No domain left behind:
is Let’s Encrypt democratizing encryption?

Maarten Aertsen\textsuperscript{1}, Maciej Korczyński\textsuperscript{2}, \textbf{Giovane C. M. Moura}\textsuperscript{3}, Samaneh Tajalizadeh-Khoob\textsuperscript{2}, Jan van den Berg\textsuperscript{2}

\textsuperscript{1}National Cyber Security Centre  
The Netherlands

\textsuperscript{2}Delft University of Technology  
The Netherlands

\textsuperscript{3}SIDN Labs  
The Netherlands

\textbf{IETF98 - IEPG}  
Chicago, IL, March 26th, 2017
Disclaimer

- None of the authors is in any way affiliated with Let’s Encrypt
- In other words: we do not speak for them
- But if you like their work, you may consider supporting them
The Encryption Rush

Ed Snowden NSA’s revelations

- Massive, widespread surveillance
- Worst nightmares came true
The Encryption Rush

Ed Snowden NSA’s revelations

Consequences:
- For many, it was a wake-up call (and panic)
- Market distrust in vendors
- Provided a great momentum for better security

Reactions:
- IETF: RFC 7258, RFC 7624
- iOS/Android: mobile phone encryption by default
- Cloud providers enabling encryption everywhere
- ...

Massive, widespread surveillance
Worst nightmares came true
More than half of web traffic is encrypted nowadays
Yet that leaves out a lot of people without HTTPS

Firefox telemetry\(^1\)

Chrome telemetry\(^2\)

---

\(^1\) [https://telemetry.mozilla.org/](https://telemetry.mozilla.org/), based on *Let’s Encrypt* stats page

\(^2\) [https://www.google.com/transparencyreport/https/metrics/](https://www.google.com/transparencyreport/https/metrics/)
Certificates are required for encryption on the web

Barriers to ubiquitous web encryption

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

*Let’s Encrypt* aims to make encrypted traffic ubiquitous

- Issue and re-issue costs: **$0.00**
- Complexity mitigated by **automation**
  1. ACME protocol
  2. and clients, e.g. Certbot

---

3. https://letsencrypt.org
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: measurements

- 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
Methodology

- Period covered: Sept. 2015-2016 (1st year)
- Results based on FQDNs reduced to 2LD/3LD form
  - a.b.c.d.com → d.com

Datasets

<table>
<thead>
<tr>
<th>Certificates →</th>
<th>Certificate transparency^6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain to IP mapping →</td>
<td>Farsight DNSDB^7</td>
</tr>
<tr>
<td>Organization mapping →</td>
<td>Methodology from previous work^8, using whois data &amp; Maxmind GEOIP2</td>
</tr>
<tr>
<td>Registration info →</td>
<td>.nl registry (SIDN)</td>
</tr>
</tbody>
</table>

^6 [https://www.certificate-transparency.org/known-logs](https://www.certificate-transparency.org/known-logs)
^7 [https://www.dnsdb.info/](https://www.dnsdb.info/)
Let’s Encrypt Adoption Rate

- Steady growth
Who’s using Let’s Encrypt?

- 98% of certificates are issued outside Alexa 1M . . .
Who’s using *Let’s Encrypt*?

- ...yet issuance is not restricted to lower end of the market
  - meaning: big players also use in their subdomains
Growth is attributed to adoption by major players
3 hosting providers are responsible for 47% of the Let’s Encrypt certified domains

November 2015

![Diagram showing growth in Let's Encrypt domains from November 2015 to September 2016.](image)
Growth is attributed to adoption by major players

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

November 2015

Let’s Encrypt domains

known domains

organisations

September 2016

Let’s Encrypt domains

known domains

organisations
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

Automation works!!
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

- Shared hosting = 10 domains/IP
- *Let’s Encrypt* reaches those with less incentive to encrypt

---

Let’s Encrypt certificates are valid for 90 days
The majority of certificates are correctly renewed after their first expiration
Let’s Encrypt: domain age use

- Case study .nl
- Determine the age of the domain when the cert was issued

Median, Q25, Q75 and number of monthly new certificates for .nl domains
Let’s Encrypt: deployment

- https scans + cert processing (lower bound)
- 25K randomly chosen Let’s Encrypt FQDN

![Bar chart showing FQDN categories and their counts. The categories include noDNS, http406error, noTLS, sniError, tlsOK-notLE, and tlsOK-LE-Expired. The y-axis represents the FQDN counts, ranging from 0 to 20k. The x-axis lists the categories. The counts are as follows: noDNS 2465, http406error 1422, noTLS 2143, sniError 141, tlsOK-notLE 2846, tlsOK-LE-Expired 15803.]
Conclusions

We show that

- *Let’s Encrypt* has been a success
  - Reduces costs & complexity
- Democratize encryption by covering low cost end of the market (shared hosting)
  - but big players also use it
- Automation works: *Let’s Encrypt*’s allows for bulk issuing
  - 3 hosting providers are responsible for 47% of the *Let’s Encrypt* certified domains
- 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.
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

Giovane C. M. Moura
giovane.moura@sidn.nl

Download our paper at:
https://arxiv.org/abs/1612.03005