Technische Universität Berlin

Fakultät IV
Fachgebiet für intelligente Netze und
Management verteilter Systeme

Bachelorarbeit in Informatik

Eine Analyse der Routing Sicherheit des Location Identifier Separation Protocol LISP

Bernd May

31. Januar 2012

Aufgabenstellerin:	Prof. Anja Feldmann, Ph. D.
Betreuer:	Msc. Jan Boettger
	Prof. Anja Feldmann, Ph. D.
Abgabedatum:	31. Januar 2012

Die selbständige und eigenhändige Anfertigung versichert an Eides statt
Berlin, den 30. Januar 2012

Unterschrift

Ich möchte mich bei den Betreuern meiner Bachelorarbeit, Jan Böttger und Anja Feldmann für ihre sachkundige und geduldige Unterstützung bedanken. Außerdem danke ich Harald und Doris Schiöberg für so manchen anspornenden Kommentar und hilfreichen Vorschlag.

Mein Dank gilt ferner all jenen, die mich in der Phase des Niederschreibens dieser Arbeit ertragen und unterstützt haben. Dazu gehören besonders Rainer, Jan, Chris, Luigi, Matthias und meine Arbeitskollegen, die die sträfliche Vernachlässigung ihrer Bedürfnisse mit Freundlichkeit und Geduld beantwortet und mir die Zeit gegeben haben, die ich brauchte.

Schlussendlich danke ich meiner Freundin Nadine für all die motivierenden und aufbauenden Worte, wenn ich mal wieder alles hinschmeißen wollte.

Danke euch allen!

Zusammenfassung

Die Forschung an Alternativen, zum aktuellen Routing-System schreitet stark voran. Ein vielversprechender Favorit unter diesen Alternativen ist das Locator Identifier Separation Protocol (LISP). Eine Betrachtung dieses Protokolls unter Sicherheitsaspekten ist bisher kaum vorgenommen worden. LISP Mapping-Systeme, ein integraler Bestandteil von LISP, sollten jedoch auch auf ihre Verwundbarkeiten untersucht werden. Von speziellem Interesse ist, ob sich bereits erforschte Verwundbarkeiten aus der Welt des BGP auch auf LISP übertragen lassen. Schutzmaßnahmen aus dem Bereich des Routings und DNS, auf Basis bekannter Systeme wie DNSSEC und S-BGP, können dann darauf angepasst werden. Gegenstand dieser Arbeit sind die Fragen, wie verwundbar LISP Mapping-Systeme sind und welche Schutzmaßnahmen aus bekannten Sicherungssystemen dagegen hilfreich sind.

Abstract

Research about an alternative for the current routing system with BGP is advancing fast. A promising candidate among the research subjects is the Locator Identifier Separation Protocol (LISP). While a lot of effort has been put into developing the specifics of routing via this new protocol, security research in this area has been rather sparse. Since LISP strongly relies on its mapping systems their vulnerabilities should be thoroughly analyzed. It is particularily interesting to find out whether security vulnerabilities which are already known of BGP can also be applied to LISP. If so, can protective systems from routing security research like DNSSEC or BGP-S be used to reduce them? These questions shall be analyzed in the following thesis.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Hier werden eine Reihe von Abkürzungen aufgeführt, die in der Arbeit häufig benutzt werden:

ALT Alternative Logical Topology

AS Autonomous System

BGP Border Gateway Protocol

BGP-GRE Border Gateway Protocol Generic Routing Encapsulation

CA Certificate Authority

CONS Content distribution Overlay Network Service

DFZ Default Free Zone

DHT Distributed Hashtable

DNS Domain Name System

DNSSEC Domain Name System Security Extension

(D)DOS (Distributed) Denial of Service

EID Endpoint Identifier

ETR Egress Tunnel Router (DFZ perspective)

HMAC Hash-based Message Authentication Code

ICANN Internet Corporation for Assigned Names and Numbers

IETF Internet Engineering Taskforce

IP Internet Protokoll

ISP Internet Service Provider

ITR Ingress Tunnel Router (DFZ perspective)

LISP Locator Identifier Separation Protocol

LISP-SEC Locator Identifier Separation Protocol Security

MR Mapping Resolver

MS Mapping Server

NERD Not so Novel EID to RLOC Database

Nonce Number used only once

OTK One Time Key

PKI Public Key Infrastructure

psBGP Pretty Secure Border Gateway Protocol

PSK Pre-Shared Key

RIR Regional Internet Registry

RLOC Routing Locator

soBGP Secure Origin Border Gateway Protocol

S-BGP Secure Border Gateway Protocol

WOT Web of Trust

1 Einleitung

Die Zahl der Einträge in den BGP-Routingtabellen der letzten Jahre hat ein zunehmendes Wachstum verzeichnet. Das hatte unter anderem eine Verstärkung der Forschungen im Bereich der Locator Identifier Splits zur Folge. Inhärenter Bestandteil dieser Methodik ist ein Mapping-System, um den Routing-Locator mit dem Endpoint-Identifier zu verbinden. Beim Entwurf dieses Systems wurden jedoch kaum sicherheitsrelevante Designkriterien berücksichtigt.

Welche fatalen Folgen Verwundbarkeiten in Routing-Protokollen haben können, zeigen die Zwischenfälle der letzten Jahre in der Routing-Infrastruktur des Internets. Als Beispiele seien hier die Umleitung von rund 15% der weltweiten Routen nach China im April 2010 [33], der Youtube-Pakistan Zwischenfall 2008 [44] oder die Abschaltung der BGP-Routen in Ägypten im Frühjahr 2011 [32] genannt. Diese und andere bekannte Verwundbarkeiten des Routing-Systems stellen eine ernstzunehmende Gefahr für die Sicherheit der Internet Infrastruktur dar.

Der Vorreiter unter den Protokollen zur Umsetzung des Locator Identifier Splits ist das Location Identifier Split Protocol (LISP). Es ist in zwei Komponenten unterteilt, Routing und Mapping, die im Wesentlichen auf BGP basieren. Aus diesem Grund ist es auch genauso verwundbar. Die Sicherheitsbetrachtungen, die bisher zu LISP durchgeführt wurden, sind zur Zeit noch nicht sehr fortgeschritten. Sie gehen außerdem von unrealistischen Annahmen aus, z.B. der Nichtexistenz von Man-in-the-Middle Angriffen. Werden diese Annahmen unterlaufen, schlagen die darauf basierenden Sicherheitsmechanismen fehl.

In dieser Arbeit werden die wichtigsten Mapping-Systeme auf ihre Stärken und Schwächen in Bezug auf anerkannten Kriterien der Routingsicherheit untersucht. Ferner werden Lösungsansätze zur Routingsicherheit, die im Laufe der Jahre innerhalb der Community erforscht wurden, erörtert. Darauf aufbauend werden ihre Anwendungsmöglichkeiten zur Absicherung von LISP näher beleuchtet.

Eine Beispielkombination, LISP-Tree und DNSSEC, wird abschließend einer genaueren Analyse unterzogen. Dabei zeigt sich, dass dies zu einer Verbesserung für die Sicherheit des LISP-Mappings führen kann und eine Vielzahl von Verwundbarkeiten reduziert.

Die vorliegende Arbeit umfasst in Kapitel 2 die Hintergrundinformationen zu LISP, den Mapping-Systemen und zu vielen ihrer bekannten Verwundbarkeiten. In Kapitel 3 findet sich eine Auswahl an prominenten Lösungsvorschlägen zur Verbesserung der Routingsicherheit im Allgemeinen. Kapitel 4 verbindet die kritische Betrachtung dieser Vorschläge in ihrer Anwendbarkeit auf LISP-Mapping mit einer ausführlichen Analyse von LISP-Tree und DNSSEC. Es folgt das Fazit in Kapitel 5 mit Überlegungen zu zukünftigen Verbesserungen sowie offener Fragen und Themenbereiche die weiterer Forschung benötigen.

2 Hintergrundinformationen

Von 1994 bis 2011 ist die Anzahl der Einträge in der BGP-Routing-Tabelle von unter 50.000 auf über 350.000 gestiegen. Davon sind mehr als 200.000 Einträge erst in den letzten sieben Jahren hinzu gekommen [38][24].

Aufgrund dieses Anstiegs gibt es seit einiger Zeit innerhalb der Routing-Community Bestrebungen, eine Trennung der Adressierung des Ziels von der des Ortes vorzunehmen. Das Forschungsgebiet wird unter dem Begriff „Routing Locator Identifier Split“ zusammengefasst. Ein prominenter Vertreter der Verfahren zur Durchführung dieser Trennung ist das sogenannte „Locator Identifier Separation Protocol“, kurz LISP. Ein integraler Bestandteil von LISP ist die Zuordnung der Adresse des Ziels, zu der Adresse des Ortes. Dieses Mapping-System kann auf unterschiedliche Weisen implementiert werden. Keine davon hat bei ihrem Entwurf die Frage nach der Sicherheit hinreichend berücksichtigt. Führt man sich die Vielzahl an Angriffsszenarien vor Augen, die allein für BGP bekannt sind, stellt dies eine beunruhigende Tatsache dar.

Es gibt zwar aus jüngerer Vergangenheit eine Sicherheitsanalyse zu LISP [43] und auch einen Entwurf zur Absicherung [36]. Beide stellen allerdings ein eher stiefmütterlich behandeltes Thema in der Arbeitsgruppe der Internet Engineering Taskforce (IETF)für LISP dar. Als nachträgliche Verbesserungen sind sie nicht nur schlecht integriert, sondern behandeln auch nur einen kleinen Teil der Verwundbarkeiten.

Dieses Kapitel gibt einen Überblick über die Funktionsweise von LISP und in Abschnitt 2.2 die vorhandenen Entwürfe für ein Mapping-System. Die Systeme im Einzelnen sind: LISP-ALT, LISP-NERD, LISP-CONS, LISP-DHT und LISP-TREE. In Abschnitt 2.3 werden bekannte Verwundbarkeiten im heutigen Routing mit BGP und ihr Einfluss auf die Sicherheit des LISP-Mapping-Systems vorgestellt und erläutert.

2.1 Das Locator Identifier Separation Protocol (LISP)

LISP [15] ist das Produkt einer Arbeitsgruppe in der Internet Engineering Taskforce (IETF), um das wachsende Problem des doppelten Verwendungszwecks der IP-Adresse zu bereinigen. Momentan wird die IP-Adresse sowohl benutzt, um die Identität eines Hosts festzulegen, als auch um den Ort zu bestimmen, an dem er sich im Internet befindet. In Folge von z.B. Multihoming, Traffic Engineering, nicht aggregierbaren Adresszuweisungen und Unternehmenszusammenschlüssen, wächst deshalb die Anzahl der einzelnen Routen in der sogenannte *Default Free Zone* (DFZ) stetig [24].

Die DFZ ist der Bereich des Internets, der größtenteils mit dem Routing zwischen den Autonomen Systemen (AS) der Endknoten beschäftigt ist. Die Routingtabellen dort enthalten eine Zuordnung von aggregiertem IP-Präfix und zugehörigem Pfad zu seinem AS. Werden diese IP-Präfixe aufgeteilt, erfordert dies zusätzliche Einträge in der Routingtabelle. Dadurch wächst sowohl die Anforderung an Speicherkapazität, als auch an die Geschwindigkeit bei der Anfragenverarbeitung.

Dieses Problem soll dadurch gelöst werden, dass die beiden Verwendungsarten der Adresse auf zwei getrennte Adressräume aufgeteilt werden. Hierzu setzt LISP an der

Grenze der DFZ an und teilt das Internet in zwei Arten von Netzen: Die Netze der Endknoten und die DFZ. Beide Netze benutzen einen eigenen Adressraum. Die Adressen aus der DFZ werden Routing Locator (RLOC) genannt, die anderen Endpoint Identifier (EID).

Um diese Teilung zu erreichen, wird vorgeschlagen, eine Tunnelarchitektur aufzubauen, die eine Zuordnung zwischen EID und RLOC vornimmt und Pakete von dem einen in das andere Netz befördert. Die dafür zuständigen Instanzen werden Egress Tunnel Router (ETR) und Ingress Tunnel Router (ITR) genannt, d.h. *Ausgang* und *Eingang*, aus der Perspektive der DFZ. Sie sind an den Schnittstellen der Netze untergebracht und nehmen eine entsprechende Kapselung der Pakete vor. Es ist durchaus möglich, dass dasselbe Gerät beide Aufgaben übernimmt.

Der LISP-Header solcher gekapselten Pakete enthält: Eine CRC ähnliche Prüfsumme, den maximalen Hop-Count zur RLOC, einen UDP-Header mit dem LISP-Port und einen IP-Header mit der RLOC als Zieladresse.

Abbildung 1 gibt einen Überblick über einen möglichen Ablauf einer Kommunikation zweier Endpunkte via LISP. Der LISP-Header wurde hier auf die RLOC von Quelle und Ziel des Pakets verkürzt. Die Rückantwort erfolgt auf die gleiche Weise. Der Übersichtlichkeit halber sind EIDs als IPv4 und RLOCs als IPv6 Adresse angegeben. Das ist bei der Umsetzung nicht zwingend erforderlich. [vergl. 15, Kapitel 4.1]:

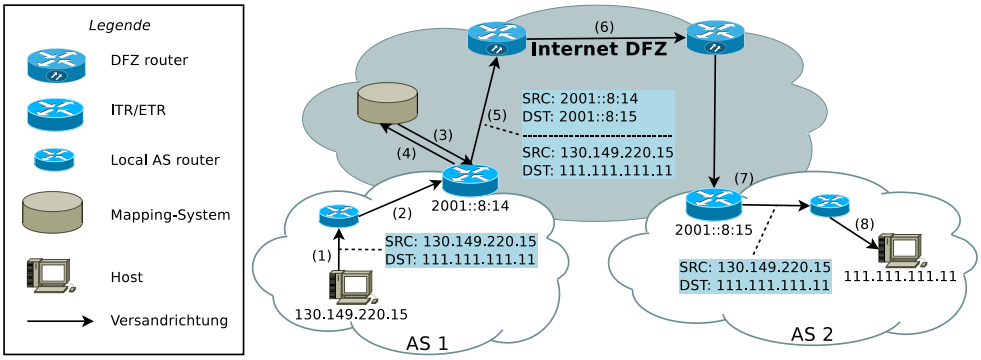

Abbildung 1: Kommunikation via LISP

1. Ein Host mit EID '130.149.220.15' von AS_1 sendet ein Paket an den Host mit EID '111.111.111.11' in AS_2.

2. Das Paket wird AS intern, auf Basis des Ziel-EID, mittels BGP zum ITR geroutet.

3. Der ITR schlägt das Mapping des EID '111.111.111.11' zum RLOC des zuständigen ETR nach. Das Mapping-System muss sich nicht in der DFZ befinden, siehe Abschnitt 2.2.

4. Antwort des Mapping-Systems mit RLOC '2001::8:15'.

5. Der ITR verpackt das Paket in einen LISP-Header, der als SRC-IP die eigene RLOC und als DST-IP die des ETR aus dem Mapping enthält. Dann versendet er es mittels BGP durch die DFZ.

6. Routing des Paketes auf Basis der RLOC durch die DFZ.

7. Ankunft des Paketes am ETR, dieser entpackt das Paket aus dem LISP Header und routet es intern mittels BGP weiter.

8. Versand des Paketes an EID '111.111.111.11' mittels BGP in AS_2.

9. Ankunft des Paketes beim Host.

Wichtig ist, dass LISP sowohl für die DFZ-Router, als auch die Router der Autonomen Systeme der Endpunkte, transparent ist. Es fügt lediglich einen Kapselungsvorgang hinzu. Die Pakete sind für die Router weiterhin IP-Pakete und werden auch weiterhin mittels BGP geroutet. Der für die Kapselung zuständige Prozess ist in großem Maße von der Beschaffung des Mappings abhängig, dem Mapping-System. Dieses Mapping-System, das eine ähnliche Funktionsweise wie das Domain Name System (DNS) für Hostnamen aufweist, wird im Folgenden beschrieben.

2.2 Das Map Server Interface (LISP-MS)

Das LISP-Mapping-System verwaltet die Zuordnung von EID zu RLOC und gibt diese Informationen an Router weiter. Ein möglicher Grundaufbau ist in [18] definiert. Der LISP-Mapping-Server wird dort als ein Rechensystem beschrieben, das ein einfaches LISP-Protkollinterface als Frontend der Endpoint-ID (EID) für Routing Locator (RLOC) Datenbank zur Verfügung stellt. Der Sinn und Zweck des LISP-MS ist die Vereinfachung der Umsetzung und des Betriebs der Ingress Tunnel Router (ITR) und Egress Tunnel Router (ETR), d.h. jener Systeme die den Zugang zum LISP-Netzwerk bilden [vergl. 18, Kapitel 1]. Diese Vereinfachung wird dadurch erreicht, dass LISP-MS die Aufgabe übernimmt, für eine mittels Map-Request angefragte EID, die zugehörigen ETR-RLOC (Mapping) zu suchen und das Ergebnis in einem Map-Reply zurückzugeben. Diese Information entnimmt das System einer Datenbank. Einige Beispiele für den Aufbau und die Funktionsweise werden in Abschnitt 2.2 näher beleuchtet. Zusätzlich werden, nach Erhalt des Map-Reply weitere Informationen bei einer der RLOC des Mappings erfragt. Dazu gehören z.B. Erreichbarkeit einer oder mehrerer RLOC aus dem Mapping, Präferenz einer RLOC für den fragenden ITR, etc.

Es werden zwei unterschiedliche Arbeitsaufgaben des LISP-Mapping-Systems unterschieden: Die des Mapping-Resolvers (MR) und die des Mapping-Servers (MS). Dabei kann ein Gerät beide Aufgaben übernehmen. Je nach Mapping-System, werden die Zuordnungen dann entweder bei Registrierung einer EID zu RLOC an einen MS übertragen (ein sogenanntes *push* Verfahren) oder es wird, wenn benötigt, vom MS der betreffende ETR befragt (*pull* Verfahren). Einige Mapping-Systeme verwenden sogar beides.

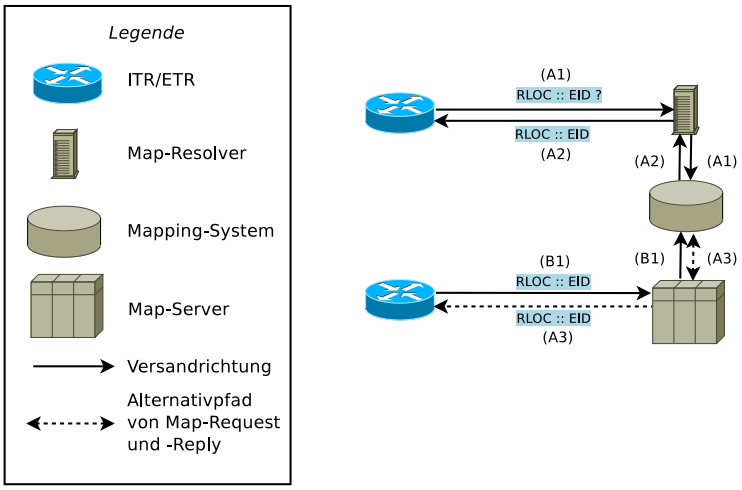

Abbildung 2: Mapping-Resolver und Mapping-Server des LISP-MS

MR sind die Teile der LISP-Infrastruktur, die einen Map-Request nach einem Mapping von einem ITR entgegen nehmen, wie in Abbildung 2 (A1) zu sehen ist [vergl. 18, Kapitel 4]. Liegt der angeforderte Datensatz vor, wird das Mapping an den ITR zurück gegeben (A2). Im Falle, dass der Datensatz nicht vorliegt, wird eine Antwort mit leerer RLOC-Adresse zurückgegeben, um dem ITR den Fehlschlag zu signalisieren (Negativeintrag). Je nach Art des verwendeten Mapping-Systems, kann der Map-Request auch an den MS oder ETR verschickt und von diesem beantwortet werden (A3).

MS nehmen die Datensätze für die Mappings von ETR an und tragen sie in die Datenbank des Mapping-Systems ein (B1). Ein Mapping ist dabei nicht zwingend statisch. Wechselt ein EID-Präfix-Inhaber seinen ETR, können sich auch die zugehörigen RLOC ändern. Man spricht dann von *Präfixmigration*. Außerdem leiten MS in einigen Datenbankumsetzungen Map-Requests an den für die EID zuständigen ETR weiter (A3).

Das Konzept des LISP-MS ähnelt stark dem DNS [39], indem es als Verzeichnis für RLOC dient. Es teilt sich auch einige der Anforderungen mit ihm, bringt aber auch eigene aus seiner Verbindung zu LISP, als Teil der Protokolle des Internets der Zukunft, mit[17]:

Skalierbarkeit ist eine Grundanforderung an zukünftige Internetsysteme, an LISP und gilt auch für das Mapping-System. Die Wichtigkeit dieser Bedingung wird klar, wenn man in Betracht zieht, dass pro Verbindungsaufbau mit einem, dem ITR unbekannten, EID-Präfix, eine Nachfrage notwendig ist. Auch bei Präfixmigrationen ist eine Folge von Updates des Mappings unabdingbar.

Caching verbessert die Skalierbarkeit. Ein Verzeichnis ohne Caching muss jede Anfrage komplett neu bearbeiten, was zu Verzögerungen im Ablauf führen kann. Daher sollte ein Mapping-System Inhalte zwischenspeichern können [28].

Sicherheit , d.h. Vertraulichkeit, Verfügbarkeit und Integrität, um beispielsweise ein Hijacking einer oder mehrerer EID-Präfixe durch einen ETR zu verhindern.

Mobility , d.h. bei wechselnden Verbindungspunkten die Möglichkeit, die zur EID gehörige RLOC zu wechseln und diese Information im Mapping-System zeitnah und effizient zu aktualisieren.

Es folgt eine Übersicht über einige Mapping-Systeme, die im Verlauf dieser Arbeit untersucht wurden. Dabei wird kurz auf das Grundkonzept des jeweiligen Systems eingegangen, gefolgt von einer Erläuterung, wie diese Idee umgesetzt wurde. Der Fokus liegt auf der Frage, wer mit wem kommuniziert und wie die Zuordnung von EID zu RLOC stattfindet. Die Mapping-Systeme sind im Einzelnen: LISP-ALT, LISP-NERD, LISP-CONS, LISP-DHT und LISP-TREE.

2.2.1 LISP Alternative Logical Topology (LISP-ALT)

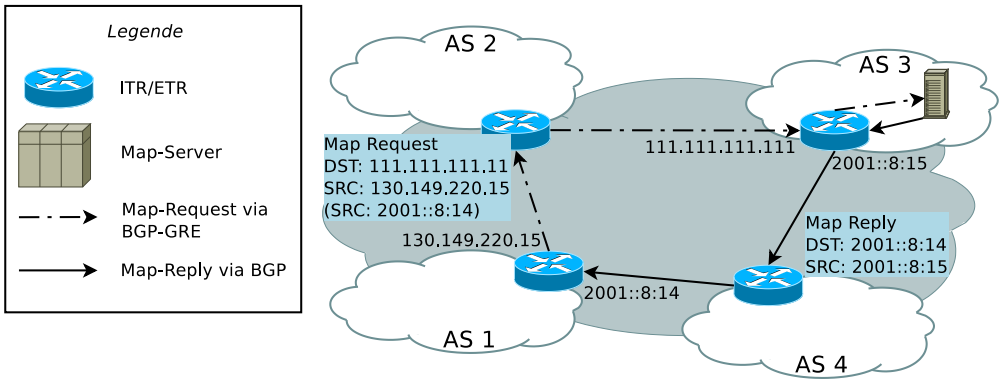

Abbildung 3: Das LISP-ALT Mapping-System

Die Kernidee von LISP-ALT [19] ist ein Overlay-Netzwerk von LISP-Routern, die Pakete mit EID als Zieladresse routen. Abbildung 3 (1) [vergl. 37] zeigt einen Map-Request für den EID des Zielrechners. Er enthält zusätzlich die RLOC des ITR oder MR und die ursprünglichen Absender- und Empfängeradressen [vergl. 19, Kapitel 4] [vergl. 7, Kapitel 4.5.2].

Der Map-Request wird durch BGP-General-Routing-Encapsulation-Tunnel (BGP-GRE-Tunnel) [16] übertragen. Diese Tunnel dienen einzig dazu, Map-Requests von einem anfragenden ITR zu einem ETR oder MS zu transportieren. Sie bilden das Anfangs erwähnte Overlay-Netzwerk.

Im Regelfall wird ein ITR die Anfrage nicht direkt an den ETR stellen, sondern seinen Map-Request an einen MR verschicken. Dieser verschickt dann den Map-Request, wenn er kein lokales, gültiges Mapping hat. Dazu nutzt er das Overlay und schickt den Map-Request an einen MS, bei dem sich der zuständige ETR registriert hat. Hier wird sowohl ein Pull-, als auch ein Push-Verfahren vorgeschlagen, um so viel Last wie möglich von den Pakete routenden Instanzen zu nehmen.

Der Map-Reply wird dann auf herkömmlichem Weg, ohne das Overlay-Netzwerk, an den RLOC des MR oder ITR geroutet. In Abbildung 3 (2) wird beispielhaft diese Antwort, mit RLOC des sendenden ETR und des ITR als Ziel, gezeigt. Man beachte, dass der Map-Request an einen EID geht, d.h. das Overlay-Netzwerk routet auf EID bzw. deren aggregierten EID-Präfixen. Der Map-Reply geht an einen RLOC und wird nicht über das Overlay-Netzwerk geroutet. Alle folgenden Pakete an das gleiche Ziel können direkt in ein LISP-Paket mit zugehörigem RLOC gepackt und durch die DFZ geroutet werden.

In LISP-ALT wird viel Wert darauf gelegt, dass das Overlay-Netzwerk topologisch so organisiert ist, dass viele EID-Präfixe aggregiert werden können. Dieser Aufbau soll durch die nahezu statische Struktur des Overlay-Netzwerks ermöglicht werden. Durch die hierarchische Topologie soll das Routing der Map-Requests so schnell und die Routing-Tabellen der ALT-Router so klein wie möglich gehalten werden.

LISP-ALT ermöglicht durch die Verwendung von BGP-GRE eine inkrementelle Migration des bestehenden Routing-Systems zu LISP. Vorteilhaft für dieses Mapping-System ist außerdem die Unterstützung durch die IETF und CISCO, die die Entwicklung eines Prototypen beschleunigt hat.

Da die BGP-GRE-Tunnel alle durch explizite Verbindung zwischen zwei Routern entstehen, erfordert es allerdings ein hohes Maß an Organisation für die Einrichtung neuer Tunnel. Hinzu kommt, dass die Zwischenspeicherung von Datenpaketen vor Erwerb des Mappings einen nicht zu vernachlässigenden Aufwand verursacht, der noch nicht hinreichend erforscht ist. LISP-ALT benötigt auch weiterhin, innerhalb seines Tunnelnetzwerks, Routen für jeden EID-Präfix. Inwiefern die geplante, hierarchische Struktur tatsächlich anwendbar und die Aggregation der EID-Präfixe möglich ist, ist ebenfalls noch nicht durch Forschung ermittelt. Aus der Betrachtung unter Sicherheitsaspekten (Kapitel 2.3.2), ergibt sich außerdem eine Reihe von möglichen Problemen. Durch den nahezu ungesicherten Versand des Map-Request über mehrere, verwundbare Hops, ist das Mapping-System zum Beispiel anfällig für Falschinformationen.

2.2.2 Not so Novel EID to RLOC Database (NERD)

Die NERD [34] ist eine Mapping-Datenbank, die im Pull-Verfahren auf alle ITR verteilt wird. Hierbei werden von den Erfindern unterschiedliche Bereitstellungsautoritäten vorgeschlagen. Beispielsweise ein auf Basis der Regional Internet Registries (RIRs), flacher, hierarchischer Aufbau der Server, die die Datenbank bereit stellen. Da ITR nur einmalig, bei Verbindungsaufbau zur NERD, die gesamte Datenbank via HTTP herunterladen müssen und danach lediglich die Änderungen, sind hier nur Map-Requests zwischen ITR

und ETR notwendig, um die Zusatzinformationen zu erfragen.

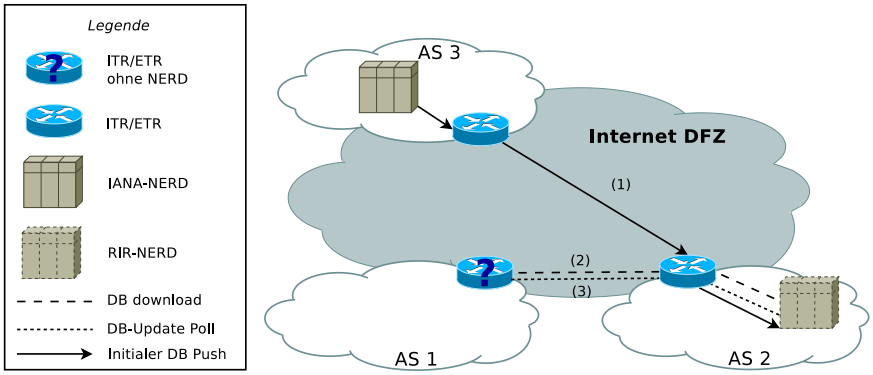

Abbildung 4: Das NERD Mapping-System, eine vollständige Kopie für jeden MS

Der Kommunikationsablauf in NERD sieht vor, dass eine vertrauenswürdige Stelle, z.B. die IANA, die NERD generiert und kryptographisch signiert. Diese Datenbank wird dann an öffentlich zugänglicher Stelle zusammen mit dem öffentlichen Schlüssel eines X509-Zertifikats [12], bereitstellt. Die Stelle kann eine Reihe von bekannten Servern sein, die z.B. von den RIRs betrieben werden, wie Abbildung 4 zeigt. Ein ITR lädt bei Inbetriebnahme die Datenbank anhand einer vorkonfigurierten Liste von global routebaren EID-Adressen, dieser Server herunter (1). Er verifiziert ihre Signatur, mittels des öffentlichen Zertifikats der vertrauenswürdigen Instanz. Bei Erfolg werden die Daten gespeichert und stehen fortan als Quelle der Mappings zur Verfügung.

Wird in Zukunft ein Update der Datenbank durchgeführt, stellt die vertrauenswürdige Instanz sowohl die neue Datenbank, als auch die Änderungen, mit zugehöriger Signatur, zur Verfügung. Diese wird dann per Push-Verfahren auf alle NERD-Server verteilt (2). Die ITR erfahren von diesen Updates mittels Polling (3). Sie laden diese dann herunter, verifizieren und speichern sie bei Erfolg.

Dieser Ansatz ist aus mehreren Gründen problematisch. Zum einen gibt es bereits Daten aus der Erforschung des BGP, die belegen, dass das Herunterladen von kompletten Datenbanken zu erheblichen Beeinträchtigungen der Verfügbarkeit führen kann [5].

Zum anderen kann der zentralistische Aufbau zu Problemen bei der Verfügbarkeit des Mapping-Systems führen. Ist die Datenbank bei einem RIR nicht erreichbar, kann das schnell den Ausfall des Mapping-Systems für einen ganzen Bereich der DFZ bedeuten.

Hinzu kommt, dass NERD zwar die Mapping-Datenbank signiert, die Erreichbarkeit und andere Informationen über die ETR, müssen aber weiterhin ungesichert über das Netz erfragt werden.

2.2.3 The Content distribution Overlay Network Service (LISP-CONS)

In dieser Variante eines Mapping-Systems orientieren sich die Autoren von LISP-CONS [8] am Aufbau von Content Distribution Networks (CDN) und empfehlen, die MR und

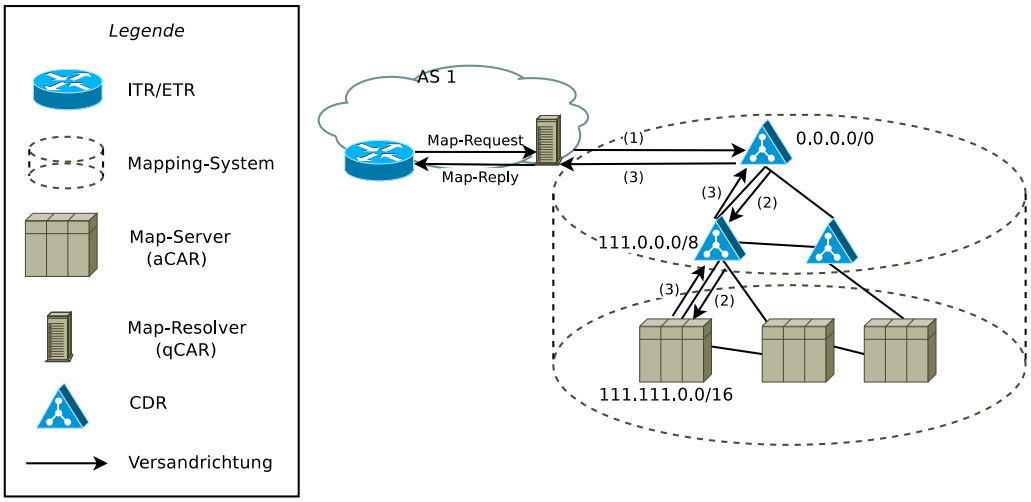

Abbildung 5: LISP-CONS, ein baumartiges Mapping-System

MS (querying Content Access Ressource, kurz CAR und answering CAR in LISP-CONS) an ein Netzwerk von Content Distribution Routern (CDR) anzuschließen. Diese werden nach aggregierten EID-Präfixen hierarchisch verbunden und bilden so einen hierarchischen Baum. Es sind allerdings auch Verbindungen zwischen Knoten auf der gleichen Hierarchiebene erlaubt. Dadurch wird erreicht, dass bei Ausfall eines Knotens Nachrichten umgeleitet und trotzdem zum Ziel gelangen können.

Bei Mapping-Requests, siehe Abbildung 5, werden diese vom MR (1), durch den Baum und über die CDR weitergeleitet (2). Dabei versenden die CDR den Map-Request immer an den untergeordneten Knoten, der für den angefragten EID-Präfix zuständig ist. Erreicht der Map-Requests einen MS, antwortet dieser mit einem Map-Reply, der erneut durch den Baum zum Anfragenden zurückgeroutet wird (3).

LISP-CONS unterscheidet dabei klar zwischen CDR, die nur Routen zu MS untereinander austauschen und den MS selbst, die die eigentlichen Mapping-Informationen besitzen. Die einzelnen Knoten des Baums, MS und CDR, sind dabei durch statisch konfigurierte Verbindungen mit einander verknüpft. Ein MS ist also immer mit dem für seine EID-Präfixe zuständigen CDR verbunden, der wiederum die EID-Präfixe seiner verbundenen MS und CDR aggregiert. Diese Routing-Informationen leitet er dann an die CDR auf der gleichen und darüber liegenden Hierarchieebene weiter.

Die Funktionsweise erinnert an einen rekursiven DNS-Lookup und macht damit sowohl einen der wesentlichen Vor- als auch Nachteile von LISP-CONS sichtbar. Durch den hierarchischen Baum kann das Mapping-System skalieren, hat aber auch den Nachteil, dass alle Anfragen von der Wurzel zu den Blättern und zurück geleitet werden müssen. Die dabei anfallenden, zu speichernden Daten können zu einem Lastproblem führen.

Unter Sicherheitsaspekten wirkt die Weiterleitung, von sowohl Map-Request als auch Map-Reply durch den gesamten Baum, ohne Schutz der Datenintegrität, fragwürdig.

2.2.4 Distributed Hashtables (LISP-DHT)

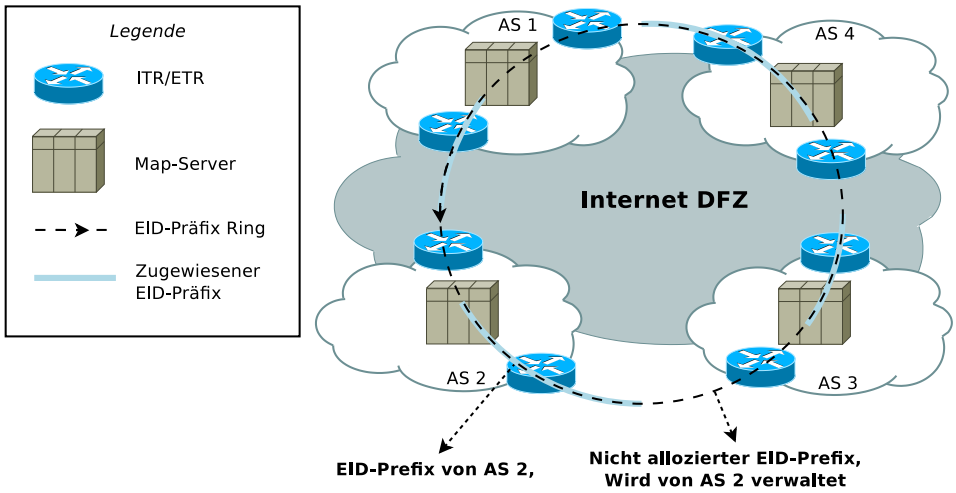

Abbildung 6: LISP-DHT, ein Mapping-System mit Distributed Hashtables [vergl. 37]

In LISP-DHT [37] wird der Vorschlag unterbreitet, ein Mapping-System mit einer modifizierten CHORD-DHT aufzubauen [45]. Die Vorteile sind die weitestgehende Selbstkonfiguration, Robustheit und Skalierbarkeit sowie ein verringerter Wartungsaufwand [3] der Mapping-Server. Hinzu kommt, dass DHTs bei Suchen nach bekannten Schlüsseln, einen sehr niedrigen Suchaufwand haben und so zeitnahe Antworten für Map-Requests ermöglichen.

In diesem speziellen Fall wird vorgeschlagen, eine abgewandelte Version von CHORD zu nutzen, bei der die Randomisierung der Zuständigkeit für einzelne IDs entfernt wurde. Somit ergibt sich ein Ring aus EIDn über den EID-Namensraum und Servern die für zusammenhängende Teilbereiche des Rings zuständig sind. Jeder Server hält sowohl die Adresse seines Vorgängers, als auch seines Nachfolgers im EID-Namensraum. Zusätzlich speichert er eine Reihe von Zeigern auf weiter entfernte Server. Im Falle, dass eine Anfrage für eine EID eintrifft, für die der Server nicht zuständig ist, wird diese an den nächst zuständigen Server weitergeleitet.

Ein ITR schickt zum Beispiel einen Map-Request an seinen Map-Resolver, der Teil des DHT sein kann oder einen Server im DHT kennt. Dieser schickt den Map-Request an den Server im DHT, der für die angefragte EID zuständig ist. Ist ein solcher nicht bekannt, wird die Anfrage an einen Server versendet, dessen EID-Zuständigkeit näher an dem angefragten EID liegt. Hat der Map-Request den zuständigen Server erreicht, kann dieser per Hash über die EID in seiner Datenbank die RLOC ermitteln. Die Antwort wird dann direkt an den anfragenden MR oder ITR zurückgesendet.

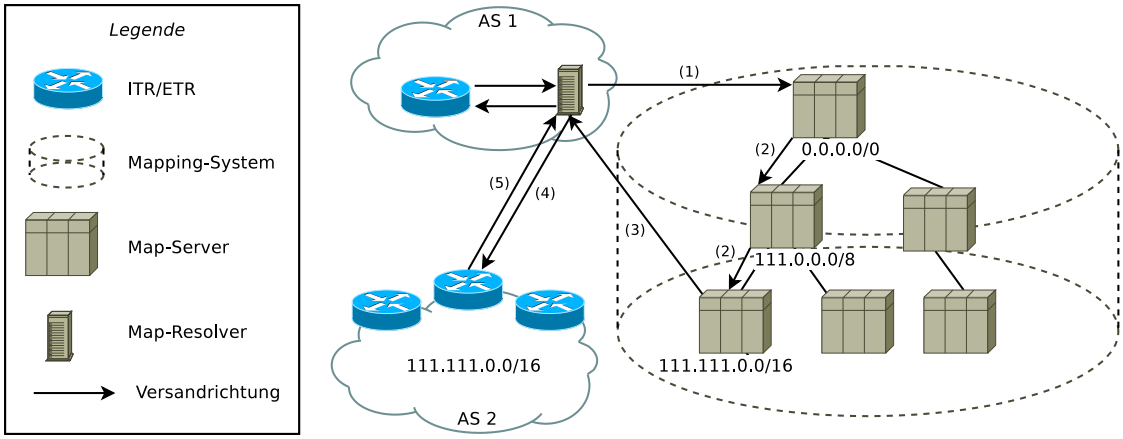

Abbildung 7: LISP Tree mit rekursivem Map-Request

2.2.5 A DNS Hierarchy (LISP Tree)

LISP Tree [27] verfolgt die Idee, dass ein Mapping-System dem bereits verwendeten DNS nicht unähnlich ist. Deshalb wird vorgeschlagen, eine hierarchische Struktur von MS zu schaffen und die Map-Requests zu teilen. Die Hierarchie wird durch die Aggregation von EID-Präfixen nach den momentanen IP-Adressvergaberichtlinien geschaffen.

Der Map-Request, nach den RLOCs der für die EID zuständigen ETR, wird an den Kopfknoten des Mapping-Systems geschickt (Discovery Phase). In Abb.2.2.5 (1) ist das zu sehen. Der Map-Request wird dann an den MS delegiert, der für den zugehörigen EID-Präfix zuständig ist (2). Dies wird fortgeführt, bis der entgültig zuständige MS gefunden wurde (d.h. keine Delegation mehr vorliegt). Dieser schickt dann die RLOCs der ETR an MR oder ITR (3). Ein zweiter Map-Request wird dann direkt an den oder die zuständigen ETR verschickt (4) und beantwortet (5) (Mapping-Phase).

Im Gegensatz zu LISP-CONS wird hier nicht direkt die RLOC zum Versand der Daten zurückgeschickt und für den Paketversand genutzt, sondern dient als Information über die RLOC der für die EID autoritativen Datenbank. Vorteilhaft ist auch die gute Skalierbarkeit, da zusätzliche EID-Präfixe lediglich einen Eintrag auf der Ebene oberhalb der MS verlangen. Ein neuer MS würde dann unterhalb des zuständigen Knotens im Mapping-System angebunden. Alternativ bestünde die Möglichkeit, einem bereits bestehenden MS auch die Zuständigkeit für den neuen EID-Präfix zuzuweisen.

Die rekursive Weiterleitung der Map-Requests kann allerdings zu einem Lastproblem führen. Ein iterativer Ansatz, wie er im heutigen DNS häufig verfolgt wird, kann hier eine bessere Lastverteilung bewirken. Zusätzlich ist auch hier die Frage, wie ein EID seine zugehörige RLOC wechselt, nicht geklärt.

2.2.6 Tabellarische Übersicht der Mapping-Systeme

Diese Übersicht ist eine Zusammenfassung der Kapitel 2.2.1 bis 2.2.5. Die Zeile Topologie beschreibt den groben, topologischen Aufbau des Mapping-Systems. Funktionalität beschreibt die Kernidee, nach der das Mapping-System arbeitet – meist ähnlich funktionierende Verzeichnis- oder Datenbanksysteme, an die das Mapping-System angelehnt ist. Unter Merkmal steht eine herausragendes Besonderheit, um das Mapping-Systems zusätzlich zu charakterisieren.

	Topologie	Funktionalität	Besonderheiten
LISP-ALT	Vermaschtes-Netz	VPN-Tunnel	EID für Map-Request, RLOC für Map-Reply
LISP-NERD	Stern	Client-Server	Zentral Signierte Datenbank
LISP-CONS	Ringerweiterter k-Baum	CDN	Integrierte Redundanz
LISP-DHT	Ring	DHT	Signierte Map-Replies
LISP-Tree	k-Baum	DNS	Doppelter Map-Request benötigt

Tabelle 1: Mapping-Systeme, ihre Topologie und Funktionalität

2.3 Verwundbarkeiten des Routings und Mappings

Die im letzten Abschnitt vorgestellten Mapping-Systeme übernehmen lediglich die Aufgabe der Zuordnung von zuständiger RLOC für angefragte EID. Sie beschäftigen sich aber nur teilweise mit der Sicherheit dieses Dienstes. Häufig waren Sicherheitsanforderungen nicht einmal Teil der Designkriterien der Mapping-Systeme oder wurden erst nachträglich hinzugefügt.

Kritisch ist auch, dass LISP und seine Mapping-Systeme auf BGP basieren [42]. Dieses hat sich in der Vergangenheit ebenfalls als verwundbar herausgestellt. Sogar die zugrunde liegenden Protokolle der Transport- und Internet-Schicht sind angreifbar, allerdings ist die Betrachtung ihrer Verwundbarkeiten nicht Bestandteil dieser Arbeit.

Da kritische Infrastruktur des Internets mit LISP betrieben werden soll, würden das Ausnutzen dieser Verwundbarkeiten zu ernsten Problemen führen. Zum Beispiel hätte ein Ausfall einer oder mehrerer BGP-Verbindungen automatisch auch einen Ausfall des darauf basierenden Teils von LISP zur Folge. Das wäre gleichbedeutend mit der Unerreichbarkeit aller Dienste im betroffenen Netz, wie etwa in Ägypten 2011 [32]. Wird BGP hingegen genutzt, um Traffic umzuleiten, kann das zu Sicherheits- und auch Performanceproblemen führen. Als Beispiel sei auf das Hijacking von etwa 15% der weltweiten Routen im April 2010 [33], durch mutmaßlich chinesische Hacker, verwiesen.

Ein Angreifer könnte auch darauf abzielen, das Routing „nur “ zu stören. Die Umleitung oder Fälschung der Mapping-Informationen ist ebenfalls möglich. Dies zu vermei-

den, ist für den Betrieb eines Mapping-Systems immanent wichtig. Ein effektiver Schutz ist deshalb im Interesse von Netzbetreibern und Nutzern.

Um effektive Schutzmaßnahmen ergreifen zu können, gibt es eine Vielzahl von Analysen und Untersuchungen zu Schwachstellen und Verwundbarkeiten im Routing [9, 10, 11, 31, 43, 50]. Allerdings wurde bisher keine genauere Analyse der Auswirkungen von Angriffen auf eines der Protokolle, durch Angriffe auf das andere, durchgeführt.

Der folgende Abschnitt stellt zunächst die wichtigen Aspekte der Netzwerksicherheit vor. Im Anschluss darauf wird auf eine Auswahl häufiger Anfälligkeiten des BGP und LISP-MS eingegangen. Die Betrachtung der Verwundbarkeiten der Mapping-Systeme, nicht der transportierten Anwendungsdaten, steht dabei im Vordergrund.

2.3.1 Aspekte der Netzwerksicherheit im Routing

Die Netzwerksicherheit im Routing teilt sich in drei Hauptziele auf [6].

Integrität bezieht sich auf das Vertrauen in die Korrektheit von Daten oder Komponenten. Dabei lässt sich Datenintegrität von Quellenintegrität, die auch oft Authentifizierung genannt wird, unterscheiden.

Die *Datenintegrität*, oder Korrektheit der versandten Daten, ist im Routing von besonderer Wichtigkeit. Um die Verfügbarkeit sowie die Verwendung der richtigen Pfade zu gewährleisten, muss das System resistent gegen Fehl- und Falschinformationen sein. Ist die Integrität einer Nachricht nicht prüfbar, ist es möglich, Informationen zu entfernen, unleserlich zu machen oder sogar zu verändern. Auf diese Weise können Daten gefälscht und zum Beispiel die Zuordnung einer RLOC zu einem EID-Präfix verhindert oder der Datenverkehr umgeleitet werden.

Quellenintegrität stellt sicher, dass nur authentifizierte und autorisierte Quellen Zugriff auf Daten haben, beziehungsweise diese verändern können. Dazu gehören Methoden zur vertrauenswürdigen Identifikation, um anschließend die Autorisierung der Quelle überprüfen zu können. Ein MR sollte z.B. nur Zuordnungen für RLOC zu EID akzeptieren, wenn der versendende MS auch für den entsprechenden EID-Präfix autorisiert ist. Bei BGP hingegen besteht die Möglichkeit, die Identität eines Peers mittels eines gemeinsamen Geheimnisses, zu prüfen.

Verfügbarkeit ist das wichtigste Ziel im Routing. Ist das Routing-System oder Teile von ihm nicht verfügbar, gelangen Daten nicht an ihren Bestimmungsort, bzw. das zugehörige Netzwerk ist nicht erreichbar. Aus diesem Grund muss es integraler Bestandteil eines Routing-Protokolls sein, diese Verfügbarkeit zu gewährleisten. Insbesondere der Umgang mit Teilausfällen und Überlastungen von Verbindungen, steht hier im Zentrum der Aufmerksamkeit. Redundante Server, Traffic-Limitierung aufgrund der Quelle oder verdächtigen Verhaltens, oder auch Umleitung von Traffic über alternative Routen, stellen Methoden dar, wie Verfügbarkeit gewährleistet werden kann.

Vertraulichkeit ist bisher ein weniger wichtiges Ziel im Routing. Für die reine Funktion der Verbindungsherstellung und des Weiterleitens von Paketen, ist die Geheimhal-

tung des Inhalts irrelevant. Im Gegenteil, je mehr Informationen zur Verfügung stehen, um so effektiver kann das System arbeiten.

Anforderungen an die Vertraulichkeit kommen meist von den Nutzern des Netzes, beziehungsweise von den Betreibern der Router. Dabei geht es vorrangig um den Schutz von Informationen über die Infrastruktur des Netzbetreibers, seine Richtlinien zur Verbindungsweitergabe im Inter-AS-Routing und Traffic-Shaping sowie Einzelheiten in der Umsetzung von Geschäftsvereinbarungen zwischen Netzbetreibern.

Lässt sich Integrität und Verfügbarkeit nicht erreichen oder gelingt es einem Angreifer die Mechanismen zu ihrer Umsetzung zu umgehen, kann dies schwere Folgen nach sich ziehen. Eine Auswahl und einige der Möglichkeiten, um Verwundbarkeiten von BGP und LISP-MS diesbezüglich auszunutzen, werden im nächsten Abschnitt erklärt. Methoden, um die Sicherheit zu verbessern und Angriffe zu verhindern, sind in Kapitel 3 erläutert.

2.3.2 Angriffe auf die Netzwerksicherheit

Matt Bishop [6] unterteilt Bedrohungen auf die genannten Sicherheitsziele in in mehrere Klassen, die wichtigsten drei sind: „. . . disclosure, or unauthorized access to information; deception, or acceptance of false data; disruption, or interruption or prevention of correct operation; and usurpation, or unauthorized control of some part of a system.“.

Die Folgen einer angewandten Bedrohung, das heißt eines Angriffs auf BGP oder LISP-MS, können anhand dieser Klassen zu Angriffszielen gruppiert werden. Jede Gruppe erfordert unterschiedliche Angriffsmethoden, die spezifisch für das angegriffene Protokoll sind. Im Zentrum der Betrachtung stehen dabei vor allem Angriffe auf das LISP-MS, beziehungsweise Angriffe auf das BGP, die Folgen für das Mapping-System haben. Dies ist eine kurze Liste der drei häufigsten Angriffsziele, Blackholing, Umleitung und Instabilität und ihrer Folgen:

Blackholing bezeichnet den Verlust von Daten, bevor sie ihr Ziel erreichen. Es entspricht der eingangs aufgezählten Bedrohung durch „disruption“. Angriffe haben deshalb häufig zum Ziel, Verbindungen zu unterbrechen oder Daten zu einem Ziel umzuleiten. Gelingt dies, kann das zum vollständigen Verbindungsausfall zu einem Teilnehmer oder Teilen des Netzes führen.

Eine Variante des Blackholing ist das sogenannte Greyholing, bei dem nur ausgewählte Daten weitergeleitet werden. Dies dient zum Beispiel dazu, den Eindruck einer funktionierenden Verbindung zu erwecken. Auf diese Weise lassen sich etwa bestimmte Inhalte filtern.

Dieses Angriffsziel lässt sich bei Verwendung von BGP erreichen, indem beispielsweise eine Verbindung zwischen zwei Routern übernommen wird. Ein Angreifer benötigt dazu die Möglichkeit, Pakete direkt an einen Router zu schicken. Gelingt es ihm dann etwa, die MD5-Authentifizierung der Router zu kompromittieren, kann er sich für den jeweils Anderen ausgeben und so unbemerkt eine authentifizierte Verbindung zu Beiden aufbauen [11]. Da er dann im Namen des Routers

agiert, dessen Identität er angenommen hat, kann er dessen Routen zurückziehen. Die Folge kann die Unerreichbarkeit aller IP-Präfixe sein, die von diesem Router aus erreicht werden konnten.

Weitere Angriffe sind zum Beispiel, die Herstellung einer unautorisierten Verbindung zu einem BGP-Router mit anschließendem Einfügen eines unautorisierten IP-Präfixes in dessen Routing-Tabelle oder die Änderung der Pfad-Priorität eines IP-Präfixes. Auch das Ausführen einer Denial-of-Service Attacke mittels einer Flut von BGP-UPDATES, um eine Verbindung zu unterbrechen ist möglich. Das Spoofen der Absenderadresse in einer BGP-UPDATE Nachricht, um falsche Informationen in einen Router einzuspeisen ist ebenfalls ein Angriff, der Blackholing bewirken kann. Wird die AS-Nummer des angegriffenen Systems zum AS-PATH eines BGP-UPDATEs hinzugefügt, kann das auch zu Blackholing führen [9].

Alle LISP-MS sind dadurch ebenfalls verwundbar [43], da zugehörige MS auf diese Weise unerreichbar gemacht werden können. Auch ist es möglich, alle Map-Replies oder nur bestimmte verschwinden zu lassen. Auf diese Weise ließen sich ausgewählte RLOCs unerreichbar machen. Map-Replies, die zu nicht belegten RLOCs oder RLOCs, die für eine EID nicht zuständig sind, zeigen, führen ebenfalls zu Datenverlusten. Auch negative Map-Replies können das bewirken. Hinzu kommen Möglichkeiten, das Traffic-Engineering eines ETR, mittels der Zusatzinformationen in einem Map-Reply, auszuhebeln. Ein Paket eines ITR an den ETR kann dann in der falschen Forwardtable landen und ebenfalls verloren gehen. Auch möglich ist es, die Erreichbarkeit von RLOC in einem Map-Reply zu manipulieren. Setzt man die Werte der Erreichbarkeit für alle RLOC auf Null, geht der empfangende ITR davon aus, dass zur Zeit keiner davon erreichbar ist. Hinzu kommen Denial-of-Service Angriffe, z.B. in Form von massenhaften Map-Requests oder indem durch Map-Replies mit gefälschter Absenderadresse andere ITRs dazu animiert werden, den ETR zu „(D)DOSen“.

Umleitung kann dazu führen, dass Daten ihr Ziel nicht erreichen. Das entspricht der Bedrohung durch „usurpation“ oder „deception“. Je nach Verwendung kann der Angriff auch zum Blackholing genutzt werden. Angriffe die Umleitungen bewirken, können dem Zweck der Vorbereitung weiterer Angriffe dienen. Darunter sind unter Anderem Denial-of-Service Angriffe, das Abhören vertraulicher Daten, das Einrichten eines Man-in-the-Middle, um verschlüsselte Verbindungen zu umgehen oder das Einspeisen von Falschinformationen zu ermöglichen. Ein weiter Verwendungszweck ist außerdem das transparente Umschalten auf redundante Hardware beim Ausfall von (Routing-)Komponenten.

Um eine Umleitung vorzunehmen ist es notwendig, entweder Teile des Systems zu kontrollieren oder aber zumindest in der Lage zu sein, Falschinformationen einzuspeisen.

Im Kontext von BGP trifft man dieses Phänomen meist unter dem Begriff „Prefix hijacking“ an. Das Hijacking ist Folge von gefälschten BGP-UPDATE Nachrichten oder fehlerhafter IP-Präfix-Aggregation [31].

LISP-Mapping-Systeme sind ebenfalls für Umleitungen anfällig, wenn keine Überprüfung der Informationen in einem Map-Reply erfolgt oder möglich ist. Auf diese Weise kann ein Angreifer eine RLOC für eine EID angeben, die zu einem von ihm kontrollierten Router gehört.

Instabilität beeinflusst die Geschwindigkeit und Zuverlässigkeit des Routings. Dieses Angriffsziel dient meist dem Zweck der „disruption“. Das kann dazu führen, dass beispielsweise bestimmte Komponenten nicht oder schwer erreichbar sind. Bei häufigem Ausfall oder Unzuverlässigkeit einer Route kann dies auch eine Umleitung über alternative Routen zur Folge haben.

Instabilität lässt sich unter Anderem durch zeitweise Überlastung von Verbindungen oder Einzelkomponenten des Systems erreichen. Fehlerhafte Informationen oder Angriffe die nur kurzfristige Blackholes bewirken können dazu ebenfalls genutzt werden.

Zu Instabilitäten bei BGP kann es zum Beispiel kommen, wenn eine Route zu einem IP-Präfix von mehreren ASs ausgeht. Man spricht in diesem Zusammenhang von „Multiple Origin Autonomous System (MOAS) conflict“ [10]. Ein Angreifer kann das bewirken, indem er BGP-UPDATE Nachrichten fälscht oder verändert, indem er beispielsweise eine existierende Route zurückzieht. Alternativ kann er sich selbst als BGP-Router eines AS ausgeben oder dessen Verbindung zu einem anderen AS-Router übernehmen. Auch das Blockieren einiger oder aller BGP-UPDATEs für einen kurzen Zeitraum, kann zu Instabilitäten bei der Verwendung von BGP führen [31]. Indem ein Angreifer eine Route in schnellen Abständen propagiert und dann wieder zurückzieht, kann er außerdem den „Route dampening algorithm“von BGP einschalten [9].

Diese Angriffe können zwar durch Sicherheitsmaßnahmen, wie die Authentifizierung und Autorisierung von Routern und Servern sowie Integritätsmechanismen zum Transportschutz der Daten, erschwert werden, wie die folgende Analyse zeigt. Dies wird aber bei keinem der LISP Mapping-Systeme vollständig angewendet:

LISP-ALT ist durch die meisten der genannten Angriffe verwundbar. Als statisch konfiguriertes Overlay, das auf BGP-GRE-Tunneln basiert, ist dieses MS gegen alle BGP-Angriffe verwundbar.

Das Mapping-System sieht keine Methoden zur Authentifizierung von MS, ITR oder ETR vor. Die Integrität der Daten wird nicht gesichert. Es gibt lediglich eine Checksum gegen unabsichtliche Übertragungsfehler. Auch die Autorität eines MS oder ETR, über den Inhalt der von ihm versendeten Map-Replies, wird nicht kontrolliert. Einzig die Nonce, die mit dem Map-Request verschickt wird, kann vor gefälschten Map-Replies schützen. Das funktioniert allerdings nur, wenn der Angreifer keine Kenntnis von dieser Nonce erhält, d.h. sich nicht auf dem Pfad des Map-Request befindet oder sie anderweitig errät (siehe TCP-Sequence-Number-Attack [4]). Befindet er sich auf dem Pfad oder errät die Nonce und ist in der Lage

Antwortpakete an den Absender des Map-Reuests zu schicken, kann er unbemerkt Map-Replies fälschen.

Auch wenn der Angreifer keine eigenen Map-Replies verschickt, schützt die Nonce nur vor Map-Replies, die nicht dieselbe Nonce enthalten. Ein manipuliertes Mapping, z.B. durch einen übernommenen Router auf dem Pfad des Pakets, fällt also nicht auf.

LISP-NERD ist anfällig für Blackholing und Instabilitätsangriffe. Zwar wird die Authentizität und Integrität der RLOC-Datenbank überprüft, aber die Erreichbarkeitsprüfung erfolgt trotzdem mittels eines Map-Requests an den zuständigen ETR. Die Autoren empfehlen, TLS [14] für diese Anfrage zu nutzen, allerdings ist das kein Bestandteil des Mapping-Systems.

Hier kann ein Angreifer also Antworten fälschen oder den Map-Request abfangen, solange er sich auf der Route befindet, die der Map-Request nimmt. Hinzu kommt, dass zwar die RLOC-Datenbank signiert ist, aber nicht definiert wurde, wie die Datenbank die Integrität neuer Einträge und ggf. die Autorisierung des Eintragenden überprüft. Ein Angreifer kann, sofern er Kontakt zur NERD bekommt, beliebige Mappings hinzufügen.

LISP-CONS schützt zwar durch den streng hierarchischen Aufbau vor dem Versenden von Map-Replies mit Einträgen, die nicht in den EID-Präfix gehören, zu dem ein jeweiliger Unterbaum gehört. Es verhindert aber nicht, dass zum Beispiel ein Router aus einem Ast unter einem Knoten, einen Map-Reply für EID eines anderen Astes, unterhalb dieses Knotens, verfasst.

Auch verifiziert ein MS oder ITR nicht, ob der Map-Reply, den er erhält, tatsächlich von dem zuständigen ETR kommt. Solange die enthaltene Nonce stimmt, wird das Mapping akzeptiert. Manipulierte Mappings fallen deshalb ebenfalls nicht auf. Aus diesem Grunde sind hier alle drei Angriffsziele erreichbar. Ein Angreifer kann zum Beispiel versuchen, einen MR mit einer Flut von Map-Replies zu „bombardieren“ bis die enthaltene Nonce mit der eines Map-Request übereinstimmt. Diesee Art Angriff ist aufgrund der Vielzahl an gesendeten Paketen noch erkennbar. Befindet sich der Angreifer aber sogar auf der Route des Map-Requests und ist in der Lage seine IP zu fälschen, kann er einen legitim erscheinenden Map-Reply versenden. Dann bleibt die Fälschung unbemerkt.

LISP-DHT macht Angriffe um einiges schwerer. Der kryptographische, zertifikatbasierte Schutz von EID-Präfixen stellt ihre Integrität sicher. Hinzu kommt, dass ein MS der dem LISPT-DHT beitreten will, zunächst seine Autoritativität, für den von ihm beanspruchten EID-Präfix Bereich, nachweisen muss. Durch den Aufbau der Map-Replies, die stets die Signatur des zur Zuordnung gehörigen Eigentümers enthalten, lassen sich diese praktisch kaum fälschen. Es ist zwar möglich, sich durch Wiedergabe belauschter Pakete (*Replay-Attack* [2, 46]) ebenfalls als autoritativer Teilnehmer auszugeben, die Einsatzmöglichkeiten sind aber begrenzt. Das liegt daran, dass eigenen Mapping-Informationen erzeugt werden können.

Trotzdem ist auch LISP-DHT anfällig gegen alle drei Angriffsarten (siehe auch [48] zu allgemeinen Verwundbarkeiten von DHTs). Sowohl Replay-Attacks als auch DOS-Angriffe können zur Unerreichbarkeit einer oder mehrerer RLOCs führen. Für ersteres muss der Angreifer allerdings ein valides Map-Reply-Paket erhalten und in der Lage sein, dieses auch wieder in die DHT zu verschicken.

Umleitungen sind ebenfalls möglich, allerdings nur begrenzt auf die Dauer der Gültigkeit eines erneut wiedergegebenen Pakets, bzw. des enthaltenen Zertifikats. Dazu muss ein Angreifer in der Lage sein, einen abgefangenen, noch gültigen Map-Reply, als Antwort auf einen passenden Map-Request zu versenden. Gelingt ihm das und hat sich das Mapping inzwischen geändert, kann Traffic vom ITR mit der falschen Zieladresse versehen werden.

Instabilitäten lassen sich vor allem durch (D)DOS-Angriffe hervorrufen, aber auch durch Manipulation der unsignierten Zusatzinformationen in einem Map-Reply, zum Beispiel der Erreichbarkeitsbits oder der Mapping-Version. Ein Angreifer muss sich dazu allerdings auf dem Pfad des Map-Reply befinden und in der Lage sein, das Original abzufangen. Dann kann er den Map-Reply verwerfen oder den Inhalt manipulieren.

Eine weitere Angriffsmöglichkeit bietet sich dadurch, dass ein Map-Reply zwar die Autoritativität für die EID bestätigt, nicht aber für die enthaltene RLOC. Dadurch kann ein MS Daten für seine EID, auf beliebige RLOC umleiten. Das setzt allerdings voraus, dass es einem Angreifer gelingt, einen MS zu übernehmen oder dass der Betreiber des MS selbst entsprechende Absichten verfolgt.

LISP-Tree sieht ebenfalls keine Authentifizierungs- oder Autorisierungsprüfungen vor. Zwar beschreiben die Autoren ein, nach EID-Präfixen hierarchisch aufgebautes Mapping-System, es wird aber nicht definiert, ob und wie sich die Server dieses Systems untereinander identifizieren.

Auch eine Überprüfung der versandten Informationen durch den ITR ist nicht vorgesehen. Dadurch kann ein MS zum Beispiel einen RLOC für einen EID weitergeben, der vom Angreifer kontrolliert wird. Dafür muss der Angreifer entweder den Map-Reply manipulieren, eine Antwort fälschen oder den MS übernehmen. In allen drei Fällen bietet LISP-Tree keine Mechanismen, um die Manipulation zu bemerken. Befragt der ITR anschließend diesen RLOC nach Mapping-Informationen, stehen dem Angreifer alle Türen zur Fälschung, RLOC- und EID-Präfix Hijacking, etc. offen.

Da auch nicht festgelegt wurde, wie ein Update dieser Datenbank erfolgt, besteht die Möglichkeit, dass ein Angreifer auch eine andere RLOC für einen EID-Präfix im Mapping-System anmeldet. Hinzu kommt, dass sowohl der Map-Reply, als auch die Antwort des ETR keinen Integritätsschutz aufweisen. Beide Nachrichten können also von einem Angreifer unbemerkt gefälscht, beziehungsweise verfälscht werden, sofern er sich auf der Route des Map-Reply befindet. Die Autoren von LISP-Tree empfehlen zwar den Einsatz von DNSSEC, stellen aber selbst keine weiteren Sicherungsmechanismen bereit.

Auffällig an allen Verwundbarkeiten ist, dass sie meistens erfordern, valide Mapping-Pakete verschicken zu können. Das heißt, sie erfordern, dass der Angreifer in der Lage ist, die Identität eines LISP-Routers anzunehmen, Pakete in die Kommunikation einzuschleusen oder im Transit befindliche Pakete zu manipulieren. Wendet ein Mapping-System Mechanismen an, um die Integrität und Authentizität von Daten zu gewährleisten, bzw. invalide Pakete zu erkennen, werden diese Angriffe wesentlich schwieriger bzw. einfacher bemerkbar. Der Schutz der Verfügbarkeit kann hingegen mit redundanten Komponenten erfolgen. So kann die Gefahr des Ausfalls durch einen (D)DOS-Angriff reduziert werden.

Die folgende Tabelle listet zur Übersichtlichkeit noch einmal die Berücksichtigung der Netzwerksicherheitsaspekte in den Spezifikationen der Mapping-Systeme auf. Dabei ist jede Spalte jeweils einem LISP-Mapping-System zugeordnet, die Zeilen zwei der drei Sicherheitsaspekte der Netzwerksicherheit. Die Vertraulichkeit wird deswegen nicht berücksichtigt, weil keine der Spezifikationen sie behandelt.

Die einzelnen Zellen enthalten ein kurzes Urteil darüber, wie stark der Aspekt in der Spezifikation des Mapping-Systems berücksichtigt wurde. Die Spanne reicht dabei von „+“, d.h. ein substantieller Teil des Protokolls berücksichtigt den entsprechenden Aspekt, über „0“und „-“bis zu „NA“. Letzteres bedeutet, die Spezifikation des Protokolls macht keine Angaben zu diesem Sicherheitsaspekt. Die anderen beiden Werte stellen eine unvollständige Anwesenheit oder großteilige Abwesenheit des Aspekts in der Spezifikation dar. Eine CRC-Prüfsumme zum Beispiel, stellt keine vollständige Integrität sicher (-), verschlüsselte Hash Message Authentication Codes (HMAC) hingegen schon (+).

	LISP-ALT	LISP-NERD	LISP-CONS	LISP-DHT	LISP-Tree
Integrität	−	+	+	+	−
Verfügbarkeit	−	NA	NA	+	NA

Tabelle 2: Netzwerksicherheit der LISP Mapping-Systeme

Das nächste Kapitel gibt einen Überblick über einige der prominenten Sicherheitssysteme für Routing und das, dem Mapping-System gar nicht so unähnliche, DNS. Insbesondere werden konzeptuell der Kommunikationsvorgang und der benötigte topologische Aufbau der Infrastruktur, unter Anwendung des Systems, erläutert. Es wird außerdem auf einige der Vor- und Nachteile eingegangen, die diese Systeme mit sich bringen.

3 Sicherungs- und Authentifizierungsverfahren

Da nun die Mapping-Systeme für LISP und einige ihrer Schwächen bekannt sind, setzt sich das folgende Kapitel mit möglichen Verteidigungsstrategien und deren Eigenschaften auseinander.

Diese Untersuchung ist sinnvoll, um zu erkennen, welche Systeme und Mechanismen gegen die Verwundbarkeiten der Mapping-Systeme schützen. Bei der Auswahl von Schutzmechanismen muss ferner gewährleistet sein, dass die Funktionen des Mapping-Systems möglichst nicht beeinträchtigt werden.

Die vorgestellten Sicherheitsysteme sind eine Auswahl der prominentesten Vertreter, die zum Schutz der Routing-Infrastruktur oder des DNS veröffentlicht wurden. Darunter ist auch eines, welches speziell für LISP entwickelt wurde. Jedes von der Systeme hat Stärken und Schwächen und keines kann den Schutz aller aufgezeigten Verwundbarkeiten abdecken. Trotzdem können sie alle zu einer erheblichen Verringerung der Angriffsfläche beitragen.

Im Einzelnen erläutert werden: S-BGP, SO-BGP, psBGP, DNSCurve, DNSSEC und LISP-SEC. Dabei wird vorallem darauf Wert gelegt, wie diese Systeme die Sicherheitsanforderungen erfüllen, die sich aus den Angriffsszenarien des letzten Kapitels ergeben. Die einzelnen Mechanismen werden in ihrem Kontext, z.B. BGP oder DNS, dargestellt. Eine Anwendung auf LISP folgt im Kapitel 4, bei der Evaluation. Abschließend werden die Ergebnisse in einer tabellarischen Übersicht in Abschnitt 3.7 zusammengefasst.

3.1 Secure Border Gateway Protocol (S-BGP)

Die Autoren einer Untersuchung der Verwunbarkeiten und Sicherheitslösungen zu BGP [9] geben zu S-BGP [30] an: „Secure BGP (S-BGP) was the first comprehensive routing security solution targeted specifically to BGP“ [vergl. 9, Kapitel 4.2.1]. Der Entwurf, zu dem es inzwischen auch experimentelle Implementationen und Bestrebungen seitens der IETF zur Standardisierung gibt, basiert auf der Verwendung von zwei Public Key Infrastructures (PKI) mittels X509 Zertifikaten [47]. Diese sind hierarchisch aufgebaut, mit den Regional Internet Registrys (RIR) und darüber der Internet Corporation for Assigned Names and Numbers (ICANN) als vertrauenswürdige Instanzen. Eine PKI wird genutzt, um Zertifikate für AS-Nummern auszustellen und deren Zugehörigkeit zu einer Organisation zu belegen. Die andere PKI ist dafür zuständig, die Zuordnung von Adressen zu bestätigen, d.h. Organisationen IP-Präfixe zuzuweisen. Die Kombination aus beidem erlaubt die Absicherung der BGP-UPDATE Nachrichten mittels zweierlei Belege:

Address Attestations sollen die Zugehörigkeit eines IP-Präfix zu einem AS belegen. Die Signatur der Organisation, der der IP-Präfix gehört, bestätigt dieses Zertifikat. Auf diese Weise kann ein Router prüfen, ob der Router eines AS berechtigt ist, sich als autoritativ für einen bestimmten IP-Präfix auszugeben.

Route Attestations werden pro AS, um das eine Route erweitert wird, ausgestellt. Das geschieht z.B. beim Propagieren einer Route für einen IP-Präfix. Dabei erweitert

jedes AS die ursprüngliche Route um seine Nummer, die Nummer des Ziel-AS und seine Signatur. Damit verhindert diese Lösung, dass ein AS vorgibt, eine Verbindung zu einem anderen AS zu haben, indem es ein oder mehrere ASe aus dem Pfad entfernt. Außerdem kann sich ein Router so als zu einem AS zugehörig authentifizieren.

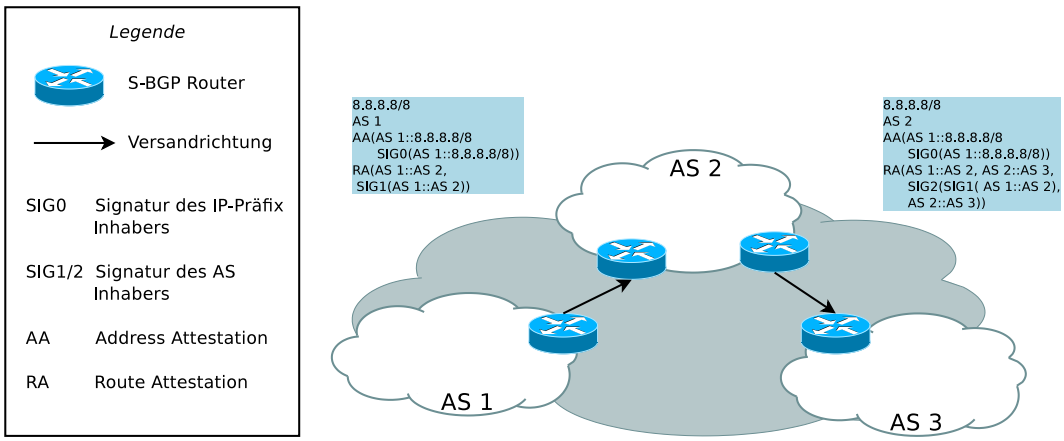

Abbildung 8: Austausch von BGP-UPDATE Nachrichten bei S-BGP

Abbildung 8 zeigt die Absicherung von BGP-UPDATE Nachrichten mittels S-BGP. Zur anschaulicheren Erklärung wurden die Nachrichten stark vereinfacht. Zum vollständigen Aufbau siehe [30]. Eine BGP-UPDATE Nachricht, die eine Route für einen IP-Präfix in AS_1 propagiert, enthält: den IP-Präfix, die AS-Nummer, die Address Attestation und die Route Attestation (1).

Ein Router, der eine solche Nachricht empfängt, validiert die Zertifikate anhand ihrer Signaturen (2). Leiten die Router aus AS_2 dieses UPDATE weiter, um eine Route zu AS_1 an AS_3 zu verkünden, fügen sie ihre Route Attestation hinzu (3). So ist es weder möglich, dass ein AS einen IP-Präfix beansprucht, zu dem es keine Verbindung hat, noch, dass ein AS vorgibt, eine Verbindung zu einem anderen AS zu haben, ohne dass es bemerkt wird.

3.2 Secure Origin Border Gateway Protocol (soBGP)

soBGP [51] ist ein Vorschlag vom Routing Protocols Deployment and Architecture (DNA) Team bei CISCO. Dieser setzt ebenfalls auf x509-Zertifikate, zur Sicherung der Routinginformationen. soBGP verfolgt zunächst einen Web-of-Trust (WoT) Ansatz bei der Vergabe von Zertifikaten an ASe. Diese Zertifikate werden dann wiederum genutzt, um ein hierarchisches System aufzubauen, dass die Zuordnung von IP-Präfix zu AS vornimmt.
Um das WoT zwischen den AS aufzubauen, wird für soBGP vorgeschlagen, eine kleine Menge an Wurzelzertifkaten zu erzeugen. Diese werden auf anderem Wege, als über

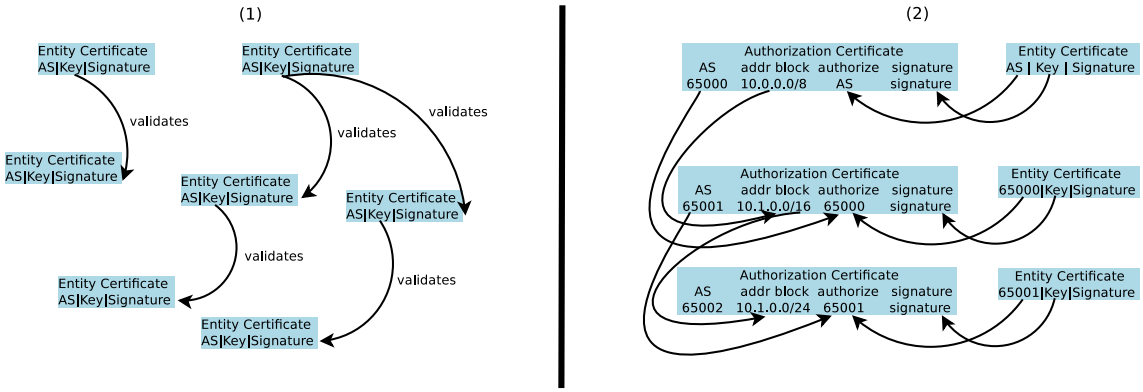

Abbildung 9: (1) Wot der Entity Certificates, (2) Hierarchische Signatur der AuthCerts

das Internet, auf den Routern verteilt. Mit den Wurzelzertifikaten werden Zertifikate von vertrauenswürdigen ASen signiert (EntityCerts), die dann weitere EntityCerts von ASen signieren können. Auf diese Weise entsteht zwischen ihnen, wie in Abbildung 9(1) [vergl. 52] zu sehen ist, ein Netz aus Vertrauensbeziehungen.

Mit dem EntityCert kann ein AS nun weitere Zertifikate signieren. Dazu gehören AuthCerts, die eine Zuordnung von AS zu IP-Präfix bezeugen. Wird ein IP-Präfix an ein anderes AS delegiert, stellt das übergeordnete AS ein AuthCert dafür aus. Abbildung 9(2) zeigt als Beispiel eine Delegation für die IP-Präfixe 10.0.0.0/8, 10.1.0.0/16 und 10.1.0.0/24 von AS 65000 zu 65001 zu 65002.

AuthCerts werden dann in PrefixPolicyCerts verpackt, die zusätzliche Richtlinien für das Routing enthalten können und verteilt. Auf diese Weise kann ein Router prüfen, ob ein IP-Präfix, der von einem AS beansprucht wird, diesem auch gehört.

Ein weiteres Zertifikat, das mit dem EntityCert signiert wird, ist das ASPolicyCert. In diesem sind Informationen über die Verbindung eines AS mit anderen AS enthalten. Zusätzlich sind Richtlinien zum Umgang mit Daten für diese AS enthalten, z.B. ob Transitservice für ein oder mehrere Routen gestellt wird. Mittels dieser Zertifikate baut ein Router dann einen Verbindungsgraphen der AS des Internets auf. Teilt ein AS nun mit, dass es einen Pfad für einen bestimmten IP-Präfix über eine Reihe von ASen kennt, kann der Router dies überprüfen. Er prüft dabei sowohl, ob das mitteilende AS, als auch die AS auf dem Pfad, eine Verbindung untereinander in ASPolicyCerts bezeugen.

soBGP stellt mittels dieser Zertifikate sicher, dass ein AS-Router zu einem AS gehört, welche ASe durch diese AS erreicht werden können und welche IP-Präfixe ein AS beanspruchen darf.

3.3 Pretty secure BGP (psBGP)

Pretty secure BGP ist eine Ableitung aus S-BGP und soBGP, die das Beste aus beiden Entwürfen vereinen soll [40]. Dabei setzt es auf eine zweigeteilte Absicherung von AS-Nummern und IP-Präfixen – eine zentrale Authorität für die Authentifizierung von

Autonomen Systemen und ein Web-of-Trust Modell zum Nachweis der Autorität über IP-Präfixe.

Als Zertifizierungsstelle der ASe werden die Regional Internet Registries (RIRs) vorgeschlagen. Bei Beantragung eines AS wird dann vom zuständigen RIR, der öffentliche Schlüssel des AS signiert. Das AS wiederum signiert Zertifikate, die belegen, dass ein Router zu ihm gehört. Damit kann ein BGP-Border-Router nachweisen, dass er auch tatsächlich berechtigt ist, UPDATE-Nachrichten für ein AS herauszugeben. Ob dabei für jeden ein eigenes Zertifkat erstellt, oder für alle Router nur ein einziges Schlüsselpaar genutzt wird, ist nicht festgelegt. Ferner wird davon ausgegangen, dass die Wurzelzertifikate der RIRs auf anderem Weg als über BGP, auf die Router verteilt werden.

Um nachzuweisen, dass ein AS authoritativ für einen IP-Präfix ist, setzt psBGP auf sogenannte „prefix assertion list (PAL)“. Diese stellen eine Liste von IP-Präfixen dar, deren Zugehörigkeit zu einem AS von dem AS bestätigt werden, das diese Liste signiert. Jedes AS erstellt solch eine Liste für seine eigenen IP-Präfixe und die seiner Nachbarn, denen es vertraut. Auf diese Weise kann ein Router, indem er die Listen eines AS und seiner Nachbarn vergleicht, verifizieren, ob ein IP-Präfix zu einem AS gehört.

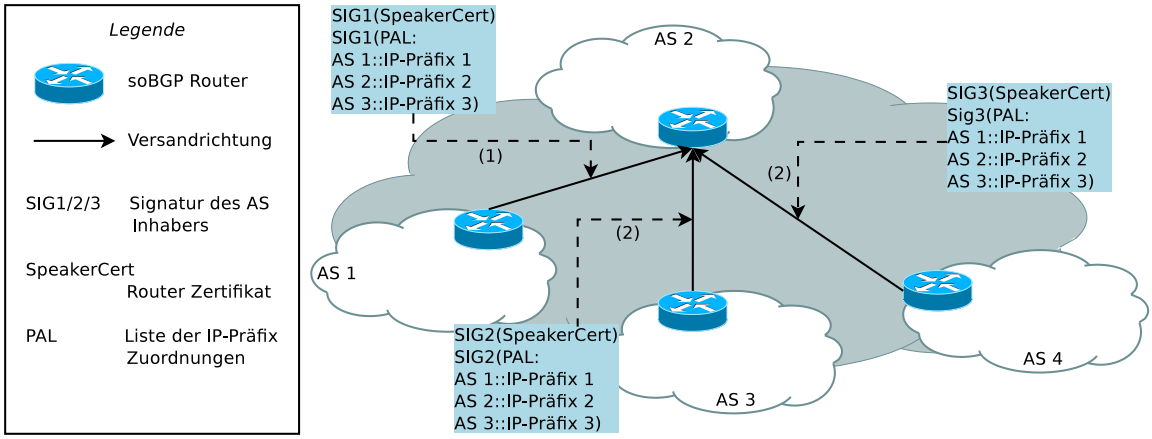

Abbildung 10: Austausch von BGP-UPDATE Nachrichten bei psBGP

In Abbildung 10 ist der beschriebene Ablauf beispielhaft dargestellt. Bei Versand der BGP-UPDATE Nachricht baut der Router von AS_1 zunächst eine sichere, authentifizierte Verbindung mit dem Router von AS_2 auf. Danach verschickt er die BGP-UPDATE Nachricht, die seine Authentifizierung (SpeakerCert) und die von ihm beanspruchten Routen enthalten (1). Der Inhalt der Nachrichten wurde der Anschaulichkeit halber stark vereinfacht. Für die vollständige Beschreibung, siehe [40]. Beide Bestandteile sind mit dem privaten Schlüssel des AS_1 signiert.

Der Router von AS_2 prüft bei Empfang, ob die Signatur für den öffentlichen Schlüssel im SpeakerCert von AS_1 stammt (Es wird davon ausgegangen, dass der Router das Zertifikat von AS_1 bereits vorher, durch eine UPDATE Nachricht, empfangen und verifiziert hat). Stimmt die Signatur, kann er den Router von AS_1 authentifizieren. Stimmt die Si-

gnatur der Nachricht, die mittels des öffentlichen Schlüssels im SpeakerCert überprüfbar ist, wurde ihre Integrität nicht verletzt. Außerdem ist sichergestellt, dass sie vom Router von AS_1 stammt.

Der Router von AS_2 überprüft dann, ob die PAL von AS_3 und AS_4 die Autorität von AS_1 über die IP-Präfixe in der Nachricht bestätigen (2). Sind alle Prüfungen erfolgreich, kann das UPDATE angenommen werden, andernfalls wird es verworfen.

Die nächsten beiden Sicherheitsysteme stammen aus dem Bereich des DNS. Wie zu Beginn von Kapitel 2.2 erwähnt ähnelt die Funktionsweise des DNS dem der LISP-Mapping-Systeme. Deswegen sind hier zwei Vertreter zur Absicherung vorgestellt.

3.4 DNSCurve

DNSCurve ist ein Entwurf des Ingenieurs Dan Berstein [13], um das DNS auf der Transportschicht mit Mechanismen der Verschlüsselung und Integrität zu versehen. Er setzt dazu auf die Verschlüsselung eines jeden versandten Datenpakets zwischen Sender und Empfänger. Im Gegensatz zu anderen Ansätzen, wird nicht mit RSA, sondern Elliptic Curve Cryptography verschlüsselt. Eine eigene Bibliothek mit Implementationen der notwendigen Algorithmen für Ephemeral Diffie-Hellman Cryptography (EDHC) erlaubt DNSCurve, die entsprechende Geschwindigkeit zu erreichen, um nahezu in Echtzeit Pakete zu ver- und entschlüsseln.

Ein Integraler Bestandteil ist die Nutzung von DNSCurve-Proxies zur Verschlüsselung des Traffics der Clients. Diese nehmen Anfragen von Clients entgegen, Verschlüsseln diese und leiten sie an den zuständigen Nameserver weiter. Dort werden die Anfragen von einem weiteren DNSCurve-Proxy entschlüsselt und an den eigentlichen Nameserver weitergeleitet. Die Antwort wird ebenfalls verschlüsselt an den Absender zurück geschickt. Dieser entschlüsselt und verifiziert sie und leitet sie dann an den Client weiter.

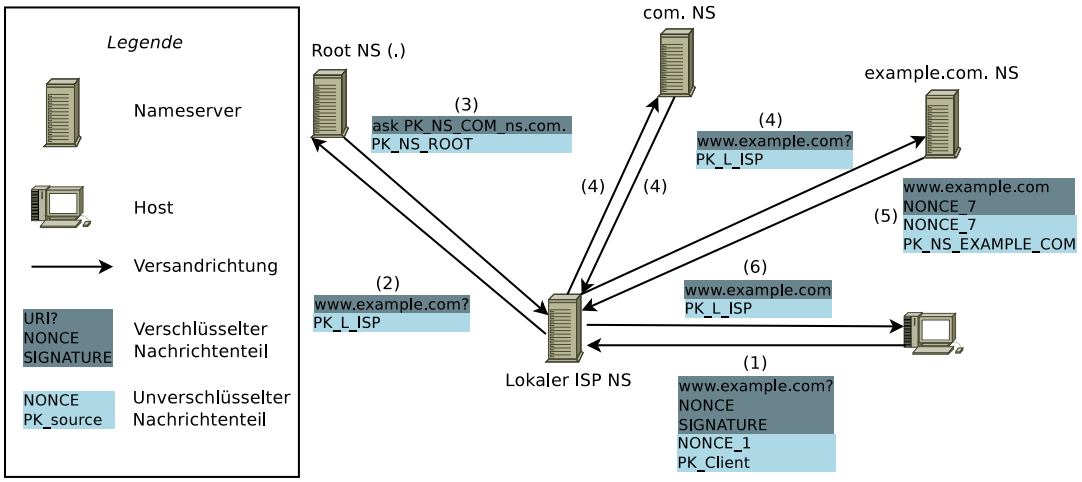

Abbildung 11: Auskunft des DNS mit DNSCurve

Abbildung 11 zeigt den Abruf der zu www.example.com gehörigen IP-Adresse. Der Client schickt zuerst eine verschlüsselte Anfrage an den DNSCurve-Resolver seines lokalen ISP (1). Dazu signiert er die DNS-Anfrage und eine zufällige, in dieser Kommunikation einzigartige, Zahl N_1 (Nonce) mit seinem privaten Schlüssel K_{client}.

$$Signature := K_{client}(Hash(www.example.com?, N_1))$$

Dann verschlüsselt er die Signatur und die Anfrage. Dazu nutzt er $SK_{PK_{client},PK_{resolver}}$, einen aus seinem privaten und dem öffentlichen Schlüssel des Empfängers ermittelten, symmetrischen Schlüssel.

$$textEncrypted\_Data \ := \ SK_{PK_{client},PK_{resolver}}(www.example.com?, N_1, Signature)$$

Im Anschluss fügt er dem Paket die zufällige Nummer N_1 und seinen öffentlichen Schlüssel PK_{client} hinzu und verschickt es. Das Paket an den DNSCurve-Proxy enthält also:

$$\text{Query\_Data} \ := \ (\ Encryptet\_Data, N_1, PK_{client}\ )$$

Der lokale DNSCurve-Resolver entpackt und entschlüsselt nach dem Empfang die Nachricht. Dazu benutzt er den selben symmetrischen Schlüssel $SK_{client,ISP}$, wie der Client. Diesen ermittelt er ebenfalls mit seinem privaten und dem öffentlichen Schlüssel des Absenders. Der Vergleich der Nonce N_1 innerhalb und außerhalb der verschlüsselten Nachricht, bestätigt ihre Integrität und Einzigartigkeit. Mittels des öffentlichen Schlüssel des Clients PK_{client}, kann dann die Integrität und Authentizität der Anfrage geprüft werden.

$$\begin{aligned}
\text{Decrypted_Data} &:= SK_{PK_{resolver},PK_{client}}(Encrypted_Data) \\
&= (www.example.com?, N_1, Signature) \\
\text{Nonce_Check} &:= Decrypted_Data(\cdots, N_1, \cdots) == Query_Data(\cdots, N_1, \cdots) \\
\text{Signature_Check} &:= PK_{client}(Signature) == Hash(www.example.com?, N_1)
\end{aligned}$$

Sind die Daten valide, kann der DNSCurve-Resolver die Anfrage weiter verarbeiten. Dazu nutzt er entweder einen in seinem Cache vorhandenen, öffentlichen Schlüssel für den Nameserver von example.com, um mit diesem in Verbindung zu treten, oder er befragt den Root-Nameserver. Dessen öffentlicher Schlüssel wurde vorher per Konfiguration festgelegt. In beiden Fällen werden, analog zu Client und DNSCurve-Resolver Verbindung, die Paketinhalte verschlüsselt. Der Übersichtlichkeit halber wurden in den weiteren Paketen der Abbildung die Signatur und Schlüssel weggelassen.

Kennt der Resolver den öffentlichen Schlüssel des zuständigen Nameservers nicht, kann er den Root-Nameserver danach befragen (2). Die Antwort enthält den, im Namen des Servers kodierten, öffentlichen Schlüssel PK_{NS_COM} (3). So kann der DNSCurve-Resolver sich iterativ, mittels verschlüsselter Anfragen, zum zuständigen Nameserver "durchfragen"(4), um diesem dann die ursprüngliche Anfrage verschlüsselt zu zusenden. Da der öffentliche Schlüssel des Anfragenden immer bereits in den Paketen enthalten ist, kann die Antwort (5,6) ebenfalls verschlüsselt erfolgen.

Ist ein Client nicht DNSCurve-fähig, agiert der DNSCurve-Resolver als transparenter Proxy und beantwortet die Anfrage auf unverschlüsselten Wege. Auf diese Weise ist es sogar möglich, als Client nicht DNSCurve, aber DNSSEC und einen DNSCurve-Resolver zu benutzen.

3.5 Domain Name System Security (DNSSEC)

Die Idee von DNSSEC [1] ist spezifisch für den hierarchischen Aufbau des DNS gedacht und speziell darauf ausgerichtet, bei minimalem Eingriff in die bestehende Infrastruktur die Integrität von DNS-Auskünften zu gewährleisten. Zu diesem Zweck wird eine Public-Private-Key PKI aufgebaut, bei der die Schlüssel der Zonen jeweils von der darüber liegenden signiert werden. Ein Client braucht so lediglich die Signatur der Rootzone speichern, um alle darunter liegenden Schlüssel zu verifizieren.

Jede Zone signiert mittels ihres Schlüssels die Einträge im Zonefile ihrer DNS-Server. Sie benutzt einen sogenannten Key-Signining-Key (KSK), dessen öffentlicher Teil, der PZSK, ebenfalls im Zonefile gespeichert wird. Der PKSK wird von der hierarchisch darüber liegenden Zone signiert und diese Signatur in ihrem Zonefile gespeichert. So kann geprüft werden, ob ein PKSK zu einer Zone gehört.

Mittels des KSK werden dann PZSK signiert. Diese Signatur wird ebenfalls im Zonefile gespeichert. So kann geprüft werden, ob der PZSK einer Zone zu ihr gehört. Der ZSK wird anschließend benutzt, um jedem Eintrag im Zonefile eine zugehörige Signatur zu geben und diese ebenfalls zu speichern (ein RRSIG-RECORD). Ein Zonefile enthält nach dieser Prozedur zusätzlich zu seinem bisherigen Inhalt:

$$
\begin{aligned}
\text{Den öffentlichen Schlüssel des KSK} &:= PKSK \\
\text{Den öffentlichen Schlüssel des ZSK} &:= PZSK \\
\text{Die Signatur des PZSK} &:= KSK(PZSK) \\
\text{Signaturen für jeden anderen Eintrag, z.B.} & \quad ZSK(www.example.com :: IP) \\
\text{Signaturen für die PKSK delegierter Zonen, z.B.} & \quad ZSK(PKSK_{subdom.example.com})
\end{aligned}
$$

Der Sinn der Zweiteilung der Schlüssel wird mit ihrer Lebensdauer sowie dem bürokratischen Aufwand eines Schlüsselwechsels begründet. Würde nur ein Schlüssel benutzt, müsste bei jedem Wechsel auch die Signatur des öffentlichen Teils, im Zonefile der übergeordneten Zone, gewechselt werden.

Hinzu kommt, dass, bei dauerhafter Benutzung eines Schlüssels zur Signatur der Einträge, eine große Schlüssellänge erforderlich wäre. Andernfalls wäre der Schlüssel, bei ausreichender Rechenleistung, Zeit und Signaturen, kompromittierbar. Bei langen Schlüsseln steigt allerdings auch der Aufwand bei der Erstellung der Signaturen.

Um beide Probleme zu vermeiden, wurde sich auf ZSK von kurzer Lebensdauer und niedriger Länge sowie KSK von hoher Lebensdauer und großer Länge geeinigt. Auf diese Weise können ZSK vom Zoneneigentümer in regelmäßigen Abständen ausgetauscht und das Generieren der Signaturen in vertretbarer Zeit erledigt werden. Die langen und sichereren KSK signieren diese ZSK und erlauben so das Validieren.

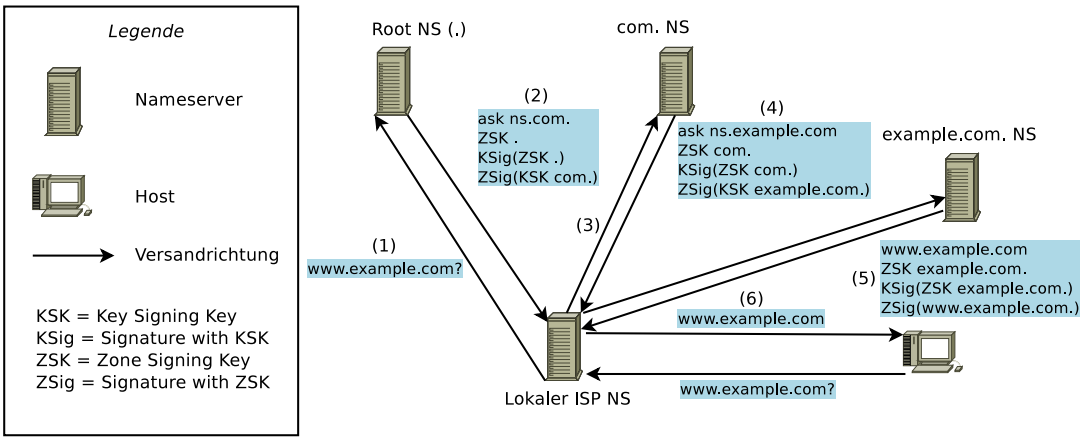

Abbildung 12: Auskunft des DNS mit DNSSEC

Abbildung 12 zeigt dabei den Kommunikationsablauf einer iterativen DNS-Anfrage für die Domain example.com. Der Client fragt dazu zunächst seinen zuständigen lokalen DNS-Resolver. Dieser beantwortet die Anfrage entweder aus seinem Zwischenspeicher oder stellt selbst eine Anfrage an den zuständigen Root-Nameserver (1). Der Root-Nameserver liefert den Eintrag für den Nameserver von .com, seinen öffentlichen ZSK, die Signaturen der beiden Einträge sowie die Signatur des öffentlichen KSK der .com-Zone zurück (2).

$$\text{Packet\_Data} := (\ \text{Nameserver Record}, ZSK_{root}(\text{Nameserver Record}), PZSK_{root}, KSK_{root}(PZSK_{root}), ZSK_{root}(PKSK_{.com})\ )$$

Der DNS-Resolver kann nun die Signatur des Eintrags prüfen. Dazu nutzt er den konfigurierten PKSK des Root-Nameservers. Ist die Antwort valide, kann er nun den Nameserver der .com-Domain nach dem Nameserver für example.com befragen (3). Die Antwort verhält sich ähnlich, wie die des Root-Nameservers (4). Schlussendlich bei ns.example.com angelangt, kann auch dessen Antwort mittels der zurück gelieferten Signaturen verifiziert werden (5). Fällt die Überprüfung positiv aus, kann der DNS-Resolver nun die Antwort an den Client senden (6).

3.6 LISP Security (LISP-SEC)

LISP-SEC [36] bietet Schutz für einige der Verwundbarkeiten von Mapping-Systemen, wie sie in Kapitel 2.3 und dem RFC-Draft über Untersuchung der Verwundbarkeiten von LISP [43] besprochen werden. Als Sicherheitssystem, das speziell für LISP entworfen wurde, soll es gegen falsche und zu große Angaben der EID-Zuständigkeit durch unbeteiligte Dritte und befragte ETRs schützen. Hinzu kommt partieller Schutz vor Denial-of-Service (DOS) und Distributed-Denial-of-Service (DDOS), Replay- und Verbindungsübernahme-Angriffen.

Die Basis von LISP-SEC bilden sogenannte „One Time Keys“ (OTK). Das sind zufällig generierte Schlüssel, die nur für jeweils einen Map-Request und Map-Reply-Zyklus verwendet werden. Solch ein OTK wird vom ITR zu Beginn einer Anfrage erzeugt, gespeichert und im LISP-Header des Map-Request eingetragen. Die entstehende Nachricht wird dann Encapsulated Control Message (ECM) [vergl. 15, Abschnitt 6.1.8] genannt.

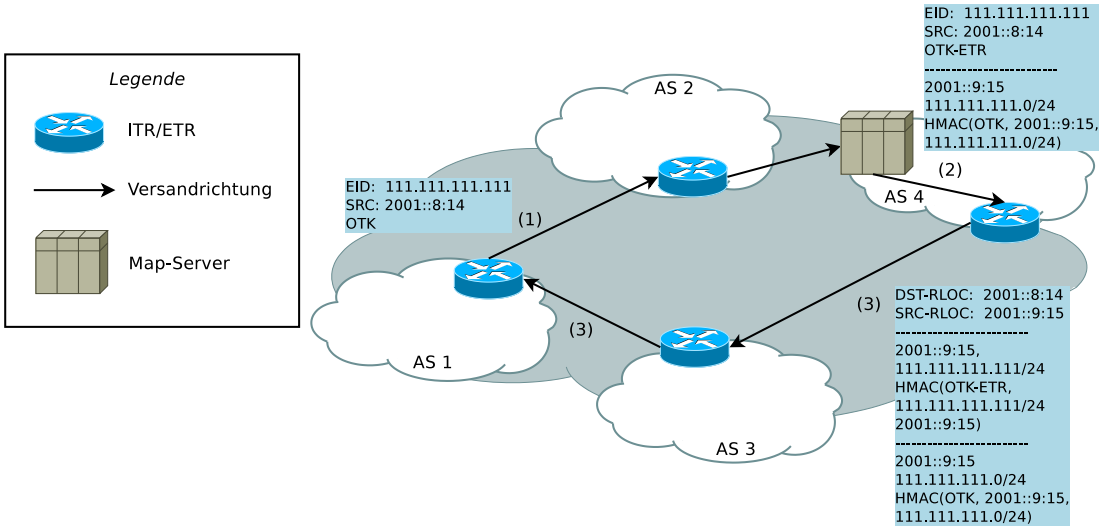

Abbildung 13: Auskunft des LISP-MS mit LISP-SEC

Der Map-Request wird dann ggf. an den MR verschickt, wobei der OTK in der ECM mit einem Preshared Secred Key (PSK) zwischen ITR und MR verschlüsselt werden sollte. Der Map-Resolver entpackt den erhaltenen Map-Request, entschlüsselt den OTK und speichert ihn. Anschließend verschickt er einen neuen Map-Request, mit dem OTK in einer ECM und seiner RLOC als Absender, an das Mapping-System, siehe Abbildung 13 (1). Das Mapping-System leitet die ECM an den für den Ziel-EID zuständigen MS weiter.

Ein MS verwaltet die RLOC des ETR und die zugehörigen Regeln und EID-Präfixe. Er sucht den passenden EID-Präfix, der zum Map-Request passt, heraus. Diesen fügt er, zusammen mit einem Hash-based Message Authentication Code (HMAC) und mit dem empfangenen Map-Request, in eine neue ECM ein. Der HMAC wird mittels des OTK berechnet, der in der empfangenen ECM enthalten war. Zusätzlich wird ein neuer OTK (ETR-OTK) mittels einer Einwegfunktion aus dem alten OTK berechnet. Dieser wird ebenfalls in die ECM eingefügt.

$$\begin{aligned} Packet\_Data \quad := \quad (\text{EID-Präfix}, HMAC_{MS} \quad &:= \quad Hash(OTK(\text{EID-Präfix})), \\ ETR-OTK \quad &:= \quad Hash(OTK), \text{Map-Request} \ ) \end{aligned}$$

Die neue ECM wird dann an den ETR geschickt (2). Auch hier sollte die Verbindung durch ein PSK geschützt werden. Befindet sich der MS im Proxymodus, führt er die folgenden Schritte des ETR selber aus, um einen Map-Reply zu schicken.

AS_4s ETR entschlüsselt bei Erhalt der ECM zunächst den OTK-ETR. Er generiert dann einen Map-Reply mit der angefragten EID zu RLOC Zuordnung. Außerdem berechnet er für diese Zuordnung, mittels des OTK-ETR, einen HMAC, um die Integrität der Antwort verifizierbar zu machen. Er kopiert anschließend die Autorisierungsinformationen aus dem ECM des MS für seinen EID-Präfix, d.h. den EID-Präfix und den HMAC. Dann verschickt er die Antwort an die RLOC des Anfragenden (3).

$$\begin{aligned} Packet\_Data \;:=\; & (\text{ EID-Präfix}, HMAC_{MS}, \text{Map-Reply}, \\ & HMAC_{ETR} \;:=\; Hash(ETR-OTK(\text{Map-Reply}))\ ) \end{aligned}$$

Der ggf. eingesetzte MR leitet die Nachricht mit geänderter Ziel-RLOC an den ITR weiter und verfährt auch auf die gleiche Weise wie der ITR mit der Antwort. Ein ITR der einen Map-Reply für einen gesendeten Map-Request erhält, prüft zunächst die Integrität der Nachricht. Dazu berechnet er den HMAC über den EID-Präfix, um die Autorisierungsinformationen des MS zu verifizieren. Außerdem berechnet er, mittels der selben Einwegfunktion, wie der MS, den OTK-ETR und prüft so die Integrität der Antwort des ETR. Schlägt eine der Integritätsprüfungen fehl, muss das Paket verworfen werden.

$$\begin{aligned} \text{EID-Präfix\_Signature\_Check} &:= Hash(OTK(\text{EID-Präfix})) == HMAC_{MS} \\ ETR-OTK &:= Hash(OTK) \\ \text{Map-Reply\_Signature\_Check} &:= Hash(ETR-OTK(\text{Map-Reply})) == HMAC_{ETR} \end{aligned}$$

Wie aus dem Ablauf ersichtlich, stellt LISP-SEC sicher, dass eine abgeschickte Antwort nicht unbemerkt manipuliert werden kann. Dies geschieht allerdings unter der Annahme, dass die empfangene Anfrage nicht bereits unterwegs, zwischen MR und MS, abgefangen und manipuliert wurde. LISP-SEC verlässt sich also darauf, dass es keine Man-in-the-Middle-Angriffe (MitM-Angriffe) gibt. Außerdem wird darauf vertraut, dass MR und MS vertrauenswürdig und mit PSKs für ihre jeweils zugeordneten ETR und ITR ausgestattet sind.

3.7 Tabellarische Zusammenfassung

Tabelle 3 zeigt eine Übersicht der Sicherheitssysteme und wie stark sie die Aspekte der Netzwerksicherheit aus Kapitel 2.3 in ihrer Spezifikation berücksichtigen.

	S-BGP	soBGP	psBGP	DNSCurve	DNSSEC	LISP-SEC
Integrität	+	+	+	+	+	0
Verfügbarkeit	0	0	0	+	0	
Vertraulichkeit	NA	NA	NA	+	NA	NA

Tabelle 3: Erreichte Sicherungsziele von Sicherheitssystemen

In Tabelle 4 sind die Sicherheitssysteme und ihre Merkmale kurz zusammengefasst. Im Einzelnen ist aufgeführt, welche kryptographische Methode zur Absicherung dient und wie die Sicherheitsziele der Authentifizierung und Integrität gewährleistet werden.

	Methode	Authentifizierung	Nachrichtenintegrität
S-BGP	X.509 Zertifikate	Zertifikat pro Router	Kryptographische Signatur
soBGP	X.509 Zertifikate	Zertifikat pro AS	Plausibilitätsprüfung
psBGP	X.509 Zertifikate	Zertifikat pro Router	Kryptographische Signatur
DNSCurve	Public-/Private-Key Verschlüsselung	Public-/Private-Key pro Client/Server	Verschlüsselung und kryptographische Signatur
DNSSEC	Public-/Private-Key Verschlüsselung	Public-/Private-Key pro Domain	Kryptographische Signatur
LISP-SEC	OTK	keine	HMAC des MS und ETR

Tabelle 4: Charakteristische Übersicht der Sicherheitssysteme

Die folgenden beiden Kapitel sollen sich nun einer möglichen Anwendung der gewonnenen Erkenntnisse widmen. Dabei steht insbesondere der Gedanke im Zentrum, eines der Mapping-Systeme mit einem der vorgestellten Sicherheitssysteme zu kombinieren. Auf diese Weise lässt sich möglicherweise eine unter dem Gesichtspunkt der Netzwerksicherheit wesentlich robustere Variante schaffen. Die Hürden für Angriffe, aber auch die Folgen eines fehlerhaft agierenden Teilnehmers, ließen sich so erheblich reduzieren.

4 Sicherere LISP-Mapping-Systeme

Einige Sicherungssysteme und die Ziele, die sie erreichen sollen, sind nun bekannt. Verbunden mit den Mapping-Systemen und ihren Verwundbarkeiten soll untersucht werden, ob sie ein sichereres Szenario für LISP ergeben können.

Da eine solche Kombination in der Praxis häufig Kompromisse in der Implementation beider Systeme erfordert, ist eine genaue Analyse des Zusammenspiels der Komponenten notwendig. Insbesondere Wiederverwendbarkeit von Know-How und Infrastruktur machen einige Kombinationen attraktiv. Systeme wie S-BGP, das sich gerade in der Entwicklungsphase befindet, oder DNSSEC, das bereits produktiv benutzt wird, bringen darüber hinaus den Vorteil der reduzierten Entwicklungskosten für die zukünftige Erforschung.

Einige Probleme mit der Umsetzung der ursprünglichen Prinzipien von LISP, wie zum Beispiel Mobilität oder Skalierbarkeit, müssen allerdings ebenfalls einer näheren Betrachtung unterzogen werden. Auch kann es in bestimmten Kombinationen zu Inkompatibilitäten zwischen den Systemen kommen, die dem ursprünglichen Zweck der Absicherung oder der Funktionalität zuwider laufen.

Im Folgenden wird deshalb kurz auf die einzelnen Kombinationen eingegangen. Dabei werden sowohl einige Vor-, als auch Nachteile bestimmter Systemverbindungen beleuchtet. Im Anschluss wird die Kombination des LISP-TREE Mapping-Systems mit der Sicherheitslösung DNSSEC näher erläutert. Zukünftige Forschungsbereiche für offene Fragen sind ebenso Thema, wie eine mögliche Alternative mit DNSCurve.

4.1 Vor- und Nachteile von Mapping-Systemen mit Sicherungsverfahren

Die Tabellen dieses Kapitels enthalten eine kurze Übersicht über die mögliche Qualität der Absicherung von Integrität und Verfügbarkeit eines Mappingsystems, in Kombination mit den vorgestellten Sicherungssystemen. Die Vertraulichkeit wird dabei, aus bereits in der Sicherheitsanalyse in Kapitel 3 genannten Gründen, nicht betrachtet. Die Bewertung erfolgte auf Grundlage der momentanen Entwürfe (Januar 2011) für die einzelnen Systeme.

Das untere Ende der Skala ist mit einem „-“ gekennzeichnet, welches eine nicht vorhandene Absicherung oder sogar Verschlechterung des Aspekts bedeutet. Ein „+“ stellt dem gegenüber eine starke Absicherung dar. Eine „0“ deutet auf das Vorhandensein von Schutzmechanismen für diesen Aspekt hin, die allerdings bekannte Nachteile haben oder ineffektiv sind. Auf die einzelnen Besonderheiten, und Kriterien, wird dann im Folgetext eingegangen. Diese sind möglichst kurz gehalten, um den Rahmen der Arbeit nicht zu sprengen. Eine ausführlichere Analyse ist Gegenstand zukünftiger Arbeit.

4.1.1 LISP-ALT

Die Sicherungssysteme S-BGP, soBGP und psBGP sind direkt für das Border-Gateway-Protokoll entworfen worden. Die BGP-GRE-Tunnel sind lediglich eine Erweiterung des BGP. Es erscheint daher sinnvoll Kombinationen mit LISP-ALT zu prüfen.

LISP-ALT	S-BGP	soBGP	psBGP	DNSCurve	DNSSEC	LISP-SEC
Integrität	0	0	0	0	+	-
Verfügbarkeit	0	0	0	0	0	0

Tabelle 5: Absicherung von LISP-ALT mit unterschiedlichen Sicherheitssystemen

S-BGP kann, nach Anpassung auf LISP, die Zugehörigkeit eines RLOC zu einem EID bestätigen. Dafür würde die Signatur des EID-Präfix Inhabers für diese Zuordnung genutzt werden. Eine der beiden PKIs wäre also statt für IP-Präfixe von Organisation, für EID-Präfixe zuständig. Mit der anderen PKI kann dann eine Organisation die Autorisierung für einen EID-Präfix sichern. Auf diese Weise ließe sich sicherstellen, dass MS nur EID-Präfixe ankünden, für die sie autorisiert sind und nur Zuordnungen herausgeben, für die sie eine valide Signatur besitzen. Wird das unter LISP-ALT liegende BGP dann noch mit dem klassischen S-BGP abgesichert, ist auch das eigentliche Routing auf den RLOCs sicherer.

Ein Problem wirft allerdings die Sicherung der LISP-Headerinformationen (siehe Kapitel 2.2) auf, wie z.B. die Erreichbarkeit bestimmter RLOC . Da diese Daten sich mit hoher Wahrscheinlichkeit häufiger ändern, als Mappings, müsste hier eine Art von On-the-fly-Signatur erfolgen. Dafür müsste der Router oder ein Proxy in der Lage sein, diese Informationen selber zu signieren. Denkbar ist ein routerspezifisches Subzertifikat der EID-PKI.

Die zusätzliche Last des Signierens und Verifizierens kann zu einem Problem für die Router führen und neue Möglichkeiten für Denial-of-Service-Angriffe bieten. Ein redundanter Proxy, der ausschließlich für die Absicherung mittels S-BGP zuständig ist (ähnlich dem in DNSCurve [13]), kann diese Last übernehmen.

Ein weiteres Problem ist der Schutz vor Replay-Angriffen. Hier kann ein time-to-live-Wert Abhilfe schaffen. Es ist allerdings nicht einfach, einen geeigneten Wert für zu finden [28].

Auch der Prozess des sog. „gleaning“, d.h. der Übernahme von Mapping-Informationen durch Router während des Transits des Map-Replies zum ITR, erfordert eine Verifikation der Signaturen.

Die statische Konfiguration von LISP-ALT kann eine Verwaltung der Zertifikate mit vertretbarem Aufwand ermöglichen. Es ist jedoch noch ungeklärt, wie gut so ein System skaliert.

Vorteil dieser Kombination ist, dass sich beide Systeme bereits im Entwicklungsstadium befinden. Eine kostengünstige Lösung wird dadurch in naher Zukunft möglich.

soBGP bringt im Wesentlichen die gleichen Vor- und Nachteile, wie S-BGP mit sich – mit ein paar kleinen Ausnahmen.

Die PolicyCerts sind ein praktischer Ansatzpunkt, um den LISP-Header zu signieren. Dadurch können zum Beispiel die Erreichbarkeitsinformationen einer RLOC nicht mehr unbemerkt manipuliert werden.

Die EntityCerts sind für die Signatur der Auskunft eines ETR oder MS nutzbar, um dessen Zugehörigkeit zu einer Organisation nachzuweisen, die für diesen EID autorisiert ist.

Ein neuer Nachteil, der sich aus der Verwendung eines Web-of-Trusts ergibt, ist die Anzahl der benötigten Zertifikate, um eine Signatur zu verifizieren. Die Abwesenheit eines Zertifikats, das die Vertrauenswürdigkeit einer Signatur bestätigt, ist in diesem Falle, kein eindeutiger Hinweis auf eine Manipulation. Es besteht die Möglichkeit, dass lediglich keine Vertrauenskette zu dem Zertifikat existiert, zu dem die Signatur gehört. In einem statischen Aufbau wie LISP-ALT besteht allerdings die Möglichkeit, zu einer engmaschigen Vernetzung der Vetrauensbeziehungen und so der Existenz eines Trust-Werts für jedes Zertifikat.

Auch bei dieser Kombination führt die Notwendigkeit der Signatur und Verifikation von Signaturen zu einem Lastproblem, das ggf. durch transparente Proxy-Server (s.o.) ausgeglichen werden kann.

psBGP folgt ebenfalls dem Schema der Signatur von Mapping-Informationen, mittels eines vertrauenswürdigen Zertifikats.

Ein Nachteil entsteht dadurch, dass ein MR jetzt auch die Prefix Assertion List der vertrauenswürdigen Nachbarn des MS oder ETR benötigt. Dadurch kann es zu zusätzlichen Verzögerungen und einer Erhöhung der Last kommen. Hinzu kommt, dass bei einem Zusammenschluss mehrerer MS, diese die Mappingzuordnung untereinander fälschen können, indem sie alle die gefälschten Zuordnungen in ihren PALs aufführen. Hier hängt der Grad der Absicherung der Zuordnung von EID zu RLOC also von der benötigten Menge an vertrauenswürdigen Signaturen ab.

DNSCurve wurde für ein hierarchisches System von Nameservern geschaffen und erfordert für den Aufbau der verschlüsselten Verbindung den öffentlichen Schlüssel des Gegenüber. Um diesen Schlüssel zu erhalten, wird eine vertrauenswürdige Stelle benötigt, bei der der Schlüssel angefragt werden kann. Da der Sinn von LISP-ALT aber darin liegt, ohne Kenntnis des Ziels einen Map-Request in die Topologie zu versenden, wird der Einsatz dieses Sicherungssystems kompliziert. Eine denkbare Lösung wäre es, bei der statischen Konfiguration der BGP-GRE-Tunnel, auch gleich die Schlüssel der ETR bzw. MS mit zu konfigurieren und diese über einen anderen Kanal auszutauschen.

Ein weiterer Nachteil von DNSCurve ist die mangelnde Möglichkeit des „gleaning “. Da die übertragenen Daten verschlüsselt sind, kann kein Transitrouter die Zuordnung auslesen. Damit wird eine gute Möglichkeit zur Performanceverbesserung des ALT verhindert. Eine Lösung wäre, die Verwendung von DNSCurve um lediglich eine signierte Verbindung zu ermöglichen.

Das Problem der Lastverteilung, durch den zusätzlichen kryptographischen Aufwand, taucht auch hier auf. Allerdings sieht DNSCurve von vornherein den Einsatz eines Proxy-Servers zur Entlastung vor.

Ein großer Vorteil ist die Verwendung von kurzlebigen Schlüsseln und Signaturen, so dass diese Kombination robust gegen Replay-Angriffe würde. Auch MitM-Angriffe sind nur noch möglich, wenn es dem Angreifer gelingt, den ETR oder MS zu übernehmen.

DNSSEC sieht ebenfalls die Signatur von Map-Replies vor. Es wird allerdings eine hierarchische Organisation der MS vorausgesetzt. Im Falle von LISP-ALT müsste also die Vertrauenswürdigkeit einer Signatur bei dem übergeordneten Knoten für den EID-Präfix verifiziert werden. Denkbar ist die Konfiguration eines oder mehrerer öffentlicher Schlüssel der Wurzelknoten. Dazu wird allerdings die Erweiterung der Mapping-Informationen, um den RLOC des nächst übergeordneten Knotens in der EID-Hierarchie, sowie um Signatureinträge, benötigt.

LISP-SEC ist als Sicherheitssystem für LISP-ALT entworfen worden. Es ist aber für Man-in-the-Middle-Angriffe anfällig, die bei einer Tunneltopologie wie der von LISP-ALT, ein nicht unwahrscheinliches Szenario sind. Da LISP-ALT auf BGP basiert ist es ebenfalls durch die bekannten BGP-MitM-Angriffe (siehe Kapitel 2.3) verwundbar.

Der zusätzliche kryptographische Aufwand zur Errechnung von OTK, kann zu Kapazitätsengpässen bei der Verarbeitung führen. Die erwähnten transparenten Proxy-Server können auch hier die ITR und MR entlasten.

Die Absicherung der Antwort durch den versandten OTK macht Manipulationen sichtbar, löst aber nicht das Problem wie die Autorisierung für eine Auskunft geprüft wird.

4.1.2 LISP-NERD

LISP-NERD	S-BGP	soBGP	psBGP	DNSCurve	DNSSEC	LISP-SEC
Integrität	+	+	+	+	+	-
Verfügbarkeit	0	0	0	0	0	0

Tabelle 6: Absicherung von LISP-NERD mit unterschiedlichen Sicherheitssystemen

Der Einsatz von LISP-NERD ist in Zukunft eher unwahrscheinlich. Das liegt unter Anderem an dem zentralistischen Aufbau des Systems, dem single-point-of-failure, den es dadurch mit sich bringt und der Unvollständigkeit des Entwurfs. Als Kombination mit anderen Mapping-Systemen könnte es jedoch zur Sicherung der Verfügbarkeit beitragen. Dieser Ansatz bietet sich auch zur Verwendung als Messknoten oder zur Verbesserung der Performance anderer Mapping-Systeme an.

S-BGP kann in Kombination mit NERD hauptsächlich zur Absicherung der Update-Nachrichten dienen. NERD sieht bereits eine Signatur der eigentlichen Mapping-Daten vor. Trotzdem muss die Integrität der Zuordnung und auch die Autorisierung des ETR, der ein Update verschickt, geprüft werden.

Insbesondere die LISP-Headerinformationen, wie zum Beispiel Erreichbarkeit oder Präferenz der RLOC, die von den Knoten nach Erhalt der Zuordnung beim zuständigen ETR angefragt werden, sollten signiert werden. Dabei kann S-BGP mit der bereits bei LISP-ALT erwähnten PKI-Aufteilung sicherstellen, dass Manipulationen der Daten bemerkt werden können. Eine Signatur on-the-fly kann dadurch notwendig werden und zu Lastproblemen führen. Redundante, transparente Proxy-Server zur Verschlüsselung (siehe Kapitel 3.4) können helfen, diese zusätzliche Last zu bewältigen.

soBGP kann die Zuständigkeit eines ETR für eine Zuordnung überprüfbar machen. Die PKI, die einen ETR mittels Signatur autorisiert, ist hier ein Web-of-Trust. Da NERD einen zentralen Ansatz für die Mapping-Datenbank verfolgt, können auch die öffentlichen Zertifikate der anderen Teilnehmer gespeichert werden. Auf diese Art muss für eine Signatur ein Zertifikat für eine Mindestzahl Partner existieren, denen die NERD vertraut.

Der Abruf der LISP-Headerinformationen wird dann ebenfalls durch das WoT gesichert und kann zu einer Reduktion der gespeicherten Zertifikate im Anfragenden ITR oder MR führen.

Das Lastproblem der vorherigen Ansätze taucht erneut, unter anderem beim Erwerb und der Verifikation dieser Zertifikate, auf. Auch hier bietet sich eine Lösung mittels transparenter Krypto-Proxies an.

psBGP erfordert kaum einen anderen Verlauf für Verifikation eines Map-Reply, als er mit S-BGP oder soBGP stattfinden würde. Allerdings muss die NERD beim Erneuern ihrer Zuordnungen, nun auch die PAL der Nachbarn eines ETR überprüfen. Dies kann durch den zentralen Ansatz der NERD erleichtert werden, wenn beim Update auch gleich die PAL mit verschickt und gespeichert wird.

Die Identität und Autorisierung eines ETR für einen RLOC, bleibt dann wieder über eine zentrale PKI der ASe abzubilden.

Das genannte Lastproblem zur Signatur und Verifikation ist auch hier vorhanden.

DNSCurve wurde zwar für ein hierarchisches System geschaffen, lässt sich jedoch für LISP-NERD adaptieren. Hierzu müssen die öffentlichen Schlüssel der ETR in der NERD hinterlegt werden. Der öffentliche Schlüssel der NERD ersetzt in diesem Falle den einer vertrauenswürdigen Wurzel.

Bei Erhalt eines Map-Replies, kann ein ITR oder MR die benötigten Erreichbarkeits- und Präferenzinformationen direkt verschlüsselt vom ETR erfragen. Der ETR antwortet dann ebenfalls verschlüsselt.

Die Überprüfung von Mappung-Updates auf die Zuständigkeit für eine EID, obliegt der NERD. Hier fehlt es bisher an einem Prüfungsmechanismus.

Da DNSCurve bereits den Einsatz von Proxy-Servern zur Verschlüsselung vorsieht, stellt sich die Frage der Lastverteilung hier nicht.

Die vollständige Ende-zu-Ende-Verschlüsselung führt dazu, dass keine Möglichkeit besteht, die RLOC oder LISP-Headerinformationen beim Transit auszulesen. „Gleaning“ wird so verhindert.

DNSSEC kann in Kombination mit NERD die gleichen Vorteile wie DNSCurve bewirken. Allerdings erlaubt es zusätzlich die Möglichkeit des „gleanings“. Die NERD muss bei Updates der EID bzw. RLOC, die Signaturen übergeordneter Präfixinhaber prüfen, um die Zuständigkeit zu verifizieren. Der verifizierte, öffentliche Schlüssel sollte dann der Auskunft über die Zuordnung von EID zu RLOC beigelegt werden.

LISP-SEC sieht hauptsächlich die OTK als Absicherung des Map-Reply vor. Der Einsatz von NERD macht sie in diesem Kontext überflüssig. Da die Datenbank bereits eine Signatur und Verifikation der Daten vorsieht, muss hier kein Hashing mit dem OTK mehr erfolgen.

Für den Einsatz zur Erfragung der Erreichbarkeit, RLOC-Präferenz und anderer Zusatzinformationen direkt vom ETR, ist der OTK allerdings nützlich. Das Konzept bleibt aber anfällig gegenüber MitM Angriffen.

Die Überprüfung von neuen Zuordnungen muss die NERD auf anderem Wege übernehmen. LISP-SEC bietet dafür ebenfalls keinen Schutzmechanismus.

4.1.3 LISP-CONS

LISP-CONS	S-BGP	soBGP	psBGP	DNSCurve	DNSSEC	LISP-SEC
Integrität	+	0	0	+	0	-
Verfügbarkeit	0	0	0	0	0	0

Tabelle 7: Absicherung von LISP-CONS mit unterschiedlichen Sicherheitssystemen

LISP-CONS weist sowohl Ähnlichkeiten mit LISP-ALT als auch CDNs auf. Die zertifikatsbasierten Mechanismen der Routing-Sicherheit und auch die Sicherheitssysteme für das DNS, lassen sich deshalb adaptieren. Einen Nachteil stellt allerdings die ungeklärte Frage nach der Möglichkeit zur EID-Präfixmigration dar (siehe Kapitel 2.2). Keines der Sicherungssysteme stellt bisher eine komfortable Lösung zur Verfügung. Hinzu kommt, dass CONS nach EID-Präfixen aufgebaut ist und so in einigen Fällen die Verifikation der Autorität eines MS über eine oder mehrere RLOC erschwert.

S-BGP muss auf LISP-CONS angepasst werden. In den beiden PKI werden zum einen Zertifikate von RLOC-Inhabern signiert, um die Zuständigkeit eines MS oder ETR

für RLOC zu bestätigen, zum anderen werden Zertifikate ausgestellt, um die Zuordnung einer EID zu einer Organisation oder Person zu bestätigen. Die Legitimität eines Map-Reply ergibt sich aus der Existenz einer verifizierbaren Unterschrift, mittels dieser beiden Zertifikate. Damit wird sowohl nachgewiesen, dass ein Router für die angegebene RLOC zuständig ist, als auch, dass der Eigentümer der EID die Zuordnung bewilligt.

Zusätzlich ermöglicht der Einsatz einer PKI die kryptographische Signatur des Map-Reply, um ihre Integrität zu bestätigen. Die Funktionsweise zum Propagieren der Routen bleibt dann die Gleichei, wie bei den Route-Attestations.

Ändert sich ein Mapping, muss die Signatur der ursprünglichen Zuordnung invalidiert werden und ein neues, Signiertes, an den zuständigen MS weitergegeben werden. In Verbindung mit Mobilität kann dies zu einem hohen Berechnungs- und Kommunikationsaufwand führen. Eine zeitlich begrenzt gültige Zuordnung oder eine Art Relaying, wie zum Beispiel bei Mobile IP [20], könnten hier Verbesserungen bewirken. Eventuell lassen sich dafür auch die Verbindungen der CDR auf der Ebene des Baums direkt oberhalb der MS nutzen.

In beiden Fällen entsteht zusätzliche Last durch Verschlüsselung und der notwendigen Kommunikation der MS, die die Verfügbarkeit des Dienstes beeinträchtigen kann. Die Notwendigkeit einer häufigen Neusignatur kann außerdem zu Sicherungsproblemen führen, bspw. bei Einbruch in einen transparenten Signaturproxy für die ETR.

Zusätzlich ergibt sich der Nachteil, dass ein anfragender ITR oder MR die Signaturen prüfen muss. Da dafür der öffentliche Schlüssel des zugehörigen Zertifikats erforderlich ist sowie im Zweifel die Kette der übergeordneten Zertifikate, kann dies zu einem erheblichen Speicheraufwand führen. Inwiefern die Prüfung einer große Menge an Zertifikaten die Verfügbarkeit beeinträchtigt, bleibt ebenfalls zu klären.

soBGP sieht ebenfalls die Verwendung zweier PKI vor. Das WOT zur Signatur vertrauenswürdiger AS-Zertifikate wird auf die Inhaber von RLOC adaptiert. Damit bestätigen sie sich gegenseitig ihre Autoritativität. Es bleibt allerdings zu klären, ob und über wieviele Hops Vertrauen transitiv ist und was passiert, wenn eine oder mehrere Organisationen einem RLOC-Besitzer das Vertrauen entziehen.

Auch ein Hijacking einer oder mehrerer RLOC ist denkbar. Indem zum Beispiel eine Gruppe vertrauenswürdiger AS ein Zertifikat signiert, das einem Anderen als dem ursprünglichen Besitzer gehört. Gleiches gilt für die Zuordnung von RLOC zu EID. Der Besitz einer EID muss, wie im ursprünglichen Entwurf, vom übergeordneten Präfixinhaber bestätigt werden. Diesem ist es damit möglich, den Nachweis zu verweigern oder sogar mehrere Signaturen herauszugeben. Auch hier bleibt die Frage nach der Transitivität des Vertrauens bestehen.

Ein Map-Reply würde in diesem System zwei Signaturen tragen, einerseits die des ETR oder MS der RLOC, andererseits die des EID-Eigentümers, der die Zuordnung bestätigt. Ein MS oder auch ein CDR könnte dann auch nur Routen innerhalb

von CONS verbreiten, für deren aggregierte EID-Präfixe er gültige Signaturen vorweisen kann.

Problematisch ist auch hier der Wechsel eines EID-Präfixes zu einer anderen RLOC. Insbesondere im Zusammenhang mit Mobilität der EID, würde jede Neuzuordnung auch eine Neusignatur erforderlich machen.

psBGP erfordert in seiner Adaption auf LISP-CONS hierarchisch organisierte Zertifikate für RLOC-Inhaber. Mit einer Signatur von diesen kann ein MS oder ETR dann nachweisen, dass er die Erlaubnis besitzt, für bestimmte RLOC Mappings herauszugeben.

Das WOT in diesem Entwurf, bei dem sich unterschiedliche RLOC-Inhaber den Besitz eines EID-Präfix bestätigen, macht jedoch ein paar Änderungen an LISP-CONS notwendig. Zunächst müsste bei einem Map-Request ein ITR oder MR mehrere Map-Replies entgegennehmen und diese vergleichen (das Äquivalent zur PAL aus unterschiedlichen AS, siehe Kapitel 3.3). Eine Möglichkeit bestünde, diese Prüfung auf die CDR auszulagern und so jeweils den Unterbäumen eines Knotens die Erstellung der PAL zu überlassen. Allerdings hat der MR oder ITR damit nicht mehr die Möglichkeit zur Prüfung der Auskunft.

Ein weiteres Hindernis entsteht bei der Mobilität einer EID. Wechselt die zugeordnete RLOC eines EID häufig (zum Beispiel weil sich der zugehörige Host in einem Fahrzeug befindet), macht dies jedes Mal auch eine Erneuerung der PAL auf den Knoten der Unterbäume im CONS erforderlich. Die zusätzliche Last kann, wie auch bei S-BGP und soBGP, zu Sicherheits- und Verfügbarkeitsproblemen führen.

DNSCurve bedarf im Einsatz mit LISP-CONS wenig Anpassung. Die ITR und MR werden mit dem öffentlichen Schlüssel des Wurzelknotens konfiguriert. Da diesem der für einen angefragten EID-Präfix zuständige, untergeordnete Knoten bekannt ist, kann er die Map-Requests verschlüsselt weiterleiten. Auf diese Weise ließe sich eine Hop-by-Hop-Verschlüsselung der Anfrage und der Antwort erreichen.

Um eine verschlüsselte Kommunikation des Anfragenden mit dem zuständigen Leaf-Knoten im CONS-Baum zu ermöglichen, böte sich eine Voranfrage nach dem öffentlichen Schlüssel an. Allerdings müsste diese iterativ von der Wurzel bis zum Blatt erfolgen und würde damit das Anfragerouting des CONS überflüssig machen. CONS wäre dann kaum von LISP-Tree zu unterscheiden.

Hinzu kommt der bekannte Nachteil, dass verschlüsselte Auskünfte „gleaning“ verhindern.

DNSSSEC im CONS setzt voraus, dass die CDR nicht nur Map-Requests weiterleiten, sondern Map-Replies und publizierte Routinginformationen auch überprüfen. Jeder CDR würde in diesem Entwurf die Signatur einer Antwort verifizieren, d.h. ob das Mapping von einem autorisierten MS oder ETR kommt. Die Frage stellt sich allerdings, wie ein MS oder ETR seine Autorität über eine oder mehrere RLOC bzw. die RLOC eines Mappings nachweist.

Hier ist eine zweite Signatur notwendig. Der Anfragende MR oder ITR würde dann neben der eigentlichen Zuordnung, auch die Signaturen sowie die öffentlichen Schlüssel aller traversierten Knoten erhalten und müsste diese prüfen. Auch hier entsteht zusätzliche Last, die die Verfügbarkeit des Systems beeinträchtigen kann.

LISP-SEC ermöglicht mit den in der Anfrage enthaltenen OTK, dass die Integrität der Map-Replies überprüft werden kann. Allerdings führt die im Entwurf getroffene Annahme der Nichtexistenz von MitM-Angriffen zur Verwundbarkeit durch eben diese. Da Map-Requests und -Replies durch das CONS geroutet werden, hat jeder traversierte Knoten die Möglichkeit zu so einem Angriff.

Ferner schützt LISP-SEC zwar mittels der OTK vor Angreifern, die nicht auf dem Pfad der Anfrage liegen. Dieses Sicherheitssystem bietet jedoch keine weiteren Mechanismen, um beispielsweise die Autorität eines MS oder ETR über die Komponenten des Map-Reply zu verifizieren. Diese Aufgabe bleibt den CDR beim Aufbau des CONS überlassen. Bei der Frage nach der Mobilität von EID bleibt zu klären, wie diese Prüfung mit wenig Aufwand und zeitnah zu bewältigen ist.

4.1.4 LISP-DHT

LISP-DHT	S-BGP	soBGP	psBGP	DNSCurve	DNSSEC	LISP-SEC
Integrität	+	+	+	0	0	-
Verfügbarkeit	0	-	-	0	-	-

Tabelle 8: Absicherung von LISP-DHT mit unterschiedlichen Sicherheitssystemen

LISP-DHT beinhaltet, wie bereits in Kapitel 2.3.2 erwähnt, eine Reihe von Sicherungsmechanismen, allerdings nicht für die RLOC. Die Sicherungssysteme für BGP und DNS können d.h. das Mapping-System sicherer machen. Das geschieht aber um den Preis eines erhöhten Aufwandes für Speicher und Validierung. Auch das Problem der Mobilität einer EID lässt sich auf Kosten des Aufwandes lösen. Ungeklärt ist auch die Frage, ob die DHT auch die LISP-Headerinformationen, wie Erreichbarkeit und Präferenz der RLOC, enthält. Wenn nicht, muss diese Auskunft ebenfalls zusätzlich abgesichert werden.

S-BGP kann den Vorteil nutzen, dass für LISP-DHT eine PKI bereits vorgesehen ist – die Zertifizierung von EID-Eigentümern. Die andere PKI, hier zur Absicherung der RLOC-Eigentümer, ist daher noch notwendig. Dadurch entwickeln sich allerdings einige Schwierigkeiten.

Bei Erhalt des Map-Reply muss ein ITR oder MR nun nicht nur die Signatur des EID-Eigentümers und die Integrität der Nachricht verifizieren, sondern auch noch die des RLOC-Eigentümers. Handelt es sich dabei um denselben, kann die Signatur im Map-Reply mitgeschickt werden. Der zuständige MS muss die Zuordnung mit

zwei Signaturen versehen oder mit einer eines Zertifikats, das die Eigentümerschaft beider Werte nachweist.

Sind EID- und RLOC-Eigentümer nicht identisch, ist zunächst eine Signaturanfrage notwendig. In dieser muss der RLOC-Eigentümer dann bestätigen, dass er das Mapping zur im Map-Reply enthaltenen EID erlaubt. Dazu benötigt er ebenfalls eine Datenbank, in der die zur Zeit mit seiner RLOC verknüpften EID verzeichnet sind, bzw. welche EID über seine RLOC erreichbar sind. Sowohl diese Datenbank, als auch die zusätzlichen Abfragen und die zusätzliche Verifikation der Signaturen, erfordern mehr Rechen- und Speicherkapazität bei ETR, MS, MR und ITR. Dadurch kann die Verfügbarkeit des Systems beeinträchtigt werden.

Weiterhin muss die Gültigkeitsdauer der Zuordnungen und der Signaturzertifikate evaluiert werden, um eine optimierte Lösung für das Verhältnis zwischen Sicherheit und Aufwand zu eruieren. Hier lassen sich eventuell Erfahrungen aus dem Bereich des DNS und DNSSEC nutzen.

soBGP sieht für seine PKI eine Web-of-Trust Architektur vor. Das bedeutet im Kontext von LISP-DHT, dass die Zertifizierung über das Eigentum an EIDn nicht mehr von einer zentralen CA vorgenommen wird. Stattdessen signieren sich die DHT-Knoten ihre Zertifikate untereinander. Ein Server muss nun für einen EID-Präfix sein Zertifikat von anderen EID-Eigentümern signieren lassen, bevor er der DHT beitritt. Dadurch erhöht sich der Verifikationsaufwand dieses Systems proportional zu der Anzahl benötigter Signaturen im WOT. Churn ist zwar in CHORD [45], das Basis des LISP-DHT bildet, laut Aussage der Entwickler nicht problematisch, da im Original aber weder häufige Authentifizierung, noch das CHORD-DHT, so wie es in LISP-DHT verwendet wird, enthalten ist, bleibt zu prüfen, ob diese Performanz erhalten bleibt.

Zusätzlich ergibt sich das Problem, dass ein MR oder ITR bei Erhalt eines Map-Reply nicht nur die Signatur des Eigentümers und einer CA, sondern auch die der anderen Signierer überprüfen muss. Aufwand entsteht durch benötigte Rechenzeit für die Verifikation und Speicher für die zusätzlichen Zertifikate.

Das Problem der Absicherung des RLOC-Adressbereichs lässt sich in diesem System lösen, indem einem EID-Eigentümer auch ein bestimmter RLOC-Adressraum zugewiesen und bestätigt wird. Werden beide Signaturen dem Map-Reply beigefügt, kann so eine Umleitung verhindert werden. Auch hier wird aber, durch eventuelle Mobilität oder Migration von EID zu anderen RLOC, ein Aushandeln der Signaturen beider Eigentümer untereinander notwendig sein.

Durch dieses Aushandeln entsteht ebenfalls auf der Seite des Anfragenden weiterer Verifikationssaufwand. Sind die Signatur des EID- und des RLOC-Eigentümers übereinstimmend, wird nur eine Prüfung der Signatur und der Unterzeichner benötigt. Ist das nicht der Fall, zum Beispiel weil die EID sich hinter einem anderen RLOC als dem ihres Eigentümers befindet, entsteht ein Mehraufwand. Bei disjunkten Unterzeichnermengen der jeweiligen Besitzerzertifikate, verdoppelt sich die Zahl der zu prüfenden Signaturen sogar.

psBGP kann durch die hierarchische Struktur der AS-Zertifikate direkt für die Zertifizierung von EID-Eigentümern adaptiert werden und bleibt so dem Konzept von LISP-DHT treu. Zur Absicherung der RLOC lässt sich die WOT-Komponente heranziehen, indem sich mehrere Eigentümer von EID-Präfixen gegenseitig ihre Mappings signieren.

Der zusätzliche Aufwand entsteht durch psBGP zum einen beim Anfragenden, in Form von zusätzlichen Verifikationsschritten der WOT-Signaturen und durch die Anforderung und den Vergleich der PAL. Zum anderen werden die MS belastet, die beim Wechsel von Mappings mit eigenen wie fremden Adressen stets auch ihre WOT-Partner informieren müssen. Eine Signatur für ein Mapping einer EID zu einer RLOC eines anderen Eigentümers, ist auch in diesem System vonnöten.

DNSCurve mit LISP-DHT führt zunächst zu dem Problem, wie der Anfragende in den Besitz des öffentlichen Schlüssels für den DHT-Knoten kommt, an den sein Map-Request geht. Eine vertrauenswürdige Stelle zum Zertifizieren von EID-Eigentümern existiert bereits. Es wäre also möglich, dem Zertifikat auch einen öffentlichen Schlüssel für die Anfragen beizulegen, bzw. den bereits Enthaltenen zu nutzen. Dann könnte ein ETR oder MR den MS anhand des EID-Präfix identifizieren und sich bei ihm nach dem zugehörigen Schlüssel erkundigen. Das setzt allerdings eine zusätzliche Kommunikationsrunde zwischen Anfragendem und MS und das Wissen über die EID-Präfix Zugehörigkeit voraus. Bei einer großen Menge von EID-Präfix-Eigentümern kann der dadurch notwendige Suchaufwand sich ähnlich zu dem jetzigen, in BGP-Tabellen vorhandenen, verhalten.

Um den Adressraum der RLOC abzusichern, wäre außerdem eine zweite PKI für RLOC notwendig. Beim Wechsel von Mappings kommt es dann zu der, in diesem Kapitel bereits mehrfach erwähnten, Signaturabstimmung zwischen EID- und RLOC-Eigentümern.

Eine Antwort auf einen Map-Request würde, nach erfolgreich ermitteltem Schlüssel, die Signatur und das Zertifikat des EID-Eigentümers, die Signatur und das Zertifikat des RLOC-Eigentümers und das eigentliche Mapping nebst LISP-Headerinformationen enthalten. Auch hier steigt der Aufwand für die Mapping-Server und der für die MR und ITR. Zusätzlich kommt der bekannte Nachteil von DNSCurve hinzu, dass bei verschlüsseltem Paket kein „gleaning“ möglich ist.

DNSSEC in Verbindung mit LISP-DHT funktioniert ähnlich wie DNSCurve, allerdings ist die PKI zur Signatur der Auskünfte bereits in das Mapping-System eingeplant. Bei Erhalt der Auskunft kann ein MR oder ITR die Signatur mittels des mitgelieferten Zertifikats verifizieren. Das Zertifikat wird durch die Signatur der CA bestätigt.

Das System hat allerdings auch die gleiche Schwäche wie DNSSEC, es sichert nicht den Namensraum ab, auf den ein Mapping abbildet. D.h. zwar kann nur der Eigentümer einer EID für diese autoritative Mappings herausgeben, aber die

RLOC, die er zuweist, ist nicht kontrolliert. Der eben bei DNSCurve erwähnte Ansatz mit einer zweiten PKI, kann auch hier Abhilfe schaffen.

Inwiefern die beiden PKI dann ihre Hierarchieebenen vertiefen, sollte ebenfalls unter Sicherheitsaspekten betrachtet werden. Es steigt nämlich nicht nur der Aufwand des Prüfenden bei der Verifikation der CA-Kette, sondern auch der des Gesamtnetzwerks beim Versand der Zuordnung. Ein weiteres Risiko stellt die Möglichkeit dar, dass eine CA kompromittiert wird. Tritt ein solcher Fall ein, kann ein gesamter Unterbaum von EID- oder RLOC-Präfixen übernommen werden.

Die Notwendigkeit der doppelten Signatur von RLOC und EID-Eigentümer sorgt auch in dieser Kombination für zusätzlichen Aufwand beim Verifizieren der Signaturen, beim Signieren und bei der Präfixmigration eines EID zu einem anderen RLOC.

LISP-SEC führt in LISP-DHT zu redundantem Integritätsschutz. Die Sicherung des Map-Reply wird in LISP-DHT bereits durch die Signatur des EID-Eigentümers übernommen. LISP-SEC beinhaltet eine ähnliche Funktionsweise mit dem gleichen Ziel. Hinzu kommt, dass im Gegensatz zu der zertifikatsbasierten Lösung LISP-SEC anfällig für MitM-Attacken ist.

Auch eine Absicherung des RLOC-Adressraums lässt sich mittels LISP-SEC nicht erreichen. Der Einsatz dieses Sicherungssystems birgt also nur geringfügige Vorteile aber zusätzlichen Aufwand. Dieser tritt in Form eines Zuwachses von Datenübertragung bei Map-Request und -Reply und der Berechnung von Prüfsummen, OTK und ihrer Verifikation auf.

4.1.5 LISP-Tree

LISP-Tree	S-BGP	soBGP	psBGP	DNSCurve	DNSSEC	LISP-SEC
Integrität	+	0	0	0	+	0
Verfügbarkeit	-	-	-	0	+	-

Tabelle 9: Absicherung von LISP-Tree mit unterschiedlichen Sicherheitssystemen

Das Mapping-System LISP-Tree ist bereits in Anlehnung an das DNS entworfen worden. Insofern lassen sich die Sicherungsmechanismen von DNSSEC und DNSCurve auch besser adaptieren als psBGP oder soBGP. Dadurch weisen diese Kombinationen aber auch die gleiche Schwäche auf wie ihre Vorbilder, namentlich die einseitige Absicherung der Namensräume. Zwar ist auch im ursprünglichen DNS eine Absicherung der reverse lookups möglich, bisher aber nicht vorgesehen. Gleiches gilt also für die Adaptierungen und ihre Absicherung der RLOC.

Ferner erlaubt die Nutzung einer auf dem DNS basierenden Architektur auch die Nutzung bereits bekannter und erprobter Verfahren, Erfahrungen und Kompetenzen auf

Personalseite sowie der hinlänglich bewiesenen Robustheit bezüglich der Verfügbarkeit. Darüber hinaus lassen sich Ansätze zum dynamischen Update des DNS [49] oder Dienste wie DYNDNS [25] nutzen, um schnell und unkompliziert Neuzuweisungen bei raschem Wechsel der Mappings zu ermöglichen.

S-BGP sieht zwei getrennte PKI vor, eine für die Routerbetreiber, eine für die Präfix-Eigentümer. Auch in LISP-Tree lässt sich diese Methode verfolgen. Ein Map-Reply des zuständigen MS wäre demnach von EID- und RLOC-Besitzer signiert und mit deren jeweiligem Zertifikat verifizierbar. So würde die Autoritativität der Auskunft bestätigt. Der Anfragende muss allerdings zusätzlich die Signaturen der Zertifikate bis zur Wurzel der PKI, prüfen.

Bei erfolgter Verifikation kann der ETR mit der RLOC des Mappings nach dem präferierten Mapping von EID zu RLOC befragt werden. Auch diese Antwort muss signiert sein und erneut verifiziert werden. In diesem zweiten Schritt kann der anfragende MR oder ITR auf zwischengespeicherte Zertifikate zurückgreifen, wenn sich die Unterzeichnergruppen überschneiden und so den Vorgang beschleunigen. Diese Methode erlaubt auch, dass Router des im Transit befindlichen Mappings diese ebenfalls verifizieren und das Ergebnis zwischenspeichern können.

Mit Hinblick auf die Frage der Mobilität bleibt zu klären, welche Werte für die Dauer der Zwischenspeicherung zu wählen sind. Eventuell können hier Erkenntnisse aus dem Bereich des DNS genutzt werden. Der Aufwand dieser Variante hängt unter anderem von der Lösung dieses Problems ab, da sich die Anzahl der benötigten Zertifikatsanfragen zur Verifikation von Signaturen, an dieser bemisst.

Ebenfalls zu klären ist das hinreichend erwähnte Problem der Signaturen, bei unterschiedlicher Eigentümerschaft von EID und RLOC. In diesem Fall müssen beide Parteien eine valide Signatur für ein Mapping ausstellen. Protokolle für dieses Art des Aushandelns sollten deshalb Thema zukünftiger Forschung sein.

soBGP kombiniert mit LISP-Tree, benötigt eine Zertifizierung der EID-Eigentümer untereinander. Das so entstehende WOT würde die Autorität eines MS für einen EID-Präfix zwar bestätigen, führt allerdings auch zu dem bekannten Problem des zusätzlichen Verifikationsaufwands auf Empfängerseite.

Wird der Namensraum der RLOC auf die gleiche Weise gesichert, kann sich der Aufwand verdoppeln. Das geschieht deshalb, weil nun beide Signaturen eines Map-Reply zunächst anhand der Delegationshierarchie und danach der Zertifikate des WOT verifiziert werden müssen. Die Höhe des zusätzlichen Aufwands hängt davon ab, wie sehr sich die Unterzeichner, bzw. ihre Zertifikate des WOT, für EID und RLOC überschneiden.

Auch der Speicheraufwand auf der Seite der Mapping-Empfänger erhöht sich. Die Zertifikate des WOT, denen direkt vertraut wird, müssen stets vorgehalten werden, um ihre Signaturen verifizieren zu können. Andernfalls erhöht sich der Kommunikationsaufwand, um bei Erhalt eines Map-Reply zunächst die zu den Signaturen gehörigen, Zertifikate zu erhalten und zu verifizieren.

Auch hier taucht das Problem auf, dass bei Wechsel eines Mappings beide Adresseigentümer ihre Signaturen zum Map-Reply hinzufügen müssen. Bei unterschiedlichen Eigentümern wird dadurch ein Verfahren zum Aushandeln und Verifizieren der Berechtigungen erforderlich.

psBGP ermöglicht es, die in LISP-Tree vorgesehene Hierarchie direkt abzusichern. Auf diese Weise kann die Authentizität eines jeden Map-Reply geprüft werden. Um die Autorität eines MS über ein Mapping zu prüfen, würde in dieser Kombination das WOT zum Einsatz kommen. Das macht es erforderlich, dass nicht nur die RLOC im Map-Reply enthalten ist, sondern auch die PAL des antwortenden MS und seiner benachbarten Knoten im Baum. Bestätigen mehrere, authentifizierte Komponenten des Baumes das Mapping, wird von der Autorität über die verwendeten EID und RLOC ausgegangen. Die Sicherheit dieser Maßnahme basiert deshalb auf der Anzahl der benötigten PAL. Bei kleiner Anzahl kann es vorkommen, dass eine Gruppe von MS im LISP-Tree in der Lage ist, unbemerkt mit unautorisierten Zuordnungen zu antworten.

Die zusätzlich benötigten Anfragen für das WOT, der erhöhte Kommunikationsaufwand unter den PAL-Partnern und die häufigen Verifikationsschritte bei Wechsel eines Mappings führen in dieser Kombination ebenfalls zu verstärktem Rechen- und Speicherbedarf.

DNSCurve in Kombination mit LISP-Tree, verschlüsselt die Kommunikation zwischen ITR oder MR und MS, sowie zwischen ITR oder MR und der RLOC, die im ersten Map-Reply enthalten war. Auf diese Weise lassen sich zuverlässig MitM-Angriffe erkennen und die Integrität von Anfrage und Antwort prüfen. Dafür muss allerdings jeder ITR oder MR mit dem öffentlichen Schlüssel der Wurzel des LISP-Tree ausgestattet werden.

Auch die zusätzliche Last ist in DNSCurve bereits in der Möglichkeit eines Proxy-Servers, der die Verschlüsselung und Verifikation vornimmt, vorgesehen. Diese Last äußert sich zum Beispiel in der notwendigen Ermittlung des öffentlichen Schlüssels von MS im LISP-Tree und des RLOC-Inhabers, der im Map-Reply genannt ist. Da Beide zunächst unbekannt sind, muss ein MR sich iterativ von Wurzel bis zum zuständigen MS durchfragen und dabei die öffentlichen Schlüssel erfahren. Die Ver- und Entschlüsselung der Map-Requests und Map-Replies trägt ebenfalls zum Rechenleistungsbedarf bei.

Die Weiterleitung zum zuständigen MS und von diesem zum zuständigen ETR oder MS für eine EID, stellt allerdings nicht die Autorität des jeweiligen Servers über die zugeordneten EID bzw. RLOC sicher. Die Prüfung, ob ein bestimmter Server für einen EID-Präfix autoritativ ist, bleibt den Betreibern der MS des LISP-Tree überlassen, bzw. dem MS, der den Map-Reply versendet.

Ein „reverse lookup“, um auch die Autorität für die gemeldete RLOC zu prüfen, ist in LISP-Tree nicht vorgesehen, allerdings wäre dies mit zusätzlichen RLOC-Zonefiles, innerhalb des Baums, möglich. Diese zweite Anfrage bedeutet zusätzliche

Last für Anfragenden, Angefragten und das Netzwerk dazwischen.

Einen weiteren Nachteil, den DNSCurve mit sich bringt ist, dass bei verschlüsselt übertragenen Map-Replies kein „gleaning“ möglich ist. Dadurch entsteht ebenfalls Last, weil mehr Map-Requests notwendig werden.

DNSSEC sichert die Integrität der Antwort und die Authentifizierung des Antwortenden. Da DNSSEC erfordert, dass topologisch übergeordnete Server im EID-Präfix-Baum eine Prüfung der Zuständigkeit für eine Domain vornehmen, wird auch die Autorität über diese Information gesichert.

Was nicht gesichert ist, ist wie auch bei DNSCurve, der „reverse lookup“, d.h. die Prüfung ob der RLOC im Map-Reply tatsächlich zur zuständigen Stelle für die EID des Map-Requests führt. Dieses Problem können zusätzliche Map-Requests für die RLOC des Map-Reply lösen.

Diese Kombination macht eine Reihe zusätzlicher Kommunikationen erforderlich. Um die Signatur eines Map-Reply zu verifizieren, muss der Anfragende zunächst alle Signaturen von der Wurzel bis zum antwortenden MS erfragen. Zusätzlich muss er Gleiches für die RLOC im Map-Reply tun. Bei unterschiedlichen Eigentümern von EID und RLOC bedeutet das doppelten Aufwand, bei gleichen Eigentümern kann ein caching der Signaturen zur Beschleunigung des Vorgangs beitragen.

Zur Verifikation des Map-Reply des ETR muss dann ebenfalls eine Signatur(kette) abgefragt werden. Hier bietet es sich an, die Signatur für den KSK (siehe Kapitel 3.5) des ETR im Map-Reply des MS zu versenden.

Mobility erfordert, wie in den vergangenen Ansätzen, eine Abstimmung von RLOC und EID-Eigentümer, um eine beidseitige Signatur der Zuordnung zu gewährleisten.

LISP-SEC geht davon aus, dass die Autorität über eine Zuordnung bereits vom MS geprüft wird. Es bleibt daher offen, wie dieser kritische Teil in der Absicherung von LISP-MS gehandhabt wird.

Das Hauptziel von LISP-SEC, die Absicherung der Nachrichtenintegrität des Map-Reply, wird auch in Kombination mit LISP-Tree nur teilweise erreicht. Es besteht die Möglichkeit, mit dem Map-Request an den LISP-Tree einen OTK mitzuschicken. Der antwortende MS verwendet diesen dann, um die Signatur der Antwort zu generieren. Bei einem MitM (wie in 3.6 beschrieben), kann der OTK aber leicht ausgetauscht werden und so das Erkennen der Fälschung verhindern.

Ein MS würde in dieser Kombination nicht nur die RLOC des zuständigen ETR im Map-Reply verschicken, sondern auch den EID-Präfix, für den der ETR autoritativ ist.

4.2 Analyse am Beispiel von LISP-Tree mit DNSSEC

Kapitel 4.1 hat gezeigt, dass eine Vielzahl von Kombinationen eines Mapping-Systems mit einem Sicherungssystem möglich sind. Jede davon hat Stärken und Schwächen, die

vom Aufbau des Mapping-Systems, der Vollständigkeit der Entwürfe und dem Anwendungsgebiet des Sicherungssystems abhängen.

Eine Kombination wird in diesem Kapitel ausführlich analysiert und der Kommunikationsablauf einer möglichen Adaption exemplarisch dargestellt. Auf diese Weise soll aufgezeigt werden, dass die Absicherung dieses LISP-Mapping-Systems mit bereits verfügbaren Mitteln möglich ist. Zusätzlich ist dieses Beispiel als Ansatz für zukünftige Forschung gedacht, die sowohl die praktische Implementierung als auch andere Kombinationen und Varianten umfassen kann.

Da der Entwurf für LISP-Tree bereits auf einem existierenden Mapping-System, dem DNS, basiert und damit einer praktischen Implementation nahe steht, wurde er als Kandidat ausgewählt. Aus den Sicherheitssystemen ist DNSSEC für dieses Beipsiel verwendet worden, da es sich bereits im Anwendungsstadium befindet und somit ebenfalls eine Wiederverwendung bestehender Infrastruktur und Kompetenzen erlaubt.

Der nachstehende Abschnitt zeigt die Vor- und Nachteile dieser Kombination auf. Dabei wird unter anderem auf den Kommunikationsablauf einer möglichen Implementation eingegangen. Desweiteren sind konkrete Vorschläge aufgeführt, wie bestehende DNS-Infrastruktur für LISP-Tree angepasst werden kann. Ferner wird erklärt, wie DNSSEC die in Kapitel 2.3 erwähnten Angriffe abwehren oder ihre Wirkung abschwächen kann. Es wird auch auf die Nachteile dieser Kombination eingegangen, zum Beispiel auf die Schwierigkeiten mit mobilen Hosts, die Absicherung der „letzten Meile“ zwischen ITR und MR, sowie die homogenisierung der DNS- und Routing-Verwaltung.

LISP-Tree Grundfunktionen

Die genaue Funktionsweise von LISP-Tree wurde bereits in 2.2.5 beschrieben, deswegen soll hier nur noch einmal kurz der übliche Ablauf vom Map-Request bis zum Map-Reply, mit einer Zuordnung von EID zu RLOC, erklärt werden.

1. Bei Erhalt eines Pakets für eine EID, schlägt ein ITR zunächst in seinem lokalen Zwischenspeicher nach, ob ein gültiger Eintrag für diese Adresse vorhanden ist. Ist das der Fall, wird das Paket mit einem LISP-Header versehen und an die zugeordnete RLOC verschickt. Liegt ein Negativeintrag (siehe Kapitel 2.2) vor, wird das Paket verworfen und eine Fehlermeldung zurückgegeben. Gibt es keine lokal gespeicherte Zuordnung, beauftragt der ITR seinen MR mit der Beschaffung.

2. Der MR kontaktiert den Kopfknoten (Wurzel) des LISP-Tree und fragt bei diesem die RLOC der Zuordnungsdatenbank für die betreffende EID an. Je nachdem ob iterativ oder rekursiv vorgegangen wird, fragt nun der Kopfknoten oder der MR die untergeordneten Knoten des Baumes ab. Dabei wird jeweils der Knoten angesprochen, an den der für die angefragte EID zugehörige EID-Präfix delegiert wurde. Erreicht die Anfrage einen der Endpunkte innerhalb des Baumes, gibt dieser entweder ein ihm bekanntes Mapping oder einen entsprechenden Negativeintrag an den MR zurück.

3. Nach Erhalt des Map-Reply gibt der MR einen enthaltenen Negativeintrag an den ITR weiter. Enthält der Map-Reply stattdessen ein Mapping, kontaktiert der MR die erhaltene RLOC, um ein genaues Mapping inklusive Zusatzinformationen, wie Erreichbarkeit oder Präferenz der RLOC zu erfragen. Erhält er diese Informationen, leitet er sie an den ITR weiter, andernfalls schickt er eine Fehlermeldung an den ITR.

4. Der ITR verfährt bei Erhalt eines Negativeintrags ebenso wie am Anfang. Erhält er jedoch ein Mapping zu der angefragten EID, kann er nun das Paket mit einem LISP-Header versehen und über das reguläre Routing verschicken. Zusätzlich kann er, bei entsprechender Konfiguration und vorhandener TTL, das Mapping zwischenspeichern, um zukünftige Pakete ohne erneute Anfrage zu versenden.

Absicherung mit DNSSEC

Fügt man diesem System nun die Mechanismen von DNSSEC hinzu, werden einige zusätzliche Informationen für den Aufbau und in den Map-Replies benötigt.

Für den initialen Aufbau des Systems muss jeder Knoten im LISP-Tree die benötigten Schlüssel (KSK und ZSK) erstellen, seine Mappings signieren und seinen KSK von dem EID-Präfix übergeordneten Knoten verifizieren und signieren lassen. Ausgehend von der Vorgehensweise im DNS, hätte dann ein jeder Knoten folgende Einträge in seiner Datenbank:

- Eine oder mehrere Zuordnungen von EID-Präfixen zu RLOC der untergeordneten Knoten im LISP-Tree. Handelt es sich um einen Leaf-Knoten, enthält der Eintrag die RLOC eines autoritativen ETR für die angefragte EID. Bei einem ETR ist hier die Zuordnung von EID zu RLOC oder ein entsprechender Negativeintrag hinterlegt.

- Für jeden Eintrag eine entsprechende kryptographische Signatur, ausgeführt mit dem ZSK (siehe Kapitel 3.5 oder [1]) des Knotens.

- Den öffentlichen Teil des ZSK und die zugehörige Signatur mit dem KSK des Knotens.

- Dein öffentlichen Teil des KSK.

- Einen oder mehrere DS-Einträge für die KSK untergeordneter Knoten, sowie die zugehörige Signatur.

Zusätzlich muss jeder ITR und jeder MR mit dem DS-Eintrag für den KSK des Kopfknotens oder direkt dem öffentlichen KSK konfiguriert werden.

Kommunikation im LISP-Tree mit DNSSEC

Ein Map-Request an das Mapping-System ist in Abbildung 14 dargestellt. Der erste

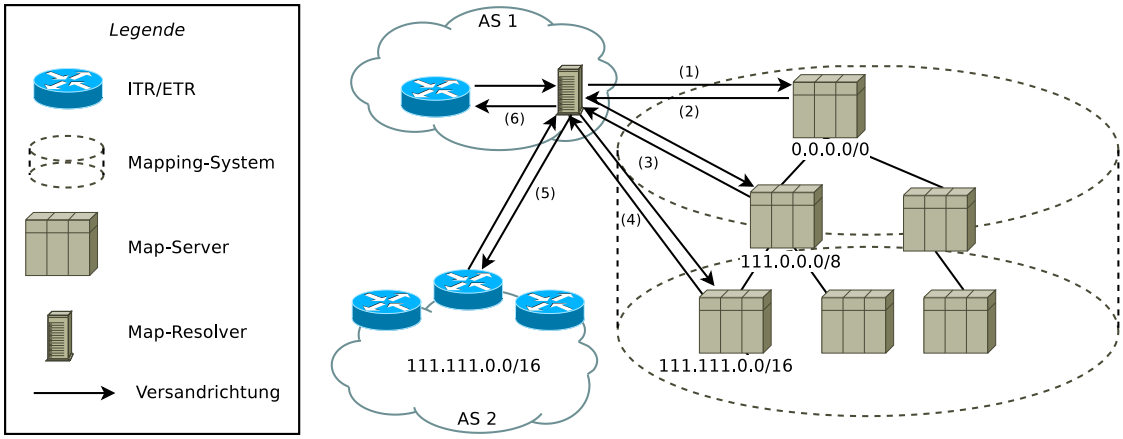

Abbildung 14: LISP-MS mittels LISP-TREE mit DNSSEC

Map-Request des ITR durch den MR aus AS_1 an den Baum läuft, analog zu LISP-Tree ohne DNSSEC, ab (1).

Die Antwort (2) enthält, neben der RLOC des nächsten zuständigen MS, auch die Signatur, den öffentlichen ZSK und KSK, sowie deren Signaturen und den DS-Eintrag für den öffentlichen KSK des nächsten MS. Der MR prüft die Schlüssel und Signaturen. Bei erfolgreicher Verifikation beginnt er iterativ, Map-Requests an die MS des LISP-Tree zu stellen (3). Die RLOC des jeweils untergeordneten, für einen EID-Präfix zuständigen MS, erhält er vom übergeordneten Knoten.

Erreicht der MR den Leaf-Knoten im Baum, erhält er ein Mapping für die RLOC eines autoritativen ETR aus AS_2 (4). Sind die Signaturen alle valide, erfragt er nun das endgültige Mapping (5). Der Map-Reply enthält weitere Schlüssel und Signaturen, die anhand des DS-Eintrags aus dem letzten Map-Reply des LISP-Tree verifiziert werden können. Sind alle Signaturen korrekt und alle Schlüssel signiert, gibt der MR das Mapping an den ITR weiter (6).

Eine alternative Möglichkeit zur Abfrage des LISP-Tree wäre, ein rekursives Vorgehen. Dabei würde der Map-Request des MR an die Wurzel des Baums und von dieser weitergeleitet werden. Jeder Knoten des Baums, einschließlich der Wurzel, müsste dann seine Schlüssel und Signaturen dem Map-Request hinzufügen. Bei Erreichen des zuständigen Leaf-Knotens, würde dieser im Map-Reply nicht nur das Mapping, seine Schlüssel und Signaturen verschicken, sondern auch die aller anderen, traversierten Knoten.

Aufgrund der nicht einschätzbaren Datenmenge, die ein MR erwarten und verarbeiten müsste und dem Umstand, dass solch ein stetig wachsender Map-Request zusätzliche Speicher- und Netzwerkanforderungen für das Mapping-System bedeutet, wird diese Methode nicht näher ausgeführt.

Analyse der Kombination

Der Ablauf in Abbildung 14 zeigt bereits einige Vor-, aber auch Nachteile dieses Systems auf.

Auf der Seite der Vorteile ist die einfache Skalierbarkeit die herausragendste. Für jede Delegation eines EID-Präfixes kommt ein Eintrag im übergeordneten Knoten des LISP-Tree sowie ggf. ein zusätzlicher MS am unteren Ende hinzu. Es spricht jedoch nichts dagegen, dass einem bereits vorhandenen MS auch die Autorität über den neuen EID-Präfix übertragen wird. Eine Redundanz der Server unter gleichem Eintrag ist im DNS bereits gang und gäbe und kann zur Lastverteilung genutzt werden.

Ein weiterer Vorteil liegt in der niedrigen Komplexität des Algorithmus und somit der Anforderungen an die benötigten Programme. Eine mögliche Implementation dieser Kombination ist die Nutzung der TXT-Records, mit bestehender DNS-Software. Auf diese Weise ließe sich ein Prototyp erstellen. Gleichzeitig würden bewährte Techniken wie Caching unter Berücksichtigung von TTL, Reverse Lookups, glueing, etc. genutzt werden können. Die Nutzung bestehender Personalexpertise aus diesem Bereich, sowie vorhandener Applikationen zur Verwaltung von Schlüsseln, Zonefiles und Zonemanagement, stellt einen weiteren Vorteil dieses Ansatzes dar.

Ebenfalls vorteilhaft ist, dass eine Vielzahl der Angriffe aus Abschnitt 2.3.2 abgewehrt, bzw. erschwert werden können. Eine unbemerkte Fälschung des im Transit befindlichen Mappings ist nahezu unmöglich, da dies die entsprechenden Signaturen invalidieren würde. Der Versand einer gefälschten Auskunft ist ebenfalls bemerkbar, da ihm die korrekte Signatur fehlt. Beides unter der Prämisse, dass der Angreifer nicht in de Besitz einer validen Signatur (z.B. durch entwendete Schlüssel) kommt.

Die Authentifizierung der MS untereinander erfolgt über die Schlüssel und ihre Signaturen. Auf diese Weise ist es nicht möglich, unbemerkt Map-Replies im Namen eines anderen MS zu verschicken, sofern man nicht selbst im Besitz von dessen Schlüssel ist. Man-in-the-Middle-Angriffe sind, bei korrekter Validierung der Signaturen, auf diese Weise stark erschwert. Diese Kombination schützt damit erfolgreich vor Umleitung und Blackholing von Traffic, durch veränderte Mappings.

Die Nachteile eines solchen Systems sind allerdings ebenfalls nicht unerheblich. Der Aufwand des Verifizierens der Schlüssel und Einträge sorgt für zusätzliche Last auf dem MR. Wie hoch diese ist und ob sie sich, beispielsweise durch redundante Server, ausgleichen lässt, werden zukünftige Untersuchungen zeigen müssen. Die Erfahrungen aus der Anwendung des DNS lassen sich hier eventuell nutzen.

Einen weiteren Nachteil stellt die einseitige Absicherung der Adressräume dar. Zwar signiert der MS, der für einen EID-Präfix zuständig ist, seine Einträge, aber nicht der Eigentümer der zugeordneten RLOC. Auf diese Weise kann ein MS bzw. Eigentümer eines EID-Präfixes sich einem beliebigen RLOC zuordnen. Zwar lassen sich fehlerhafte Einträge (im Sinne von falschem Format oder unzulässige Werte) filtern, gegen Gefälschte besteht jedoch kein Schutz. Da im zweiten Schritt der Anfrage die vom MS zurück

gemeldete RLOC angefragt wird, ließe sich so ein DOS-Angriff durchführen oder Daten umleiten.

Abhilfe kann hier eine zweite Anfrage an den LISP-Tree schaffen. Dabei wird, ähnlich dem „reverse lookup“ des DNS, nach der Zuordnung einer EID für die gemeldete RLOC gefragt. Stimmen beide Auskünfte überein und sind die Signaturen valide, ist das Mapping von beiden Eigentümern autorisiert. Diese Lösung erhöht aber die Last im Mapping-System, da eine zusätzliche Anfrage an den LISP-Tree notwendig wird. Kombiniert man dies mit mobilen Hosts, wird das Problem komplexer.

Wechselt eine EID die zugehörige RLOC, weil z.B. der Host zu dem die EID gehört in ein anderes Rechenzentrum umgezogen wird, müssen auch die Zuordnungen im LISP-Tree geändert und neu signiert werden. Hierzu fehlt es zur Zeit noch an einer Möglichkeit des „handoff“ (siehe z.B. [22]), insbesondere eines kryptographisch signierten. Der Eigentümer der EID müsste nachweisen, dass er dazu berechtigt ist, das Mapping zu ändern. Gleiches müsste der Eigentümer der neuen RLOC ausführen. Beim Umzug eines Servers mag das noch manuell zu bewältigen sein, bei der Berücksichtigung schneller, mobiler Hosts jedoch, muss über eine dynamische, protokollbasierte Variante nachgedacht werden. Ein Host, der in rapider Abfolge seine zugeordnete RLOC ändert (weil er sich z.B. in einem fahrenden Auto befindet), ist sonst unerreichbar oder überlastet das Mapping-System. Diese Kombination dient somit nicht der Problemlösung, wie ein Update der Datenbank gesichert wird.

Wird der MS eines ITR nicht vom gleichen Eigentümer betrieben, stellt sich außerdem die Frage nach der Absicherung der Kommunikation. Einem Angreifer wäre es sonst möglich, die Nachricht im finalen Transit zu verändern, wenn es ihm gelänge, den Map-Reply vom MR umzuleiten. Auch ein Hijacking des MS sollte in dem Kontext nicht unbeachtet bleiben. Der Angreifer hätte so die Möglichkeit, sämtliche Map-Requests eines ITR mit falschen oder veränderten Antworten zu bedienen. Zwar ließe sich das Problem durch die Weiterleitung aller Einträge und Signaturen umgehen, allerdings würde der Validierungsaufwand dann wieder beim ITR liegen, was zu Lastproblemen führen kann. Als Folge bietet sich der Betrieb eines bzw. mehrerer eigener MS für jeden ITR-Betreiber an oder der Einsatz von IPSEC [29] oder Vergleichbarem.

Zusätzlich führt diese Kombination von Mapping-System und Sicherungssystem dazu, dass sowohl Routing als auch DNS, vom selben System betrieben werden. Das macht die Entwicklung von Angriffen, die beide betreffen, einfacher. Eine Verwundbarkeit des DNS würde dann auch eine des Routings und umgekehrt bedeuten.

Letztlich führt diese Art der Abfrage von Zuordnungen zu diversen Problemen mit der Vertraulichkeit der Daten. Da diese nicht verschlüsselt werden, können sie von jedem auf der Transitstrecke befindlichen Rechner mitgelesen werden. Außerdem ermöglicht eine „reverse lookup“ Lösung, wie oben beschrieben, die Standortbestimmung einer EID. Wechselt die zugeordnete RLOC, lassen sich aus den Veränderungen sogar Bewegungsmuster ermitteln. Diese und weitere Nachteile bei der Vertraulichkeit bedürfen der zukünftigen Evaluation durch Forschung.

Wie zu erkennen ist, besteht noch einiger Bedarf an weiterer Untersuchung von Möglich-

keiten zur Absicherung des Mapping-Systems. Die Vor- und Nachteile dieser Kombination sollten anhand einer Implementation genauer evaluiert werden, um ggf. Lösungen zu erarbeiten. Dies liegt jedoch außerhalb des Umfangs dieser Arbeit.

Im folgenden und letzten Kapitel werden die Erkenntnisse dieser Arbeit noch einmal zusammen gefasst, auf die noch offenen Fragen und Forschungsgebiete hingewiesen, sowie nicht behandelte Fragestellungen aufgezeigt. Enthalten ist außerdem ein Ausblick auf die bestehenden Projekte in Zusammenhang mit LISP, insbesondere der Absicherung des Mapping-Systems.

5 Fazit

In der vorliegenden Arbeit wurde ausführlich auf die Funktionsweise von LISP und der zugeordneten Mapping-Systeme eingegangen. Die mangelhafte Absicherung dieser Systeme stand dabei im Fokus und wird zukünftig weiter erforscht werden müssen. Mit den vorgestellten Sicherungssystemen für Routing und DNS wurden einige Möglichkeiten erörtert, wie sich eine Verbesserung dieses Zustands erreichen lässt. Jede der vorgestellten Kombinationen hat ihre Vor- und Nachteile, die bei Implementation und weiterer Untersuchung berücksichtigt werden müssen. In der Tat weisen einige Kombinationen so gravierende Nachteile auf, dass es unwahrscheinlich ist, dass sie in naher Zukunft weiterentwickelt werden. Darunter sind alle Mapping-Systeme, die DNSCurve verwenden. Der Nachteil das Mappings nicht gecached werden können, hätte vermutlich einen ähnlichen Effekt wie auf das DNS. Auch soBGP und psBGP erscheinen als ungeeignet, da bei ihnen die Kontrolle über einen EID-Präfix nicht mehr vollständig beim Eigentümer, sondern im WoT liegt.

Es sollte außerdem beachtet werden, dass die präsentierten Sicherungssysteme lediglich eine Auswahl an prominenten Vertretern darstellen. HiBGP [41], IRV [21] oder SPV [23] und andere Systeme können ebenfalls zur Absicherung beitragen und bedürfen einer eingehenden Analyse.

Im Kontext der ständigen Weiterentwicklung und Forschung an LISP und LISP-MS (diese Arbeit basiert auf dem Stand vom Januar 2012), muss zwangsläufig auch eine Reevaluation der Ergebnisse dieser Arbeit erfolgen. Wichtig ist auch, dass diese Arbeit noch keine Antwort auf konkrete Fragen nach der Performanz hinsichtlich Geschwindigkeit, Speichererfordernis, TTL des Cachings, etc. gibt. Um diese zu beantworten, ist eine Implementation und ggf. eine Simulation realitätsnaher Routingbedingungen unabdingbar.

Des weiteren muss auch die Zahl der Angriffe und Verwundbarkeiten des Routings bedacht werden. Naturgemäß kann diese Arbeit nur auf bekannte Angriffe eingehen. Auch aus diesem Grunde sollte die Evaluation der Sicherheit der LISP-MS, in regelmäßigen Abständen wiederholt werden. Dabei sollte auch die Abhängigkeit des LISP von BGP nicht außer Acht gelassen werden. Solange BGP nicht ähnliche Untersuchungen und Verbesserungen erfährt, bleiben höher gelagerte Protokolle angreifbar.

In dieser Arbeit wurde das Problem des Datenschutzes nicht näher betrachtet. Zwar gibt es zum jetzigen Zeitpunkt noch verhältnismäßig wenig Forschung in diesem Bereich im Vergleich zur Datensicherheit, aber gerade in Verbindung mit LISP, kann das notwendig werden. Die Zuordnung von EID zu RLOC in Verbindung mit IPv6, führt fast zwangsläufig zu Datenbanken, die den Aufenthaltsort eines jeden Geräts anhand seines RLOCs bestimmen können. Auch die Map-Requests, die ein ITR verschickt oder die Änderungen der RLOC einer EID, führen zu potentiellen Verletzungen der Privatsphäre. Sei es in Form von Bewegungsprofilen oder Identifikation des Nutzers auf Basis der angefragten Mappings.

Darüber hinaus streift diese Arbeit Probleme im Bereich der Modellierung von Ver-

trauen durch Zertifikate. Diese wurden in jüngerer Zeit häufiger in Frage gestellt und benötigen der Überarbeitung. Als Beispiel sei hier auf die Angriffe auf Comodo oder DigiNotar verwiesen [26, 35]. Vielleicht ergibt sich aus dieser Überarbeitung dann auch eine Lösung für die Umsetzung von abgesicherter Mobilität mit LISP. Diese führt bisher leider zwingend zum Bruch der Transparenz für den End-Host, da dieser den Transfer seiner EID zu anderen RLOC autorisieren muss.

Weitere Forschungsfragen betreffen die Einführung von IPv6 und die damit verbundene, steigende Anzahl an IP-Adressen und Routing-Tabellen-Einträgeni; die Weiterentwicklung von LISP-SEC um Schutzmaßnahmen vor MitM-Angriffen; den Einfluss der Sicherungsmechanismen auf das Routing und die darauf aufsetzenden Dienste und höheren Protokollschichten und die Bedeutung von Virtualisierung für mögliche Sicherungskonzepte.

Zukünftige Untersuchungen der LISP-MS-Sicherheit werden sich angesichts dieser Vielzahl von Fragen und des Umstands, dass LISP sich noch in der Entwurfsphase befindet, mit einer stetigen Reevaluation auseinandersetzen müssen. Dabei sollte nicht das eigentliche Ziel aus den Augen verloren werden: Skalierbares, sicheres und performantes Routing.

Literatur

[1] Arends, R. ; Austein, R. ; Larson, M. ; Massey, D. ; Rose, S.: DNS Security Introduction and Requirements. Version: März 2005. http://www.ietf.org/rfc/rfc4033.txt. IETF, März 2005 (Internet Request for Comments 4033). – Forschungsbericht. – Updated by RFC 6014

[2] Aura, Tuomas: Strategies against Replay Attacks. In: *In Proceedings of the 10th IEEE Computer Security Foundations Workshop*, IEEE Computer Society Press, 1997, S. 59–68

[3] Awerbuch, Baruch ; Scheideler, Christian: Towards a scalable and robust DHT. In: *Proceedings of the eighteenth annual ACM symposium on Parallelism in algorithms and architectures*. New York, NY, USA : ACM, 2006 (SPAA '06). – ISBN 1–59593–452–9, S. 318–327

[4] Bellovin, S. M.: Security problems in the TCP/IP protocol suite. In: *SIGCOMM Comput. Commun. Rev.* 19 (1989), April, S. 32–48. http://dx.doi.org/10.1145/378444.378449. – DOI 10.1145/378444.378449. – ISSN 0146–4833

[5] Ben Houidi, Zied ; Meulle, Mickael ; Teixeira, Renata: Understanding slow BGP routing table transfers. In: *Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*. New York, NY, USA : ACM, 2009 (IMC '09). – ISBN 978–1–60558–771–4, S. 350–355

[6] Bishop, Matt: *Computer Security: Art and Science*. Addison-Wesley Professional, 2002 http://www.worldcat.org/isbn/0201440997. – ISBN 0201440997

[7] Böttger, Jan: *Routing Security – Current Inter-domain Routing Security Evaluation and Mapping System Security for Locator-Identifier Separation in Future Internet Routing*, Ruhr-Universität Bochum, Lehrstuhl für Netz- und Datensicherheit, Masterarbeit (Master thesis), September 2009

[8] Brim, S. ; Chiappa, N. ; Farinacci, D. ; Fuller, V. ; Lewis, D. ; Meyer, D.: LISP-CONS: A Content distribution Overlay Network Service for LISP / IETF Secretariat. Version: April 2008. https://tools.ietf.org/html/draft-meyer-lisp-cons-04. 2008 (draft-meyer-lisp-cons-04.txt). – Internet-Draft

[9] Butler, Kevin ; Farley, Toni ; Mcdaniel, Patrick ; Rexford, Jennifer: A Survey of BGP Security Issues and Solutions / AT&T Labs - Research, Florham Park, NJ. 2004. – Forschungsbericht

[10] Chin, Kwan-Wu: On the characteristics of BGP multiple origin AS conflicts. In: *Telecommunication Networks and Applications Conference, 2007. ATNAC 2007. Australasian*, 2007, S. 157 –162

[11] Convery, S. ; Cook, D. ; Franz, M.: Bgp attack tree / IETF Secretariat. Version: Februar 2004. https://tools.ietf.org/html/draft-ietf-rpsec-bgpattack-00,. 2004. – Internet-Draft

[12] Cooper, D. ; Santesson, S. ; Farrell, S. ; Boeyen, S. ; Housley, R. ; Polk, W.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Version: Mai 2008. http://www.ietf.org/rfc/rfc5280.txt. IETF, Mai 2008 (Internet Request for Comments 5280). – Forschungsbericht

[13] Dempsky, Matthew: DNSCurve: Link-Level Security for the Domain Name System / IETF Secretariat. Version: Februar 2010. http://tools.ietf.org/id/draft-dempsky-dnscurve-01.txt. 2010 (draft-dempsky-dnscurve-01.txt). – Internet-Draft

[14] Dierks, T. ; Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.2. Version: August 2008. http://www.ietf.org/rfc/rfc5246.txt. IETF, August 2008 (Internet Request for Comments 5246). – Forschungsbericht. – Updated by RFCs 5746, 5878, 6176

[15] Farinacci, D. ; Fuller, V. ; Meyer, D. ; Lewis, D.: Locator/ID Separation Protocol (LISP) / IETF Secretariat. Version: Januar 2012. https://tools.ietf.org/html/draft-ietf-lisp-20. 2012 (draft-ietf-lisp-20.txt). – Internet-Draft

[16] Farinacci, D. ; Li, T. ; Hanks, S. ; Meyer, D. ; Traina, P.: Generic Routing Encapsulation (GRE). Version: März 2000. http://www.ietf.org/rfc/rfc2784.txt. IETF, März 2000 (Internet Request for Comments 2784). – Forschungsbericht. – Updated by RFC 2890

[17] Feldmann, Anja: Internet clean-slate design: what and why? In: *ACM SIGCOMM Computer Communications Review (CCR)* 37 (2007), July, Nr. 3, 59–64. http://dx.doi.org/10.1145/1273445.1273453. – DOI 10.1145/1273445.1273453. – ISSN 0146–4833

[18] Fuller, V. ; D.Farinacci: LISP Map Server Interface / IETF Secretariat. Version: Januar 2012. https://tools.ietf.org/html/draft-ietf-lisp-ms-15. 2012 (draft-ietf-lisp-ms-15.txt). – Internet-Draft

[19] Fuller, V. ; Farinacci, D. ; Meyer, D. ; Lewis, D.: LISP Alternative Topology (LISP+ALT) / IETF Secretariat. Version: März 2011. https://tools.ietf.org/html/draft-ietf-lisp-alt-06. 2011 (draft-ietf-lisp-alt-06.txt). – Internet-Draft

[20] Glass, S. ; Hiller, T. ; Jacobs, S. ; Perkins, C.: Mobile IP Authentication, Authorization, and Accounting Requirements. Version: Oktober 2000. http://www.ietf.org/rfc/rfc2977.txt. IETF, Oktober 2000 (Internet Request for Comments 2977). – Forschungsbericht

[21] Goodell, Geoffrey ; Aiello, William ; Griffin, Timothy ; Ioannidis, John ; McDaniel, Patrick ; Rubin, Aviel: Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing. In: *In Proc. NDSS*, 2003

[22] Hsieh, Robert ; Seneviratne, Aruna: A comparison of mechanisms for improving mobile IP handoff latency for end-to-end TCP. In: *Proceedings of the 9th annual international conference on Mobile computing and networking*. New York, NY, USA : ACM, 2003 (MobiCom '03). – ISBN 1–58113–753–2, S. 29–41

[23] Hu, Y.C. ; Perrig, A. ; Sirbu, M.: SPV: Secure path vector routing for securing BGP. In: *ACM SIGCOMM Computer Communication Review* Bd. 34 ACM, 2004, S. 179–192

[24] Huston, Geoff: *BGP Routing Table Analysis Reports*. `bgp.potaroo.net`. Version: Januar 2012

[25] Inc., Dyn: *Managed DNS, Outsourced DNS & Anycast DNS*. `http://dyn.com/dns/`. Version: Januar 2012

[26] Inc., Vasco Data S.: *Incident report on attack on diginotar*. `http://www.vasco.com/company/press_room/news_archive/2011/news_diginotar_reports_security_incident.aspx`. Version: Januar 2012

[27] Jakab, L. ; Cabellos-Aparicio, A. ; Coras, F. ; Saucez, D. ; Bonaventure, O.: LISP-TREE: A DNS Hierarchy to Support the LISP Mapping System. In: *Selected Areas in Communications, IEEE Journal on* 28 (2010), october, Nr. 8, S. 1332 –1343. `http://dx.doi.org/10.1109/JSAC.2010.101011`. – DOI 10.1109/JSAC.2010.101011. – ISSN 0733–8716

[28] Jung, Jaeyeon ; Sit, E. ; Balakrishnan, H. ; Morris, R.: DNS performance and the effectiveness of caching. In: *Networking, IEEE/ACM Transactions on* 10 (2002), oct, Nr. 5, S. 589 – 603. `http://dx.doi.org/10.1109/TNET.2002.803905`. – DOI 10.1109/TNET.2002.803905. – ISSN 1063–6692

[29] Kent, S. ; Seo, K.: Security Architecture for the Internet Protocol. Version: Dezember 2005. `http://www.ietf.org/rfc/rfc4301.txt`. IETF, Dezember 2005 (Internet Request for Comments 4301). – Forschungsbericht. – Updated by RFC 6040

[30] Kent, Stephen ; Lynn, Charles ; Seo, Karen: Secure Border Gateway Protocol (S-BGP). In: *IEEE Journal on Selected Areas in Communications* 18 (2000), S. 582–592. `http://dx.doi.org/10.1109/49.839934`. – DOI 10.1109/49.839934

[31] Kranakis, Evangelos ; Oorschot, P. C. ; Wan, Tao: *Security Issues in the Border Gateway Protocol (BGP)*. 2005

[32] Labovitz, Craig: *Egypt loses the Internet.* http://asert.arbornetworks.com/2011/01/egypt-loses-the-internet/. Version: Januar 2012

[33] Labovitz, Craig: *Report to Congress of the U.S.-China Economic and Security Review Commission.* http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf. Version: Januar 2012

[34] Lear, E.: NERD: A Not-so-novel EID to RLOC Database / IETF Secretariat. Version: März 2010. https://tools.ietf.org/html/draft-lear-lisp-nerd-08. 2010 (draft-lear-lisp-nerd-08.txt). – Internet-Draft

[35] Ltd., Comodo C.: *Incident report on attack of reseller account.* https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html. Version: Januar 2012

[36] Maino, F. ; Ermagan, V. ; Cabellos, A. ; Saucez, D. ; Bonaventure, O.: LISP-Security / IETF Secretariat. Version: März 2011. https://tools.ietf.org/html/draft-maino-lisp-sec-00. 2011 (draft-maino-lisp-sec-00.txt). – Internet-Draft

[37] Mathy, Laurent ; Iannone, Luigi: LISP-DHT: towards a DHT to map identifiers onto locators. (2008), S. 61:1–61:6. http://dx.doi.org/10.1145/1544012.1544073. – DOI 10.1145/1544012.1544073. ISBN 978–1–60558–210–8

[38] Meng, X. ; Xu, Z. ; Zhang, B. ; Huston, G. ; Lu, S. ; Zhang, L.: IPv4 address allocation and the BGP routing table evolution. In: *ACM SIGCOMM Computer Communication Review* 35 (2005), Nr. 1, S. 71–80

[39] Mockapetris, P.V.: Domain names - implementation and specification. Version: November 1987. http://www.ietf.org/rfc/rfc1035.txt. IETF, November 1987 (Internet Request for Comments 1035). – Forschungsbericht. – Updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966

[40] Oorschot, P.C. v. ; Wan, Tao ; Kranakis, Evangelos: On interdomain routing security and pretty secure BGP (psBGP). In: *ACM Trans. Inf. Syst. Secur.* 10 (2007), July. http://dx.doi.org/10.1145/1266977.1266980. – DOI 10.1145/1266977.1266980. – ISSN 1094–9224

[41] Qiu, Jian ; Gao, Lixin: Hi-BGP: A Lightweight Hijack-proof Inter-domain Routing Protocol. 2006. – Forschungsbericht

[42] Rekhter, Y. ; Li, T. ; Hares, S.: A Border Gateway Protocol 4 (BGP-4). Version: Januar 2006. http://www.ietf.org/rfc/rfc4271.txt. IETF, Januar 2006 (Internet Request for Comments 4271). – Forschungsbericht

[43] Saucez, D. ; Iannone, L. ; Bonaventure, O.: LISP Security Threats / IETF Secretariat. Version: März 2011. http://tools.ietf.org/html/draft-saucez-lisp-security-03. 2011 (draft-saucez-lisp-security-03.txt). – Internet-Draft

[44] Singel, Ryan: *Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net*. http://www.wired.com/threatlevel/2008/02/pakistans-accid/. Version: Januar 2012

[45] Stoica, Ion ; Morris, Robert ; Karger, David ; Kaashoek, M. F. ; Balakrishnan, Hari: Chord: A scalable peer-to-peer lookup service for internet applications. In: *SIGCOMM Comput. Commun. Rev.* 31 (2001), August, S. 149–160. http://dx.doi.org/10.1145/964723.383071. – DOI 10.1145/964723.383071. – ISSN 0146–4833

[46] Syverson, Paul: A Taxonomy of Replay Attacks. In: *In Proceedings of the 7th IEEE Computer Security Foundations Workshop*, Society Press, 1994, S. 187–191

[47] Tuecke, S. ; Welch, V. ; Engert, D. ; Pearlman, L. ; Thompson, M.: Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile. Version: Juni 2004. http://www.ietf.org/rfc/rfc3820.txt. IETF, Juni 2004 (Internet Request for Comments 3820). – Forschungsbericht

[48] Urdaneta, Guido ; Pierre, Guillaume ; Steen, Maarten van: A Survey of DHT Security Techniques. In: *ACM Computing Surveys* 43 (2011), Januar, Nr. 2. – http://www.globule.org/publi/SDST_acmcs2009.html

[49] Vixie, P. ; Thomson, S. ; Rekhter, Y. ; Bound, J.: Dynamic Updates in the Domain Name System (DNS UPDATE). Version: April 1997. http://www.ietf.org/rfc/rfc2136.txt. IETF, April 1997 (Internet Request for Comments 2136). – Forschungsbericht. – Updated by RFCs 3007, 4035, 4033, 4034

[50] Wan, Tao ; Oorschot, P. C. ; Kranakis, Evangelos: A Selective Introduction to Border Gateway Protocol (BGP) Security Issues. In: *In Proc. of NATO Advanced Studies Institute on Network Security and Intrusion Detection*, IOS Press, 2005

[51] White, R.: Architecture and Deployment Considerations for Secure Origin BGP / IETF Secretariat. Version: Juni 2006. https://tools.ietf.org/html/draft-white-sobgp-architecture-02. 2006. – Internet-Draft

[52] White, R.: *Securing BGP Through Secure Origin BGP*. https://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/securing_bgp_sobgp.html. Version: Januar 2012

Abbildungsverzeichnis

Tabellenverzeichnis