da diese logarithmische Pfadlängen bei Einsatz Identifikator-basierter Routing-Strategien garantieren, allerdings kann keine dieser Strukturen so simpel konstruiert und verwaltet werden, wie die bekannten CAN-Graphen. Da eine geringe Verwundbarkeit gegenüber bandbreitenerschöpfenden Angriffen an dieser Stelle als primäres Ziel anzusehen ist, wird mit dem *Persistent Overlay Network* eine in [GRS12] vorgestellte Graphkonstruktion realisiert, welche auf regulären Graphen basiert.

Dabei sieht das Verfahren die Erzeugung einer 4-regulären Graphstruktur vor, welche Ähnlichkeiten zu zufälligen Graphen aufweist. Zunächst erscheint dabei eine Konstruktion 3-regulärer Graphen zwar naheliegender, allerdings ist deren Generierung ohne Inkonsistenzen im Allgemeinen Fall nicht möglich, da keine 3-regulären Graphen von ungerader Größe existieren. Der im Rahmen des Vorhabens entworfene Ansatz versieht jeden Knoten mit zwei eindeutigen Koordinaten x und y, wobei $0 < x, y < 1$ gilt. Diese Koordinate kann beispielsweise aus dem jeweiligen öffentlichen Schlüssel abgeleitet werden. Bezüglich jeder dieser Koordinaten wird schließlich eine Ringstruktur etabliert, in welcher die beteiligten Knoten anhand der entsprechenden x- bzw y-Werte sortiert angeordnet sind. Da jeder Knoten mit einem linken und einem rechten Nachbarn auf jedem Ring verbunden ist, ist der resultierende Graph 4-regulär, solange keine topologischen Anomalien vorliegen (beispielsweise durch lokal identische Nachbarn auf beiden Ringen).

Natürlich ergeben sich bei der Verwendung einer solchen Overlay-Struktur Nachteile

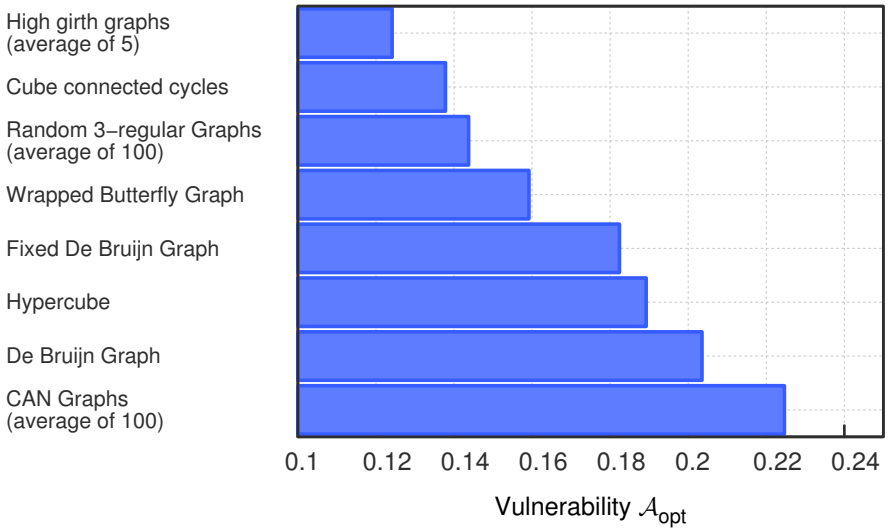

Abbildung 7: Vergleich bekannter Graphstrukturen

bezüglich der Routing-Effizienz gegenüber Strukturen, welche in Hinblick auf ein Identifikator-basiertes Routing optimal konstruiert wurden. Optimales Shortest-Path-Routing kann dabei nur bei Kenntnis der gesamten Topologie realisiert werden. Diese basiert allerdings lediglich auf den Knotenkoordinaten und kann im Verlauf des Verfahrens propagiert werden. Insbesondere aus Privacy-Gründen sind Routing-Strategien auf Basis lokalen Wissens allerdings zu bevorzugen. Hierbei kann die eindeutige Ordnung in der konstruierten Topologie verwendet werden, um die Distanz zwischen zwei Knoten i und j unter Zuhilfenahme einer Greedy-Strategie und der entsprechenden Weiterleitung über denjenigen lokalen Nachbarn, welcher die geringste Distanz zum Ziel aufweist, sukzessive zu minimieren.

Weiterführende Details zu Topologiekontrolle und Besonderheiten der Routing-Strategie können dabei der bereits erwähnten Veröffentlichung [GRS12] entnommen werden.

3.1.3 DoS-Resistenz gegen dynamische Angriffe

Insbesondere aufgrund des vollständig verteilten Grundprinzips hat sich das SOLID-Verfahren bereits zu Beginn des Vorhabens als resistent gegenüber klassischen DoS-Angriffen herausgestellt. Allerdings sind mit gepulsten und dynamischen Angriffstechniken vergleichsweise neue Strategien bekannt, welche die Verfügbarkeit und Stabilität eines VPNs signifikant reduzieren können. Dabei lag es zu Beginn des Vorhabens zunächst nahe, die konstruktionsbedingte Resistenz des SOLID-Verfahrens gegenüber diesen Strategien zu untersuchen. Dabei konnten insgesamt durchaus positive Ergebnisse beobachtet werden, was erneut weitestgehend auf die fehlenden exponierten Angriffspunkte des verteilten SOLID-Verfahrens zurückzuführen ist. In den zugrunde liegenden Transportnetzinfrastrukturen typischer Szenarien besteht darüber hinaus in der Regel nur eine geringere Anfälligkeit im Kernbereich des Netzes, weshalb sich die Auswirkungen von Angriffen auf die Randbereiche beschränken. Unter anderem gilt dies auch für die heutige Internet-Infrastruktur. Im Allgemeinen sind die Auswirkungen von dynamischen DoS-Angriffen bei Einsatz des SOLID-Verfahrens daher lokal

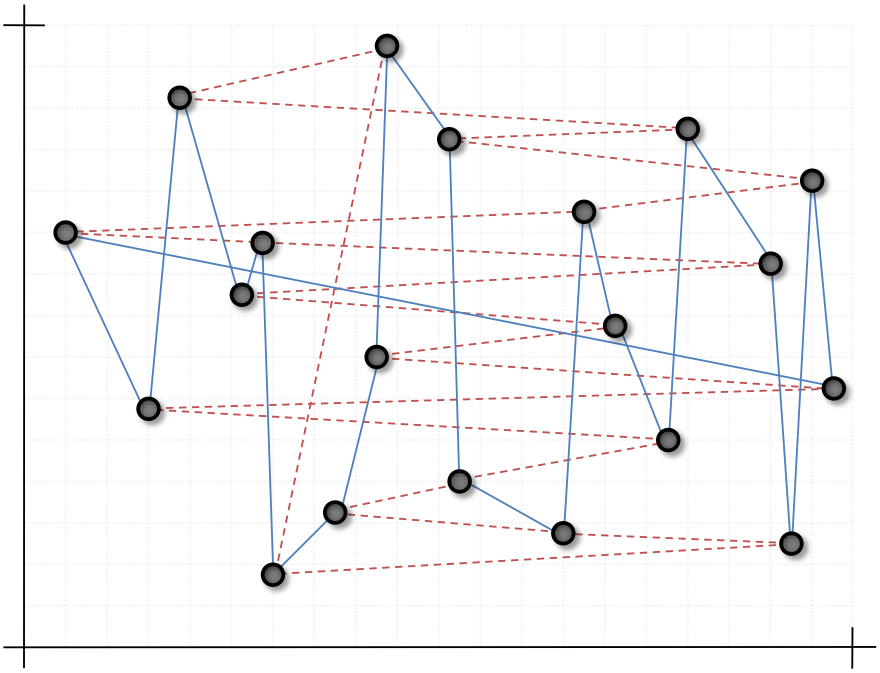

Abbildung 8: Beispielhafte Darstellung der Persistent-Overlay-Network-Topologie

begrenzt.

Um darüber hinaus auch die Selbstreparaturmechanismen der SOLID-Topologiekontrolle bezüglich gepulster und dynamischer Angriffe zu untersuchen, wurden verschiedene Angriffsmuster unter Zuhilfenahme umfangreicher Simulationsstudien durchgeführt. In Abbildung 9 wird der charakteristische Verlauf eines Angriffes und insbesondere dessen Auswirkung auf die Ende-zu-Ende Verfügbarkeit für ein Beispielszenario dargestellt. Dabei erfolgt der Angriff im hervorgehobenen Zeitfenster zwischen 2000 und 4000 Sekunden nach Start der Simulation. Dargestellt wurden hierbei Mittelwerte für jeden Zeitpunkt über 64 Simulationsläufe. Auf eine Darstellung der transienten Phase bis zur Systemstabilisierung wurde verzichtet. Um praxisnahe dynamische Angriffe verschiedener Stärke nachzubilden wurde dabei die starke Korrelation mit Paketverlustraten verwendet. Die Verlustwahrscheinlichkeit am Bottleneck-Link wird dabei für alle Pakete – unabhängig davon, ob es sich um Angriffs- oder Nutzdatenverkehr handelt – als gleich angenommen. Bei genauerer Betrachtung der Abbildung wird deutlich, dass die mittlere Ende-zu-Ende-Konnektivität im Rahmen eines Angriffes etwas abfällt. Ein vergleichsweise starker Angriff mit einer Verlustrate von 0.95 erwirkt dabei im Rahmen eines Angriffsimpulses mit einer gewählten Pulsbreite von 300 Sekunden signifikante Auswirkungen auf die Ende-zu-Ende-Konnektivität, während ein vergleichbarer Konnektivitätsverlust von schwächeren Angriffen nicht erreicht wird. Dies ist im Wesentlichen auf die zügige Selbstreparatur des SOLID-Verfahrens zurückzuführen. Nach Ende jedes Angriffsimpulses werden zuvor betroffene Knoten unverzüglich wieder in die Topologie integriert, wodurch die ursprüngliche Konnektivität zügig wiederhergestellt wird.

Letztlich wurde im Zuge der durchgeführten simulativen Bewertung deutlich, dass das SOLID-Verfahren insbesondere im Vergleich zu anderen VPN-Autokonfigurationsansätzen

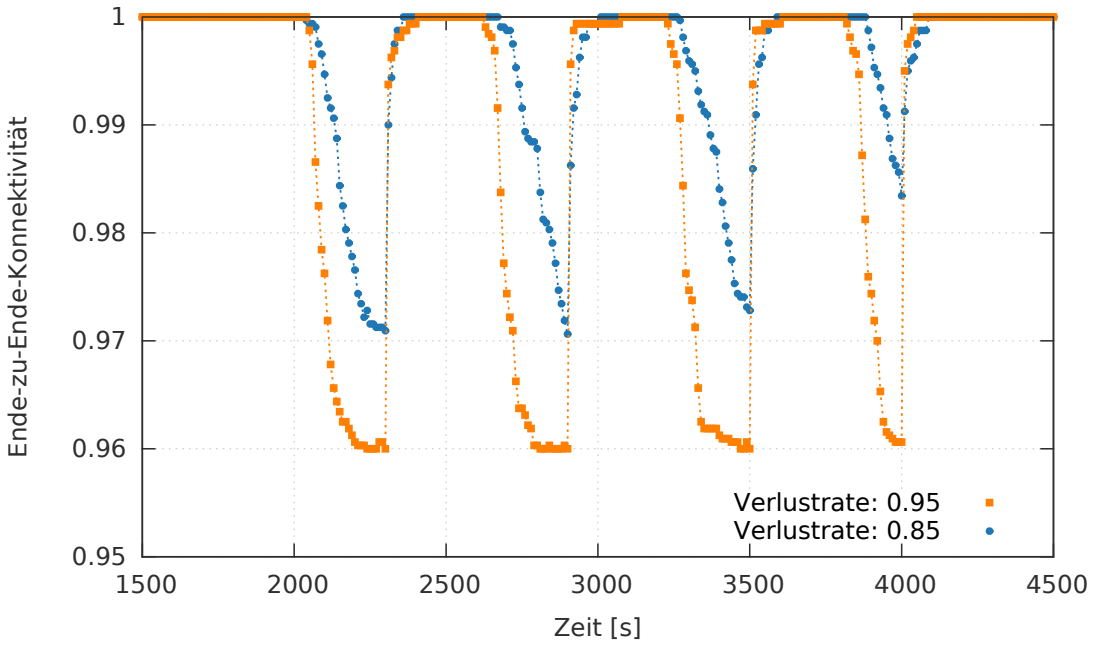

Abbildung 9: Mittlerer zeitlicher Verlauf eines gepulsten Angriffes auf ein VPN-Gateway und entsprechende Auswirkungen auf die Ende-zu-Ende-Konnektivität des Gesamtsystems.

keine unmittelbaren Schwächen gegenüber gepulsten Angriffen aufweist. Unabhängig davon kann der Durchsatz der typischerweise von Applikationen verwendeten TCP-Verbindungen durch gepulste Angriffe dennoch signifikant minimiert werden. Entsprechende Angriffsmethoden sind beispielsweise in [KK06, GBM04] erläutert. Durch eine solche Vorgehensweise resultiert ein – zumindest lokaler – Einbruch der Dienstgüte, da betroffene Ende-zu-Ende-Verbindungen letztlich unbenutzbar werden. Um diesen Effekten unter Verwendung gezielter Gegenmaßnahmen entgegenzuwirken, müssen entsprechende Angriffe zunächst zuverlässig erkannt werden. Daher wurde im Rahmen des Arbeitspaketes ein Detektionsverfahren entworfen und in den SOLID-Prototypen integriert. Dabei werden folgende Kriterien zur Angriffserkennung herangezogen:

- **Paketverlustraten:** Der vermutlich populärste Indikator für Verbindungsstörungen ist die beobachtete Paketverlustrate über einen dedizierten Zeitraum. Dazu werden im konkreten Fall die *Packet*- und *Replay*-Counter der aktiven IPsec-Sicherheitsbeziehungen verwendet, um entsprechende Verlustraten auf der jeweils verwendeten Netzwerkschnittstelle abzuleiten.
- **Heartbeat-Nachrichten:** Zur Überwachung von Verbindungen verwendet das SOLID-Verfahren unter anderem einen periodisch ausgelösten Heartbeat-Mechanismus. Konsekutive Verluste entsprechender Heartbeat-Nachrichten sind dabei ein starker Indikator für einen Verbindungsausfall.
- **Jitter:** In normalen Lastsituationen sind starke Schwankungen der beobachteten Paketverzögerungen in den heute vorherrschenden, öffentlichen Netzen selten zu beobachten. Dementsprechend ist dieser *Jitter* ein Indikator für überlastete Ver-

bindungen, da dieser häufig auf Probleme in den traversierten Zwischensystem, wie beispielsweise stark variierende Warteschlangen-Füllstände, zurückzuführen ist.

- **Zeitlicher Verlauf:** Alle genannten Indikatoren werden dabei über ein definiertes Zeitfenster betrachtet. Um Schwingungseffekte zu vermeiden, welche durch ausgewählte Gegenmaßnahmen (wie beispielsweise den Wechsel der verwendeten Netzwerkschnittstellen, falls eine Mehrfachanbindung vorliegt) hervorgerufen werden können, wurde eine Hysterese integriert, welche die Ausfallerkennung im Falle einer kürzlichen Erkennung im Rahmen eines definierten Zeitfensters verzögert.

Diese Kriterien bilden schließlich die Grundlage für ein passives Verfahren, welches zur Laufzeit diejenigen charakteristischen Störungen der Verbindungen erkennt, welche mit hoher Wahrscheinlichkeit auf einen gepulsten Angriff zurückzuführen sind. Eine fehlerhafte Erkennung ist aufgrund der in einem solchen Fall ohnehin vorliegenden anderweitigen signifikanten Störung der jeweiligen Verbindung in der Regel nicht als störend anzusehen.

3.1.4 Dynamische Reaktion auf DoS-Angriffe

Auf Basis der im Arbeitspaket *DoS-Resistenz gegen dynamische Angriffe* gewonnen Erkenntnisse wurden in diesem Arbeitspaket zunächst Maßnahmen entworfen, um den Einfluss von DoS-Angriffen zu minimieren, falls dies in Anbetracht der jeweiligen Transportnetzumgebung möglich ist. Unter anderem ist dies in Szenarien der Fall, in denen der von einem DoS-Angriff betroffene Knotenpunkt über alternative Netzwerkschnittstellen verfügt, welche nicht von einem DoS-Angriff betroffen sind, aber eine Kommunikation mit anderen Knotenpunkten des VPN ermöglichen.

Ein solches Szenario ist anhand eines Beispiels in Abbildung 10 schematisch dargestellt. Während andere VPN-Gateways keine Mehrfachanbindung an das öffentliche Netz aufweisen, verfügt das zum Netzbereich 6 gehörige Gateway über mehrere entsprechende Schnittstellen. Ist schließlich eine dieser Schnittstellen von einem DoS-Angriff betroffen, wird infolge einer Erkennung durch die im Rahmen des Arbeitspaketes *DoS-Resistenz gegen dynamische Angriffe* entworfene Heuristik zunächst versucht, bestehende Sicherheitsbeziehungen mithilfe der MOBIKE-Erweiterung [Ero06], welche bereits aus dem Mobil-SOLID-SINA-Vorhaben bekannt ist, proaktiv an die alternative Netzwerkschnittstelle zum öffentlichen Netz zu übergeben. Daneben existiert für eine beispielhafte Sicherheitsbeziehung zum Gateway des geschützten Netzbereiches 2 ein weiterer möglicher, indirekter Pfad (über die gesicherten Netzbereiche 5 und 4) durch das Transportnetz. Hierbei ist zu bemerken, dass eine Übertragung einer direkten Sicherheitsbeziehung auf eine andere Schnittstelle mithilfe der MOBIKE-Erweiterung nicht erfolgreich ist, falls die betroffenen Gateways anschließend nicht mehr direkt erreichbar sind. Dementsprechend wird auf eine entsprechende proaktive Übertragung verzichtet, allerdings steht der indirekte Pfad durch das Transportnetz im Rahmen einer Neuaushandlung der Beziehung zur Verfügung und wird vom SOLID-Verfahren konfiguriert und verwendet, falls die direkte Anbindung an das Transportnetz nicht zur Verfügung steht.

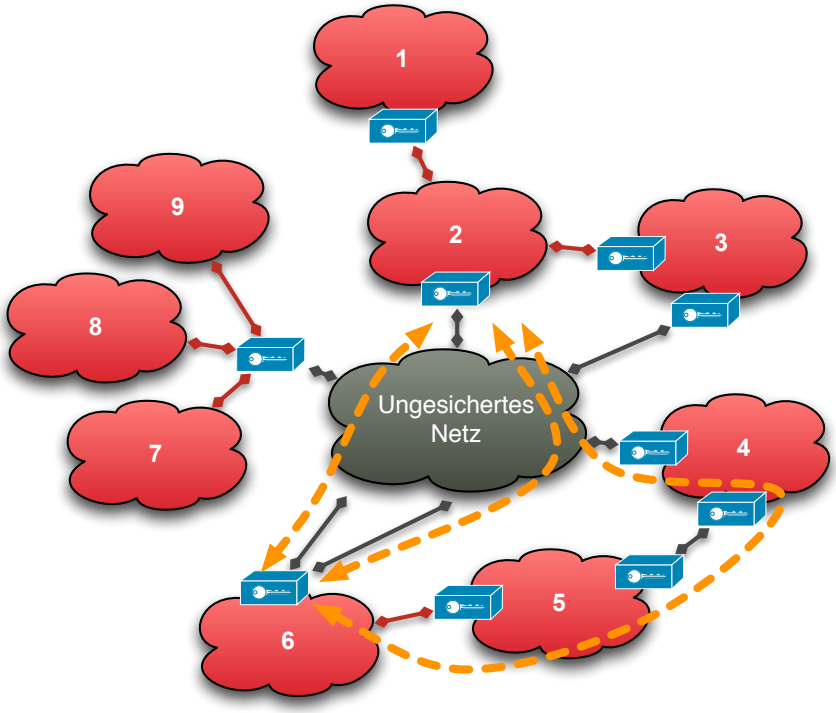

Abbildung 10: Beispielhaftes Transportnetzszenario mit einem VPN-Gateway, welches sich am Rand des gesicherten Netzbereiches 6 befindet und über mehrere Schnittstellen zum öffentlichen Netz verfügt.

Daneben wurden ein Verfahren entworfen, welches eine zügige Reaktion auf Ausfälle von Teilbereichen des öffentlichen Netzes erlaubt. Diese können neben geographisch korrelierten Anomalien, Katastrophen oder administrativen Fehlern unter anderem auch durch DoS-Angriffe auf Infrastrukturkomponenten ausgelöst werden. Dabei werden proaktive Ersatzpfade eingerichtet, welche in Hinsicht auf einen möglichen Ausfall der jeweiligen direkten Transportnetzverbindung mithilfe indirekter Kommunikation im VPN-Overlay Konnektivitätsverlust vermeiden. Um mit hoher Wahrscheinlichkeit einen indirekten Ersatzpfad auszuwählen, welcher nicht vom entsprechenden Ausfall der direkten Transportnetzverbindung zwischen zwei VPN-Knoten betroffen ist, werden die geographischen Positionen der Teilnehmer zur Ersatzpfadplanung herangezogen. Dazu wurde im Rahmen des Arbeitspaketes ein verteiltes, skalierbares Verfahren entwickelt, welches die geographische Position von VPN-Teilnehmern mit ausreichender Genauigkeit abschätzt [GRBS13, GSRS14], ohne für den Großteil dieser Teilnehmer einen Zugriff auf externe Dienste, wie beispielsweise GPS oder datenbankgestützte Lokalisierungsansätze, vorauszusetzen. Auf Grundlage der geschätzten geographischen Position werden schließlich vielversprechende Ersatzpfade ausgewählt und verwaltet. Eine Veröffentlichung einer konkreten Auswahlstrategie und Ersatzpfadverwaltung wird nach dem Abschluss des Vorhabens angestrebt.

Traditionelle DoS-Angriffe zielen darauf ab, den Netzwerklink eines Opfers über einen längeren Zeitraum komplett auszulasten, sodass dieser keine Möglichkeit mehr hat, Daten zu senden oder zu empfangen. Dies wird meist durch ein Bot-Netz realisiert,

damit die Angriffsbandbreite hoch genug ist und das Opfer möglichst lange ausgeschaltet werden kann. Dieser beständige Angriff hat jedoch, neben seinen hohen Kosten, den Nachteil, dass dessen Herkunft relativ einfach (zum Beispiel durch flow-basiertes Monitoring) ermittelt und Gegenmaßnahmen eingeleitet werden können. Eine weitere, kostengünstigere Angriffsart stellen die low-rate DoS-Angriffe dar. Diese Angriffe basieren nicht auf dem dauerhaften Blockieren des Kommunikationskanals, sondern führen lediglich kurze, gepulste Störungen durch. Diese werden genutzt, um TCP-Verbindungen, die etwa 90% des gesamten Nutzdatenverkehrs ausmachen, zu beeinträchtigen. Fehlen einer TCP-Verbindung zu viele Bestätigungen, beginnt diese damit, die unbestätigten Daten erneut zu übertragen und auf deren Bestätigung zu warten. Die Zeitspanne zwischen zwei solchen Retransmits verdoppelt sich jeweils, sofern keine Bestätigung für die gesendeten Daten empfangen werden kann. Nun reicht es, den Kommunikationskanal genau dann auszulasten, wenn ein Retransmit stattfindet, wodurch dies nicht empfangen und daher auch nicht bestätigt werden kann. Dadurch kann die Angriffsdauer und damit die benötigte Bandbreite stark reduziert werden kann, da auf eine dauerhafte Auslastung des Kommunikationskanals verzichtet werden kann. Dies bietet dem Angreifer zusätzlich den Vorteil, dass er schwerer durch flussbasierte Überwachung zu detektieren ist. Im Vergleich zu den traditionellen DoS-Angriffe besitzt der Angreifer des Weiteren die Möglichkeit, mit dem gleichen Bandbreitenbudget mehr Ziele anzugreifen. Diese Angriffsart wurde bereit in [KK06] vorgestellt und erfolgreich durchgeführt.

Im Rahmen dieses Arbeitspaketes wurde sowohl ein Versuchsaufbau zur Durchführung solcher Angriff auf das SOLID-System eingerichtet, als auch eine geeignete Gegenmaßnahme entworfen und evaluiert. Der Versuchsaufbau ist dabei in Abbildung 11 dargestellt. Er besteht aus vier Systemen, welche mit leistungsfähigen Netzwerkkarten ausgestattet wurden und jeweils Verkehr bis zu einer Bandbreite von 1 Gigabit pro Sekunde erzeugen können. Diese Systeme simulieren einen verteilten Angriff auf einen Router, welcher für die Verbindung der zwei VPN-Systeme notwendig ist. Fällt dieser Router durch eine Überlastung aus, ist auch kein Datenaustausch zwischen den beiden VPN-Systemen mehr möglich und die Kommunikation der beiden Clients (durch zwei Laptops dargestellt) fällt aus.

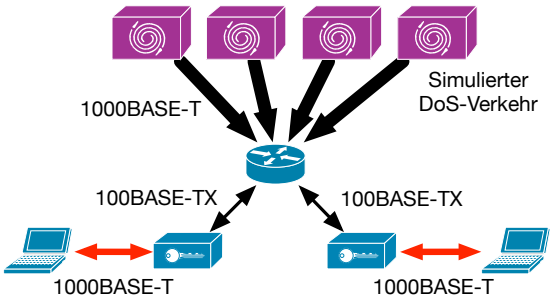

Abbildung 11: Versuchsaufbau zur Durchführung gepulster DoS-Angriffe auf den SOLID-Prototyp

Im Rahmen dieses Arbeitspaketes wurde ein Verfahren entwickelt und untersucht, um die negativen Auswirkungen eines gepulsten DoS-Angriffes zu minimieren. Zu beachten ist, dass die Detektion eines gerade stattfindenden (gepulsten) DoS-Angriff

im Allgemeinen nicht möglich ist. Dies liegt zum einen daran, dass gepulster und damit nur kurz auftretender DoS-Verkehr schlecht detektierbar ist. Zum anderen muss das Gateway nicht selbst das direkte Opfer des Angriffs sein. Wird, wie in Abbildung 11 dargestellt, der Router vor dem Gateway angegriffen, hat dies die gleichen negative Auswirkungen wie ein direkter Angriff. Da jedoch keinerlei Angriffsverkehr das Gateway erreicht, hat dieses auch keine Möglichkeit einen Angriff zu detektieren.

Daher wurde ein Verfahren entwickelt, dass auf eine Detektion von DoS-Angriffen verzichten kann, jedoch trotzdem die Auswirkungen minimiert. Diese Verfahren basiert auf dem proaktiven Wiedereinspielen von TCP-ACK-Paketen und wurde Denial-of-Service Countermeasure via ACK Replay (DoSCAR) genannt. Dazu werden alle aktiven TCP-Ströme des System überwacht und jeweils deren letztes gesendetes Paket gespeichert. Im Falle eines gepulsten Angriffs, treten Paketverluste in den betroffenen Strömen auf. Ist ein Angriffsintervall beendet, würde das TCP auf den nächsten Timeout warten und bei dessen Eintritt ein Retransmit auslösen, das aber dann wiederum vom nächsten Impulse des Angreifers gestört wird. Da die TCP-Ströme überwacht werden, können die beeinträchtigten Ströme durch das ausbleiben jeglicher Pakete als ausgefallen detektiert werden. In diesem Falle beginnt das DoSCAR-System mit dem beständigen Wiedereinspielen (in einem konfigurierbaren Zeitfenster) des letzten gespeicherten Paketes dieses Stroms. Sobald ein Angriffsimpuls beendet ist, gelangt ein solches Paket zum Kommunikationspartner, wodurch dieser eine Bestätigung für diese Daten sendet. Trifft diese Bestätigung dann anschließend beim Gateway ein, kann die Kommunikation bis zum nächsten Angriffsimpuls normal fortgesetzt werden. Dadurch können die Auswirkungen eines gepulsten DoS-Angriffs stark abgemildert werden, da eine normale Kommunikation in den Intervallen zwischen den jeweiligen Angriffen ermöglicht werden kann. In den Abbildungen 12 und 13 sind ist jeweils der Durchsatz einer TCP-Verbindung während eines gepulsten DoS-Angriffes (Angriffsintervalle in Grau) ohne (Abb. 12) beziehungsweise mit (Abb. 13) DoSCAR-Schutz dargestellt.

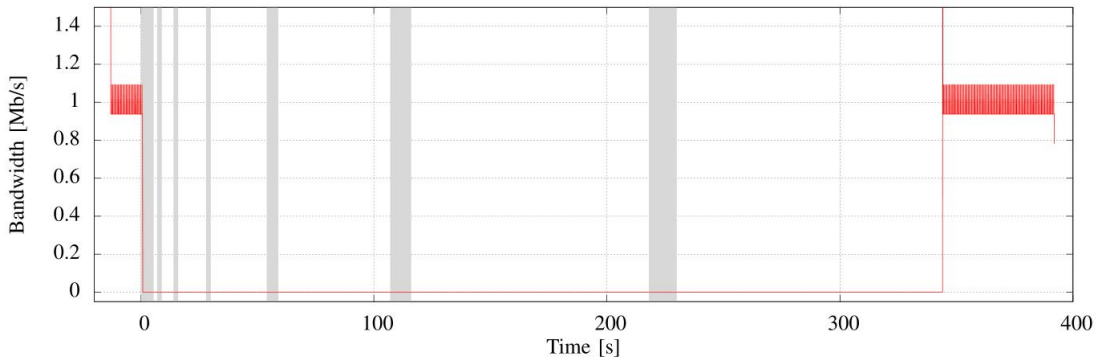

Abbildung 12: Angriffsverlauf ohne DoSCAR-Schutz

Das im Rahmen dieses Arbeitspaketes entstandene DoSCAR-System und weiterführende Erläuterungen und Experimente sind im Artikel [TBR15] beschrieben und derzeit bei der IEEE CNS 2015 zum Review eingereicht.

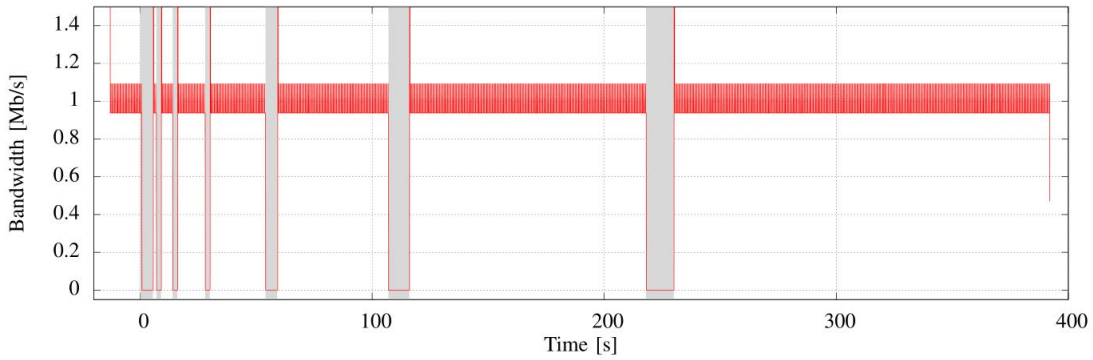

Abbildung 13: Angriffsverlauf mit DoSCAR-Schutz

3.1.5 Implementierungssicherheit

Eine Vielzahl der praktischen Schwächen verschiedener existierender VPN-Lösungen ist auf exponierte Angriffspunkte der jeweils konkreten Implementierung zurückzuführen. Um das SOLID-Verfahren auch hinsichtlich der Implementierungssicherheit zu stärken, wurden daher im Rahmen des Arbeitspaketes *Komponentenweise Zerlegung* zunächst zusätzliche Methoden entwickelt, um Teile der Implementierung, beispielsweise entsprechend der jeweils benötigten Rechte, zu isolieren.

Darüber hinaus wurde das durch IPsec-Policies erzeugte Regelwerk ergänzt, indem zusätzliche Firewall-Regeln verwendet werden, um die sicherheitskritische Forwarding-Komponente redundant abzusichern. Dabei wird auf den verwendeten Unix-Plattformen auf die *iptables*-Programmfamilie zurückgegriffen. Dementsprechend werden auf Ebene des Betriebssystems nur diejenigen Paketflüsse erlaubt, welche auch durch IPsec-Policies gestattet werden.

Automatisierte Kontrolle des Quellcodes Die Wartung und Kontrolle von Quelltext hinsichtlich seiner korrekten Funktionsweise und etwaiger Fehler kann durch unübersichtlichen oder schlechten Programmierstil äußerst negativ beeinflusst werden. Dadurch können Fehler, die bei gut strukturiertem Quellcode offensichtlich sind, leicht übersehen werden. Um dies zu vermeiden, wurde ein System eingerichtet, dass den gesamten Quellcode auf seine Übersichtlichkeit und Strukturiertheit hin überprüft. Dazu wurden verschiedene Code-Conventions (beispielsweise eine Reglementierung, dass jeweils nur eine Anweisung pro Zeile stehen darf) definiert. Jeder neu hinzukommende Code, der von einem Mitarbeiter oder einer studentischen Hilfskraft implementiert wurde, muss diesen Konventionen genügen, damit ein Übersetzen überhaupt möglich wird. Erst wenn alle aufgestellten Konventionen eingehalten werden, kann der Quellcode übersetzt und automatisiert getestet werden. Durch dieses System kann ein einheitlicher und gut strukturierter Programmierstil, der ein gezieltes Code-Review sowie eine effiziente Fehlersuche ermöglicht, für das gesamte Projekt durchgesetzt werden.

Sicherheitsüberprüfungen zur Laufzeit Eine weitere Stärkung der Sicherheitseigenschaften konnte durch die Einführung von umfangreichen Security-Checks erreicht werden. Diese wurden an den sicherheitskritischen Stellen des SOLID-Quellcodes eingepflegt und beschreiben jeweils Bedingungen, die beim Durchlauf dieses Codesegmentes garantiert werden müssen. Beispielsweise kann auf diese Weise geprüft werden, ob eine auf einem nicht vertrauenswürdigen Netzwerk-Interface eingehende Nachricht auch verschlüsselt war, oder ob bestimmte Sender- und Empfängeradressen korrekt eingetragen sind. Es wurden zwei Arten von Security-Checks implementiert, wobei zwischen tolerierbaren und *harten* Checks unterschieden wird. Schlägt ein tolerierbarer Check fehl, wird zu diesem Vorfall eine Log-Meldung generiert und ein Event an das Monitoring- und Managementsystem weitergeleitet. Ein Ausschnitt aus diesem System ist in Abbildung 14 dargestellt. Hier werden die jeweils fehlgeschlagenen Security Checks für jedes Gateway des VPN-System und deren Stelle im Quellcode festgehalten. So kann der zuständige Administrator bei auftretenden Unregelmäßigkeiten das Systemverhalten, ausgehend von dem gemeldeten Punkt, eingehender untersuchen. Security-Checks, die als hart gekennzeichnet wurden, müssen zwingend eingehalten werden, um die Vertraulichkeit des Verfahrens an jeder Stelle gewährleisten zu können. Schlägt ein solcher Check fehl, muss von einer größeren Fehlfunktion oder den Auswirkungen eines (internen) Sabotage-Angriffes (siehe 3.1.7) ausgegangen werden. In diesem Falle, wird das Gateway geordnet heruntergefahren und tritt aus dem VPN aus, um mögliche sicherheitsrelevante Folgeschäden vermeiden zu können. Dadurch ermöglichen die entwickelten Security-Checks eine bessere Kontrolle des (sicherheitsrelevanten) Zustandes des Gateways und können im Fehlerfall durch das Abschalten des betroffenen Gateways eine mögliche weitere Kompromittierung unterbinden.

Abbildung 14: Monitoring-System für fehlgeschlagene Security Checks

3.1.6 Effizienzoptimierungen

Zu Beginn des Vorhabens war der entstandene SOLID-Prototyp zwar bereits mit einem großen Funktionsumfang ausgestattet und kam aufgrund der getroffenen Entwurfsentscheidungen mit sehr begrenztem Zustandswissen aus – allerdings war er auf Effizienz bezüglich der Bandbreite und Reaktionsgeschwindigkeit optimiert. Mit Blick auf die anstehende Produktisierung wurde eine weitere Optimierung, insbesondere bezüglich der von Verwaltungsnachrichten verwendeten Bandbreite, bereits im Vorfeld des Vorhabens als sinnvoll angesehen. Dementsprechend wurden zunächst sinnvolle Ratenlimitierungen für verschiedene Overlay-Nachrichtentypen, wie beispielsweise die häufig ausgelösten Suchanfragen, entworfen und in den Prototypen integriert. Darüber hinaus wurden die im Rahmen des Verfahrens häufig aktualisierten Peer-Objekte verkleinert. Im Laufe des Verfahrens wird dabei der aktuelle Verbindungszustand berücksichtigt, sodass in der Regel nur veränderliche Objektteile ausgetauscht werden.

Portierung auf VoIP-Endgeräte Andere Maßnahmen werden insbesondere dann notwendig, wenn das Verfahren unmittelbar auf ressourcenarmen Endgeräten zum Einsatz kommen soll. Unter anderem wurde dabei angestrebt, dass der SOLID-Prototyp direkt auf handelsüblichen Voice-over-IP-Telefonen verwendet werden kann. Zum einen war dazu eine Reduzierung des Speicherbedarfs notwendig, weshalb der Speicherverbrauch des SOLID-Basisverfahren zielgerichtet verringert und darüber hinaus eine SOLID-Version mit minimalem Speicherbedarf abgeleitet wurde. Zum anderen war dazu insbesondere eine größere architekturorientierte Portabilität notwendig, welche durch eine Vielzahl zusätzlicher Anpassungen, beispielsweise bezüglich der Objektserialisierung, erwirkt wurde. In der Folge ist das SOLID-Verfahren nun auch auf Architekturen mit *Big-Endian*-Speicherorganisation einsetzbar.

Effizienter Betrieb mit Smartcard-basierter Authentisierung Durch die Anbindung einer neuen Smartcard-Generation kann darüber hinaus nun ECDSA für digitale Signaturen im Rahmen der IKE-Authentisierung verwendet werden. Dabei können im Vergleich zu RSA-basierten Signaturen deutlich kürzere Schlüssel verwendet werden, wodurch letztlich die Aushandlung von Sicherheitsbeziehungen beschleunigt wird. Auch wurde eine optionale Funktion zur Beschleunigung der initialen Kommunikation implementiert. Hierfür wurden alle Smartcards mit einem Pre-Shared-Key ausgestattet. Aus diesem kann für gegebene Quell- und Zieladressen ein symmetrischer Sitzungsschlüssel abgeleitet werden. Dazu muss jedoch Quell- oder Zieladresse aus dem Netzbereich stammen, für den die Smartcard zugelassen ist. Mithilfe dieses schnell generierbaren Sitzungsschlüssel können die ersten Nutzdatenpakete einer Kommunikation bereits verschlüsselt gesendet werden, während die Aushandlung der anschließend genutzten SA noch bearbeitet wird. Dieser Geschwindigkeitsvorteil macht sich beispielsweise bei einem VoIP-Telefonat bemerkbar, da das Telefonat nun direkt geschaltet werden kann und nicht bis zum Abschluss der zeitaufwändigen Schlüsselaushandlung gewartet werden muss. Hierbei ist zu beachten, dass nur die ersten Pakete einer Kommunikation mit dem Geheimnis, welches vom Pre-Shared-Key abgeleitet wurde, verschlüsselt werden. Diese Art der Verschlüsselung wird gestoppt, sobald die eigentliche Sicherheitsbeziehung ausgehandelt oder ein Zeitfenster für die

Aushandlung überschritten wurde. Auf diese Weise kann sichergestellt werden, dass die anschließende Kommunikation die vollständige Ende-zu-Ende-Sicherheit aufweist. Teile der dabei entstandenen Software-Architektur werden dieses Jahr auf der D-A-CH security vorgestellt [WRS15].

Lastbalancierung in heterogenen Szenarien Neben diesen Maßnahmen, welche sich unmittelbar auf den eigentlichen Implementierungsprozess beziehen, stand auch die redundante Auslegung von Sicherheitsgateways im Fokus dieses Arbeitspaketes. Insbesondere in heterogenen Szenarien kann dabei durch eine redundante Auslegung der VPN-Gateways, welche für bestimmte Netzbereiche verantwortlich sind, nicht nur zusätzliche Robustheit gegenüber Transportnetz-, Administrations- und Hardwarefehlern erwirkt werden, sondern gleichzeitig eine sinnvolle Lastbalancierung an exponierten Standorten ermöglicht werden.

Dabei sind prinzipiell zwei Arten von Last zu unterscheiden: im Rahmen der Einrichtung von Sicherheitsbeziehungen anfallende Last für Authentisierungsprotokolle und darin integrierte Schlüsselaushandlungen und die Last für die Sicherung der eigentlichen, durch das VPN zu sichernden Datenpakete.

Werden VPN neu eingerichtet und kollektiv neue Sicherheitsbeziehungen angelegt kann insbesondere anfallende Last durch Authentisierungsprotokolle und darin integrierte Schlüsselaushandlungen signifikant sein. Insbesondere in Szenarien, in denen eine direkte Erreichbarkeit zwischen allen Sicherheits-Gateways durch proaktives Einrichten aller realisierbaren Sicherheitsbeziehungen angestrebt wird, können initial mehrere Stunden vergehen, bis das VPN einsatzfähig ist. Dies ist im Wesentlichen auf den notwendigen Einsatz von Krypto-Smartcards zurückzuführen. Um der Bildung potentieller Flaschenhälse in großen VPN mit Beteiligung exponierter Punkte, wie beispielsweise Rechenzentren, entgegen zu wirken, wurde bereits im Rahmen des Mobil-SOLID-SINA-Vorhabens eine transparente Lösung erdacht. Diese basiert auf Cluster-Bildung, also einem Einsatz mehrerer Sicherheits-Gateways für einen gemeinsamen Netzbereich. Weiterführende Details zu diesem Verfahren können der entstandenen Veröffentlichung [GTR+13] entnommen werden. Im Rahmen dieses Arbeitspaketes wurde dieses Verfahren vollständig in den SOLID-Realsystem-Prototypen integriert und in einer Reihe von Szenarien getestet.

3.1.7 Erkennung und Behandlung interner Sabotage-Angriffe

In typischen Szenarien sind Angreifer in der Regel innerhalb des ungeschützten, öffentlichen Netzes lokalisiert. Insbesondere im VPN-Umfeld sind allerdings auch Angreifer denkbar, welche in einem geschützten Netzbereich zu finden sind und dadurch auch Möglichkeiten haben, Teilbereiche des VPNs anzugreifen, welche aus dem öffentlichen Netz gar nicht adressierbar sind. Bandbreitenerschöpfende Angriffe aus dem gesicherten Netzbereich können dabei von den Gateways limitiert werden, indem bekannte *Traffic-Shaping*-Methoden verwendet werden, welche letztlich als Datenratenbegrenzung bezüglich der jeweils verwalteten Netzbereiche anzusehen sind.

Insbesondere infolge einer Kompromittierung einzelner SOLID-Gateways können

allerdings auch Angriffe auf das VPN-Routing eine ernstzunehmende Bedrohung darstellen, welche mit diesen Lösungen nicht ausgeräumt werden kann. Aufgrund dieser Gefährdungslage wurde im Rahmen dieses Arbeitspaketes an das thematisch vorangegangene *Mobil-SOLID-SINA*-Vorhaben angeknüpft und weiterführende Fragestellungen der Routing-Sicherheit hinsichtlich interner Angreifer untersucht.

Um die Auswirkungen entsprechender Angriffe auf das VPN zu minimieren, ist eine geeignete Detektion notwendig. Dazu ist das Verhalten der eigenen Nachbarschaft und entfernter Kommunikationspartner zunächst zu beobachten. Unter anderem ist es schließlich sinnvoll, die im SOLID-Verfahren häufig verwendeten Suchanfragen an Nachbarn weiterzuleiten, welche als *vertrauenswürdig* gelten und deren Antwortwahrscheinlichkeit entsprechend hoch ist. Prinzipiell kommt dabei zunächst sowohl eine Einschätzung von Knoten als auch der verwendeten Pfade in Frage. Bei genauerer Betrachtung stellt sich beides allerdings als wenig zufriedenstellend heraus: Für indirekt erreichbare Knoten kann aufgrund mangelnder Zuordenbarkeit von Paketverlusten keine zuverlässige Aussage über deren Vertrauenswürdigkeit getroffen werden, während für Pfadbewertung ein umfassendes Wissen notwendig wäre.

Bewertung von Antwortwahrscheinlichkeiten Allerdings hat sich ein alternativer Ansatz als sinnvoll erwiesen. Dabei betrachten die Knoten die Kommunikation mit ihren Nachbarn über einen längeren, definierten Zeitraum und erstellen diesbezüglich einfache Statistiken, beispielsweise den Anteil beantworteter Suchanfragen. In der Praxis kann dieser Anteil natürlich durch verschiedene Faktoren beeinflusst werden. Unter anderem zählen dazu Störungen des Transportnetzes, welche beispielsweise in drahtlosen Szenarien nicht unüblich sind. Darüber hinaus kann es beispielsweise auch während der Startphase von VPN-Teilen zu Nachrichtenverlust kommen, falls das gesuchte Ziel aufgrund kurzzeitiger Topologie- oder Routing-Instabilitäten nicht gefunden werden kann.

Neben diesen praktisch nicht vermeidbaren Fehlerfällen kann die Antwortwahrscheinlichkeit auch von verschiedenen Angriffstypen beeinträchtigt werden. Dabei führen beispielsweise vergleichsweise einfache Blackhole-Angriffe, bei denen sämtliche Pakete unterdrückt werden, zu geringeren Antwortwahrscheinlichkeiten. Darüber hinaus können auch gezielte DoS-Angriffe und die damit verbundene Überlastsituation die Antwortwahrscheinlichkeiten reduzieren. Befindet sich ein Knoten an Positionen des Netzes, welche aufgrund besonderer Netzstrukturen wie Verschachtelungen von Angreifern besonders beeinträchtigt werden, kann die entsprechende Antwortwahrscheinlichkeit ebenso sinken. Dementsprechend reflektiert diese Antwortwahrscheinlichkeit nicht nur das unmittelbare Verhalten eines Knotens, sondern beurteilt auch dessen Umgebung, die sich letztlich durch die Bewertungen vermittelnder Knoten ergibt.

Da für einen Austausch untereinander das nötige Vertrauen fehlt, muss dieser Indikator von jedem Knoten separat ermittelt werden. Eine prinzipielle Alternative stellen *Exponential-Information-Gathering*-Algorithmen dar [LSP82], mit deren Hilfe es möglich ist, Knotenbewertungen auszutauschen, solange es sich bei weniger als $1/3$ der Knoten um Angreifer handelt. Über einen entsprechenden Austausch könnten dabei auch Bewertungen bezüglich Knoten erworben werden, zu denen kein unmittelbarer Kontakt bestand. Allerdings erzeugen diese Algorithmen eine Nachrichtenanzahl,

welche quadratisch von der Knotenanzahl abhängig ist, wodurch sich diese Verfahren aufgrund der schlechten Skalierbarkeitseigenschaften in der Praxis nicht eignen und ein Einsatz daher verworfen wurde, so dass die Bewertung nun lediglich aufgrund eigener Beobachtungen vorgenommen wird.

Bewertung des Jitters Zusätzlich zur Antwortwahrscheinlichkeit lassen sich noch weitere Kriterien finden, welche zur Bewertung eines Knotens und dessen Routing-Entscheidungen herangezogen werden können. Dazu zählt der Jitter, welcher Hinweise auf Schwankungen innerhalb der Laufzeiten von Paketen gibt. Diese Schwankungen können prinzipiell verschiedene Ursachen haben und sind, ähnlich den Antwortwahrscheinlichkeiten, entweder direkt auf den benachbarten Knoten oder auf dessen Umgebung zurückzuführen. Auch an dieser Stelle ist es denkbar, dass lediglich das Transportnetz überlastet ist – allerdings betrifft dies in homogenen Transportnetzen typischerweise alle Knoten. In heterogenen Transportnetzszenarien ergibt sich durch eine Auswertung des Jitters letztlich eine Bevorzugung stabiler Verbindungen, wodurch sich – wie auch im weiteren Verlauf deutlich wird – im Zuge der hieran anknüpfenden Maßnahmen keine Nachteile ergeben. Andere Ursachen sind in verschiedenen externen und internen Angriffen zu suchen, beispielsweise auch im Zuge dynamischer DoS-Angriffe, weshalb Jitter bereits bei der Erkennung von (externen) DoS-Angriffen in Abschnitt 3.1.3 angeführt wurde.

Gewichtete Routing-Entscheidungen und Anknüpfen an Mobil-SOLID-SINA
Auf Basis der ermittelten Antwortwahrscheinlichkeiten und des Jitters kann nun das Overlay-Suchverfahren angepasst werden. Bisher erfolgte die Auswahl des bestmöglichen Ziels für Suchanfragen entsprechend des verwendeten Greedy-Verfahrens anhand der logischen Distanz zum Ziel, wodurch die Anzahl der weiterleitenden Knoten möglichst gering gehalten wurde. Während kleinere Umwege nun zwar unter anderem zu einer höheren Verzögerung führen, können auf den kürzesten Overlay-Pfaden befindliche Angreifer gegebenenfalls umgangen werden. Dementsprechend wurde die Wahl lokaler Zwischenziele angepasst, sodass nicht nur die logische Distanz im Overlay berücksichtigt wird, sondern mit den ermittelten Antwortwahrscheinlichkeiten und Jitter auch weitere Faktoren, welche zuvor beobachtet wurden und möglicherweise auf die Präsenz eines Angreifers schließen lassen.

Aus der Antwortwahrscheinlichkeit pA, der Verzögerungsschwankung jit und der logischen Distanz d ergibt sich schließlich die Bewertung r eines Knotens folgendermaßen:

$$r = \frac{d}{d_{max}} \cdot w_d + \left(1 - \frac{pA}{pA_{max}}\right) \cdot w_{pA} + \frac{jit}{jit_{max}} \cdot w_{jit}$$

Entsprechend des ursprünglichen Distanzgedankens ist eine vergleichsweise kleinere Bewertung r eines Knotens dabei als besser anzusehen. Für eine gute Bewertung sollte dementsprechend eine hohe Antwortwahrscheinlichkeit und eine geringe Distanz sowie kleine Verzögerungsschwankungen vorliegen. Jedes Kriterium kann dabei durch die zusätzlichen Gewichte w_d, w_{pA} und w_{jit} individuell gesteuert werden. Insbesondere wird hierdurch auch eine zielgerichtete Anpassung an dedizierte Szenarien ermöglicht.

Diese Bewertung kann schließlich mit einem stochastischen Routing-Verfahren kombiniert werden, welches im Rahmen des Arbeitspaketes *Routing-Sicherheit* des vorangegangenen *Mobil-SOLID-SINA* entworfen wurde. Durch die Kombination einer zusätzlichen stochastischen Komponente und der hier vorgestellten Metrik zur vorherigen Gewichtung der Weiterleitungsziele wird es einem etwaigen internen Angreifer deutlich erschwert, den Pfad von Kontrollnachrichten vorherzusagen und gegebenenfalls zu manipulieren.

3.1.8 Anpassungen am SINA-Produkt

Zur Integration des Prototyps waren einige Anpassungen sowohl an SOLID als auch am SINA-Produkt notwendig.

Die Konfiguration von Komponenten der SINA-Box wird sowohl während des Startvorgangs als auch zur Laufzeit von einem Konfigurations-Dienst durchgeführt. Anstatt wie bisher die auf- und abzubauenden Sicherheitsbeziehungen direkt an strongSwan zu melden wurde SOLID derart angepasst, dass es stattdessen den Konfigurations-Dienst kontaktiert und dort diesbezügliche Änderungen einträgt. Dieser Dienst wiederum verwaltet alle bekannten Sicherheitsbeziehungen, zu denen auch die über das SINA Management statisch eingetragenen Beziehungen zählen, und kommuniziert Änderungen schließlich weiter an strongSwan. Neben Sicherheitsbeziehungen werden vom Konfigurations-Dienst auch Statusinformationen über andere Komponenten der SINA-Box verwaltet. Hier waren ebenfalls Anpassungen notwendig, so dass SOLID aktuelle Informationen über aufgebaute Sicherheitsbeziehungen periodisch an den Konfigurations-Dienst meldet. Diese Statusinformationen wurden über verschiedene externe Schnittstellen zugänglich gemacht. Hierzu zählen die LCD-Anzeige der SINA-Box, das sowohl lokal als auch entfernt erreichbare Adminmenü, SNMP, sowie das Syslog, welches nach Aktivierung eines speziellen Trigger-Ports über das SINA Management durch entsprechende Statusinformationen erweitert wurde.

Für die Komponente strongSwan war es erforderlich, zur Integration des Prototyps eine Versionsaktualisierung durchzuführen, um alle von SOLID benötigten Funktionen bereitstellen zu können. Zusätzlich wurden kleinere Anpassungen und Erweiterungen implementiert, unter anderem um Rückmeldungen bezüglich auf- und abgebauten Sicherheitsbeziehungen an SOLID zu ermöglichen.

Aufgrund der bisher größtenteils autonomen Funktionsweise des SOLID-Prototyps ist es notwendig gewesen, einige seiner Autokonfigurationsmechanismen mit der SINA-Box kompatibel zu machen. Hierzu zählen das Anlegen von IPTables-Regeln und die Verwaltung der XFRM-Richtlinien, aber auch die intensive Nutzung des Policy-Routings durch SOLID.

Da die SINA L3 Box das IP Protokol in der Version 6 unterstützt, musste die vorhandene SOLID Implementierung um eine IPv6-Kompatibilität erweitert werden. Dadurch haben sich mehrere Herausforderungen ergeben. Einerseits musste für den Linux Kernel ein neuer Tunnel-Modus implementiert werden. Dieser sogenannte NBMA-Modus wird von SOLID benötigt, um Tunnelendpunkte dynamisch konfigurieren zu können, ist zuvor aber nur für IPv4 verfügbar gewesen. Anschließend daran ist es für IPv6 zusätzlich erforderlich gewesen, die Tunnelendpunktadressen für innere und

äußere Tunnel zu separieren. Darüber hinaus haben sich insbesondere im Linux Kernel aufgrund der aktuell geringen Verbreitung von IPv6 eine überdurchschnittlich hohe Anzahl an unvorhergesehenen Fehlern ergeben, die behoben werden mussten.

Das Attestieren von geschützten Netzbereichen wurde von SOLID bisher über eine spezielle Erweiterung im signierten Nutzerzertifikat ermöglicht. Für den Einsatz in der SINA-Umgebung hat sich dieses Verfahren jedoch als Nachteil herausgestellt, da es keine strikte Trennung von Zertifizierungsinstanz und Konfigurationsinstanz erlaubt. Als Alternative schreibt das SINA Management die geschützten Netzbereiche stattdessen in eine separate, signierte Konfigurationsdatei. Diese wird von SOLID während der Bootstrapping-Phase mit anderen Boxen ausgetauscht und erlaubt somit gleichermaßen eine Verifikation der annoncierten Netzbereiche anderer Boxen.

Um sowohl die Robustheit gegenüber Ausfällen einzelner Boxen zu ermöglichen als auch die Skalierbarkeit für große Netze zu verbessern, bietet SOLID einen Cluster-Modus an. Dieses Verfahren benötigt den Betrieb eines OSPF-Netzes auf roter Seite der Box, welches ebenfalls vom SINA Backuprouting eingesetzt wird. Hierbei waren einige Änderungen notwendig, um die bestehenden Mechanismen zur Konfiguration und Abfrage des OSPF-Netzes weiterverwenden zu können.

Darüber hinaus sind eine Vielzahl kleinerer Anpassungen erfolgt, beispielsweise die Unterstützung der IPsec-Erweiterung für Extended Sequence Numbers, das Auslesen des CUG-Schlüssels von der Smartcard, Verbesserungen der Unterstützung von 64-Bit-Architekturen sowie das Ermöglichen der Path MTU Discovery.

3.1.9 Test und Leistungsverhalten

Während der Anpassung des SINA-Produktes und der Integration des SOLID-Prototyps sind eine Vielzahl automatisierter Tests entwickelt worden. Darunter fallen einfache Szenarien zum Testen des Bootstrapping-Verhaltens und zur Abfragbarkeit von Statusinformationen. Darüber hinaus wurden auch Tests für komplexere Szenarien entwickelt, wie beispielsweise NAT-Szenarien, die Verwendung zusätzlicher Gateways zwischen zu schützenden Netzbereichen und der SINA Box, Topologien mit indirekt angeschlossenen Boxen sowie Boxen mit mehr als einer schwarzen Netzwerkschnittstelle, die Unterstützung von Quality of Service (Copy TOS) sowie die korrekte Funktionalität von Path MTU Discovery, das Weiterleiten von Wirkverkehr über den SOLID-Ring und Tests bezüglich des Cluster-Modus. Ebenso entstanden sind Tests zur Prüfung der Kompatibilität bezüglich anderer Mechanismen der SINA Box, wie beispielsweise Online-Management via LDAP, die Funktionalität von SINA Remote Software Update (SRSU) und SINA Remote Configuration Update (SRCU), Kompatibilität mit Hot Standby 1 sowie die fehlerfreie Zusammenarbeit mit statisch konfigurierten Sicherheitsbeziehungen aus dem SINA Management.

Neben automatisierten Tests wurden manuelle Leistungsmessungen durchgeführt, um den Durchsatz der Box zu ermitteln und schließlich auch steigern zu können. Durch den Einsatz vieler kleiner, sich ergänzender Mechanismen konnte der Netzwerk- und Kryptodurchsatz der Box in einigen Szenarien signifikant gesteigert werden. Hierzu zählen das Deaktivieren von Conntrack-Prüfsummen, die Verwendung von AEAD-Algorithmen wie beispielsweise AES-GCM, die Aktivierung von SSSE3 für

64-Bit-Systeme, der Einsatz von AES-NI sowie das Anwenden des skb_cow_data-Patches auf den Linux Kernel, um den Empfangspfad zu entlasten. Ebenso konnte durch eine verbesserte Verteilung der Interrupts auf die vorhandenen CPU-Kerne eine Durchsatzsteigerung erreicht werden.

3.2 Wichtigste Positionen des zahlenmäßigen Nachweises

3.2.1 TU Ilmenau

Insbesondere aufgrund einer angespannnten Arbeitsmarktsituation an der TU Ilmenau zu Beginn der Förderperiode konnte die angestrebte Zeitplanung nicht eingehalten werden. Durch die Gewährung einer kostenneutralen Verlängerung von Seiten des Projektträgers konnten die formulierten Projektziele allerdings vollständig erreicht werden.

Die im Förderantrag geschilderte Kostenplanung für das Vorhaben wurde dabei – mit einer kostenneutralen Ausnahme – vollständig umgesetzt: Statt der ursprünglich beantragten 48 Personenmonate wurden auf Seiten der TU Ilmenau bis zum Projektende insgesamt 52 Personenmonate für Beschäftigte TVöD/TV-L E 12 bis E 15 aufgewendet. Dies konnte durch Einsparungen in anderen Kostenstellen kostenneutral geschehen. Ein entsprechend veränderter Einsatz der zur Verfügung stehenden Mittel wurde in den letzten Monaten der Förderperiode als sinnvoll erachtet und war notwendig, um alle abschließenden Arbeiten in den Arbeitspaketen *Effizienz-Optimierung* und *Erkennung und Behandlung von Sabotage-Angriffen* effizient durchführen zu können. Eine ausschließliche Bearbeitung der Thematik mit wissenschaftlichen Hilfskräften im November und Dezember 2014 wurde dabei aufgrund der zuvor gewonnenen Erkenntnisse und der dadurch zusätzlich notwendig gewordenen Implementierungsarbeiten und umfangreichen Testszenarien von Seiten der TU Ilmenau nicht als sinnvoll erachtet. Infolge der zusätzlichen Betreuung durch die mit dem Projekt vertrauten wissenschaftlichen Mitarbeiter konnte allerdings auch an dieser Stelle eine Gefährdung der Projektziele vollständig vermieden werden.

In nachstehender Tabelle werden die wichtigsten Positionen des zahlenmäßigen Nachweises aufgeführt und im Folgenden näher erläutert.

Position	Ausgaben
Beschäftigte TVöD/TV-L E 12 bis E 15	241.074,16 €
Studentische Hilfskräfte	31.081,08 €
Dienstreisen	7.946,97 €
Simulations- und Emulationsserver	16.886,10 €
SINA Box (1 HE, 5 LAN)	3808,00 €

Die Personalkosten stellen die größte Ausgabenposition in Bezug auf das DoS-Resist-VPN-Vorhaben dar. Diese Kosten verteilen sich dabei auf drei wissenschaftliche Mitarbeiter, welche über verschiedene Zeiträume mit dem Projekt betraut waren, und insgesamt 12 Studenten, welche für eine hilfswissenschaftliche Tätigkeit im Rahmen des Vorhabens gewonnen werden konnten. Die Konzeption und Planung sowie wesentliche

Teile der Implementierung und Evaluierung von Lösungsansätzen für Teilaufgaben der jeweiligen Arbeitspakete wurde dabei von den wissenschaftlichen Mitarbeitern durchgeführt. Im Rahmen der Implementierung und Evaluierung wurden die mit dem Projekt betrauten Mitarbeiter dabei von wissenschaftlichen Hilfskräften unterstützt. Auch bei der Erstellung von Programmteilen und Konfigurationen, welche als Voraussetzungen für die unmittelbare Bearbeitung von Arbeitspaketen notwendig waren, konnten die wissenschaftlichen Hilfskräfte wichtige Unterstützung leisten. Beispielsweise konnte unter anderem die umfangreiche Integration der neuen Token-Generation zu einem wesentlichen Teil von studentischen Hilfskräften realisiert werden, wodurch darauf basierende Neuerungen im Rahmen des Arbeitspaketes *Effizienzoptimierung* erst möglich wurden. Darüber hinaus wurden auch im DoS-Resist-VPN-Vorhaben automatisierte Testfälle für in der Entwicklung befindliche Teilkomponenten zu einem wesentlichen Teil von studentischen Hilfskräften erstellt, wodurch eine erste grundlegende Qualitätskontrolle bereits im Rahmen des Entwurfsprozesses gewährleistet werden konnte. Bezüglich der Kostenübersicht ist zu beachten, dass die Gehaltskosten aus den Monaten November und Dezember 2014 nur kalkulatorisch enthalten sind, wodurch die finalen Beträge leicht abweichen können.

Die entstandenen inhaltlichen Ergebnisse wurden dabei auf zahlreichen internationalen Konferenzen präsentiert. Im Rahmen dieser Konferenzen wurden die entstandenen Lösungsansätze mit einem interessierten Fachpublikum diskutiert und dabei auch die Angemessenheit und Qualität der entwickelten Verfahren erörtert. Daneben wurde auch im Rahmen dieses Vorhabens ein enger Kontakt zur Forschungs- und Entwicklungsabteilung unseres Projektpartners, der secunet Security Networks AG, gepflegt. Durch die vorherige Zusammenarbeit in gemeinsamen Projekten und die damit verbundenen Erfahrungen konnte im Rahmen des Projektes zum großen Teil auf Dienstreisen zum Entwicklungsstandort in Dresden verzichtet werden. Nichtsdestotrotz erfolgte eine enge Diskussion und Zusammenarbeit hinsichtlich aktueller Fortschritte und entworfener Lösungen.

Viele der Verfahren, welche in den verschiedenen Arbeitspaketen entstanden sind, konnten repräsentativ in kleinen Testszenarien und unter Zuhilfenahme der bestehenden Infrastruktur des Fachgebiets Telematik/Rechnernetze bewertet werden. Andere Lösungen, beispielsweise im Umfeld dynamischer Reaktionen auf DoS-Angriffe, erforderten die Evaluierung anhand sehr großer Szenarien mit großen Lastmengen. Da eine Evaluierung anhand eines realen Netzwerkes an dieser Stelle nicht in Frage kommt, ist die Durchführung realitätsnaher Simulationsstudien unumgänglich. Hierfür war die Anschaffung geeignet leistungsstarker Server (3 Simulations- und Emulationsserver) notwendig: Zum einen ist die realitätsnahe Lastgenerierung in den untersuchten Szenarien vergleichsweise rechenintensiv, zum anderen wurde insbesondere im Arbeitspaket *Konfiguration DoS-resistenter Strukturen*, beispielsweise im Rahmen der Angreifermodellierung, mit NP-schweren Problemen gearbeitet, deren Berechnung (für noch handhabbare Problemgrößen) signifikante Rechenleistung voraussetzen. Um die Portierung des Verfahrens auf die SINA-Plattform von Seiten der TU Ilmenau effizienter unterstützen zu können, wurde darüber hinaus eine SINA-Hardwareplattform in das Testbed des SOLID-Prototypen integriert. Hierdurch konnten unter anderem Plattform-spezifische Teilprobleme zügig untersucht und aufgelöst werden.

Weitere Investitionen in das Testbed des SOLID-Prototypen am Fachgebiet Telema-

tik/Rechnernetze waren nur in geringem Maße notwendig. Dies ist im Wesentlichen darauf zurückzuführen, dass zum großen Teil auf Technik zurückgegriffen werden konnte, welche bereits im Rahmen des Vorhabens Mobil-SOLID-SINA angeschafft wurde. Da der Testaufbau zum großen Teil modular eingerichtet wurde, konnten notwendige Anpassungen und neue Szenarien zügig und unter begrenztem Aufwand realisiert und eingebunden werden.

3.2.2 secunet Security Networks AG

Analog dazu werden in der nachstehenden Tabelle die wichtigsten Positionen des zahlenmäßigen Nachweises des secunet aufgeführt.

Position	Ausgabe
Personalkosten	86679,83 €
Dienstreisen	0,00 €
Erweiterung des automatisierten Testsystems	2867,22 €

Die größten Ausgabeposition im Rahmen des Projektes stellten die Personalkosten dar. Diese verteilten sich auf mehrere Mitarbeiter der Firma secunet Security Networks AG sowie auf einen Studenten. Dieser war wesentlich bei der Weiterentwicklung der automatischen Testumgebung beteiligt und leistet hierbei wertvolle Unterstützung durch Programmiertätigkeit. Das SINA-Testbed wurde mit geeigneter Hardware erweitert, um Tests in Bezug auf das Leistungsverhalten durchführen zu können.

3.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Im Folgenden werden die einzelnen Arbeitsschritte der jeweiligen Arbeitspakete auf deren Notwendigkeit und Angemessenheit hin analysiert.

3.3.1 Komponentenweise Zerlegung

Eine Möglichkeit der IT-Sicherheit, das Schadenspotential eines Angreifers zu senken, ist das Prinzip der geringsten Privilegien. Hierbei werden einem Programm ausschließlich die Rechte und Privilegien gewährt, die es für eine normale und fehlerfreie Ausführung benötigt. Dadurch können die Möglichkeiten des Angreifers eingeschränkt werden, sollte dieser das Programm kompromittieren und für seine Zwecke nutzen. In diesem Arbeitspaket wurde, ausgehend vom Prinzip der geringsten Privilegien, an einer Möglichkeit zur Aufteilung des monolithischen Prototyps gearbeitet. Durch die Aufteilung des Prototyp auf mehrere Komponenten kann eine Entkopplung der Komplexität von der Angriffsfläche erreicht werden. Benötigen die komplexen Komponenten keine besonderen Rechte, werden dem Prozess, in dem sie implementiert sind, bei dessen Ausführung auch keine Rechte gewährt. Da die Wahrscheinlichkeit eines ausnutzbaren Programmierfehlers mit wachsender Komplexität steigt, ist die Wahrscheinlichkeit hoch, dass ein Angreifer über solch ein komplexes Quellcodesegment das Programm kompromittieren kann. Da er dadurch im Anschluss jedoch keine

Rechte besitzt, die er ausnutzen könnte, kann der potentielle Angriffsschaden stark eingeschränkt werden.

Möchte man eine solche Separation durchführen um die Sicherheit des Gesamtsystem zu steigern, benötigt man jedoch zuvor einen Plan, an welchen Stellen die Separation durchgeführt werden soll. Dieser muss festlegen, welche Funktion welchem Prozess zugeordnet wird. Auch ergibt sich daraus, welche Prozess im Anschluss welche Rechte benötigt und wie sich die Interfaces zwischen den einzelnen Prozessen gestalten. Da für die automatisierte Erstellung eines solchen Plans viele Details und Einflussfaktoren (wie die Kosten der Interprozesskommunikation, die Verteilung der Privilegien und Komplexität und das entstehende Interface-Risiko) berücksichtigt werden müssen, beschäftigte sich dieses Arbeitspaket mit der Evaluierung möglicher Methoden zur Partitionserstellung und -analyse, die einer späteren automatisieren Zerlegung zwingend vorrausgehen müssen. Insbesondere mit Blick auf die angestrebte Einschränkung des Schadenspotentials von Angriffen sind die im Rahmen des Arbeitspaketes geleisteten Arbeiten als gewinnbringend und angemessen zu erachten.

3.3.2 Konfiguration DoS-resistenter Overlay-Strukturen

Eine signifikante Resistenz gegenüber Verfügbarkeitsangriffen war bereits im Vorfeld des DoS-Resist-Vorhabens als unmittelbarer Vorteil des verteilten SOLID-Verfahrens und der charakteristischen Ring-basierten Overlay-Topologie anzusehen. Um diese Resistenz insbesondere im Hinblick auf besonders sicherheitskritische Szenarien jedoch weiter zu stärken, wurden im Rahmen des Arbeitspaketes alternative Graphstrukturen untersucht. In Vorbereitung der Konstruktion eines besonders sabotagereistenten und effizienten Overlay-Systems wurden dabei zunächst Strukturen untersucht, die eine hohe Resistenz vermuten ließen. Dabei konnte unter anderem erkannt werden, dass Knotengrad, Vermaschung und insbesondere Taillenweite wesentlichen Einfluss auf die Resistenz der Graphstruktur haben. Überzeugen konnten dabei insbesondere Strukturen mit logarithmischem Durchmesser. Als resistenteste Struktur ist jedoch der Zufallgraph mit konstantem Knotengrad anzusehen, welcher allerdings für den Einsatz in Peer-to-Peer-Overlays weniger geeignet ist, da ein effizientes Greedy-Routing im Allgemeinen nicht ermöglicht werden kann.

Basierend auf dem Zufallsgraphen mit konstantem Knotengrad wurde schließlich ein Verfahren zur Topologiekontrolle entwickelt, welches eine deterministische Berechnung der Nachbarn ausgehend von zweidimensionalen Koordinaten vornimmt, die durch Hashing einer eindeutigen Knotenidentifikation gewonnen werden. Dabei wird eine Struktur erzeugt, die sich nahezu identisch zu einem Zufallsgraphen mit Knotengrad vier verhält. Aufgrund des koordinatenbasierten Ansatzes ist hier jedoch ein Greedy-Routing möglich. Außerdem kann jeder Knoten allein mit dem Wissen der Knotenidentifikationen eine globale Sicht der Topologie gewinnen, wodurch sich auch optimale globale Routing-Verfahren vergleichsweise günstig realisieren lassen. Eine Kombination beider Verfahren erlaubt es, den Kompromiss zwischen Organisationsaufwand und Routing-Effizienz an die Anwendung anzupassen.

Mit dem entwickelten Ansatz steht eine Alternative zur Ring-basierten Topologiekontrolle zur Verfügung, welche nachweislich eine sehr hohe Resistenz bezüglich Verfügbarkeitsangriffen aufweist, durch die Verdeckung der öffentlichen Adressen und

die dadurch auch in direkten Szenarien indirekt abgewickelte Kommunikation über die Overlay-Struktur allerdings einen gewissen Effizienzverlust impliziert.

3.3.3 DoS-Resistenz gegen dynamische Angriffe

Mit dem Aufkommen von gepulsten und dynamischen Angriffstechniken veränderte sich die Bedrohungslage hinsichtlich der DoS-Resistenz von VPN in der jüngeren Vergangenheit. Im Rahmen des Arbeitspaketes konnte zunächst gezeigt werden, dass die Auswirkungen entsprechender DoS-Angriffstechniken im Allgemeinen lokal begrenzt sind, was erneut auf das verteilte Grundprinzip von SOLID zurückzuführen ist. Darüber hinaus werden durch diese Angriffe keine Schwingungen oder Instabilitäten im SOLID-VPN erzeugt – ein Umstand der angesichts der verteilten Topologiekontrolle nicht selbstverständlich ist und daher einer näheren Untersuchung bedurfte.

Des Weiteren wurde der Fokus im Rahmen dieses Arbeitspaketes zunächst auf die Erkennung entsprechender Angriffstechniken gelegt, welche als wesentliche Vorbereitung für die im Rahmen des Arbeitspaketes *Dynamische Reaktion auf DoS-Angriffe* entwickelten Gegenmaßnahmen anzusehen sind. Das entworfene Verfahren verzichtet dabei auf aktive Messungen, welche unter Umständen die Situation lediglich verschlechtern würden, und hat dementsprechend einen passiven Charakter.

3.3.4 Dynamische Reaktion auf DoS-Angriffe

In diesem Arbeitspaket wurde thematisch an das Arbeitspaket *DoS-Resistenz gegen dynamische Angriffe* und die dort entstandene Erkennungsheuristik angeknüpft. Im Wesentlichen wurden dabei zusätzliche Gegenmaßnahmen entworfen und umgesetzt, welche darauf abzielen, die Verfügbarkeit unmittelbar betroffener VPN-Verbindungen in Angriffsszenarien aufrecht zu erhalten. Dies ist in der Regel genau dann möglich, wenn die vorliegenden Transportnetzgegebenheiten prinzipiell alternative Pfade zur Verfügung stellen, beispielsweise im Falle einer Multihoming-Anbindung von VPN-Gateways. Darüber hinaus wurden Szenarien adressiert, in denen Komponenten des Kernbereichs von DoS-Angriffen betroffen sind. Das hierbei entstandene Verfahren zur Ersatzpfadkonstruktion verspricht dabei auch in allgemeinenen Fehlersituationen eine deutliche Resistenz gegenüber Konnektivitätsverlusten, insbesondere in sehr weiträumigen Szenarien.

Weitere Gegenmaßnahmen beziehen sich auf eine gepulste Angriffstechnik, welche Charakteristika der TCP-Staukontrolle ausnutzt, um Datenübertragungen auf der betroffenen Verbindung zu unterbinden. Die Brisanz dieser Technik ergibt sich dabei aus deren hoher Effizienz und schlechten Erkennbarkeit. Der entwickelte DoSCAR-Ansatz nutzt dabei die Wiedereinspielung von Bestätigungen, um die Auswirkungen dieses Angriffs signifikant einzuschränken. Dabei handelt es sich um ein passives Verfahren, welches ohne Erkennung auskommt, wodurch die schlechte Erkennbarkeit der adressierten Angriffe vernachlässigbar wird.

Gemeinsam erzielen die entstandenen Erweiterungen einen weitreichenden Schutz gegenüber herkömmlichen und gepulsten DoS-Angriffen. Die Eigenschaften des verteilten SOLID-Verfahrens werden dabei an keiner Stelle geschwächt.

3.3.5 Implementierungssicherheit

Durch eine Steigerung der Implementierungssicherheit kann eine Steigerung der Sicherheit des gesamten Systems erreicht werden. Da SOLID zukünftig als Sicherheitslösung zur Firmen- bze. Behördeninternen Kommunikation angeboten werden soll, ist eine hohe Gesamtsicherheit unabdingbar. Daher wurden in diesem Arbeitspaket mehrere Maßnahmen realisiert, die der Steigerung der Implementierungssicherheit dienen. So konnte durch das redundante Auslegen sicherheitskritischer Programmfunktionalitäten, wie die parallele Verwaltung von IPsec-Policies und entsprechenden Firewall-Regeln, die Wahrscheinlichkeit von kritischen Systemfehlern gesenkt werden. Die Aufstellung und Durchsetzung von Konventionen, die die Struktur und Lesbarkeit des SOLID-Quellcodes regeln und damit die Fehlersuche einfacher gestalten, trägt ebenfalls zum Ziel des Arbeitspaketes bei. Schlussendlich konnte durch die systemweite Einführung diverser Sicherheitschecks, die Überwachung des Systemzustandes hinsichtlich seiner Sicherheitseigenschaften verbessert werden, sodass im Fehlerfall der Administrator informiert oder sogar einzelne betroffene Systeme heruntergefahren werden können.

3.3.6 Effizienzoptimierungen

Da der bisherige VPN-Ansatz prototypisch entwickelt wurde, wurde dem Thema der Effizienzoptimierung bislang keine große Bedeutung beigemessen. Soll eine VPN-Lösung aber in einer Organisation zur Sicherung der gesamten Kommunikation eingesetzt werden, muss diese nicht nur sicher und robust, sonder auch möglichst effizient sein, um bei den Anwendern Akzeptanz zu finden. Daher wurden in diesem Arbeitspaket verschiedene Punkte umgesetzt, um die Effizienz und Geschwindigkeit von SOLID zu erhöhen.

Zur Optimierung wurden zum einen interne Strukturen, wie die Verwaltungsnachrichten und andere interne Datenstrukturen, angepasst. Hier konnte mit einer Verringerung des notwendigen Speicherplatzes interner Objekte und einer Senkung der Senderaten der Verwaltungsnachrichten eine Steigerung der Performanz erreicht werden. Zum anderen wurde der Kompilierungsprozess angepasst, um SOLID auf ressourcenschwachen Endsystem lauffähig zu machen. Dadurch konnte erreicht werden, dass SOLID auch auf handelsüblichen Voice-over-IP-Telefonen und auf Architekturen mit *Big-Endian*-Speicherorganisation verwendet werden kann.

Durch die Unterstützung der aktuellen Java Card-basierten Smartcard-Generation konnte die Aushandlung von Sicherheitsbeziehungen beschleunigt werden. Dadurch kann in kritischen Situationen, wie dem zeitgleichen Anlaufen großer Netzbereiche oder der Wiederinbetriebnahme nach einen Netz- oder Stromausfall, die zeitliche Verzögerung, die durch die hohe Aushandlungslast entsteht, reduziert werden.

3.3.7 Erkennung und Behandlung interner Sabotage-Angriffe

In Anbetracht des sensiblen Ausgangslage in heutigen VPN-Szenarien sind interne Angreifer ein nicht zu vernachlässigendes Thema. Von internen Angriffen kann dabei gesprochen werden, wenn die Quellen in den geschützten Netzbereichen zu finden sind.

Bereits in diesem Fall ändert sich die Bedrohungslage, da Teile des Netzes angegriffen werden können, welche aus dem öffentlichen Netz heraus nicht adressierbar sind. Innerhalb des VPN kann dabei allerdings mit *Traffic Shaping* reagiert werden.

Infolge einer Kompromittierung einzelner VPN-Gateways entstehen darüber hinaus weitere ernstzunehmende Bedrohungen. Bereits im vorangegangenen Vorhaben *Mobil-SOLID-SINA* wurde diesem Thema daher große Aufmerksamkeit gewidmet. Aufgrund der besonderen Brisanz wurde im Rahmen dieses Arbeitspaketes daran angeknüpft. Dabei wurde eine Detektionsheuristik auf Basis von Antwortwahrscheinlichkeiten und Jitter entworfen. Anschließend wurde das, im Rahmen des Mobil-SOLID-SINA-Vorhabens entwickelte, stochastische Routing-Verfahren adaptiert, sodass auf Grundlage der beobachteten Kriterien im Overlay-Netz Weiterleitungsziele gewählt werden, welche mit höherer Wahrscheinlichkeit zur Benutzung nicht kompromittierter Pfade führen.

Interne Angreifer werden von konkurrierenden Verfahren typischerweise nicht adressiert, insbesondere aufgrund des zunehmenden VPN-Betriebs in mobilitätsorientierten, unsicheren Umgebungen – und der damit verbundenen höheren Wahrscheinlichkeit einer Kompromittierung einzelner VPN-Knoten – ist eine praktische Einbeziehung entsprechender Angriffe nach wie vor als notwendig anzusehen.

Hinsichtlich der angestrebten Forschungsschwerpunkte des Vorhabens in den Bereichen angriffsresistenter VPN-Topologien, dynamischer DoS-Angriffe und der Implementierungssicherheit konnten durch die geleisteten Arbeiten im Rahmen der verschiedenen Arbeitspakete signifikante Fortschritte erzielt werden. Dabei ergab sich die Notwendigkeit der durchgeführten Arbeiten bereits aus der Ausgangssituation und insbesondere des Bedrohungspotentials heutiger Denial-of-Service-Angriffe. Mit der insgesamt als sehr erfolgreich anzusehenden Bearbeitung der Arbeitspakete konnten schließlich auf Seiten der TU Ilmenau alle inhaltlichen Ziele des Vorhabens realisiert werden.

3.3.8 Anpassungen am SINA-Produkt

Um den wirtschaftlichen Erfolg des SOLID-SINA-Vorhabens sicherzustellen, ist eine zügige Produktisierung als notwendig zu erachten. Im Rahmen des Arbeitspaketes wurde dementsprechend eine zügige Integration des SOLID-Verfahrens und der SINA-Produktfamilie angestrebt.

Dies umfasste unter anderem notwendige Anpassungen am Konfigurationsdienst, die Integration einer aktualisierten strongSwan-Version, aber auch Modifikationen an der SINA-Plattform, welche durch den Einsatz der Autokonfigurationsmechanismen des SOLID-Verfahrens notwendig wurden, beispielsweise bezüglich des Anlegens von IPTables-Regeln oder der Verwaltung von XFRM-Richtlinien. Darüber hinaus wurde im Rahmen des Arbeitspaketes auch die notwendige Kompatibilität des Gesamtverfahrens mit IPv6 sichergestellt und der Lastbalancierungsmechanismus des SOLID-Verfahrens integriert. Daneben wurde eine Vielzahl weiterer implementierungslastiger Anpassungen durchgeführt.

Die Notwendigkeit der verschiedenen Anpassungen am SINA-Produkt ergibt sich dabei letztlich unmittelbar aus der angestrebten zügigen Produktisierung des Auto-

konfigurationsverfahrens.

3.3.9 Tests und Leistungsverhalten

Parallel zur Integration des SINA-Produkts und des SOLID-Verfahrens wurden eine Reihe automatisierter Tests entwickelt. Dies ist grundsätzlich notwendig, um die Erfüllung der zu realisierenden Anforderungen und die Qualität der Implementierung sicherzustellen. Neben vergleichsweise einfachen Tests zu spezifischen Teilkomponenten wurden dabei auch Testfälle für komplexe Szenarien entwickelt. Darüber hinaus wurden verschiedene manuelle Performanz-Messungen durchgeführt. Durch eine Reihe von Anpassungen an der Schnittstelle zur Plattform wurde auf Grundlage der gewonnenen Erkenntnisse schließlich das Leistungsverhalten der entstehenden Lösung verbessert.

Die Notwendigkeit der im Rahmen dieses Arbeitspaketes durchgeführten Arbeiten ergibt sich dabei unmittelbar aus den Zielen der Qualitätssicherung, insbesondere in Hinblick auf Fehlerfreiheit und Performanz des Verfahren.

3.4 Voraussichtlicher Nutzen und insbesondere Verwertbarkeit der erzielten Ergebnisse

Der ursprüngliche Verwertungsplan hat sich im Projektzeitraum nicht geändert und besitzt dementsprechend weiterhin Gültigkeit. Die Produktisierung des SOLID-Verfahrens ist in den vergangenen Monaten stetig vorangeschritten, womit eine baldige Aufnahme in die SINA-Produktpalette und eine anschließende Vermarktung erwartet werden kann. Im Rahmen des Vorhabens konnte dabei insbesondere der Umgang mit Denial-of-Service-Angriffen und transportnetzbedingten Ausfällen gestärkt werden. Durch die Stärkung der Verfügbarkeitseigenschaften des Verfahrens in entsprechenden Szenarien wird auch dessen Position gegenüber konkurrierenden Verfahren weiter verbessert.

Selbst populäre Bibliotheken und Komponenten mit signifikanter Verbreitung im Hochsicherheitsumfeld sind nicht vor praktischen Implementierungsfehlern geschützt. Dies wird bereits anhand einer Reihe von sicherheitskritischen Programmfehlern deutlich, welche jüngst große mediale Aufmerksamkeit erfuhren, wie dem *Heartbleed*-Bug in der verbreiteten *OpenSSL*-Bibliothek. Gerade in Anbetracht der Komplexität des verteilten SOLID-Verfahrens ist daher die Sicherheit der Implementierung zu hinterfragen. Dementsprechend wurden im Rahmen des Vorhabens verschiedene Methoden und Werkzeuge entwickelt, um diese Bedenken auszuräumen und die praktische Implementierung angesichts der fortgeschrittenen Produktisierung zu stärken. Neben den unmittelbaren Methoden des Arbeitspaketes *Implementierungssicherheit* sind dabei die Methoden der *Komponentenweisen Zerlegung* hervozuheben, welche eine Software-Dekomposition und anschließende Ausführung von Teilkomponenten mit jeweils minimal notwendigen Rechten anstreben.

Ebenfalls mit unmittelbarem Blick auf den Produktisierungsprozess wurde die Effizienz des SOLID-Verfahrens in verschiedenen Szenarien signifikant verbessert. Dies betrifft beispielsweise die fortgeschrittene Integration des Lastbalancierungsverfahrens für heterogene Szenarien, welche bereits zum Ende des Mobil-SOLID-SINA-Vorhabens er-

dacht wurden, oder den optionalen Einsatz einer temporären Pre-Shared-Key-basierten Verschlüsselung von Nutzdaten während der Aushandlung von Sicherheitsbeziehungen, welche beispielsweise in praktisch sehr relevanten VoiP-Szenarien für eine unmittelbare Nutzbarkeit der Verbindung sorgt, ohne generell auf die Vorzüge einer Smartcard-basierten Authentisierung und Schlüsselaushandlung verzichten zu müssen.

Aus Sicht der secunet stellt sich die konkrete Marktsituation derzeit folgendermaßen dar: Ein wichtiger Einflussfaktor für das Umsatzwachstum sind die Entwicklungen in der IT-Bedrohungslage, welche im Blick auf Schwachstellen von IT-Systemen, auf Bedrohungsszenarien in bestimmten Technologien und auf Gefahren im Bereich der kritischen Infrastruktur betrachtet werden können. Potenzielle neue Bedrohungen sowie Kosten- und Effizienzüberlegungen bilden den Hintergrund für die aktuellen Trends auf der Nachfrageseite und die Attraktivität der einzelnen Marktsegmente.

Neben einzelnen Segmenten haben auch bestimmte Regionen ein besonderes Wachstumspotenzial. Um in diesen Märkten in Zukunft erfolgreich zu sein, müssen wir als Anbieter relevante Wettbewerbsfaktoren berücksichtigen. Der Schutz von IT-Infrastrukturen, Informationen und Wissen gewinnt branchenübergreifend weiter an Bedeutung: Über alle Segmente hinweg planen nach Forrester-Umfragen über 30% der Unternehmen eine Erhöhung des IT-Sicherheitsbudgets. Dabei wird der Anteil der IT-Sicherheit am IT-Gesamtbudget mittlerweile auf ca. 10% beziffert. Grundlage für diesen allgemeinen Trend ist u. a. das Bestreben, Informationen und Applikationen online unternehmensweit verfügbar zu machen, sowie die wachsende Bedeutung von effizienten IT-gestützten Prozessen als Wettbewerbsvorteil.

Wie in den vorherigen Abschnitten schon angedeutet, ist die in diesem Projekt zu fördernde Technologie neu und bietet somit einen einzigartigen Wettbewerbsvorteil. Die zu Grunde liegende Technologie für die Autokonfiguration in eher statischen Szenarien wurde zum Patent angemeldet. Um den erreichten Vorsprung weiter auszubauen ist es nun wichtig, sowohl den Ansatz im Hinblick auf dessen Resistenz gegenüber praktischen Bedrohungen weiter zu entwickeln als auch die Produktisierung voranzutreiben, um auch den wirtschaftlichen Erfolg der Technologie sicherzustellen. Auf Grund der Marktposition von secunet ist ein entsprechender Marktzugang vorhanden, über den die Technologie in die notwendige Anwendungsbreite geführt werden kann. Gleichzeitig können die Attraktivität der Produkte weiter erhöht und neue Einsatzszenarien erschlossen werden, beispielsweise im zivilen Katastrophenschutz. Zudem profitieren die bisherigen Kunden der secunet erheblich von neuen Einsatzmöglichkeiten, die insbesondere den Behörden und Organisationen mit Sicherheitsaufgaben (BOS) zu Gute kommen. Vor allem kann aber durch die neuen Alleinstellungsmerkmale ein wesentlich besserer internationaler Marktzugang gesichert werden.

Mit der SINA-Client-Technologie wird sich in den folgenden Jahren eine breite Einsatzbasis bilden, die prädestiniert ist, mit der SOLID-Lösung ausgestattet zu werden. Mit der dann deutlich vereinfachten und zudem robusteren VPN-Konfiguration erschließen sich zum einen weitere Einsatzszenarien, zum anderen werden Konfiguration und Betrieb deutlich vereinfacht. Zum heutigen Zeitpunkt ist die Skalierbarkeit des Einsatzes durch administrative Aufwendungen einigermaßen begrenzt bzw. zieht entsprechende laufende Kosten nach sich. Eine SOLID-basierte Lösung kann vorhandene Szenarien in ihren Betriebskosten reduzieren und die Skalierbarkeit neuer Lösungen deutlich

verbessern.

secunet hat die SOLID Lösung um Laufe des Projekts mit der SINA L3 Box 3.9 zur Produktreife geführt. Die SINA L3 Box 3.9 wird im Sommer 2015 fertiggestellt und nach der geplanten Zertifizierung durch das BSI im Rahmen der Produktverkäufe vermarktet. Durch die etablierten Kundenbeziehungen kann secunet die Erfahrungen und Wünsche der Kunden beim Einsatz der Technologie kurzfristig in neue Produktgenerationen einfließen lassen. Die Verbreiterung der Kundenbasis stabilisiert auch die regelmäßigen Einnahmen aus Lizenzzahlungen und Subskription-Gebühren, die eine marktgerechte Weiterentwicklung sicherstellen. Neben den im Rahmen von Wartungsverträgen bedienten Kunden in einer bereits schon beachtlichen Stückzahlenbasis wird erwartet, dass durch die neue Funktionalität auch ein erheblicher Anstieg im Neukundengeschäft erzielt werden kann. Damit wird ein zusätzliches Umsatzvolumen von mehreren Mio. EUR p.a. im Produktgeschäft erwartet.

Im Zuge der fortschreitenenden Produktisierung steht die secunet im Rahmen der vertrieblichen Aktivitäten im steten Kontakt mit konkreten Interessenten für den Einsatz eines verteilten VPN. Dabei wird die secunet in den Gesprächen mit Netzbetreibern und möglichen Bedarfsträgern von Seiten der TU Ilmenau direkt unterstützt. Darüber hinaus ist davon auszugehen, dass die im Rahmen des Vorhabens entstandenen Publikationen der TU Ilmenau die Position des Verfahrens weiter stärken.

3.5 Ergebnisse dritter Seite mit Relevanz bezüglich des Vorhabens

Nach wie vor sind keine Bestrebungen im Umfeld anderer VPN-Autokonfigurationsverfahren bekannt, welche mit den Zielsetzungen des abgeschlossenen Vorhabens vergleichbar sind. Somit wurden von dritter Seite keine Ergebnisse offenbar, welche signifikante Relevanz bezüglich des Vorhabens haben.

3.6 Liste entstandener und geplanter Veröffentlichungen

Im Kontext des DoS-Resist-VPN-Vorhabens sind im Projektzeitraum eine Reihe von Veröffentlichungen entstanden.

[GRBS13] Grey, M. ; Rossberg, M. ; Backhaus, M. ; Schaefer, G.: On Distributed Geolocation by Employing Spring-Mass Systems. In: *IEEE GIIS* (2013)

[GRS12] Girlich, Franz ; Rossberg, Michael ; Schaefer, Guenter: On the Construction of Denial-of-Service-Resilient Overlay-Network. In: *CRITIS* (2012)

[GRS14] Girlich, Franz ; Rossberg, Michael ; Schaefer, Guenter: On the Resistance of Overlay Networks against Bandwidth Exhaustion Attacks. In: *Telecommunication Systems Journal (Special Issue)* (2014)

[GSRS14] Grey, M. ; Schatz, D. ; Rossberg, M. ; Schaefer, G.: Towards Distributed Geolocation by Employing a Delay-Based Optimization Scheme. In: *IEEE ISCC* (2014)

[GTRS15] Grey, M. ; Theil, M. ; Rossberg, M. ; Schaefer, G.: Towards a Model for Global-Scale Backbone Networks. In: *IEEE ICC* (2015)

[RGR14] Rothenberger, R. ; Grau, S. ; Rossberg, M.: Dominating an s-t-Cut in a Network. In: *SOFSEM* (2014)

[TBR15] Theil, M. ; Backhaus, M. ; Rossberg, M.: Network-supported Resistance against Low-Rate Denial-of-Service Attacks. In: *Eingereicht für IEEE CNS* (2015)

[TRS15] Trapp, Markus ; Rossberg, Michael ; Schaefer, Guenter: Program Partitioning Based on Static Call Graph Analysis for Privilege Separation. In: *IEEE ISCC* (2015)

[WRS15] Wendland, Philip ; Rossberg, Michael ; Schaefer, Guenter: Offene Software-Architektur für moderne Smartcards. In: *D-A-CH security* (2015)

Die fortgeschrittenen Forschungs- und Entwicklungsarbeiten am SOLID-Prototypen konnten im Rahmen verschiedener Veranstaltungen einem Fachpublikum präsentiert werden. Die breite Akzeptanz zeigt sich dabei beispielsweise auch am GI/ITG/VDE Communication Software Award 2013, welcher infolge einer Demonstration auf der insbesondere im deutschsprachigen Raum sehr anerkannten Konferenz *IEEE Networked Systems* (ehemals KiVS) verliehen wurde. Darüber hinaus wurde das SOLID-Verfahren und die daran beteiligten Mitarbeiter des Fachgebiets Telematik/Rechnernetze mit dem *Thüringer Forschungspreis 2013 für Angewandte Forschung* ausgezeichnet.

4 Zusammenfassung und Ausblick

Zusammenfassend ist festzuhalten, dass die Arbeit an den formulierten Arbeitspaketen im Rahmen des Vorhabens sehr erfolgreich war und alle wesentlichen Zielstellungen des DoS-Resist-Vorhabens realisiert werden konnten.

Aufgrund der angespannten Arbeitsmarktsituation zu Beginn des Vorhabens entstand sowohl auf Seiten der TU Ilmenau als auch bei der secunet zunächst eine Verzögerungen im Projektverlauf, allerdings hat sich die Situation im weiteren Verlauf des DoS-Resist-Vorhabens entspannt. Durch die Gewährung einer kostenneutralen Projektverlängerung konnten die noch offenen Arbeitspunkte nachgeholt werden, wodurch alle geplanten Arbeitspakete letztlich vollständig umgesetzt werden konnten.

Zusammenfassend bleibt somit herauszustellen, dass die inhaltlichen Ziele des Vorhabens in vollem Umfang erreicht wurden. Darüber hinaus sind keine Ergebnisse von dritter Seite bekannt geworden, welche Relevanz bezüglich des abgeschlossenen Vorhabens haben. Schließlich ist zu bemerken, dass sich Position und dabei insbesondere die Aussichten auf einen wirtschaftlichen Erfolg der SOLID-Lösung mit der im Rahmen des Vorhabens gewonnenen Technologie und Expertise weiter verbessert haben.

An dieser Stelle möchten wir daher sowohl dem Bundesministerium für Bildung und Forschung als auch dem VDI/VDE Innovation + Technik als Projektträger einen herzlichen Dank für die gewährte Unterstützung aussprechen.

Relevante externe Verweise

[BFT11] Baker, Stewart A. ; Filipiak, Natalia ; Timlin, Katrina: *In the Dark: Crucial Industries Confront Cyber Attacks*. McAfee, Incorporated, 2011

[Ero06] Eronen, Pasi: IKEv2 mobility and multihoming protocol (MOBIKE). (2006)

[GBM04] Guirguis, Mina ; Bestavros, Azer ; Matta, Ibrahim: Exploiting the Transients of Adaptation for RoQ Attacks on Internet Resources. In: *Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP '04)*, 2004, S. 184–195

[GTR+13] Grey, Michael ; Trapp, Markus ; Rossberg, Michael ; Schaefer, Guenter ; Martius, Kai: Skalierbare Lastbalancierung autokonfigurierter VPN. In: *13. Deutschen IT-Sicherheitskongress, Bonn, Deutschland* (2013)

[KK06] Kuzmanovic, Aleksandar ; Knightly, Edward W.: Low-rate TCP-targeted denial of service attacks and counter strategies. In: *IEEE/ACM Trans. Netw.* 14 (2006), August, Nr. 4, 683–696. `http://dx.doi.org/10.1109/TNET.2006.880180`. – DOI 10.1109/TNET.2006.880180. – ISSN 1063–6692

[KK08] Korns, Stephen W. ; Kastenberg, Joshua E.: Georgia's cyber left hook. In: *Parameters* 38 (2008), Nr. 4, S. 60–76

[Les07] Lesk, Michael: The new front line: Estonia under cyberassault. In: *IEEE Security & Privacy* 5 (2007), Nr. 4, S. 0076–79

[LSP82] Lamport, Leslie ; Shostak, Robert ; Pease, Marshall: The Byzantine generals problem. In: *ACM Transactions on Programming Languages and Systems (TOPLAS)* 4 (1982), Nr. 3, S. 382–401

[OSV14] *OSVDB, Open Source Vulnerability DataBase*. `http://osvdb.org/`. Version: Oktober 2014

[SR14] Schäfer, Günter ; Rossberg, Michael: *Netzsicherheit*. dpunkt-Verlag, 2014

Berichtsblatt

1. ISBN oder ISSN	2. Berichtsart (Schlussbericht oder Veröffentlichung)
geplant	Schlussbericht

3. Titel

Zusammenfassender Abschlussbericht für das Gesamtvorhaben DoS-Resist-VPN

4. Autor(en) [Name(n), Vorname(n)]	5. Abschlussdatum des Vorhabens
Grey, Michael Trapp, Markus Roßberg, Michael Schäfer, Günter Schlögel, Robin Heinlein, Alexander	Dezember 2014
	7. Form der Publikation

8. Durchführende Institution(en) (Name, Adresse)	9. Ber. Nr. Durchführende Institution
Fachgebiet Telematik/Rechnernetze Technische Universität Ilmenau Helmholtzplatz 5 98693 Ilmenau secunet Security Networks AG Kronprinzenstrasse 30 45128 Essen	- 10. Förderkennzeichen 16BY1202 11. Seitenzahl 39

12. Fördernde Institution (Name, Adresse)	13. Literaturangaben
Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	19 14. Tabellen 2 15. Abbildungen 14

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)
Statusseminar, Bonn, 17.9.2013

18. Kurzfassung

Die Nutzung moderner Kommunikationstechnologien ermöglicht heutzutage den zügigen Austausch von Informationen zwischen verschiedenen Standorten von Firmen und Behörden. Gleichzeitig wird unsere Gesellschaft immer abhängiger von der Verfügbarkeit dieser Technologien. Gerade im Kontext virtueller privater Netze (VPN) stellen bandbreitenerschöpfende Angriffe dabei eine besondere Bedrohung dar, da illegitime Daten aufgrund der Verschlüsselung nicht von den jeweiligen Internet-Service-Providern gefiltert werden können.

Im Rahmen des DoS-Resist-VPN-Vorhabens wurde ein bestehendes Autokonfigurationsverfahren für IPsec-basierte VPN, das sogenannte „Secure OverLay for IPsec Discovery“, um Maßnahmen zur Erhöhung der Resistenz gegenüber DoS-Angriffen erweitert. Darüber hinaus wurde die Integration in die „Sichere Inter-Netzwerk Architektur“-Produktlinie der secunet Security Networks AG vorangetrieben, die Beherrschbarkeit der Technologie gesteigert und damit für einen breiten Einsatz vorbereitet.

19. Schlagwörter
Virtuelle Private Netze, Denial-of-Service, Verfügbarkeit, Secure Overlay for IPSec Discovery, SOLID

20. Verlag	21. Preis

Document Control Sheet

1. ISBN or ISSN	2. type of document (e.g. report, publication) report

3. title

Zusammenfassender Abschlussbericht für das Gesamtvorhaben DoS-Resist-VPN

4. author(s) (family name, first name(s))	5. end of project December 2014
Grey, Michael Trapp, Markus Roßberg, Michael Schäfer, Günter Schlögel, Robin Heinlein, Alexander	6. publication date
	7. form of publication

8. performing organization(s) (name, address)	9. originator's report no.
Fachgebiet Telematik/Rechnernetze Technische Universität Ilmenau Helmholtzplatz 5 98693 Ilmenau secunet Security Networks AG Kronprinzenstrasse 30 45128 Essen	10. reference no. 16BY1202
	11. no. of pages 39

12. sponsoring agency (name, address)	13. no. of references 19
Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	14. no. of tables 2
	15. no. of figures 14

16. supplementary notes

17. presented at (title, place, date)
Statusseminar, Bonn, 17.9.2013

18. abstract

Nowadays, virtual private networks (VPN) are an adequate solution to protect confidential communications between multiple companies or locations authorities. However, in this context, bandwidth exhausting denial-of-service attacks must be considered to be a critical thread as illegitimate traffic cannot be filtered by internet service providers due to the applied traffic encryption.

Within this project, an existing VPN prototype ("Secure OverLay for IPsec Discovery (SOLID)") was augmented with additional measures that significantly increase the resistance on Denial-of-Service attacks. The extensions have been tested and evaluated in both, a real system as well as in a simulation environment. Moreover, the integration process of SOLID and the product line „Sichere Inter-Netzwerk Architektur" developed and marketed by secunet Security Networks AG received a strong boost, leading to an enhanced controllability of the technology and a significantly improved preparation for broad application and deployment.

19. keywords
Virtuelle Private Netze, Denial-of-Service, Verfügbarkeit, Secure Overlay for IPSec Discovery, SOLID

20. publisher	21. price