Council of European National
Top-Level Domain Registries

IETF 115

Ruim 100 werkgroep-sessies, 2 ‘technology deep dive’-sessies, een 2-daagse IETF-hackathon en diverse side events

MARCO DAVIDS AND CASPAR SCHUTIJSER, SIDN LABS

Inhoud

Inleiding

De 115e IETF werd gehouden van 5 tot 11 november 2022 in Londen.

De missie van de Internet Engineering Taskforce (IETF) is het internet beter maken. En iedereen kan zich hierbij aansluiten. Het meeste werk gebeurt online, via mailinglijsten. Daarnaast is er 3 keer per een conferentie. De 115e IETF-meeting vond plaats van 5-11 november in Londen.

Met 1.630 deelnemers, was het een goedbezochte (hybride) meeting. Er waren 854 (ruim 52%) deelnemers fysiek aanwezig, opnieuw een stijging ten opzichte van de vorige meeting, want bij de 114e meeting lag dit percentage nog op 43%. De overige deelnemers volgden de meeting online.

De IETF-hackathon, waar 39 projecten voor waren aangemeld, werd bezocht door 452 deelnemers (350 on-site, 102 remote).

Ook ditmaal waren er nog coronamaatregelen van kracht. In de 'meeting rooms' waren mondmaskers verplicht, daarbuiten waren deze alleen maar aanbevolen (wat voor de meeste deelnemers aanleiding was om ze af te doen). Uiteindelijk zijn 4 gevallen van COVID gerapporteerd[1], tegenover 17 gevallen na afloop van de vorige meeting.

IETF-conferenties bestaan uit een volgepropte week. Er waren onder andere ruim 100 werkgroepsessies, een 'HotRFC', een plenaire sessie, 2 'technology deep dive- sessies (over QUIC) in de vroege ochtend, en daarnaast nog tal van 'side meetings'. Onderwerpen als versleuteling, internetcensuur, mensenrechten en privacy vormden daarbij een rode draad.

Het informele deel

Het weekend voorafgaand aan de IETF-conferentie wordt afgetrapt met enkele meer informele onderdelen, namelijk een hackathon, de 'IEPG' en de 'HotRFC'.

Hackathon

Op zaterdag werd aangevangen met de inmiddels traditionele hackathon. Hier worden toepasbaarheid en interoperabiliteit van concepten getoetst. Het credo van de IETF is tenslotte: "*rough consensus* ***and*** *running code*". Daarnaast moet het sociale aspect niet worden onderschat. Deelnemers van verschillende organisaties werken samen en leren elkaar beter kennen. Groepjes ontstaan spontaan en er word gewerkt aan diverse experimenten, zoals bijvoorbeeld vroege implementaties van een concept van versie 5 van het NTP-protocol of het uitgebreid rapporteren van DNS-fouten, wat leidde tot een werkend prototype. En dit zijn maar enkele onderwerpen uit de lange lijst. 2 dagen lang wordt er druk overlegd en geprogrammeerd. In totaal namen zo'n 452 enthousiastelingen hieraan deel. De hackathon wordt afgesloten met presentaties van de resultaten.

1 Dit aantal werd naderhand nog aangepast. Zie: https://www.ietf.org/blog/ietf-115-post-meeting-survey/

Bron: https://www.ietf.org/blog/ietf115-catchup/

IEPG

De zondagochtend begint steevast met de IEPG, waar onderwerpen met een operationele component aan bod komen, hoewel dit ruim wordt geïnterpreteerd. Dit keer was er onder meer een presentatie van Geoff Houston (APNIC Labs) over DoH versus DoT. De onderzoekers hebben onder andere gekeken naar de 'uptake' van beide protocollen. Dat is op zich lastig te meten, maar APNIC heeft beperkte inzage in de data van Cloudflare's 1.1.1.1 resolver, waaraan in elk geval te zien is of de DNS-verzoeken binnenkwamen via DNS-over-TLS (DoT) of DNS-over-HTTPS (DoH), of gewoon via klassieke DNS over poort 53 (Do53). Weliswaar is het marktaandeel van Cloudflare beperkt, in vergelijking tot bijvoorbeeld Google's Public DNS, maar desondanks is de data statistisch significant. Enkele van de conclusies zijn dat verreweg het meeste verkeer, zo'n 77%, nog op basis van Do53 is en dat DoT met zo'n 3% nog nauwelijks wordt gebruikt. De percentages verschillen per land en een opvallende uitschieter hierbij is Laos, waar het percentage DoT-gebruik om onduidelijke redenen veel hoger ligt. Het DoH-gebruik van zo'n 19% lijkt samen te hangen met het initiatief van Mozilla om de DoH-standaard te activeren in zijn Firefox-browser.

HotRFC lightning talks

De zondag werd afgesloten met de HotRFC lightning talks, waarbij sprekers allerlei thema's aanstippen of ideeën kunnen pitchen en daar feedback over vragen. In dit geval staat 'RFC' niet voor 'Request For Comments' (zoals de documenten geproduceerd door de IETF worden genoemd), maar voor 'Request For Conversation'. Het tempo ligt hoog; voor vragen stellen is geen tijd en feedback volgt achteraf.

In tijdsloten van 4 minuten kwamen tal van ideeën en onderwerpen voorbij. Zo greep Philip Hallam-Baker de acquisitie van Twitter door Elon Musk aan om zijn idee voor 'Everything'

nog eens onder de aandacht te brengen. Dat betreft een open document-formaat, dat kan dienen als onderliggende technologie voor een brede scope aan socialemediatoepassingen met end-to-end beveiligde communicatie en dataopslag.

Andrew Campling presenteerde over 'Encrypted Client Hello (ECH) Deployment Considerations'. ECH is een nieuwe TLS-extensie, die resterende privacyproblemen binnen TLS oplost. Want hoewel TLS-verbindingen versleuteld zijn, geldt dit niet voor potentieel gevoelige informatie zoals bijvoorbeeld de SNI of de ALPN-lijst. Zodoende kan het opzetten van een versleutelde TLS-verbinding toch nog wat informatie prijsgeven, wat in principe onwenselijk is. Maar ECH zelf, heeft ook weer bepaalde implicaties en impact. Denk aan sommige beveiligingsmaatregelen, die met ECH niet meer goed functioneren, omdat ze juist slim gebruikmaakten van de beschikbare informatie in de 'client hello', die met ECH niet meer uit te lezen is.

John Border maakte in zijn presentatie reclame voor een 'side event' over 'EToSat' (Encrypted Transport over Satellite). En Rich Kulawiec hield een pleidooi over de implicaties van massale securityscans, die op veel plekken alarmen kunnen doen afgaan en daardoor tijd en geld kunnen kosten. Hij vroeg zich af of dit als een probleem wordt ervaren en zo ja, of dit iets is wat kan en moet worden aangepakt?

Hans-Dieter Diep (LIACS/CWI) sprak over TMP (Time Modulation Protocol), een door de EU gefinancierd onderzoeksproject, dat gaat over een nieuwe techniek voor het vergroten van de end-to-end-privacy van communicatiekanalen met behulp van precisieklokken, zoals atoomklokken.

En Dan Sexton, CTO van de Internet Watch Foundation, ten slotte - vroeg zich af: "Is Privacy Preserving Web Filtering Possible?" en kondigde ook een 'side event' aan over dit dilemma. Hij ziet mogelijke technische oplossingen, waaronder homomorfe encryptie, om dit mogelijk te maken.

Dit is een selectie uit de volledige lijst van presentaties, waarbij opviel dat zaken als versleuteling en privacy vaak terugkomen als thema.

Technology Deep Dive

De 'deep dives' worden georganiseerd door de IESG. Dit is een experiment en er wordt nog gesleuteld aan het format. Het idee is om tijd te nemen om wat dieper op de techniek te kunnen ingaan. Het gaat dus om educatieve, informatieve sessies. Tijdens deze IETF waren er 2 bijeenkomsten in de vroege ochtend, waarbij dieper werd ingegaan op QUIC, een veelbelovend nieuw netwerkprotocol dat flink in de belangstelling staat.

Formele gedeelte

Uit de vele werkgroep-sessies lichten we er 2 uit:

ADD (gedeelde sessie met DPRIVE)

Hier stonden we vorige keer al vrij uitgebreid bij stil en daarom volstaan we met de opmerking dat 'Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS' binnenkort wordt bijgewerkt op basis van feedback van grote publieke resolvers, zoals Google Public DNS.

Voor de CENTR-gemeenschap is sectie 3 uit dit document relevant, waarin je leest:

```
An authoritative server SHOULD implement and deploy DNS-over-TLS
(DoT) on TCP port 853.

An authoritative server SHOULD implement and deploy DNS-over-QUIC
(DoQ) on UDP port 853.
```

Nu is dit document alleen nog maar een concept en daarom niet bindend, maar het staat wel in de belangstelling en dus kunnen zaken snel veranderen. Het kan daarom geen kwaad om alvast na te denken over de mogelijke implicaties van bovenstaande tekst.

DNSOP WG

Bij IETF115 waren er verschillende updates, maar hoorden we geen significant belangrijke nieuwe dingen.

Side meetings

De 'side meetings', ook wel bekend als BOF's, zijn bijeenkomsten die buiten het officiële programma worden georganiseerd, vaak met de bedoeling om te discussiëren over de mogelijke oprichting van een nieuwe wekgroep. Er waren tijdens IETF115 weer verschillende van dit soort side meetings. We lichten er één uit; over post-kwantumcryptografie.

Hierbij gaat het om het beveiligen van data met algoritmes die bestand zijn tegen de verwachte overweldigende rekenkracht van toekomstige kwantumcomputers. Dat lijkt misschien nog ver weg, maar is nu al relevant. Want geheime, versleutelde communicatie die wordt onderschept kan worden opgeslagen. En deze kan dan later, als er kwantumcomputers zijn, met terugwerkende kracht misschien alsnog worden gedecodeerd. Daarom is het zaak om daar nu al op te anticiperen.

Daarom wordt er al enige tijd nagedacht over het oprichten van een post-kwantumcryptografie-werkgroep (PQC WG).

Werkgroepen hebben een zogenaamd 'charter'; een beknopte tekst die beschrijft wat het specifieke probleem is dat de werkgroep wil gaan aanpakken en welke resultaten de groep wil bereiken. Tijdens deze side meeting werd er gediscussieerd over hoe het charter van

de voorgestelde PQC-werkgroep er uit zou moeten gaan zien. In het voorgestelde charter zou de werkgroep onder andere een forum moeten bieden voor discussie over problemen gerelateerd aan de transitie naar post-kwantumcryptografie en ervaringen die relevant zijn voor werk binnen de IETF op dit vlak. Maar het is expliciet niet de bedoeling dat deze werkgroep zelf nieuwe cryptografische protocollen gaat ontwikkelen.

IAB open meeting

De IAB open meeting biedt de mogelijkheid voor directe interactie tussen de gemeenschap en de IAB. De sessie bevatte de gebruikelijke updates, maar daarnaast presenteerde Mahsa Alimardani van het Oxford Internet Institute en ARTICLE 19 over hoe internettechnologie Iraanse demonstranten kan ondersteunen en vertelde Simone Basso van het Open Observatory of Network Interference (OONI) over hun censuurmetingen in Iran.

IRTF open meeting

Het belangrijkste van de IRTF Open Meeting is het uitreiken van de Applied Networking Research Prize (ANRP). De winnaars presteren dan ook hun onderzoeksresultaten. Zo sprak Gautam Akiwate over zijn onderzoek naar het risico op domeinnaam-hijacks en pleitte Daniel Wagner voor meer en betere samenwerking tegen DDoS-aanvallen.

IRTF

IETF-werkgroepen richten zich gewoonlijk op het produceren van internetstandaarden, maar daarnaast is er een aantal groepen die zich richten op breder onderzoek. Deze vallen onder de Internet Research Task Force (IRTF). Daar komen regelmatig interessante onderwerpen voorbij.

Zo is de toenemende centralisatie van het internet (en het tegengaan daarvan) een onderwerp binnen de Decentralized Internet Research Group (dinrg). Deze werkgroep werkt momenteel aan een interessant document getiteld 'A Taxonomy of Internet Consolidation'. Dit is bedoeld om de discussie beter te stroomlijnen door zaken te duiden en eenduidige definities (van de term 'consolidatie') te bieden. In het verlengde hiervan wordt er gewerkt aan een document getiteld 'Protocol and Engineering Effects of Consolidation'.

De Measurement and Analysis for Protocols (maprg)-sessies staan bekend om hun kwalitatief goede inhoud. Deze keer met wederom diverse interessante presentaties.

Bij de vorige IETF-meeting ging het nog over de resultaten van een onderzoek naar DoH-resolvers. Maar tijdens deze 115e ging het al over de impact van de nieuwste aanwinst op dit gebied, namelijk DNS-over-QUIC (DoQ). Een voorzichtige conclusie is dat DoQ bijdraagt aan het sneller laden van eenvoudige webpagina's (een verbetering van 10% ten opzichte van DoH).

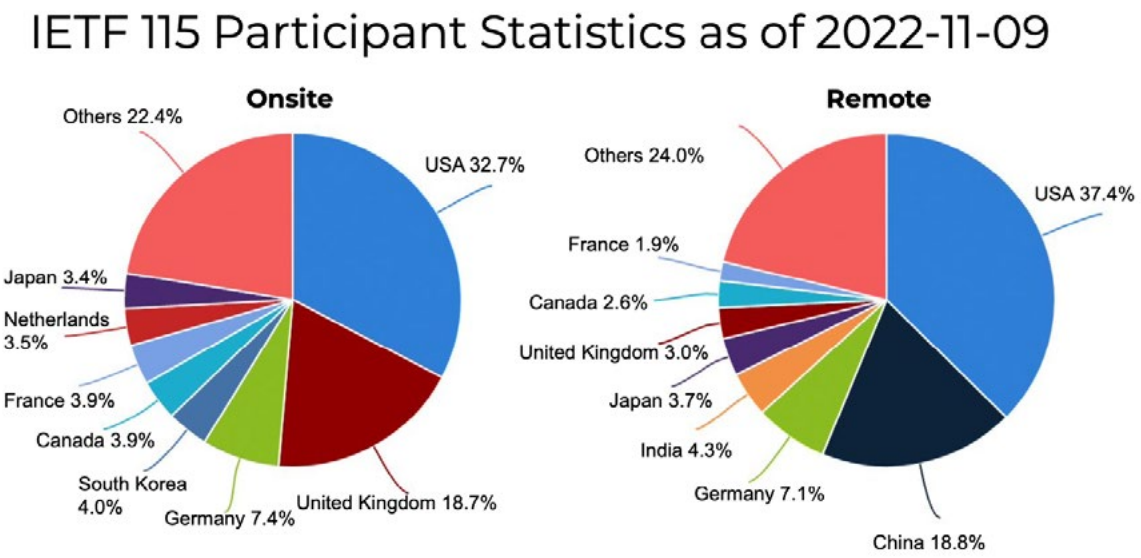
Een andere presentatie ging over een onderzoek naar de performance van Starlink, het satellietnetwerk voor breedbandinternettoegang, van SpaceX. De prestaties van Starlink qua bandbreedte zijn vergelijkbaar met een 100 Mbit/s-verbinding over land. Maar er treedt wel vaker verlies op, zelfs onder lichte belasting.

En ook dit keer was er aandacht voor de oorlog van Rusland tegen Oekraïne. Er is namelijk onderzocht of er een verschuiving waarneembaar was (sinds de start van het conflict op 24 februari 2022) in het .ru- en .рф-topleveldomein. Denk daarbij aan de hosting van websites, de gebruikte 'autoritatieve nameservers' of de uitgifte van TLS-certificaten. De conclusie is dat Rusland al ruim voor de aanvang van het conflict ervan doordrongen was dat het internet een drukmiddel zou kunnen worden. En er werden significante verschuivingen waargenomen. Maar die hebben voor Rusland niet geleid tot existentiële problemen.

Sinds een halfjaar worden er pogingen ondernomen om de toekomstgerichte nieuwe internetarchitectuur genaamd SCION te standaardiseren binnen de IETF. Op dit moment vindt deze discussie vooral plaats binnen de Path Aware Networking Research Group (panrg). Eén van de belangrijke stappen die is ondernomen is het kort beschrijven van SCION en vervolgens het opsplitsen van SCION in losse componenten waarover dan los gediscussieerd kan worden over standaardisatie. Ook is er nu een document beschikbaar over de SCION control-plane PKI. Bij IETF 115 werd een statusupdate gegeven.

Epiloog

IETF115 was wederom een hybride conferentie. Ten opzichte van de 114e meeting was de 'onsite' aanwezigheid opnieuw toegenomen. De intentie is om de IETF-conferenties voorlopig nog in hybride vorm te blijven organiseren. Dat betekent dat 'remote' deelnemers ook actief kunnen deelnemen via Meetecho. Hoewel dit nog niet altijd soepel verloopt, gaat het wel steeds beter.



Bron: https://datatracker.ietf.org/meeting/115/materials/slides-115-ietf-sessa-ietf-chair-iesg-report-00

De volgende IETF-conferentie is van 25 tot 31 maart 2023 in Yokohama.

Council of European National
Top-Level Domain Registries

Over CENTR

CENTR is de vereniging van Europese landcode-top-level domein (ccTLD)-registers, zoals .de voor Duitsland of .si voor Slovenië. CENTR telt momenteel 52 volwaardige en 9 geassocieerde leden - samen zijn ze verantwoordelijk voor meer dan 80% van alle geregistreerde domeinnamen wereldwijd.

De doelstellingen van CENTR zijn het bevorderen van en deelnemen aan de ontwikkeling van hoge normen en 'best practices' onder ccTLD-registers.

Volledig lidmaatschap staat open voor organisaties, rechtspersonen of individuen die een landcode-topniveaudomeinregister beheren.

CONTACT

CENTR VZW/ASBL
Belliardstraat 20
1040 Brussel, België
0885.419.166 | RPR Brussels

+32 2 627 5550

secretariat@centr.org

www.centr.org

VOLG ONS

Volg ons op Twitter of LinkedIn om op de hoogte te blijven van de activiteiten en rapporten van CENTR