netidee

STIPENDIEN

Measuring the Gap between Standardization, Implementation and Adoption of Internet Standards

Zwischenbericht | Call 19 | Stipendium ID 7314

Inhalt

1 Einleitung....3

2 Status....3

2.1 Meilenstein 1 – CountryMonitor Publikation....3
2.2 Meilenstein 2 - Messplattformen....4
2.3 Meilenstein 3 – Vierte Publikation....4

3 Zusammenfassung Planaktualisierung....5

1 Einleitung

Seit dem Einreichen meines Projektes ist meine zweite Publikation meiner Dissertation zum Thema *“Measuring the Gap between Standardization, Implementation and Adoption of Internet Standards” auf der Internet Measurement Conference (Core Ranking: A) in Madrid akzeptiert und veröffentlicht worden.* Ich habe damit zur Forschung wie man Internet Standards im IPv6 Internet messen kann, beigetragen und eine neue Methodik entwickelt um aktive IPv6 Geräte zu finden.
In der Phase seit der Einreichung habe ich mit meiner dritten Publikation (Meilenstein 1) gewidmet. Diese ist bei der Internet Measurement Conference 2025 eingereicht und wird bis Mitte August reviewed.
Im Rahmen der TMA Konferenz im Juni 2025 in Kopenhagen konnte ich ein Poster vorstellen zum Thema CT logs und wie darin das österreichische Internet abgebildet ist.
Mein weiterer Plan ist es eine vierte Publikation zum Thema CT Log offenes Datenset oder der Geolokation von IPv6 Addressen als Follow-Up zu meiner zweiten Publikation anzustreben, welche zwar nicht für das erfolgreiche Abschließen notwendig ist, aber meiner Forschung mehr Reichweite bringt.

2 Status

2.1 Meilenstein 1 - CountryMonitor

CountryMonitor ist die Bezeichnung für eine dreijährige Messung des Ukrainischen IP Adressraum seit 2. März 2022. Dabei wurde die Paketumlaufzeit und die Antwortrate zu Ukrainischen IP Addressraums beobachtet.
Erkenntnisse:
- Großflächig Verbreitete Standards erlauben durch aktives Messen den Rückschluss auf geopolitische Ereignisse.
- Antwortende Geräte sind meist Provider-Equipment welches länger Verfügbare Notstromversorung aufweist als Router beim Endkunden. Das heißt die Dunkelziffer der beobachtenden Ausfälle könnte noch größer sein.
- Die Hauptursache in nicht-fronlinien Gebieten in der Ukraine sind Stromausfälle. Starke Korrelation mit einem von Ukrenergo veröffentlichten Datenset zu Stabilisierungsausfällen des Stromnetzes in mehreren Oblasten.

- Bisherige Methodiken missen Einblicke in kleinere regionalere Provider, was wir mit Full Block Scans ausgleichen können.
- Rerouting des Internets lässt sich durch das Aufzeichnen der Paketumlaufzeiten messen.

Meine Forschung konnte ich im Rahmen der ATNOG Q1/25 in Linz vor österreichischen Netzwerkbetreibern präsentieren. Weiters wurde die Arbeit beim Security Meetup bei Dynatrace vorgestellt und wird auf der IKT 25 in Dornbin ebenfalls präsentiert.

2.2 Meilenstein 2 – Messplattformen

Ich versuche die im Rahmen meiner Forschung durchgeführten Messungen als Messplattformen der Internet community zu Verfügung zu stellen.
So misst email-security-scans.org die Verbreitung und sichere Umsetzung von Email Standards.
Die Adaption neuer Standards ist durch meinen Fokus auf weitere Publikationen in den Hintergrund geraten.
Die bereits vorhandenen Platfformen werden auf meiner Stipendienseite Netidee & auf meiner persönlichen Homepage veröffentlicht.

2.3 Meilenstein 3 – Vierte Publikation

Anstatt von Geolocation von IP Addressen hat sich das Thema an dem ich in Q1/25 neben CountryMonitor geforscht habe zu CT Logs entwickelt.

Ein Großteil des österreichischen Internets benutzt Domainnamen um auf Ressourcen im Internet zuzugreifen. Um verschlüsselt darauf zuzugreifen werden TLS Zertifikate benötigt, welche nach Ausstellung durch eine CA in den CT Logs gespeichert werden. Diese Vorraussetzung macht CT Logs eine optimale Datenquelle für österreichische Domains, welche ihr Service über HTTPS anbieten. Um ein Gefühl dafür zu bekommen wie groß die Anzahl der Domains ist, messen wir die Anzahl der einzigartigen Domains pro Tag die in verschiedenen Logs auftauchen. Betreiber solcher CT Logs sind unter anderem große Unternehmen wie Google, Cloudflare, aber auch Letsencrypt, eine eigene Zertifikatsstelle, betreibt Logserver. Eine Liste der Betreiber findet sich hier: CT Log Betreiber. Im Zeitraum von März 2025 bis Mai 2025 (75 Tage) beobachten wir durchschnittlich 70-80 Millionen ausgestellte Zertifikate in den Logs, das entspricht 3-3.5M pro Stunde. Insgesamt haben wir 3.4 Milliarden einzigartige Domainnamen bobachten, davon 7.8 Millionen .at Domains. Betrachten wir diese auf Second-Level Granularität (SLD Ebene), also <domain>.at statt www.<domain>.at finden wir 637K (tausend) einzigartige Zertifikate.

In Zukunft kann dieses Datenset benutzt werden um Internet Standard Messungen representativer zu gestalten. Der Plan ist es nach Präsentation dieses Datensets bei der Traffic Measurement Conference in Copenhagen dieses Datenset den Internet Yellow Pages hinzuzufügen.

3 Zusammenfassung Planaktualisierung

Der erste und wichtigste Meilenstein meiner Dissertation ist abgeschlossen. Aus diesem würde sich ein neuer Meilenstein ergeben sollte die Publikation auf der IMC25 nicht akzeptiert werden.
Aus meiner Forschung sind mehrere Artifakte entstanden, die neben einer eigenen Messplatfform auch den Code zu den durchgeführten Messungen beinhaltet.
Das Thema meiner vierten Publikation hat sich auf CT Logs fokusiert. Geolocation in IPv6 konnte auf Grund mangelnder Hardware bisher noch nicht gemessen werden.
Der Meilenstein einer vierten Publikation bleibt aufrecht.

Nach der Rückmeldung im August zur IMC25 kann die Dissertationsschrift verfasst werden. Dies verschiebt sich von Juli auf August 2025.