No domain left behind

is Let's Encrypt democratizing encryption?

M. Aertsen[1], M. Korzyński[2], G. Moura[3]

[1]National Cyber Security Centre
The Netherlands

[2]Delft University of Technology
The Netherlands

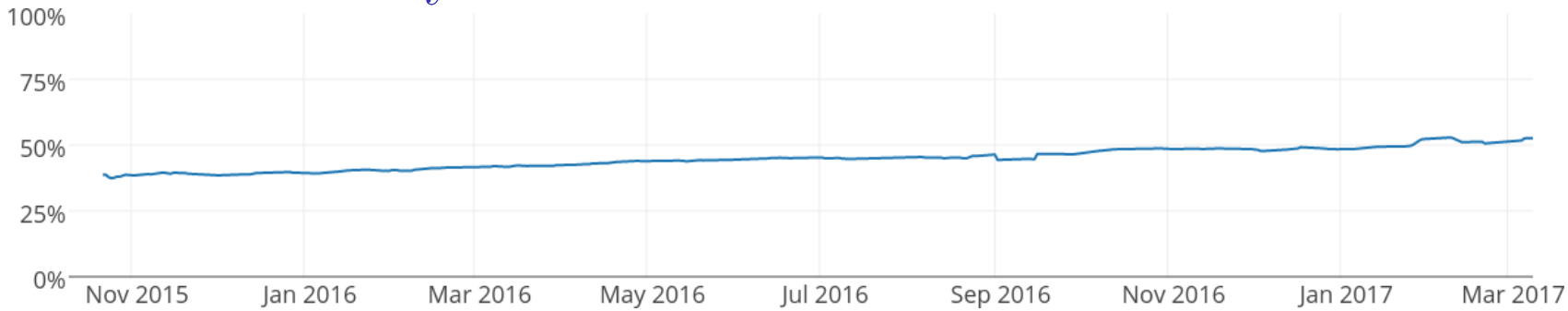
[3]SIDN Labs
The Netherlands

ICANN58, Tech day

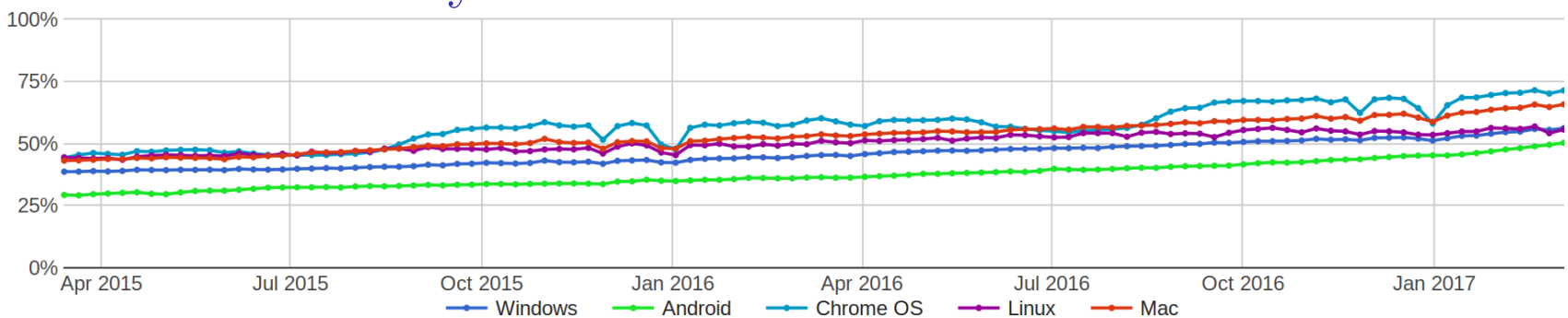
More than half of web traffic nowadays is encrypted

Yet that leaves out a lot of people without HTTPS

Firefox telemetry[1]



Chrome telemetry[2]



[1] https://telemetry.mozilla.org/, plot based on *Let's Encrypt* stats page

[2] https://www.google.com/transparencyreport/https/metrics/

Certificates are required for encryption on the web

Obtaining and deploying certificates is not free

- Cost: purchase, deployment and renewal
- Complexity: request, deployment (at scale)

Let's Encrypt[3] aims to make encrypted traffic ubiquitous

- Reducing certificate cost of purchase, renewal to zero
- Automation of request, issuance and deployment
  (ACME: protocol[4] and clients, e.g. Certbot[5])

[3] https://letsencrypt.org

[4] https://ietf-wg-acme.github.io/acme/

[5] https://certbot.eff.org/

No domain left behind

Is *Let's Encrypt* democratizing encryption?

Research question

"In its first year of certificate issuance,
has Let's Encrypt been successful in democratizing encryption?"

Approach

- Analyze issuance in the first year of *Let's Encrypt*
- Show adoption trend from various perspectives
- Analyze coverage for the lower-cost end of the market

Contribution

We show that

- 98% of certificates are issued outside Alexa 1M
  - yet issuance is not restricted to lower end of the market
- *Let's Encrypt*'s growth is attributed to adoption by major players
  - 3 hosting providers are responsible for 47% of the *Let's Encrypt* certified domains
- Issuance is dominantly for the lower-cost end of the market (shared hosting)
- The majority of certificates are correctly renewed after their first expiration (90 days)

And find that

Let's Encrypt has indeed started to democratize encryption.

Methodology

Period covered

One year of *Let's Encrypt* certificate issuance, Sept 2015-2016

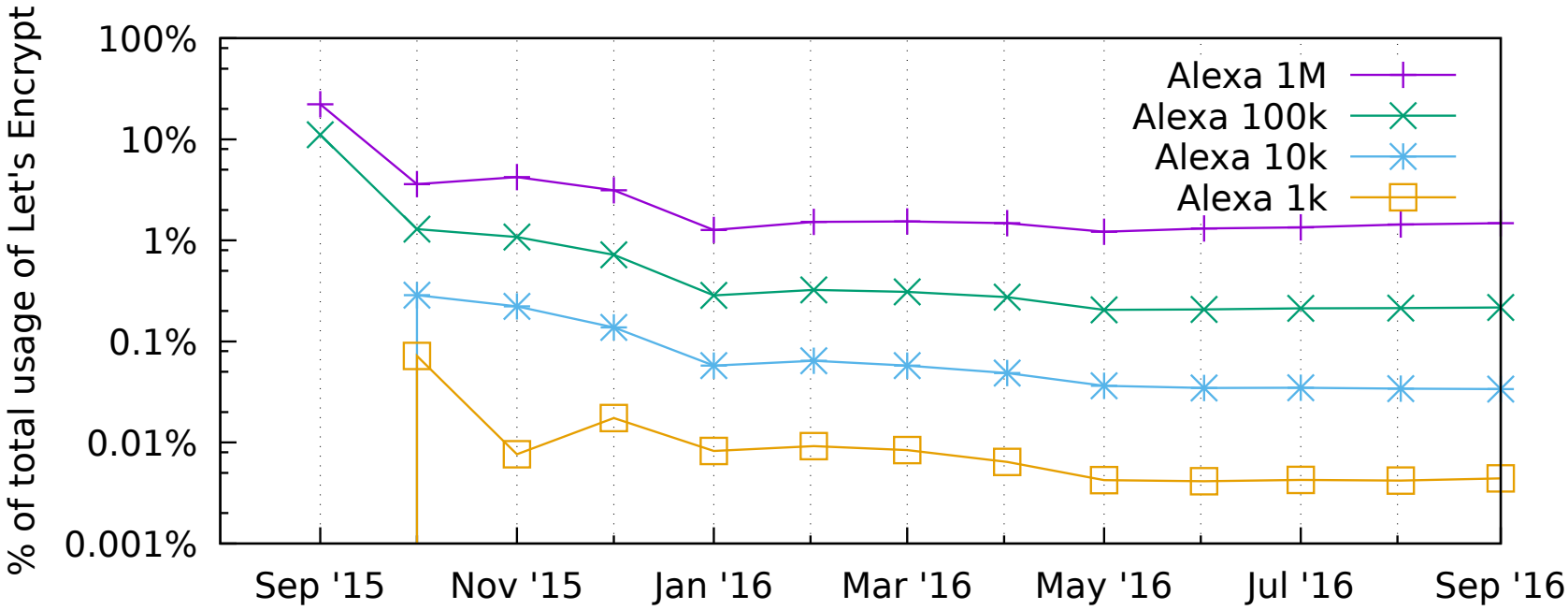
Results based on FQDNs reduced to 2LD/3LD form

- e.g. `example.org` (2LD) or `example.co.uk` (3LD), depending on availability per TLD registry

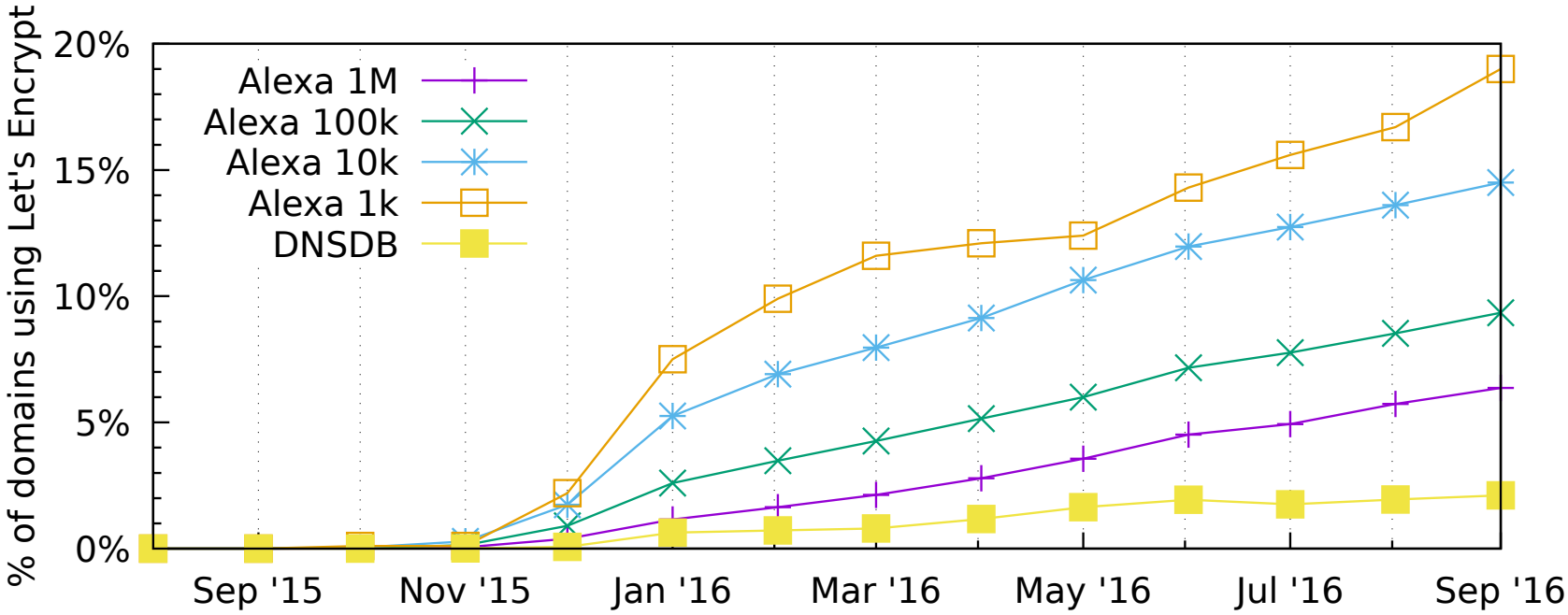
Datasets

Certificates	Certificate transparency
Domain to IP mapping	Farsight DNSDB
Organization mapping	Methodology from previous work, using `whois` data & Maxmind GEOIP2

98% of certificates are issued outside Alexa 1M ...



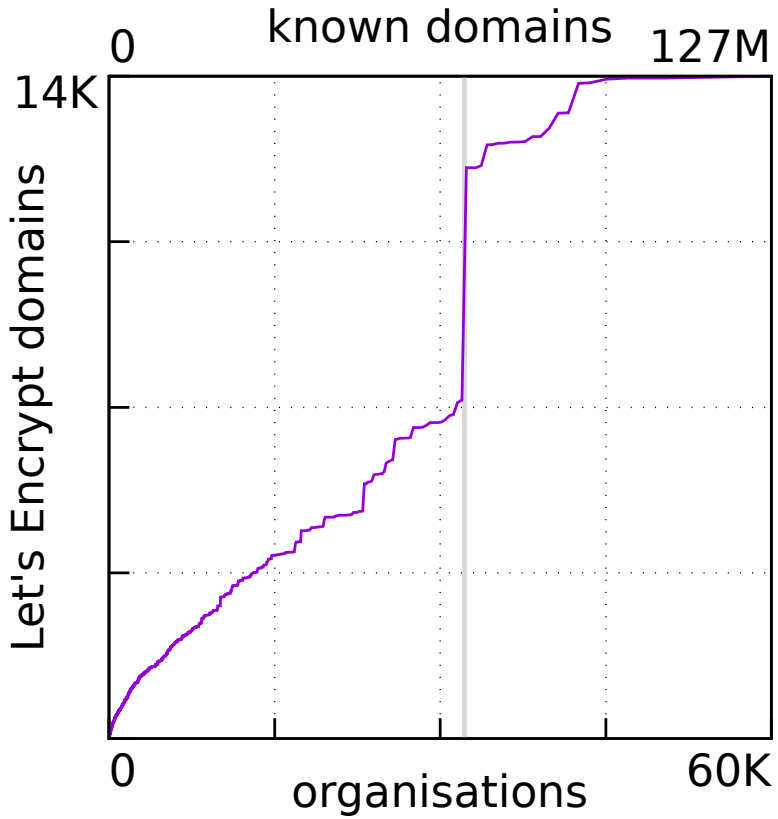
...yet issuance is not restricted to lower end of market



Growth is attributed to adoption by major players

3 hosting providers are responsible for 47% of the *Let's Encrypt* certified domains

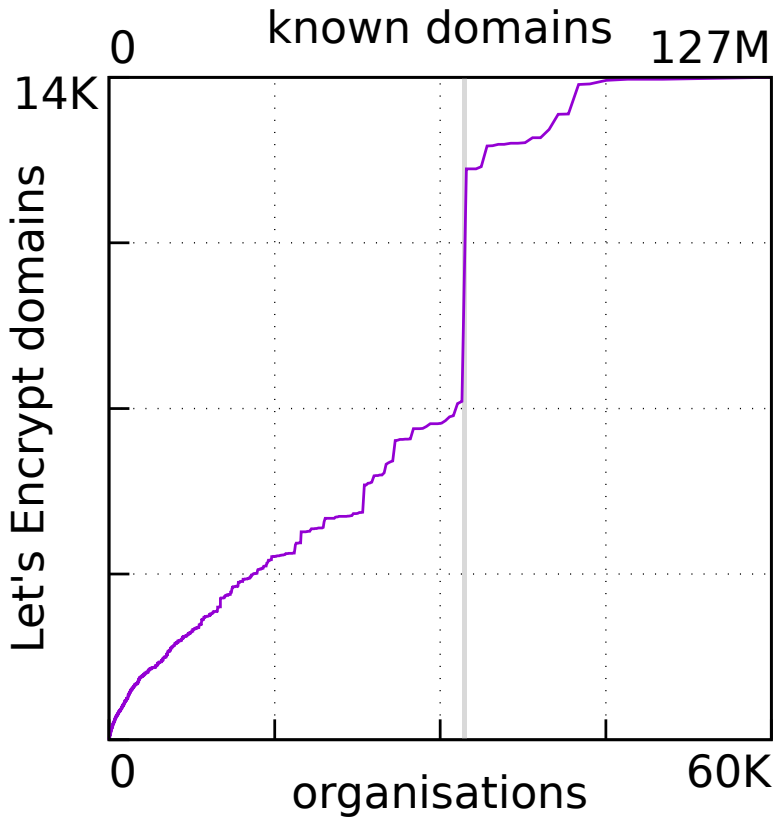
November 2015



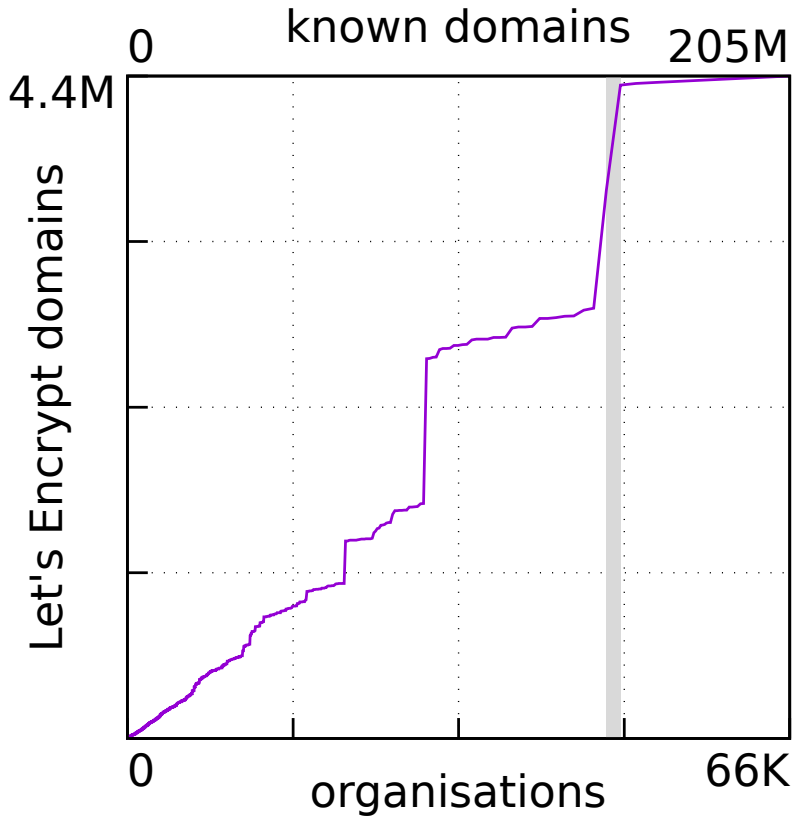
Growth is attributed to adoption by major players

3 hosting providers are responsible for 47% of the *Let's Encrypt* certified domains

November 2015



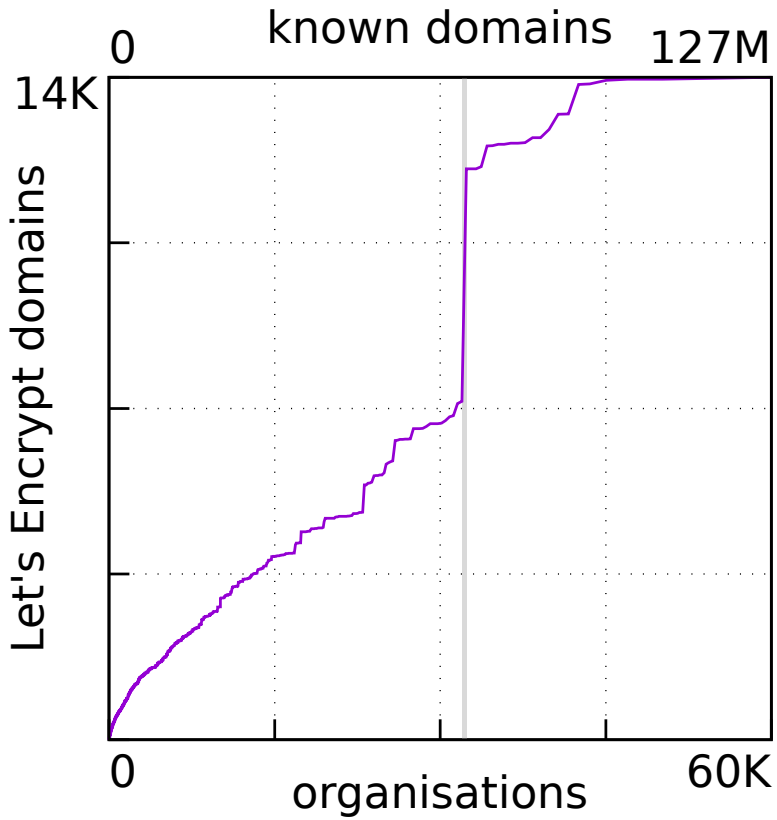
September 2016



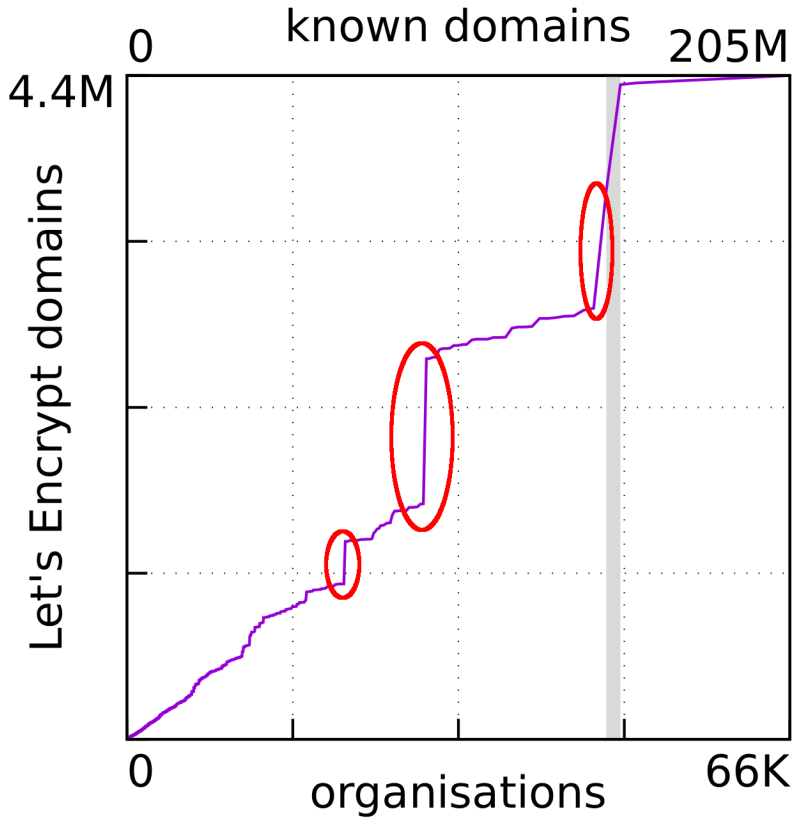
Growth is attributed to adoption by major players

3 hosting providers are responsible for 47% of the *Let's Encrypt* certified domains

November 2015

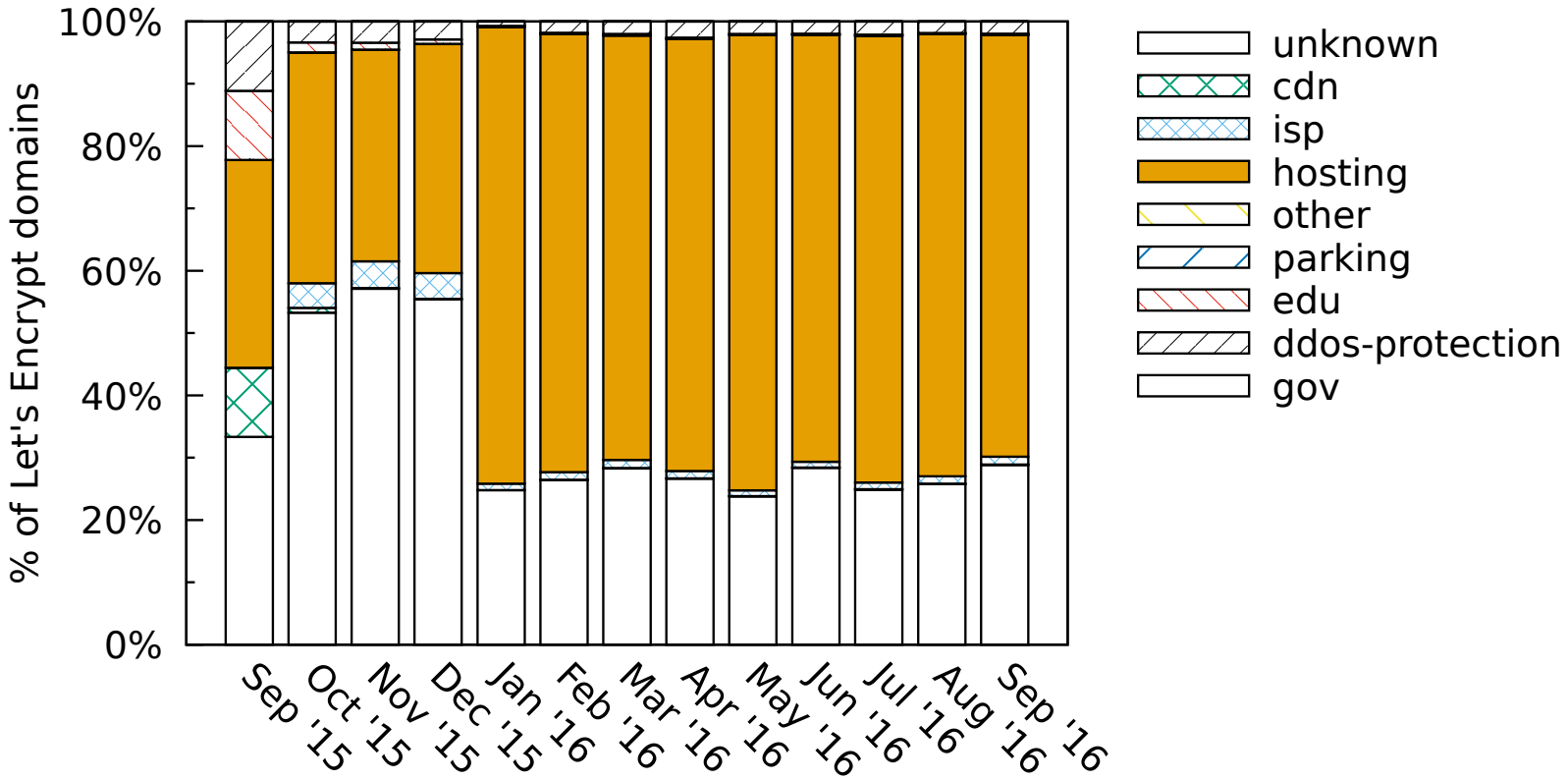


September 2016



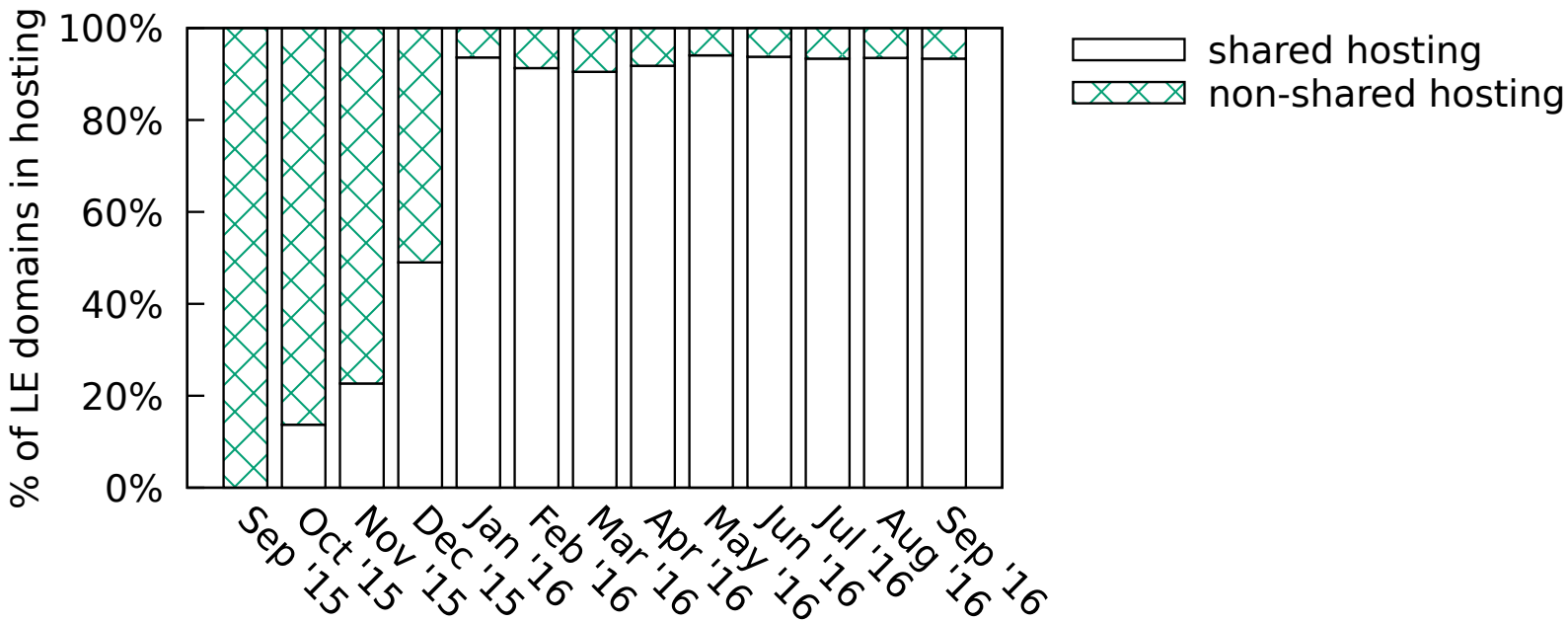
Issuance is dominantly for web hosting

So far, no surprises



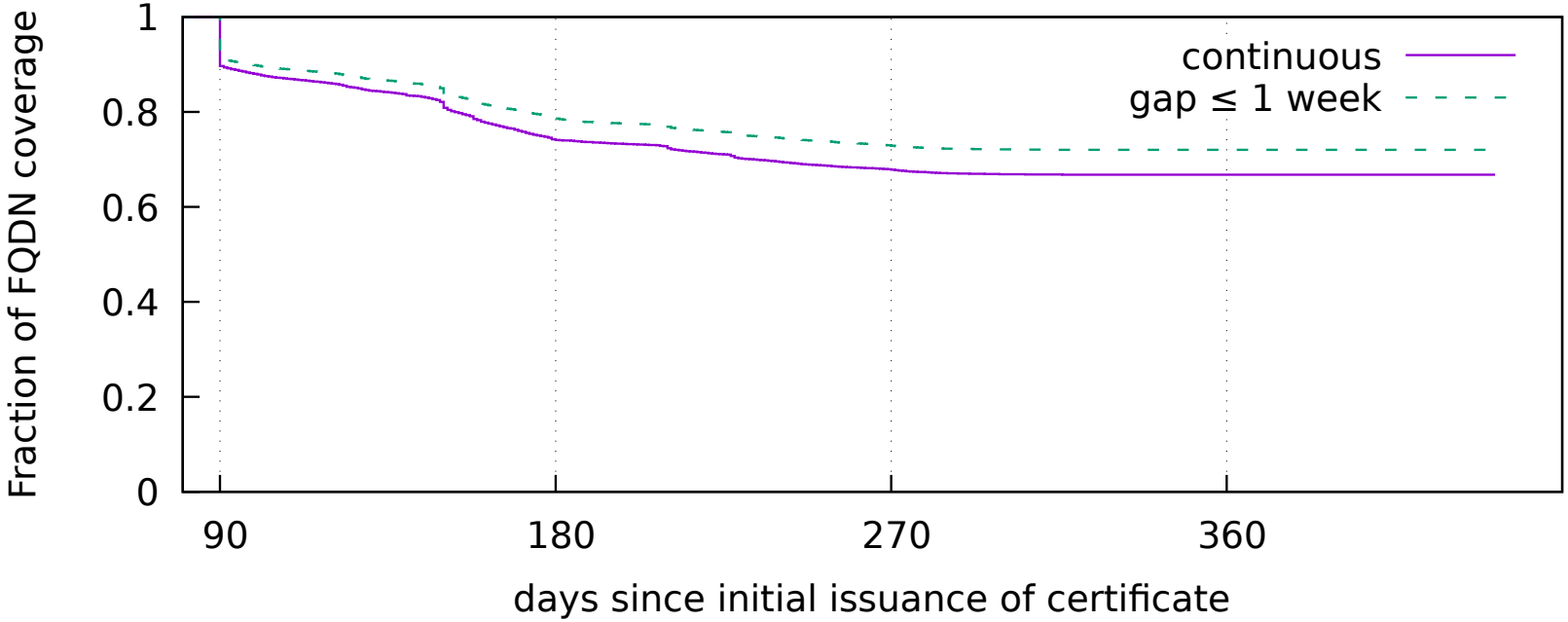
Over 90% of domains in hosting are on shared hosting

Issuance is dominantly for the lower-cost end of the market



Let's Encrypt certificates are valid for 90 days

The majority of certificates are correctly renewed after their first expiration



Summary

We find that *Let's Encrypt* has indeed started to democratize encryption

Certificate issuance in the first year of *Let's Encrypt*

- used widely, dominated by the low-cost share of the market (shared hosting)
  - which would be unlikely to deploy the complex and costly X.509 certificates before
- enables big hosting providers to issue and deploy certificates for their customers in bulk
  - thus quickly and automatically enable encryption across a large number of domains
  - e.g. 47% of *Let's Encrypt* certified domains are hosted at three large hosting companies (Sept 2016)
- 70% of the *Let's Encrypt* certified domains remain active after the first issuance of the certificate[6]

[6] *Let's Encrypt* certificates expire after three months

In conclusion

Future work

- extend measurement period
- issued versus deployed
  - active scans on shared hosting require prior knowledge of domains served (SNI)
- use by malicious actors

Contact details

Maarten Aertsen
maarten.aertsen@ncsc.nl

Maciej Korzyński
maciej.korczynski@tudelft.nl

Giovane Moura
giovane.moura@sidn.nl

For more information, including related work & references, please see arXiv:1612.03005 (pending publication)

Absolute and relative growth

Time series for FQDNs, domains, and DNSDB ratio