Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Ausarbeitung Seminar

Marco Schneider

Border Gateway Protocoll
Analyse & Angriffserkennung

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Inhaltsverzeichnis

1 Einleitung

Zu den Netzwerkeinstellungen eines gewöhnlichen Arbeitsplatz-PCs gehört neben der eindeutigen IP-Adresse auch ein Gateway. An das Gateway werden alle Pakete geschickt, die der PC nicht direkt in seinem Netzwerk zustellen kann. Diese Hierarchie setzt sich weiter fort: kann der Firmenrouter das Paket auch nicht zustellen, sendet dieser das Paket über seinen Gateway zu seinem Provider.

Bei den Providern funktioniert diese Hierarchie jedoch nicht mehr: es gibt keinen Gateway mehr. Damit die Pakete das Ziel doch erreichen, gibt es eine Instanz, welche die Pakete direkt an den ensprechenden Router weiterleitet. Dies ist die sog. default-free-zone, d.h. es ist die höchste Hierarchieebene im Routingsystem des Internet. Damit dieses System einwandfrei funktioniert, müssen alle Teilnehmer ein gemeinsames Protokoll benutzen: das Border Gateway Protocoll (BGP).

1.1 Motivation

Das Internet ist das Resultat einer Idee, Computer mittels einer universellen Abstraktionsschicht zu verbinden und so eine systemorientierte Rechnerkommunikation zu ermöglichen - unabhängig von dem physischen Übertragungsweg bzw. der Übertragungstechnik. Durch den Erfolg und den Wunsch nach einer Vernetzung aller Computer wurde das Internet immer größer und komplexer. In diesem Gebiet ist viel Bewegung: Forschung und Wissenschaft suchen ständig nach neuen Methoden, die bisherige Technik zu verbessern oder zu erweitern.

Das Border Gateway Protocol (BGP) ist der de-facto Standard des EGP[1] - also des Routings zwischen den verschiedenen IP-Netzen. Der erste Entwurf des heutigen BGP4 wurde bereits 1995 als Neuauflage für das BGP3 eingericht (1). Natürlich gab es viele Veränderungen zur Verbesserung des BGP4, dennoch wird dieses Protokoll nicht in absehbarer Zeit abgelöst werden (2), wie z.B. IPv4 durch IPv6 - ein weiterer Grund, sich mit dem Thema tiefer auseinanderzusetzen.

Das Internet entwickelt sich zu einer Ende-zu-Ende Topologie (3). Techniken wie der Multicast werden immer wichtiger durch den ressourcenschonenden Umgang mit der zur Verfügung

[1] Exterior Gateway Protokoll

stehenden Infrastruktur, deswegen kann ein Einblick in das Rückgrat des Internet sehr hilfreich sein für die Optimierung dieser Multicast-Ströme. Die INET-Gruppe[2] der HAW Hamburg forscht auf diesem Gebiet - jedoch gibt es keine praktischen Experimentiermöglichkeiten am Backbone-Routing.

Durch eine Kooperation mit dem *Berlin Commercial Internet Exchange e.V.*[3] (BCIX) ist es möglich, diese Lücke zu schließen. Dazu wurde ein Hardware-Router der Firma Brocade angeschafft, welcher direkt am BCIX ein eigenes (Test-) Prefix propagieren wird. Die Erkenntnisse können zur Validierung anderer Projekte (z.B. des Routing-Atlas[4]) benutzt werden.

1.2 Problemstellung

Um einen Messplatz am BCIX etablieren zu können, bedarf es nicht nur der vorhandenen Hardware und einer Kooperation: Fehlkonfigurationen können großen Schaden anrichten.

Expertise ist allerdings nicht nur beim Konfigurieren des Routers gefragt, sondern auch beim Messen und Analysieren von BGP-Updates. Zum Validieren eines Routingpfades reicht eine Anfrage an die Routing-Tabelle, doch möchte man potenzielle Angriffe erkennen können, müssen über einen längeren Zeitraum sämtliche Updates ausgewertet werden. Dabei spielt der eigene Standpunkt in der Topologie eine große Rolle, denn je nach Standort ändert sich die Perspektive auf die Topologie. Dies muss man bei aktiven oder passiven Messungen berücksichtigen, da sich die Ergebnisse von den öffentlichen (weiter oben in der Hierarchie angesiedelten) Messplätzen unterscheiden können. Dabei sind es genau diese Feinheiten, die von Interesse sind: Durch den Standort Deutschland sollen bessere und genauere Ergebnisse z.B. für den Routing-Atlas erzielt werden.

Zu dieser Problemstellung soll ein Messplatz am BCIX eingerichtet werden, in dem verschiedene Messungen teilautomatisiert durchgeführt werden können. Standardfunktionen wie die Anzeige eines Routingpfades sowie Differenzen zu bestimmten öffentlichen Messplätzen sollen ermöglicht werden. Zusätzlich soll die Analyse von eingehenden BGP-Updates mitgeschnitten und ausgewertet werden. Das Ziel soll ein unabhängiges Looking-Glass mit infrastruktureller Nähe zum deutschen Internet sein. Das bereitgestellte Toolkit soll einfach bedienbar sein, zusätzlich soll es kompatibel zum Routing-Atlas Projekt sein, um die Ergebnisse zeitnah und ohne großen Aufwand verifizieren zu können.

[2] http://inet.cpt.haw-hamburg.de/
[3] http://www.bcix.de/bcix/
[4] ein Projekt der INET-Gruppe der HAW Hamburg

1.3 Aufbau dieser Arbeit

Der Einführungsteil dieser Arbeit endet mit diesem Kapitel. Im folgenden Rückblick-Kapitel werden die bisherigen Arbeiten bis zum heutigen Stand noch einmal kurz vorgestellt inklusive deren Änderungen zum ursprünglichen Thema. Darauf folgt die Umsetzung, welches in die beiden Unterkapitel Analyse und Angriffserkennung unterteilt ist. Im ersten Teil der Analyse geht es primär um die technische Umsetzung der reinen Analysemethoden, während bei der Angriffserkennung zwei verschiedene Methoden miteinander kombiniert werden sollen. Das vorletzte Kapitel zeigt noch einmal die Risiken auf, die Zusammenfassung bildet den Schlussteil.

2 Rückblick

In diesem Kapitel werden die bisherigen Ergebnisse von Anwendungen 1 + 2, sowie dem Projekt 1 erläutert. Die sich daraus ergebenden Änderungen werden jeweils kurz diskutiert ohne Reihenfolge deren Relevanz.

2.1 Anwendungen 1 + 2

Anwendungen 1 beschäftigt sich hauptsächlich mit der Einarbeitung in das Thema. Der Titel war damals „Border Gateway Protocoll - Monitoring, Fluss-Messungen und -Optimierungen“ und sollte ein grundlegendes Verständnis des Backbone-Routing im Internet vermitteln. Das Grundthema ist gleich geblieben, von daher gibt es keine nennenswerte Erkenntnisse aus Anwendungen 1 für diese Arbeit.

Anwendungen 2 ist hauptsächlich vom Einarbeiten in die (aktuelle) Literatur zu diesem Thema geprägt. Viele verschiedene und vergleichbare Ansätze wurden diskutiert und bewertet mit deren Relevanz für das eigene Thema. Der Titel änderte sich geringfügig zu „Border Gateway Protocoll - Monitoring, Topologie und Sicherheit“. Das Thema wurde also in Richtung Topologieanalyse und Sicherheit im BGP-Routing erweitert, während die Flussmessungen per SFlow sowie die Optimierungen herausgestrichen wurden.

Der Grund dafür war, dass es bereits umfangreiche Literatur gibt in dem Bereich Flussmessung und eigene Ergebnisse auf diesem Gebiet keine besseren oder genaueren Erkenntnisse liefern wird, als jene, die in fremden Projektgruppen schon vorliegen.

Während der Recherche in Anwendungen 2 wurde mehrfach deutlich, dass Sicherheit in BGP aktuell eine große Rolle spielt, da das Protokoll seit 1995 unverändert besteht und keine Sicherheitsmechanismen protokollseitig vorhanden sind. Diese Fragestellung passt thematisch zum Routing-Atlas und hilft, ein genaues Bild von dem Routingsystem in lokaler Nähe zu Deutschland zu erhalten. 2005 schon wurde in (4) festgestellt, dass eine hohe Genauigkeit mittels vieler verteilerter Looking-Glasses erreicht werden kann, aber es wäre für den Routing-Atlas wünschenswert, wenn man Zugriff auf eigene Datenbestände direkt aus Deutschland hat. Aus diesem Grunde wurde das Thema „Topologie und Sicherheit“ mit aufgenommen.

2.2 Projekt 1

Projekt 1 ist der Teil der Arbeit, welcher die praktische Umsetzung neben den theoretischen Hintergründen aus Anwendungen 1 + 2 hervorbringt. Für diesen praktischen Teil steht ein Brocade-Router CER 2024 zur Verfügung, welcher in einer Testumgebung konfiguriert und getestet wurde. Inzwischen läuft dieser Router im 24/7-Betrieb und wird mit aktuellen Routing-Updates aus dem BCIX in Berlin versorgt.

Während der Testphase konnte ermittelt werden, dass der Router sich nicht eignet, um ein Projekt wie Oregon's RouteViews nachzustellen, da der Router über keine Exportfunktion der BGP-Daten verfügt. Somit können keine Dumps der aktuellen Routing-Information-Base erstellt werden, auch können die eingehenden und ausgehenden Updates nicht gespeichert werden. Es ist jedoch ohne Probleme möglich, auf die aktuelle (im Gerät gespeicherte) Routingtabelle zuzugreifen und so an die gewünschen Informationen zu kommen.

Um die BGP-Updates mitzuschneiden wird also noch ein zweiter BGP-Speaker benötigt, diesen Part übernimmt der BIRD[1] Routing Daemon. Dies ist eine freie Software, welche einen komplett implementierten Software-BGP-Router zur Verfügung stellt. Dieser Software-Router ist bereits in Berlin im Einsatz und wird später parallel zum Hardware-Router laufen um analysieren zu können, ob es Differenzen zwischen dem Gerät und der Software gibt.

Das Thema hat sich für Projekt 2 ein wenig verändert und heißt nun „Border Gateway Protocoll - Analyse & Angriffserkennung". Damit soll der Focus stärker auf das Auswerten von BGP-Informationen sowie mögliche Erkennung von Angriffen gelegt werden.

[1] http://bird.network.cz/

3 Umsetzung

3.1 Analyse

Die Analyse von BGP-Daten ist an sich nicht viel mehr, als ein einfaches Parsen von Texten. Natürlich muss eine entsprechende Logik „hinter“ dem Parsen stecken, um verwertbare Ergebnisse zu bekommen. Das Hauptproblem aber ist, dass ein MRT[1]-Dump kein Plain-Text, sondern nur nur maschinenlesbaren Code enthält.

Doch bevor man diese Daten parsen kann, muss man sie erst einmal bekommen. Dabei hilft der BIRD Routing Daemon, welcher die Möglichkeit von einem Export aller BGP-Nachrichten bietet. Diese müssen mittels Script wie bei einem Logrotate in regelmäßigen Abständen „weggeschrieben“ werden, sodass man z.B. für jede Stunde einzeln die Daten abrufen kann. Zum Vergleich: Das Routeviews-Projekt[2] stellt alle 15 Minuten einen Dump bereit, welcher die Größe von ca. 1 MB hat.

Zum Umwandeln der MRT-Dumps gibt es fertige Scripte, zum Beispiel den „BGP Parser“[3] des Internet Research Lab der UCLA. Die Daten werden umgewandelt in ein menschenlesbares XML-Format, welches wiederum die Grundlage für Auswertungen z.B. im Bereich Route-Flapping sein können. Es gibt eine Vielzahl solcher Scripte, deren man sich bedienen kann um die Umwandlung nicht selber implementieren zu müssen. Gerade die aus dem Forschungsbereich stammenden Scripte wie der UCLA sind ausreichend verifiziert, um sicherzugehen, dass es hierbei keine Probleme oder einfach falsche Ergebnisse gibt.

Route-Flapping ist der Mechanismus, dass eine Route im Internet nicht stabil ist, sondern zwischen zwei Pfaden „umherspringt“. Dieses Verhalten ist nicht wünschenswert, da das Zielprefix durch die zeitlich versetzten Updates an die folgenden Router dafür sorgen, dass das Prefix nicht erreichbar ist. Aus diesem Grund haben viele Routerhersteller auch eine Erkennung für dieses Verhalten implementiert, sodass das Flapping zu einer Abschaltung eines Peerings führen würde.

---

[1] Multi-threaded Routing Toolkit

[2] http://www.routeviews.org/

[3] http://irl.cs.ucla.edu/software/bgpparser.html

Um Route-Flapping zu erkennen gibt es verschiedene Ansätze, z.B. (5) und (6). Ein einfacher und pragmatischer Algorithmus ist jedoch, die eingehenden Routen-Updates über einen bestimmten Zeitraum zu analysieren und anhand dieser Information festzustellen, ob es sich um eine Fehlkonfiguration handelt, oder ob die Routenupdates legitim sind. Sofern die Route sich nicht anhaltend öfter als 1-2x pro Tag ändert, kann von keinem Fehler ausgegangen werden. Wenn allerdings sich die Route öfter als 2x am Tag ändert, besonders verdichtet auf einen Zeitraum von wenigen Stunden, ist dies sicher eine Fehlkonfiguration und sollte schnellstmöglich behoben werden. Ansätze, wie diese Probleme einzudämmen sind, stellt ebenfalls (6) bereit.

Einhergehend damit möchte man in manchen Fällen wissen, ob ein Router überhaupt erreichbar ist - unabhängig vom AS-Level. Dazu kann man sich einem überall präsenten Mechanismus bedienen: *Ping*. So einfach es klingt kann mit einem zeitgesteuerten Ping ermittelt werden, ob das AS überhaupt erreichbar ist. Dies macht vor allem Sinn, wenn man die allgemeine Stabilität zu einer ASN untersuchen möchte auf AS- sowie auf IP-Level.

Dazu ist jedoch der Standort in der Topologie ein wichtiger Faktor, wenn ein AS angepingt werden soll, welches weit entfernt ist und es Probleme wie Route-Flap-Damping (RFD) gibt, dann muss der Standort in einem Teil des Netzes sein, wo diese Probleme nicht bestehen - oder am besten direkt im Netz des betreffenden AS. Andernfalls ist das zu untersuchende AS nicht erreichbar, bzw. man bekommt nur unzuverlässige Ergebnisse.

Jedoch ist der Standort noch weit aus wichtiger für die Ergebnisse als für die reine Analyse des RFD: Je nach Topologie ändert sich die Sicht auf das gesamte Internet! Weit oben in der Topologie ist der hierarchische Aufbau erkennbar und keine privaten Peerings zwischen ISPs, während von „unten“ in der Topologie ein feingranularer Blick zu erwarten ist und somit die Peerings zwischen ISPs erkenn- und nutzbar sind. Dies liegt an der einfachen Gegenbenheit, dass Upstream-Provider für den Transit-Verkehr Geld verlangen. Um dies zu umgehen, sind die „kleineren“ Provider bemüht, möglichst viel vom Traffic direkt zu den Empfängern zu schicken - ohne Umleitung über Upstreamprovider.

3.2 Angriffserkennung

Es gibt verschiedene Angriffsszenarien im Internet. Dazu zählen grundlegend das Blackholing, ein Imposture- oder Interception-Angriff.

Das Blackholing ist der typische Denial-of-Service (DoS) Angriff, also der Versuch, das Ziel zu stören. Der Imposture-Angriff ist auch bekannt als Spoofing: Der Angreifer versucht, das eigentliche Ziel vorzutäuschen. Ein Interception-Angriff ist der klassische Man-In-The-Middle Angriff und versucht, die Daten irgendwie „mitzuhören“.

Für die beiden ersten Szenarien wird man versuchen, eine spezifischere Route zum Ziel ins Internet zu propagieren, während man beim Man-In-The-Middle versuchen wird, den AS-Pfad zu manipulieren. Natürlich kann man auch die erstgenannten Szenarien durch Pfadmanipulation erreichen, es ist aber komplizierter.

3.2.1 Monitoring

Um festzustellen, ob ein Angriff erfolgt ist, kann man rein passiv die BGP-Updates auswerten. Die Grundlage bildet die Tatsache, dass der Standort in der Topologie sich in der Regel wenig verändert. Eine legitime Änderung wäre z.B., wenn ein Kunde eines ISP sein eigenes AS künftig betreiben möchte und der AS-Pfad vom ISP zum Kunden wandert - oder andersherum. Im Bild 3.1 sieht man dies schematisch dargestellt.

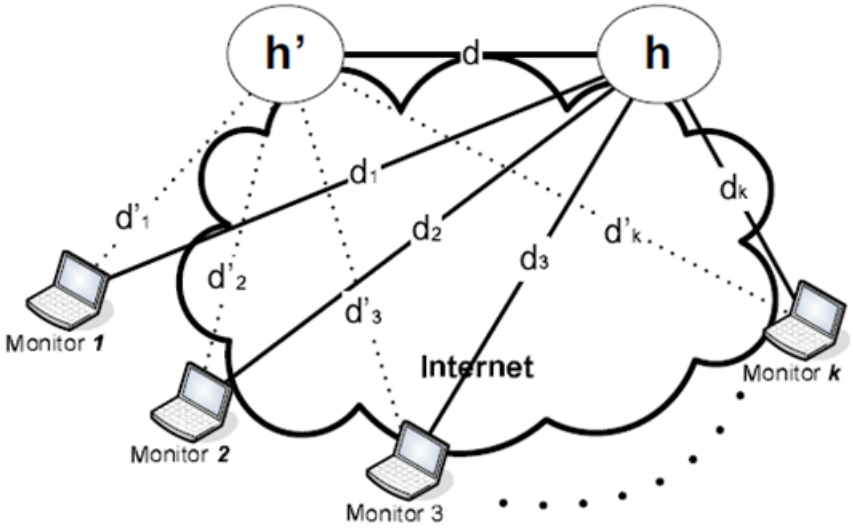

Abbildung 3.1: Monitoring Network Location aus (7)

Es besagt, dass die Distanz d bei einer (legitimen) Co-Location in etwa gleich sein muss, also $d_i \approx d_i'$. Vergleicht man nun also die Updates miteinander, so kann man eine größere Abweichung feststellen und ggf. so einen Angriff erkennen. Leider ist dies kein sicheres Indiz für einen Angriff, da eine globale Firma durchaus einmal die eigene Webseite für Wartungsarbeiten von Europa nach Amerika „verlegen“ könnte.

Einen möglichen Imposture-Angriff kann man im Prinzip nach der selben Methode erkennen, nur dass der Grenzwert δ eingeführt wird. Wenn für einen Monitor $|d_i - d_i'| \geq \delta$ gilt, wird ein möglicher Angriff detektiert. Dabei ist zu beachten, dass eine größere Anzahl von Monitoren

nur Sinn macht, wenn diese auch über die ganze Welt verteilt sind, da wie schon erwähnt, die Routingpfade bei lokaler Nähe i.d.R. gleich sind.

Sind mehrere Monitore vorhanden, führt man den Erkennungsindex D ein.

$$D = \max_{0<i<k} |d_i - d_i'|$$

D gibt die größte Abweichung des Pfades an und kann z.B. als Indikator für Relevanz einer Änderung dienen. Je größer D wird, desto wahrscheinlicher ist ein Angriff und sollte durch weitere Monitore überprüft werden.

Um einen Interception-Angriff zu erkennen, bedarf es noch einer kleinen Änderung in der Formel vom Imposture-Angriff, da der Angreifer das Interesse hat, dass die Daten das ursprüngliche Zielprefix erreichen:

$$|d_i - d_i' + d| \geq \delta$$

Leider erkennt dieser Ansatz nur „einfache“ Interception-Ansätze. Ein Angriff nach der Idee von (8) kann nicht erkannt werden, da sich das angreifende AS als Endpunkt für das Zielprefix ausgibt und die Daten mittels Tunnel zu einem nahe am „echten“ Zielprefix liegenden (und somit nicht angegriffenen) AS weiterleitet. Glücklicherweise würde dieser Angriff aber auffallen durch den ersten Ansatz: Bei einem Update von dem angreifenden AS kann leicht festgestellt werden, dass die Distanz zwischen angreifendem und echtem AS zu groß ist für eine plausible Änderung.

3.2.2 Pfadunterschiede

Ein weiterer Ansatz für ein sehr genaues Ergebnis baut auf der oben genutzten Grundlage auf, dass die AS-Pade zu lokal nahen ASN annähernd gleich sein müssen. In Bild 3.2 sieht man die grundlegende Idee: man benötigt ein Referenz-AS in lokaler Nähe zu dem zu überwachenden AS.

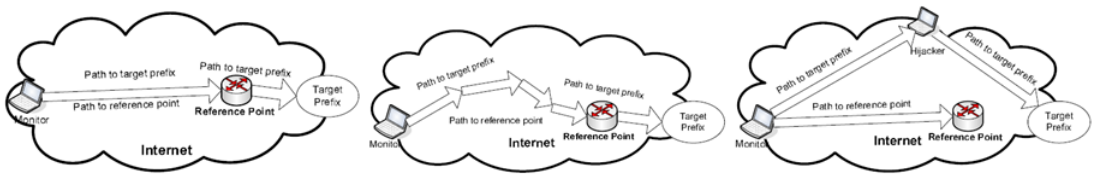

Abbildung 3.2: Path Disagreement aus (7)

Durch die Topologie ergibt sich, dass von Monitorpunkt aus die Pfade von Monitor zu Referenzpunkt und vom Monitor zum Zielprefix annähernd gleich sein müssen, insbesondere was den

ersten Teil des Pfades zum Referenzpunkt betrifft. Wird der Pfad geändert z.B. durch legitime Routenänderungen (Loadbalancing, Routerdefekt, ...), so müssen sich beide Pfade bis zum Referenzpunkt annähernd gleich ändern.

Wenn nun ein Angreifer das Zielprefix umleiten möchte, so kann unabhängig vom (8)-Ansatz festgestellt werden, dass der Pfad vom Referenzpunkt stark zum Zielprefix abweicht. So kann schnell festgestellt werden, ob es sich um eine Interception handelt oder nicht.

Dieser Ansatz ist primär interessant, da durch die Kooperation mit dem BCIX „unser“ AS als Referenzpunkt (in lokaler Nähe von Deutschland) von anderen Looking-Glasses benutzt werden kann. Somit kann eine Vielzahl öffentlicher Looking-Glasses genutzt werden, um diesen Ansatz verteilt aufzubauen und mit hoher Genauigkeit zu verifizieren.

3.2.3 Kombination der Methoden

Die in diesem Kapitel vorgestellten Methoden habe alle Vor- und Nachteile. Damit eine möglichst genaue Information über einen möglichen Angriff gewonnen werden kann, liegt es nahe, die Methoden zu kombinieren. Um den Aufwand nicht zu groß werden zu lassen, kann z.B. die einfache (passive) Methode aus 3.2.1 als Trigger verwendet werden. Wenn ein Pfadunterschied festgestellt wird, dann können die anderen Messmethoden folgen um diesen „Alarm“ zu verifizieren bzw. zu widerlegen.

Es bleibt auszuwerten, ob und wie viel die Kombination der verschiedenen Methoden an Genauigkeitsvorteil bringt und ob der Aufwand gerechtfertigt ist, oder ob nach erfolgreicher Auswertung dieses eigenen Messplatzes doch weiter auf fremde Datenbestände zurückgegriffen wird.

4 Risiken

Das Hauptrisiko liegt von Anfang an im Bereich des Aufwandes. Es ist weiterhin schwer, den tatsächlichen Aufwand des Projektes abzuschätzen und ob alle gewünschten Funktionen tatsächlich implementiert werden können. Die Grundfunktionalität wird sicher erreicht werden, jedoch können zusätzliche Feinheiten viel Zeit rauben.

Weiterhin ist fraglich, ob die Angriffserkennung auch tatsächlich funktionieren wird - also ob überhaupt „echteÄngriffe stattfinden. Wie auch die meisten anderen Ausarbeitungen werden i.d.R. Angriffsszenarien künstlich hervorgerufen - ob tatsächlich ein „echter“ Angriff oder eine Fehlkonfiguration passiert, kann im Vorwege nie gesagt werden. Daher kann die Angriffserkennung schlimmstenfalls nur mit selber provozierten Tests überprüft werden.

Die Filterregeln der Upstreamprovider können eventuell auch noch ein Problem darstellen, da mögliche Angriffe bereits im Vorfeld gefiltert werden und so gar nicht bis zu dem Router vordringen. Gegen dieses Problem hilft nur ein Peering mit möglichst vielen, unterschiedlichen, größeren und kleineren Providern. Da eine Open-Policy auch ein erhebliches Risiko darstellt, ist es fraglich, ob wirklich eine größere Anzahl von Partnern für dieses Projekt gewonnen werden kann.

Abschließend kann es natürlich passieren, dass die lokal gewonnenen Ergebnisse nicht besser sind als jene, welche man aus öffentlichen Looking-Glasses bekommen kann. Dies wäre jedoch kein Nachteil, da man die Herkunft/Plausibilität der Daten verifizieren kann.

5 Zusammenfassung

Es soll ein Messplatz für BGP-Messungen und -Auswertungen eingerichtet werden. Die dazu notwendige Hardware ist vorhanden, eine Kooperation mit einem großen ISP auch. Es soll anhand von BGP-Update Nachrichten ermittelt werden, wie stabil die Routingpfade im *deutschen Internet* sind und es sollen Angriffe ermittelt werden können.

Die vorherigen Arbeiten ergaben, dass bereits auf diesem Gebiet geforscht wurde, jedoch sind die Aussagen allgemeingültig und nicht spezifisch für das deutsche Internet. Genau dies liegt aber im Fokus, sodass ein eigener Messplatz etabliert werden soll, damit genauere Ergebnisse vorliegen.

Da das Verfahren zur Entdeckung von Angriffen mittels reiner Analyse der BGP-Daten nicht ausreichend ist, sollen zusätzlich noch zwei weitere Verfahren eingesetzt und kombiniert werden, sodass eine genaue Aussage getroffen werden kann, ob es sich um einen Angriff handelte oder nicht. Dies soll automatisiert werden, sodass das System passiv im Hintergrund läuft und sich „meldet“, sobald eine Bewertung des Sachverhaltes durch einen Menschen erforderlich wird.

Die daraus resultierenden Daten sollen im Projekt Routing Atlas der INET-Gruppe der HAW-Hamburg zur Verfügung gestellt werden, um dortige Erkenntnisse zu verifizieren oder zu widerlegen.

Literaturverzeichnis

[1] Y. Rekhter and T. Li, “A Border Gateway Protocol 4 (BGP-4),” IETF, RFC 1771, March 1995.

[2] A. Doria, E. Davies, and F. Kastenholz, “A Set of Possible Requirements for a Future Routing Architecture,” IETF, RFC 5772, February 2010.

[3] C. Lumezanu, “Using internet geometry to improve end-to-end communication performance,” Ph.D. dissertation, University of Maryland, 2009.

[4] B. Zhang, R. Liu, D. Massey, and L. Zhang, “Collecting the internet as-level topology,” *SIGCOMM Comput. Commun. Rev.*, vol. 35, pp. 53–61, January 2005. [Online]. Available: http://doi.acm.org/10.1145/1052812.1052825

[5] R. Govindan and A. Reddy, “An analysis of internet inter-domain topology and route stability,” in *INFOCOM ’97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, vol. 2, apr 1997, pp. 850 –857 vol.2.

[6] P. Smith and C. Panigl, “Recommendations on route-flap damping.” RIPE, 2006. [Online]. Available: http://www.ripe.net/ripe/docs/ripe-378

[7] C. Zheng, L. Ji, D. Pei, J. Wang, and P. Francis, “A light-weight distributed scheme for detecting ip prefix hijacks in real-time,” *SIGCOMM Comput. Commun. Rev.*, vol. 37, pp. 277–288, Aug. 2007. [Online]. Available: http://doi.acm.org/10.1145/1282427.1282412

[8] H. Ballani, P. Francis, and X. Zhang, “A study of prefix hijacking and interception in the internet,” *SIGCOMM Comput. Commun. Rev.*, vol. 37, pp. 265–276, August 2007. [Online]. Available: http://doi.acm.org/10.1145/1282427.1282411