Accountable Internet Protocol

Otto von Wesendonk
Betreuer: Heiko Niedermayer
Seminar Innovative Internet Technologien und Mobilkommunikation WS09/10
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: wesendon@in.tum.de

Kurzfassung
Das *Accountable Internet Protocol* wurde von einer Gruppe amerikanischer Forscher als Alternative zum heutigen *Internet Protocol* vorgeschlagen. Das Ziel dieses Protokolls ist es, durch selbstzertifizierende Adressen per Public-Key Kryptographie, IP Pakete verlässlich und schwer fälschbar zu machen und dadurch das Routing der Pakete abzusichern. Dieses neue Verfahren soll helfen viele Probleme, wie IP-Spoofing, Route-Hijacking oder Denial-of-Service Attacken entgegen zu wirken und soll dabei gleichzeitig einfacher wartbar sein als es heutige Lösungen sind. Das wird hauptsächlich durch den Einsatz von Selbstzertifizierung und den Verzicht auf eine zentrale Schlüsselverwaltung (PKI) erreicht. In dieser Arbeit wird dieser Vorschlag vorgestellt und mit den jetzt gebräuchlichen Herangehensweisen verglichen.

Schlüsselworte
Accountable Internet Protocol, Internet, Sicherheit, Selbstzertifizierung

1. Einleitung
Im Rahmen des *Future Internet* Blocks dieses Seminars, soll in dieser Arbeit das *Accountable Internet Protocol* (AIP) vorgestellt und besprochen werden. Das Internet entstand zu einer Zeit, in der Computersicherheit kein Problem darstellte. Basierend auf diesem Fundament, haben wir heute die Konsequenzen zu bewältigen. AIP ist ein Konzeptentwurf von einer Gruppe Forscher aus mehreren renommierten, amerikanischen Universitäten [**1**] [**2**]. Die, vor wenigen Jahren entwickelte, Idee besteht darin, das heutige *Internet Protocol* durch AIP zu ersetzen und um damit mehrere Sicherheitsprobleme aus der Welt zu schaffen. Es ist ein Experiment, das zeigen soll, wie man Sicherheitsbestrebungen ins Extreme treiben kann und wie dadurch den Unsicherheiten in heutigen Netzen entgegen gewirkt werden könnte. Diese Probleme, wie Adress-Spoofing, Route-Hijacking und Denial-of-Service werden zum großen Teil, durch die unzureichende Validierbarkeit von IP-Adressen verursacht. AIP stellt hierfür eine Lösung dar. Den Autoren ist dabei klar, dass es sich dabei um einen langfristigen Plan handelt, da es unmöglich ist eine solche Umstellung kurzfristig durchzuführen.

Gliederung In Abschnitt 2 wird der Grundaufbau des Protokolls erklärt und gezeigt wie AIP-Adressen, im Gegensatz zu IP-Adressen aussehen. In Abschnitt 3 werden die Folgen für das Routing durch AIP beschrieben. Abschnitt 4 beschäftigt sich mit den Sicherheitsmechanismen, die von AIP angewendet werden und in Abschnitt 5 wird die dafür benötigte Schlüsselverwaltung besprochen. In Abschnitt 6 wird der Vergleich zu heutigen Verfahren gesucht und die Machbarkeit einer Migration besprochen.

2. Aufbau des Protokolls
Die Grundidee des *Accountable Internet Protocol*s besteht darin, Adressen verlässlich und somit auch identifizierbar zu machen. Im Folgenden soll der Aufbau von AIP Adressen und die Konsequenzen für Routing dargestellt werden.

2.1 Grundstruktur von AIP
AIP Adressen sind hierarchisch aufgebaut. Sie bestehen aus einem Host-Bezeichner und einem oder mehreren Netzwerkkomponenten. Wie beim Internet Protokoll, ist jeder Host in ein Netzwerk eingebettet, das wiederum Teil eines weiteren Netzwerks sein kann usw.

Der Host-Bezeichner wird *Endpoint Identifier* (EID) genannt und ist global unikal. Das ist ein wichtiger Unterschied zu IP, ganz gleich in welches Netzwerk man sich verbindet, der EID bleibt identisch. Um eine Mehrfachverbindung in das gleiche Netzwerk zu ermöglichen, hat der *Endpoint Identifier* am Ende eine acht Bit lange Interfacekennung: EIDif_1 , EIDif_2 etc. Dadurch ist es möglich, sich beispielsweise über eine Ethernet- und eine WLAN-Verbindung gleichzeitig, in dasselbe Netzwerk zu verbinden.

EIDs werden einem Netzwerk zugeordnet, dieses Netzwerk wird *Accountability Domain* (AD) genannt und entspricht in etwa einem autonomen System. Wie bei den *Endpoint Identifier*, ist auch der AD Teil einer AIP Adresse global einzigartig. Dadurch ergibt sich folgender Grundaufbau einer Adresse **AD:EIDif_1**.

Um die Organisation und auch das Routing zu vereinfachen, können *Accountability Domains* beliebig viele Subdomänen besitzen. Diese interne, hierarchische Struktur ist jedem AD Betreiber dabei selbst überlassen. Jede Subdomain ist selber auch eine *Accountability Domains* und hat damit auch eine global einzigartige Bezeichnung. Dadurch ergibt sich folgende, zusammengesetzte Adressstruktur:

$$\mathbf{AD_1{:}AD_2{:}\ldots{:}AD_N{:}EID}if_1$$

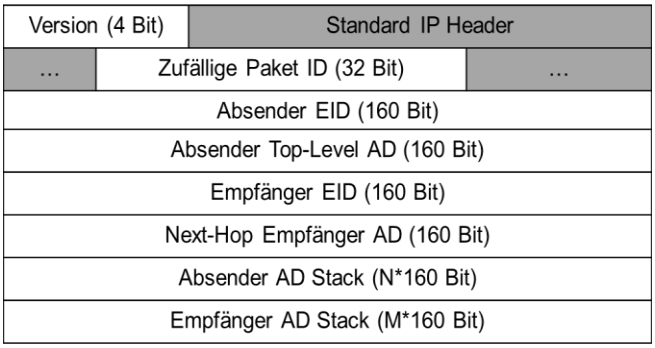

Abbildung 1: AIP Header Aufbau

Das Hauptmerkmal des *Accountable Internet Protocol* ist die Selbstzertifizierung durch Public-Key Kryptographie. Jede Adresskomponente, AD als auch EID, stellt einen Public-Key zur Verfügung, dessen Hash den Name der Komponente darstellt. Das erlaubt einem, den Kommunikationspartner eindeutig zu identifizieren. Dazu werden Nachrichten mit seinem privaten Schlüssel signiert und diese Signatur kann über die Absenderadresse verifiziert werden. AIP ist damit eines der ersten Protokolle, welche Verschlüsslung auf der IP-Ebene verwendet [**1**]. Die Vorteile dieser Herangehensweise werden in den folgenden Abschnitten besprochen werden.

Version: 8 Bit	Public-Key: 144 Bit	Interface 8: Bit

Tabelle 1: Aufbau einer Adresskomponente

Dem geschuldet ist die Adresskomponente 160 Bit lang. Die ersten acht Bits werden für die Version der Chiffre verwendet, die mittleren 144 Bits sind der Hash des Public-Keys und die letzten acht Bits bestimmen das Interface. Das Feld für die Chiffreversion wurde integriert um die Verschlüsselungsalgorithmen ändern zu können. Public-Key Kryptographie funktioniert unter der Prämisse, dass es nicht ausreichend Rechenleistung gibt um den Schlüssel zu knacken. Da sich dies über die Zeit hinweg ändern wird, wurde dem mit der Versionierung entgegengewirkt.

In Abbildung 1 sieht man den typischen Aufbau eines AIP Headers. Er ist dem Aufbau eines IP-Headers recht ähnlich, aber man erkennt deutlich, dass die benötigten Bits deutlich höher sind.

3. Routing

In diesem Abschnitt wird das Routing mit AIP erklärt und welche Konsequenzen, die hierarchischen Adressen dafür haben. Außerdem wird gezeigt, dass AIP mobile Hosts vereinfacht.

3.1 Routing mit AIP

Im Gegensatz zum *Internet Protocol* bezieht sich die Route nicht auf Prefixes und Aggregation, sondern auf die Adresskomponenten der AIP Adressen. So lange ein Paket die Ziel *Accountable Domain* nicht erreicht hat, orientiert sich die Route nur anhand der Hauptdomäne. Dafür kann z.B. das heutzutage verwendete *Border Gateway Protocol* (BGP) verwendet werden. Erreicht das Paket die Hauptdomäne, wird es, falls existent, zu der nächsten Subdomäne im Adressstack geleitet. Dazu können die gleichen Protokolle, wie die für das Routing innerhalb eines autonomen Systems gedachten (z.B. OSPF), verwendet werden. Dieser Vorgang wird solange wiederholt bis schließlich die AD erreicht wird, indem sich der Zielendpunkt befindet. Innerhalb dieses letzten AD wird nur noch anhand der EID geroutet. Router orientieren sich nur an der jeweils nächsten AD bzw. EID, vorhergehende oder folgende Hierarchieebenen müssen nicht beachtet werden.

Dieser Umstand ermöglicht es, sich bei der Routenbeschreibungen von *Interdomain Routing* nur auf die Hauptdomänen zu beschränken. EIDs und AD tieferer Hierarchiestufen müssen somit nicht in der Routenbeschreibung enthalten sein. Dadurch sind AD-Betreiber nicht gezwungen, ihre innere Topologie in Form von Routenbeschreibungen preiszugeben.

Auf der anderen Seite hat diese Herangehensweise auch einen Nachteil, der vor allem bei größeren Domänen zum Tragen kommt. Die Verwendung von AIP verhindert es AD in mehrere Teile durch Prefixes aufzuteilen Dies wird heutzutage oft dazu verwendet um Routen und dessen Belastungen feiner kontrollieren und steuern zu können. Um dieses Problem muss man sich Gedanken über die Granularität der einzelnen AD machen. So könnte man die global sichtbaren AD in mehrere, kleinere aufteilen. Ein großer ISP könnte z.B. für verschiedene Regionen jeweils eine Hauptdomäne zur Verfügung stellen. Eine weitere Möglichkeit ist es, die Interface Bits der Accountability Domains zu verwenden, um die Routen zu spezialisieren. Man wäre dadurch zwar auf die dafür vorgesehenen acht Bit beschränkt, aber laut den Entwicklern von AIP wird in der Praxis kaum mehr benötigt [**1**]. Die Verwendung der Interface-Bits erlauben dabei trotzdem, die von AIP vorgesehene Authentifizierung durch die öffentlichen Schlüssel durchzuführen.

3.2 Mobilität

AIP selber, wie IP, hat keinen Mechanismus, der sich um die Mobilität, also das Wechseln eines Hosts von einem, in das nächste Netzwerk kümmert. Dazu müssen auf AIP bzw. IP aufbauende Protokolle in höheren Netzwerkschichten sorgen. Die Mobilität wird aber in dem Sinne unterstützt, dass die positiven, sicherheitsrelevanten Fähigkeiten dadurch nicht verloren gehen und wie dadurch die sichere Mobilität doch vereinfacht wird. Die Autoren von AIP nennen dabei *TCP Migrate* und das *Host Identity Protocol* [**3**] als mögliche Migrationsprotokolle.

Wenn man sich mit einem mobilen Host verbinden möchte, bindet man sich an die EID des Hosts. Wie anfangs beschrieben, ist die EID global einzigartig. Dadurch, muss sie bei einem Wechsel in ein anderes Netzwerk nicht geändert werden und das stellt für die Kommunikationspartner, über die Migration hinweg, die Authentizität des Gegenüber sicher. Wechselt man also sein Netzwerk, so ändert sich nur der AD Teil seiner Adresse. Während einer Verbindung müssen sich die Kommunikationspartner ihren Netzwerkswechsel jeweils kommunizieren. Für einen initialen Verbindungsaufbau wird ein Naming Service, wie DNS, gebraucht um den momentanen Aufenthaltsort auszutauschen. Alternativ kann man einen Home Agent benutzen, der sämtliche Kommunikation an den jeweiligen Host weiterleitet.

3.3 DNS

Anstatt von IP Adressen werden AIP Adressen in das *Domain Name System* eingetragen. Ist ein Host zu mehreren Accountability Domains gleichzeitig verbunden, so müssen diese, falls gewollt, entsprechend hinterlegt werden. Das Interface des Hosts wird dabei implizit durch die EID festgelegt. Um die durch AIP gewonnene Sicherheit nicht durch Falscheinträge zu untergraben, sollten die DNS entsprechende Sicherheitsverfahren für die Eintragung vorgesehen. Diese Absicherung ist aber kein Bestandteil von AIP sondern von DNS selber, z.B. DNSSec. AIP-Adressen können aber dafür verwendet werden, Einträge zu ändern, indem diese Änderungsbeantragungen mit der AIP-Adresse signiert werden. Das DNS kann dann die Signatur, mit der davor eingetragenen AIP-Adresse vergleichen und damit verifizieren.

3.4 Skalierbarkeit

Wie erklärt, sind einzelne AIP Adresskomponenten schon alleine 160 Bit lang. Eine AIP Adresse, kann folglich aus mehreren, solchen Komponenten bestehen, das steht im krassen

Unterschied zu den 128 Bit einer IPv6 Adresse. Gleichzeitig erfordert auch der durchgehende Gebrauch von Kryptographie mehr Ressourcen als bei IP. Aus dem Grund beschäftigen sich die Erfinder des *Accountable Internet Protocols* intensiv mit der Skalierbarkeit. Dabei werden das Wachstum des Internets, der Routen und teilnehmenden Hosts, sowie die weitere Entwicklung in der Prozessor- und Speicherindustrie beobachtet und bewertet. Diese Arbeit geht nicht weiter auf diese Problematik ein und verweist auf Kapitel 4 der AIP-Vorstellung [**1**] . Eins sei vorweg genommen, die Autoren gehen davon aus, dass eine Realisierung von AIP technisch möglich wäre.

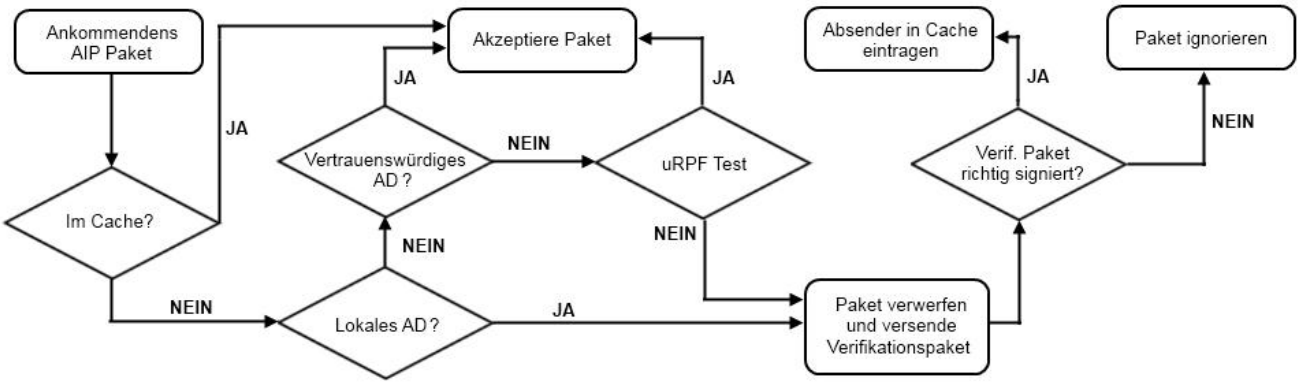

Abbildung 2: Ablauf der Paketverifikation

4. Sicherheit durch AIP

Nach dem in den letzten Abschnitten der Aufbau von AIP und dessen Konsequenzen für Routing erläutert wurde, wird in diesem Abschnitt erklärt, wie AIP zu mehr Sicherheit in Netzwerken führt. Dabei liegt der Fokus vor allem auf der Public-Key Kryptographie, die es einem ermöglicht die Echtheit einer Adresse eines Pakets zu überprüfen.

4.1 Verifikation von Adressen

Ein großes Problem in heutigen Netzwerken ist Adress-Spoofing. Dabei fälscht der Angreifer die Quelladresse eines IP-Pakets, so dass nicht mehr nachvollziehbar ist, wer Urheber dieses Pakets ist. Spoofing ist vor allem bei Spammern sehr beliebt. Wird eine nicht erreichbare Adresse angegeben, kann dies schon durch einen einfachen Handshake, wie bei TCP, zu einem Abbruch der Verbindung führen. Schwieriger ist es allerdings, wenn eine gültige und gleichzeitig abhörbare Adresse benutzt wird. Ein Angreifer könnte beispielsweise in einem öffentlich WLAN, die Adresse eines anderen Teilnehmers verwenden und hätte trotzdem die Möglichkeit auf Antworten zu reagieren.

Um Adressen zu verifizieren verbindet AIP *Unicase Reverese Path Forwarding* (uRPF) mit einem Verifikationsmechanismus, der mit dem öffentlichen Schlüssel der Adresse arbeitet. uRPF wird schon heute verwendet. Dabei wird kontrolliert, ob die Quelladresse eines ankommenden Pakets auf das gleiche Interface zeigt, von dem es gekommen ist.

Im Folgenden soll erläutert werden wie dieser Mechanismus bei AIP im speziellen funktioniert. Dabei wird zuerst die Verifikation der EID Komponente, der Adresse, betrachtet:

Empfängt ein Router ein Paket mit einer, ihm unbekannten, EID verwirft der Router dieses Paket und erzeugt ein Verifikationpakets. Dieses Verifikationspaket enthält die Quell- und Zieladresse, wie auch einen Hash des empfangen Pakets. Zusätzlich enthält es noch das Interface an dem das ursprüngliche Paket den Router erreicht hat. Der Router signiert dieses Verifikationspaket mit einem regelmäßig wechselnden, zufällig generierten geheimen Wert. Anschließend wird es dann zurück an die Quelladresse gesendet. Damit der Absender fortwährend Pakete schicken kann, muss er auf dieses Verifikationpaket reagieren. Dazu muss er das empfangene Verifikationspaket mit seinem privaten Schlüssel signieren und zurück an den Router schicken. Kann sich der Absender, durch erfolgreiches antworten auf das Verifikationspaket, beim Router identifizieren, speichert dieser die Adresse des Absenders in seinem Cache. Durch dieses Verfahren müssen sich die Router nicht merken welchem Absender sie Verifikationpaket gesendet haben, da diese Information in der signierten Antwort des Bittstellers steht.

An dieser Stelle soll nochmal festgehalten werden, dass dabei kein Schlüsselaustausch oder PKI notwendig ist, da die Adresse selber der öffentliche Schlüssel bzw. dessen Hash darstellt.

Die Verifikation der Pakete zwischen zwei *Accountability Domains* hat eine weitere Zwischenstufe bevor der gleiche Verifikationsmechanismus wie bei den *Endpoint Identifier* angewendet wird. Zunächst wir geprüft, ob das Paket von einer vertrauensvollen Domäne kommt. Ist das der Fall wird das Paket ohne weitere Überprüfung weitergeleitet. Dadurch erspart man sich redundante Kontrollen und entlastet damit das Netzwerk. Vertraut man der AD nicht, so wird eine uRPF Prüfung durchgeführt. Dabei wird eine Nachricht zur Absenderadresse des Pakets geschickt und dann beobachtet ob die Antwort über dasselbe Interface ankommt, wie das vorhergehende. Diese Überprüfung kann bei asynchronen Routen fehlschlagen. Fällt diese Prüfung schließlich positiv aus, wird das Paket akzeptiert. Schlägt die Prüfung fehl, so wird das Verifikationsverfahren, dass schon für die EID vorgestellt wurde, angewendet. Damit wird endgültig über das Paket entschieden.

4.1.1 Caching von verifizierten Adressen

Um nicht jedes Paket einzeln zu verifizieren wurde ja bereits der Cache von AIP Adressen der Router angesprochen. Verifiziert sich ein Absender, wird dessen Adresse *AD:EID* im Cache abgelegt. Falls viele Pakete sich aus derselben Accountability Domain erfolgreich verifizieren, führt es dazu, dass der Router dieser Domäne vertraut. Das heißt, dass er alle Adressen dieser Domäne aggregiert und die einzelnen Cacheeinträge durch einen Wildcard-Eintrag *AD:** ersetzt. Der Hauptgrund für diese Aggregation ist das Wachstum des Adresscache zu vereinfachen. Dieses Vorgehen birgt aber auch einen Angriffspunkt.

Obwohl diese Funktion aus Performanzgründen durchaus notwendig ist, stellt es gleichzeitig eine Angriffsfläche dar. Gibt es genug infiltrierte Teilnehmer in einem Netzwerk, ist es einem Angreifer möglich, einen Wildcard-Eintrag zu erzeugen. Dadurch ist der Damm gebrochen und der Angreifer kann mit gefälschten EIDs Pakete verschicken.

4.2 Beispielhafte Topologie einer Accountability Domain

Um als Betreiber einer *Accountability Domain* die Belastung des Netzwerkes etwas zu reduzieren, könnten verschiedene Router unterschiedliche Rollen einnehmen.

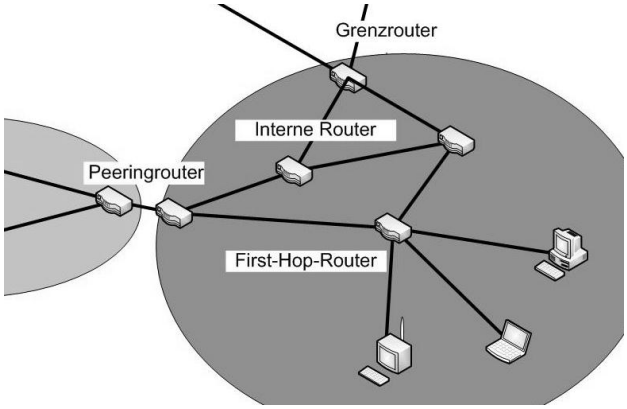

Abbildung 3: Beispielhafte Topologie

So könnte ein **Grenzrouter** sämtliche Pakete, die das Netzwerk ansteuern überprüfen, bevor sie weitergeleitet werden. **First-Hop-Router** könnten sich um die Validierung der Hosts kümmern, bevor diese durch das Netzwerk kommunizieren können. Innerhalb der Domäne wären **interne Router**, die sich nur um die Weiterleitung und das eigentliche Routing kümmern. Die internen Router müssten bei diesem Aufbau keine Überprüfung durchführen, da sie sich auf die äußeren Router verlassen. Als dritte Rolle könnte man schließlich noch sogenannte **Peeringrouter** einführen. Diese befinden sich an Grenzen vom eigenen Netzwerk zu anderen, vertrauensvollen, Netzwerken. Peeringrouter könnten den Verkehr dann ohne weitere Überprüfung in das angelegene Netzwerk weiterleiten. Peering geschieht meistens nur nach einer vertraglichen Vereinbarung, wodurch ein gewisses Vertrauen vorausgesetzt wird.

4.3 Protokollerweiterung für DoS-Schutz

Wie anfangs beschrieben, sieht das *Accountable Internet Protocol* auch den Schutz vor bestimmten Denail-of-Service Attacken vor. Um diesen Schutz zu gewährleisten wurde das *Shut-off Protocol* eingeführt.

Dieses Protokoll erlaubt es einen Empfänger dem Sender *ein Shut-off Paket* (SOP) zu schicken, woraufhin der Sender zeitweise aufhört weitere Pakete zu schicken. Um dieses Verfahren anwenden zu können werden intelligente Network Interface Cards, sogenannte smart-NIC benötigt. Dabei sieht der Ablauf wie folgt aus:

Ein Empfänger A erhält zu viele Pakete auf einmal und entscheidet sich dem sendenden Kommunikationspartner B ein *Shut-off Paket* zu schicken. Dieses Paket enthält eine TTL (time-to-live) Zeitangabe, den Hash des empfangenen Pakets, sowie seine EID. Dieses Paket wird durch A signiert und an B gesendet, woraufhin dieser aufhört weitere Pakete zu senden. Die Zeitspanne, die gewartet werden soll, wird durch die TTL im SOP spezifiziert, darf aber maximal fünf Minuten betragen. Um Replay-Attacken zu verhindern, muss sich die smart-NIC jeweils die Hashes der zuletzt gesendeten Pakete merken und hört folglich nur auf zu senden, falls der Hash des Pakets im signierten SOP sich im Speicher befindet. SOP ist außerdem ein Anwendungsbeispiel für die selbstsignierenden Adressen. Diese werden in dem Fall des Shut-off Protocols dafür verwendet, die Authentizität des SOP zu gewährleisten.

Ein Angreifer mit modifizierter Hardware kann diese Anfragen natürlich ignorieren, SOP hat aber ein anderes Ziel. Es soll vor allem vor infiltrierten Systemen schützen, wie es zum Beispeil bei Botnets der Fall ist. Dabei kann der Schaden, der durch ungewollte Wirtsysteme ausgeht, minimiert werden. Das zeigt auch warum es wichtig ist, dass diese Funktionalität in der NIC implementiert ist.

Für Server bräuchte man leistungsfähige smart-NICs, aus dem Grund wird empfohlen SOP in diesem Fall zu deaktivieren. Die Argumentation dahinter geht davon aus, dass Server sich in den meisten Fällen sowieso in professionell verwalteten Umgebungen befinden. Daher ist SOP eher als Schutz für kleinere Hosts gedacht.

5. Schlüsselverwaltung

AIP macht starken Gebrauch von Kryptographie. Die Besonderheit des Entwurfs ist die Verwendung von Selbstzertifizierenden Schlüsseln, wodurch keine Public-Key Infrastruktur (PKI) benötigt wird. In diesem Abschnitt soll erläutert werden wie diese Schlüssel verwaltet werden und wie man deren Missbrauch behandelt.

5.1 Schlüsselkompromittierung

Wie bereits erwähnt wurde, bestehen die Adresskomponenten einer AIP Adresse aus den Hashsummen der öffentlichen Schlüssel. Das heißt auch, dass kein Mapping zwischen Namen und Adresse für die Schlüssel notwendig ist, weil der Name die Adresse ist. Diese Adressen können, wie es heute bei IP geschieht, in einem DNS hinterlegt werden und sind dadurch auffindbar.

Falls ein Schlüssel, der für eine Adresse verwendet wird, in irgendeiner Form kompromittiert wird, muss ein neuer Schlüssel erzeugt werden und die Änderung der alten Adresse bzw. Schlüssel muss an alle Beteiligten kommuniziert werden. Falls die Adresse in einem DNS hinterlegt ist, muss man diese erneuern. Wird die Adresse einer *Accountability Domain* kompromittiert, muss auch diese die Adresse erneuern und die Änderung bzw. den Rückruf der alten Adresse über alle Routen hinweg kommunizieren.

5.2 Schlüssel-Registry

Um die im letzten Abschnitt genannten Probleme zu vereinfachen und gleichzeitig die Erkennung von Missbrauch zu unterstützen führen die Autoren von AIP globale bzw. domänenspezifische Registries ein. Diese Registries sind für AIP nicht notwendig, allerdings wird durch ihre Verwendung die Sicherheit deutlich erhöht.

Die Registries können mehrere verschiedene Typen von Einträgen haben, wobei die Einträge jeweils mit der AIP Adresse signiert sein können. Durch die Selbstzertifizierung und die daraus folgende Möglichkeit der Signierung, kann eine solche Registry komplett automatisiert betrieben werden. Alle Einträge werden durch die Adresse des Einträgers verifiziert.

Daher sind diese Registries auch nicht als PKI oder ähnliches zu vergleichen. Es wird kein Dritter zur Validierung der Einträge gebraucht.

- ***Schlüssel*** $\{K_{PK}, PK\}$
  Zuordnung von Hash auf den eigentlichen öffentlichen Schlüssel. Eine Signierung ist hierbei nicht notwendig. Dieser Eintrag dient einfach der Auflösung des öffentlichen Schlüssels, der dann für weitere Zwecke verwendet werden kann.

- **Widerruf** $\{K, \text{widerrufen}\}_K^{-1}$
  Im Fall einer Kompromittierung des Schlüssels, können Adressen widerrufen werden. Um einen solchen Widerrufungseintrag einstellen zu können, muss er durch den mit dem alten Schlüssel signiert werden. Router können dann beispielsweise Adressen immer mit der Registry abgleichen und damit kontrollieren, ob ein möglicher Angreifer eine alte, invalide Adresse verwendet.

- ***Peering*** $\{A, K_A, B, K_B\}_{KA}^{-1}$ $\{A, K_A, B, K_B\}_{KB}^{-1}$
  Peering-Vereinbarung können auch in einer Registry hinterlegt werden. Dabei wird ein Tupel bestehend aus den Adressen der beiden Peering-Teilnehmer hinterlegt, die dann jeweils von jedem Teilnehmer signiert werden. Dadurch kann zum Beispiel die Beziehung zu einer anderen *Accountability Domain* überprüft werden.

- ***Zugehörigkeit zu einer AD*** $\{AD,EID\}_{AD}^{-1}, {}_{EID}^{-1}$
  Um die Zugehörigkeit zum Netzwerk zu verifizieren können, falls zutreffend, die Accountability Domain als auch der Endpointidentifier, jeweils signiert, hinterlegt werden. Das DNS kann dies benutzen um Einträge zu validieren, damit Angreifer, sich nicht einer falschen AD zuordnen oder ähnliches. Außerdem ist dies ein hilfreicher Eintrag um Missbrauch zu erkennen. Ein Host kann beispielsweise öfter seinen eigenen Eintrag abrufen, sollte für seine EID mehrere bzw. unbekannte Einträge bestehen, ist es wahrscheinlich, dass ein Angreifer seinen Schlüssel stehlen konnte.

- ***MAC-Adressen*** $\{Router, MAC_X, X\}_{Router}^{-1}, {}_{KX}^{-1}$
  Host können ihre MAC-Adresse bei ihrem First-Hop-Router registrieren. Dadurch können Angreifer, auch wenn sie in Besitz des Schlüssels gekommen sind, sich nicht mit einer anderen MAC-Adresse mit diesem Router verbinden.

Aber auch diese Hilfsmittel können nichts dagegen ausrichten, wenn der Host selber infiltriert wurde.

6. Bewertung

In den bisherigen Abschnitten wurde AIP ausführlich vorgestellt. Dabei wurden immer wieder die Ähnlichkeiten zu der heutigen Implementierung dargestellt. Dieser Abschnitt widmet sich aber gezielt dem Vergleich und damit gleichzeitig einer Bewertung des *Accountable Internet Protocol*.

6.1 Umsetzung und Vergleich zu IPSec

Bei AIP handelt es sich um einen Konzeptentwurf. Das heißt, dass es sich um eine Idee handelt, die das Internet sicherer machen könnte. Aber im Gegensatz zu anderen Ansätzen, wie IPSec, basiert die Idee darauf, die komplette IP Schicht auszutauschen. Wie man anhand von IPv6 sehen kann, ist solch ein Unterfangen eine riesige Aufgabe, die sich über einen langen Zeitraum zieht. Die Problematik der Anwendung liegt weniger in der technischen Machbarkeit, wie in Abschnitt 3.4 kurz erwähnt wurde, sondern viel mehr in der Trägheit eines so großen Systems. Mit IPSec, als Erweiterung für das heutige IPv4 und als fester Bestandteil von IPv6, gibt es Ansätze, die praktisch angewendet werden oder es in Zukunft sicherlich werden**.** Wie AIP bringt IPSec Kryptographie in die Internetschicht, auch wenn das vom OSI-Modell nicht vorgesehen ist [**4**]**.** Es bietet die Möglichkeit der Authentifizierung und Verschlüsselung von IP-Paketen. Werden diese Eigenschaften richtig verwendet, kann man damit eine ähnliche Sicherheitsinfrastruktur wie AIP etablieren. Wohingegen IPSec hauptsächlich Point-to-Point Sicherheit erzeugt, setzt AIP schon beim Routing an [**5**]. Der Hauptunterschied bleibt, und das wird auch noch in den nächsten Abschnitten dargestellt, darin, dass AIP ohne PKI agiert. Zusammen mit dem enormen logistischen Aufwand einer solchen Umstellung, ist es fraglich, ob dieses Protokoll praktische Anwendung finden wird. Auf der anderen Seite erhebt es auch gar nicht diesen Anspruch und möchte viel mehr einen alternativen Weg zur Lösung dieser Probleme darstellen. Die Autoren von AIP wissen durchaus, dass AIP deutlich teurer, im Sinne der Performanz, ist. Es wird sich zeigen, ob man mit der heutigen Herangehensweise diese Probleme im Griff halten kann oder ob man in Richtung einer AIP-ähnlichen Infrastruktur migrieren wird.

6.2 Absicherung von Routen

AIP hat Stärken wenn es um die Absicherung von Routen innerhalb von Netzwerken geht. Durch die Selbstzertifizierung können nur Berechtigte neue Routeninformation propagieren, was einfach, alleine durch die Adresse des Einstellers, überprüft werden kann. Aktuelle Ereignisse zeigen, dass es Bemühungen gibt, diese Absicherung auf Basis von IP zu vollziehen. Wie *heise online* [**6**] im September berichtete, haben sich eine Runde großer IT Unternehmen dazu entschlossen, ein PKI System für das Routing einzuführen. Dieses System funktioniert auf Basis vorhandener Technologien und soll in Zukunft enger mit dem BGP integriert werden. Als Beispiel für diese Integration kann S-BGP [**7**], also Secure-BGP, dienen. Auch S-BGP basiert auf einer PKI und authentifiziert Routen über Zertifikate. Das ist ein Beispiel dafür, dass diese Probleme auch ohne AIP gelöst werden können.

6.3 Selbstzertifizierung gegen PKI

AIP löst viele Probleme, indem es selbstzertifizierende Adressen anstatt einer Public-Key Infrastruktur benutzt. Durch dieses Verfahren wird unnötiges Mapping reduziert und es erlaubt automatisierte Verifikation von Adressen und ähnlichem. PKI sind fehleranfällig und schwerer wartbar, weil diese Automatisierung nur teilweise implementiert werden kann. Das heißt aber nicht, dass Selbstzertifizierung alle Probleme löst. Es fehlt die Verbindung der Adresse zur Person. Selbstzertifizierung in AIP bedeutet, dass jeder seine Adresse und damit gleichzeitig Schlüssel selber ausrufen kann. Das heißt aber auch, dass man mehrere Adressen ausrufen kann, folglich kann man sich doch nicht unter allen Umständen auf

diese Adressen verlassen. Selbstzertifizierung erlaubt es einem aber auch eine gewisse Anonymität zu wahren, im Gegensatz zur PKI, wo man sich registrieren muss und damit identifizierbar ist. Diese Diskussion soll an dieser Stelle nicht fortgeführt werden, doch könnte sie vielleicht einen Denkanstoß geben.

7. Zusammenfassung

Das *Accountable Internet Protocol* ist ein Konzeptentwurf für eine Alternative zu der heutigen IP Infrastruktur. Es zeigt wie das Internet aussehen könnte, wenn Sicherheit die aller höchste Priorität hätte. Es geht viel weniger darum, diese Architektur tatsächlich einzuführen, als viel mehr zu zeigen, was man alles besser hätte machen können und was man in Zukunft noch verbessern kann. Es zeigt, dass Accountability, also Zurechenbarkeit, für ein sicheres Internet notwendig ist. Auch wenn AIP nicht der Weg zur Zukunft sein sollte, ist aber gleichzeitig klar, dass Verfahren gefunden werden müssen, um mit den angesprochenen Problemen umzugehen. Adress-Spoofing und Route-Hijacking wird es auch weiterhin geben, aber AIP hat gezeigt, dass man es Angreifern deutlich schwerer machen kann. Dabei agiert AIP, wie deutlich beschrieben, nicht mit einer Public-Key-Infrastruktur. Vielmehr verfolgt es den innovativeren Weg der Selbstzertifizierung, die viele Verfahren spürbar vereinfacht. Es ist durchaus vorstellbar, dass Protokolle wie IPSec, die ein fester Bestandteil von IPv6 sind, um Ideen aus AIP erweitert werden. So könnte eventuell die Punkt-zu-Punkt Authentifizierung so erweitert werden, dass auch eine Authentifizierung während des Routen möglich ist. In welche Richtung die Entwicklung tatsächlich geht, wird aber nur die Zukunft zeigen.

8. Literaturverzeichnis

1 D. G. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon and S. Shenker. Accountable Internet Protocol (AIP). (Seattle, Washington, USA. 2008), SIGCOMM'08 ACM.

2 D. G. Andersen, H.i Balakrishnan, N. Feamster, T. Koponen, D. Moon and S. Shenker. Holding the Internet Accountable. (Atlanta, GA, USA November 2007), Proc. 6th ACM Workshop on Hot Topics in Networks (Hotnets-VI).

3 R. Moskowitz, P. Nikander, P. Jokela, T. Henderson. *RFC 5201: Host Identity Protocol*. Network Working Group, 2008.

4 Eckert, Claudia. *IT-Sicherheit 5. Auflage*. Oldenburg Wissenschaftsveralg GmbH, Oldenburg, 2008.

5 S. Kent, R. Atkinson. *RFC: 2401 Security Architecture for the Internet Protocol*. Network Working Group, 1998.

6 Ermert, Monika. Netzbetreiber wollen Routen sichern. *heise online*, http://www.heise.de/newsticker/meldung/Netzbetreiber-wollen-Routen-sichern-854376.html (Nov. 2009).

7 S. Kent, C. Lynn, K. Seo. Design and analysis of the Secure Border Gateway Protocol (S-BGP). (2000), DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings.