TLS 1.3 in Practice:
How TLS 1.3 Contributes to the Internet

Published in: the Web Conference 2021
Authors: Hyunwoo Lee, Doowon Kim, Yonghwi Kwon

Summarized by

Sangwon Lim (sangwonlim@snu.ac.kr)

2022-08-10

Contents

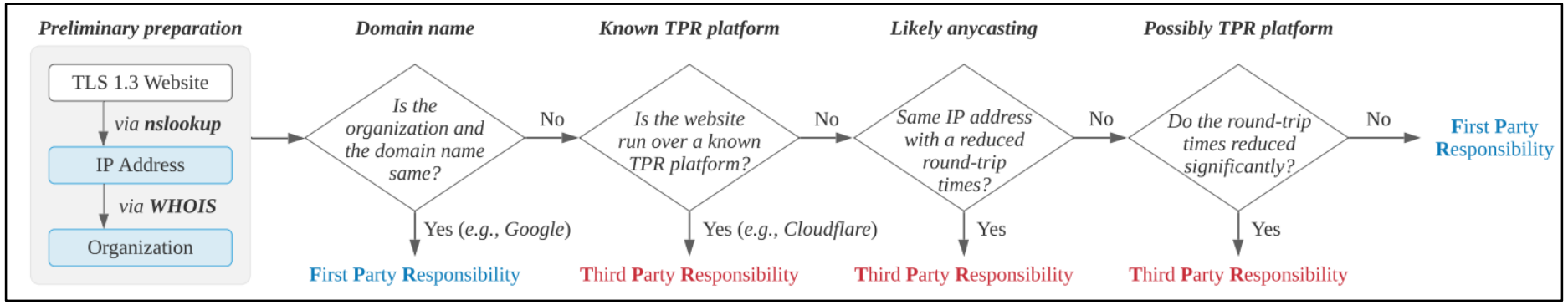
Introduction

- Transport Layer Security (TLS) has become the de-facto standard protocol for secure communications
  - ✓ As of October 2020, more than 90% of Internet traffic is communicated over TLS

- The authors look closely at TLS 1.3 in practice due to the significant impact of TLS in the web ecosystem
  - Adoption
  - Security
  - Performance
  - Implementation

Data Collection (1/2)

- Data Types
  - (D1) Security Parameters
    - ✓ *ClientHello* and *ServerHello*
  - (D2) Handshake Messages
    - ✓ *TLS 1.2 and TLS 1.3 full handshake*
  - (D3) Platform Information
    - ✓ *whether first-party responsibility (FPR) or third-party responsibility (TPR)*



< Platform Identification >

Data Collection (2/2)

- Targets
  - Alexa 1M websites
- Period
  - Sept. 17th, 2018 ~ Dec. 31st, 2020 (837 days[1])
- Observatory
  - Eight different AWS regions: Eastern North America (Ohio), Western North America (California), South America (San Paulo), Western Europe (Paris), South Africa (Cape City), East Asia (Seoul), Southeast Asia (Mumbai), and Oceania (Sydney)

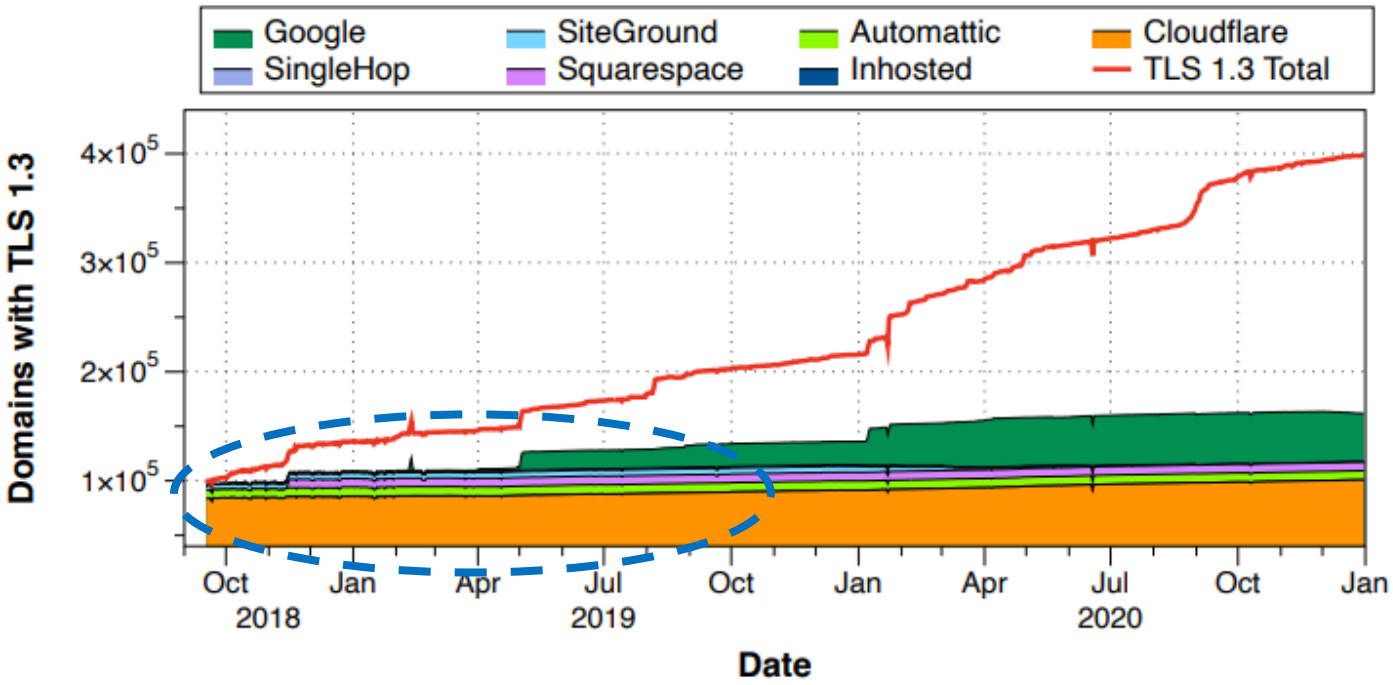
1) There were network outages for 17days, which are pruned out from the dataset

TLS 1.3 in practice

- Adoption
- Security
- Performance
- Implementation

TLS 1.3 Adoption

- It is mainly led by TPR[1)] platforms such as CDNs and web hosting companies

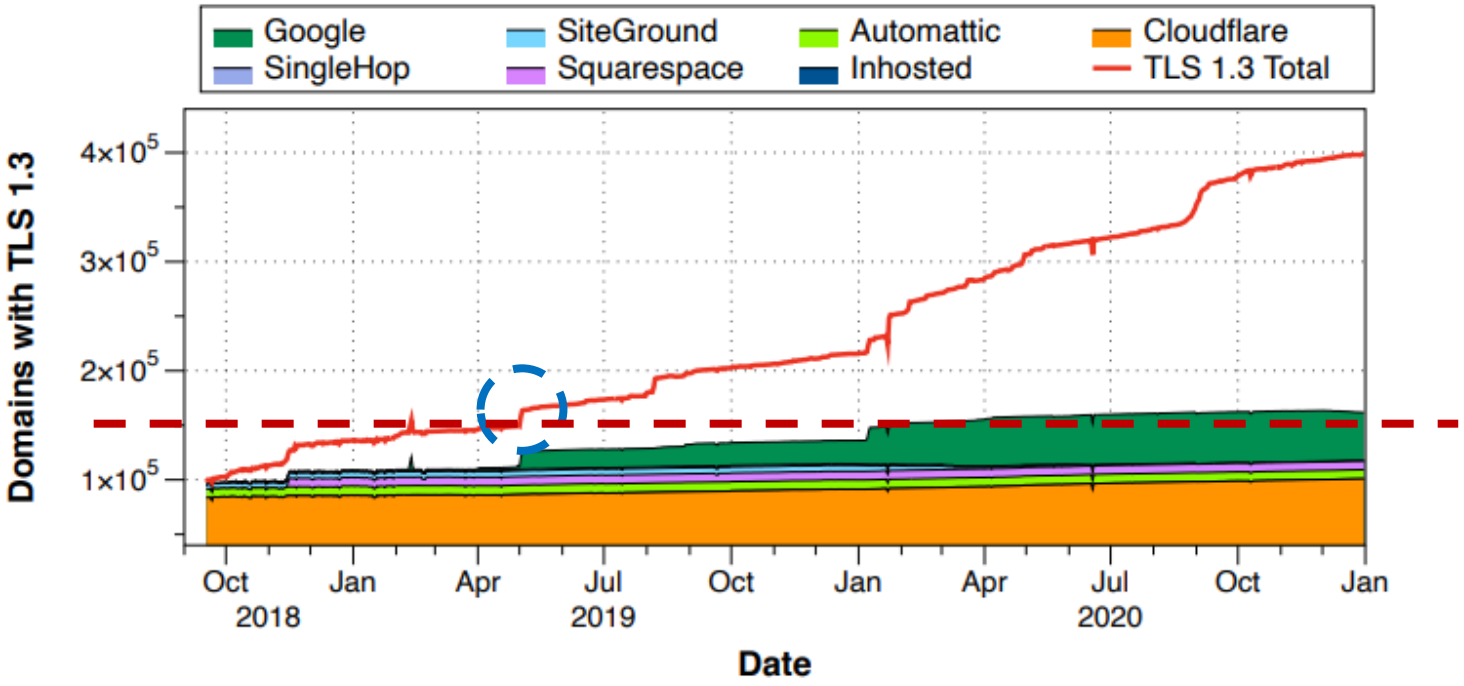


< TLS 1,3 adoption ratio by platforms >

1) Third-party responsibility

TLS 1.3 Adoption

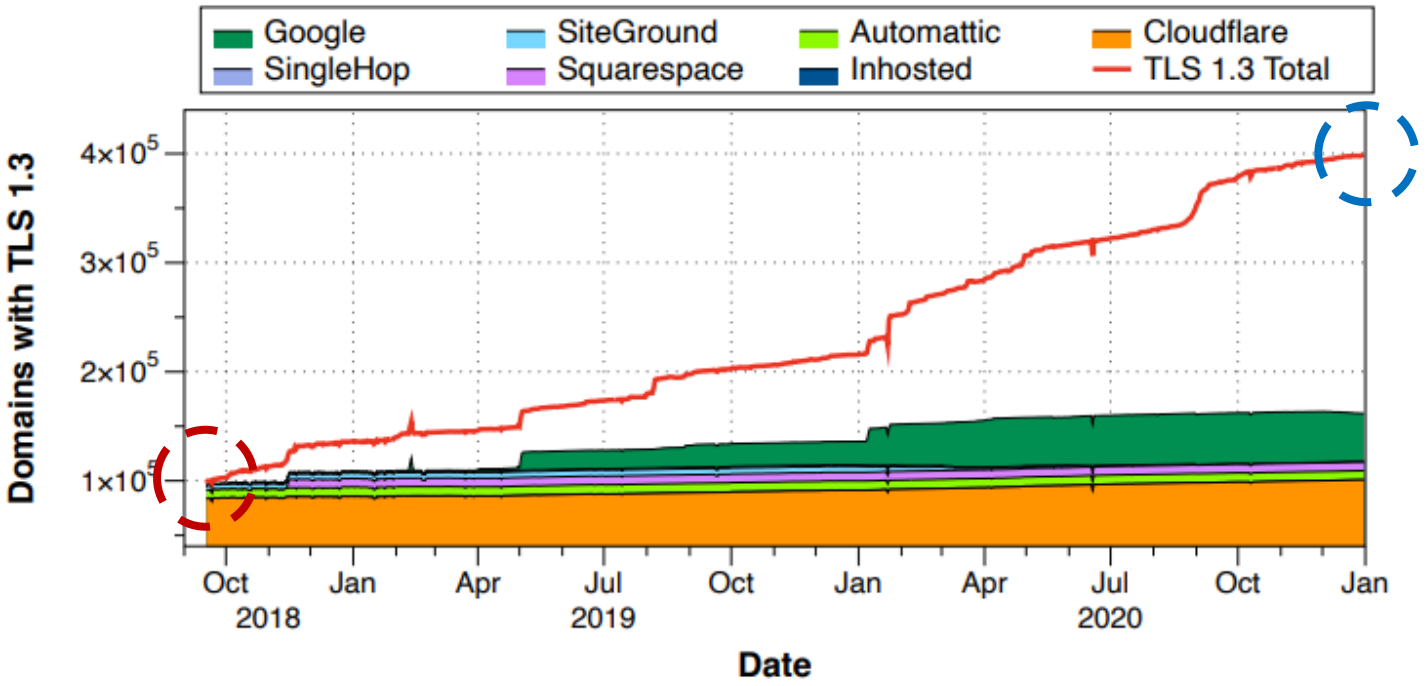
- It takes only 264 days (Apr. 30th, 2019) after TLS 1.3 was officially approved (Aug. 10th, 2018) to reach over 15% adoption
  - ✓ The shift from TLS 1.1 to TLS 1.2 needed around five years to reach the 15% adoption



< TLS 1,3 adoption ratio by platforms >

TLS 1.3 Adoption

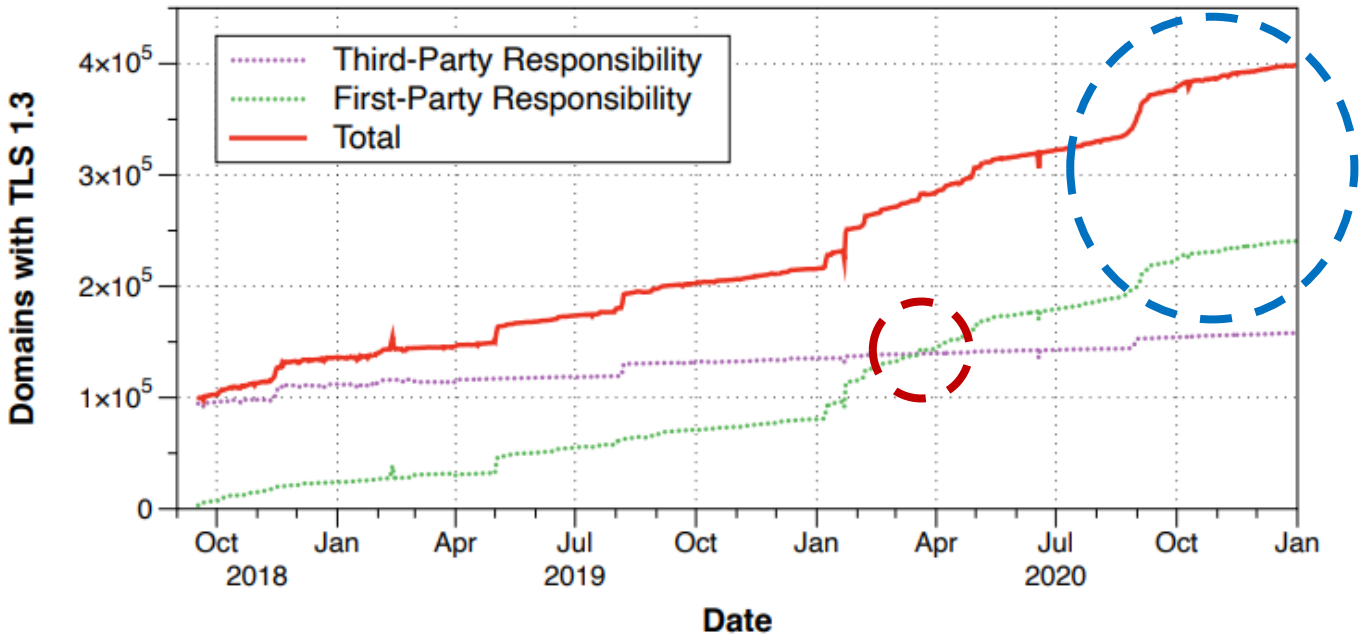
- The ratio of TLS 1.3 adoption is continuously increasing
  - ✓ From 11.78% on Sept. 17th, 2018 to 48.09% on Dec. 31st, 2020



< TLS 1,3 adoption ratio by platforms >

TLS 1.3 Adoption

- The recent increase is caused by websites served over FPR[1)] platforms
  - ✓ After Mar. 20th 2020, websites over FPR platforms account for more than 50% of the TLS 1.3 adoption

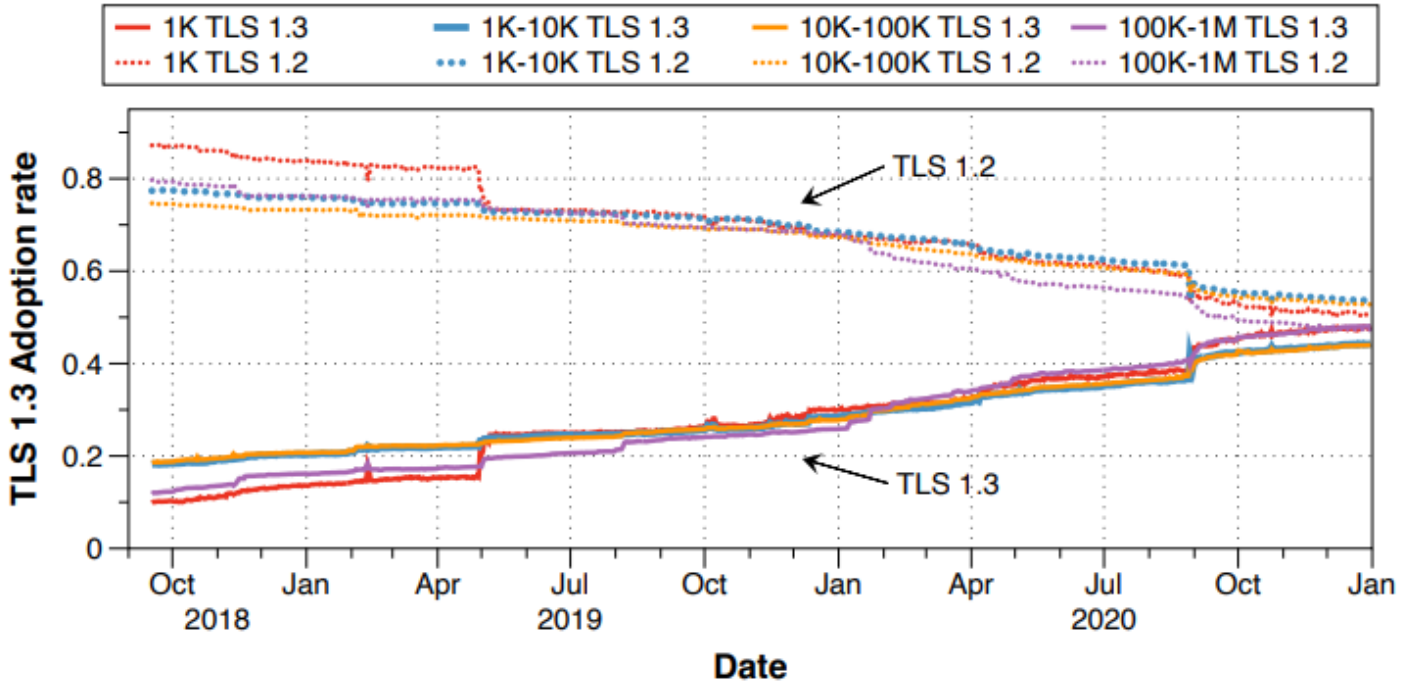


< TLS 1.3 adoption ratio by who has responsibilities >

1) First-party responsibility

TLS 1.3 Adoption

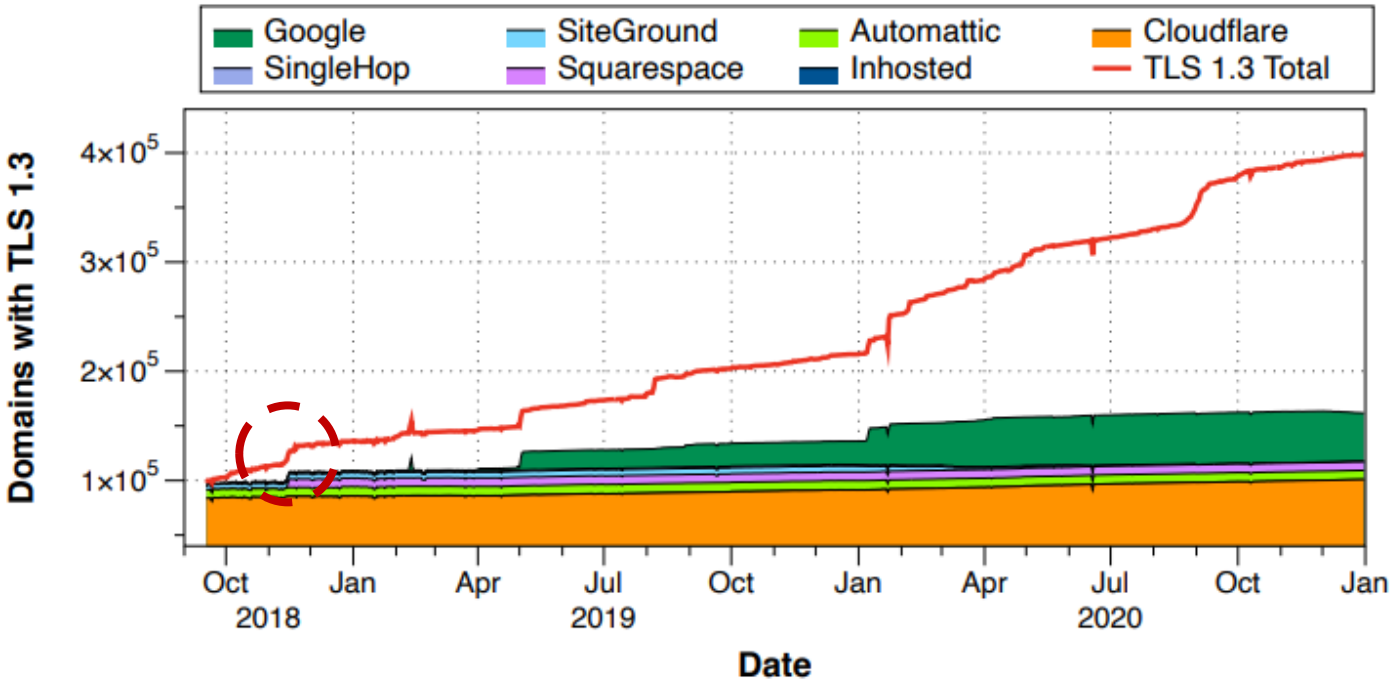
- There is no strong positive correlation between the Alexa ranks and the TLS 1.3 adoption rate



< TLS 1.3 adoption ratio by Alexa rank >

TLS 1.3 Adoption

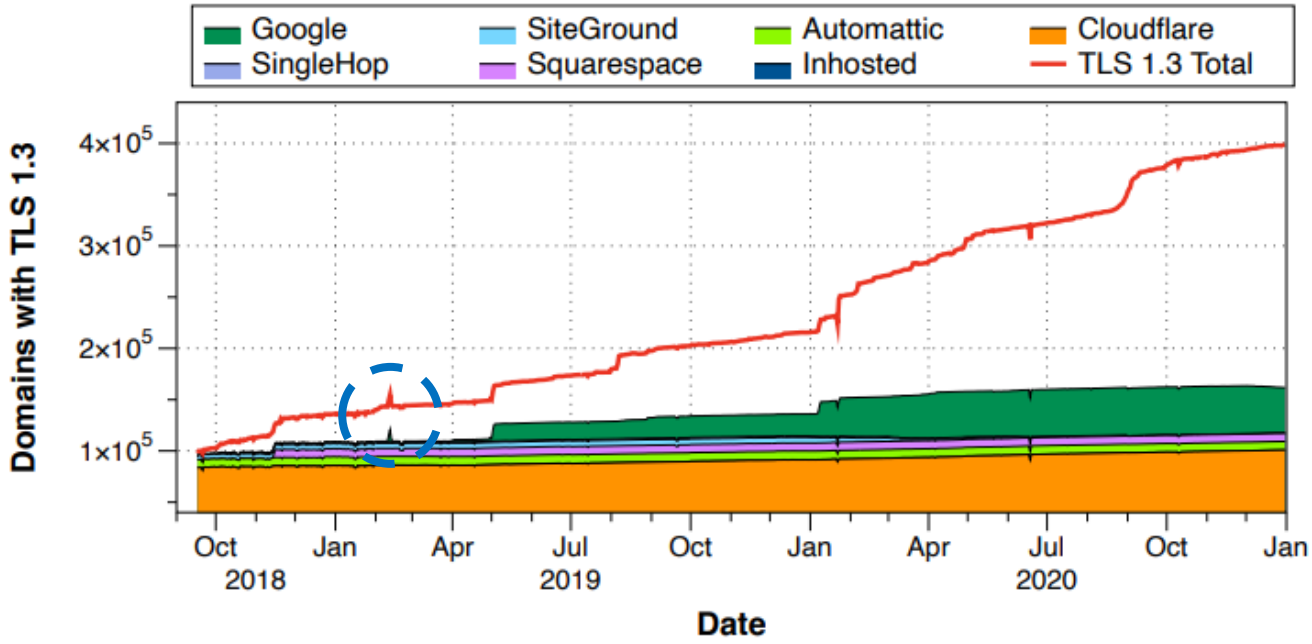
- *Inhosted* initiated support for TLS 1.3 for 1,696 websites on Nov. 14th, 2018
- *Squarespace* enabled TLS 1.3 for 4,789 websites on Nov. 15th, 2018 and other 3,001 websites on Nov. 16th, 2018



< TLS 1,3 adoption ratio by platforms >

TLS 1.3 Adoption

- On Feb. 10th, 2019, only 649 websites supported TLS 1.3 by Google Platform
- The number increased to 6,760 and 11,962 websites on Feb. 11st and 12nd, respectively
- It dropped to 664 websites on Feb. 14th



< TLS 1,3 adoption ratio by platforms >

TLS 1.3 in practice

- Adoption
- Security
- Performance
- Implementation

TLS 1.3 Security

- 61.5% of TLS 1.3 websites are directly upgraded from TLS 1.2

Pattern	FPR	TPR	Total
1.0 → 1.3	1,267 (0.5%)	543 (0.3%)	1,810 (0.5%)
1.1 → 1.3	20 (0.0%)	4 (0.0%)	24 (0.0%)
1.2 → 1.3	174,870 (72.7%)	70,265 (44.5%)	245,135 (61.5%)
1.3	11,702 (4.9%)	63,815 (40.4%)	75,517 (19.0%)
Unstable	52,653 (21.9%)	23,454 (14.8%)	76,107 (19.1%)
Total	240,512 (100.0%)	158,081 (100.0%)	398,593 (100.0%)

< Changes of TLS version upgrade[1)] >

1) The highest TLS versions that each website supports in our observation period

TLS 1.3 Security

- Security Benefits
  - 4,829 (TLS 1.3 supported) websites that have upgraded to use **forward-secret cipher suites** from non-forward-secret cipher suites
  - 17,094 sites have changed non-AEAD cipher suites to **AEAD cipher suites** by upgrading to TLS 1.3

TLS 1.3 Security

- 19.1% of the websites support TLS 1.3 on a particular day but falls back to TLS 1.2 later

Pattern	FPR	TPR	Total
1.0 → 1.3	1,267 (0.5%)	543 (0.3%)	1,810 (0.5%)
1.1 → 1.3	20 (0.0%)	4 (0.0%)	24 (0.0%)
1.2 → 1.3	174,870 (72.7%)	70,265 (44.5%)	245,135 (61.5%)
1.3	11,702 (4.9%)	63,815 (40.4%)	75,517 (19.0%)
Unstable	52,653 (21.9%)	23,454 (14.8%)	76,107 (19.1%)
Total	240,512 (100.0%)	158,081 (100.0%)	398,593 (100.0%)

< Changes of TLS version upgrade[1)] >

1) The highest TLS versions that each website supports in our observation period

TLS 1.3 Security

- Two representative scenarios cause the instability
  - Case #1: Downgraded again after being upgraded to TLS 1.3
  - Case #2: Migration to servers with lower TLS versions

	FPR	TPR
Case #1	32,013 (60.8%)	5,392 (23.0%)
Case #2	12,597 (23.9%)	15,099 (64.4%)
Both	2,031 (3.9%)	1,636 (7.0%)
Others[1)]	6,012 (11.4%)	1,327 (5.7%)
Total	52,653 (100.0%)	23,454 (100.0%)

< Websites of unstable TLS 1.3 >

1) The instability occurs because of the multiple platform services

TLS 1.3 Security

- Others
  - How many days the websites sustain their lower TLS versions

Case	FPR	TPR
Case #1	97.4 (78)	80.7 (47)
Case #2	211.5 (157)	121.8 (43)
Both	236.5 (188)	139.7 (61)

< Average (and median) of downgraded days per case >

  - Regional Differences
    - ✓ 357 cases in which clients from different regions establish different TLS version sessions
    - ✓ Some platforms only support TLS 1.2 in certain regions

TLS 1.3 in practice

- Adoption
- Security
- Performance
- Implementation

TLS 1.3 Performance

- The average performance gain of TLS 1.3 is more than 57.9%[1)]
  - The most significant improvements is in South Africa since it is located (on average) geographically farther from the Alexa 1M websites
  - The correlation between the round-trip time and the FPR gain is 0.87

	Eastern N. America	Western N. America	South America	Western Europe	South Africa	East Asia	South East Asia	Oceania
Round Trip Time (ms)	51.7	61.2	102.9	40.5	138.1	120.9	136.2	126.6
Average of Gain (%)	76.7	63.1	66.1	57.9	76.8	72.9	77.1	59.0
Average of FPR Gain (%)	84.6	83.3	86.9	78.9	91.1	88.9	87.3	86.4
Average of TPR Gain (%)	69.0	41.1	45.2	34.3	58.9	57.8	66.6	27.9

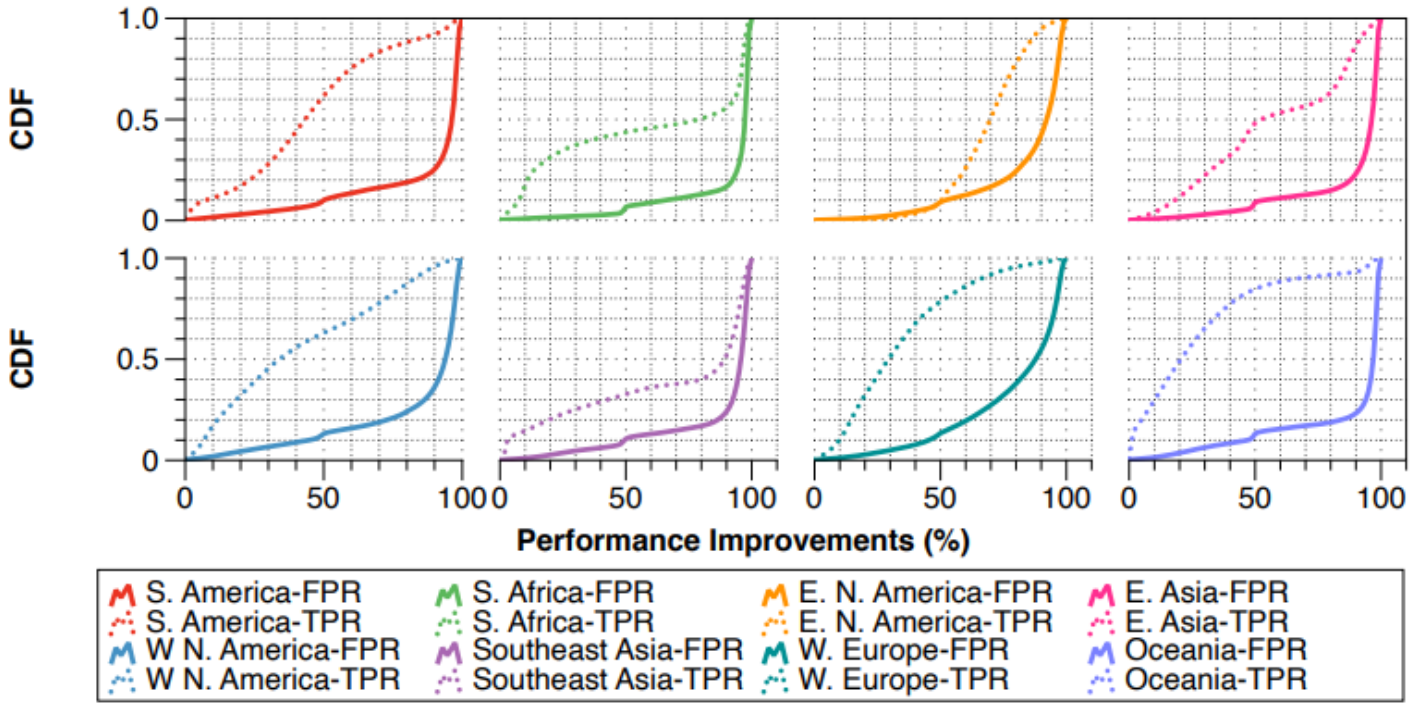
< Averaged round trip time and performance gain >

1) The performance gain defined as

$$\left(1 - \frac{\text{(Elapsed Time for TLS 1.3 Full Handshake)}}{\text{(Elapsed Time for TLS 1.2 Full Handshake)}}\right) \times 100\ (\%)$$

TLS 1.3 Performance

- TLS 1.3 can be more beneficial to websites which cannot use CDN services
  - ✓ The TPR platform servers tend to be closer to the clients



< Delay latency of the TLS 1.3 handshake >

TLS 1.3 in practice

- Adoption
- Security
- Performance
- Implementation

TLS 1.3 Implementation

- Downgrade Attack Protection
  - Server
    - ✓ **Most of the TLS 1.3 servers embed the downgrade sentinels** in their ServerHello
    - ✓ While 98 servers (0.03%) do not embed the sentinels
    - ✓ 39 (out of the 98 servers, 39.8%) are over the Facebook platforms
  - Client
    - ✓ Firefox: started on Jan. 7th, 2020, **516 days after** TLS 1.3 was approved (Aug. 10th, 2018).
    - ✓ Chrome: started on Apr. 13rd, 2020, **613 days after** –
    - ✓ Edge: does **not** support it **yet**

TLS 1.3 Implementation

- Certificate Extensions
  - Server
    - ✓ Of the total 399K TLS 1.3 websites, **71 websites (0.02%)** include their **SCTs**[1)]
    - ✓ **98,861 websites** (**28.4%** out of 399K TLS 1.3 websites) provide **OCSP**[2)] responses, but **39.3% out of 101,155 responses fail in verification**

1) Signed certificate timestamps
2) Online Certificate Status Protocol

TLS 1.3 Implementation

- Many critical security features of TLS 1.3 are not fully implemented yet in the client-side libraries

TLS Library	Version	Downgrade Protection	Certificate Extensions[1)]
Apple CoreTLS	167	○	○
BoringSSL	Latest*	●	●
Fizz	Latest*	○	○
Mozilla NSS	3.61	●	●
OpenSSL	1.1.1i	●	●
WolfSSL	4.6.0	●	○

*: The source code is cloned from the public repository on Feb. 5th, 2021. ●: fully supported. ○: not fully supported.

< Whether TLS Libraries incorporate the two new features of TLS 1.3 >

1) SCTs & OCSP

TLS 1.3 Implementation

- Many TLS libraries' vulnerabilities can be addressed by adopting TLS 1.3

TLS Library	Total	Category 1	Category 2	Category 3
BoringSSL	2	0	1	1
Fizz	2	0	0	2
Mozilla NSS	3	0	1	2
OpenSSL	25	0	4	21
WolfSSL	18	2	1	15
Total	**62**	**2**	**13**	**47**

< CVEs regarding the TLS Libraries >

- Category 1) the vulnerability introduced due to TLS 1.3
- Category 2) the vulnerability that can be addressed if TLS 1.3 is adopted
- Category 3) the vulnerability that is not related to any particular version of TLS

Conclusion

- This paper presents a comprehensive analysis of TLS 1.3 in terms of its adoption, security, performance, and implementation

- Observations
  1. The adoption rate of TLS 1.3 has rapidly increased compared to the previous versions of TLS, led mainly by third-party platforms such as CDNs
  2. Websites(19.1%) suffer from unstable support for TLS 1.3
  3. TLS 1.3 achieves reduced delays over TLS 1.2, which is more beneficial for first-party responsibility platforms than third-party responsibility ones
  4. Many implementations of TLS libraries do not properly support the new features of TLS 1.3, and many vulnerabilities can be mitigated by simply adopting TLS 1.3