

TLS Measurement



Soraya Alli
Martin Petrauskas
CY4740 - Network Security



1.

Project Overview

Project Overview

- **SSL/TLS Analysis** of world's **top 10,000 visited websites**
 - list retrieved from **Tranco** (tranco-list.eu) on **March 4, 2020**
- **SSL Labs API**
 - Interested in overall **grade**, supported **protocols** and susceptibility to **vulnerabilities**
- Breakdowns by **industry**, **geography**, and **logarithmic**.
- **Prior study** surveyed ~450k sites from **Alexa's** top 1 million with a **focus on cipher suites and key negotiation**

Analyzing 10,000 Sites

- SSL Labs API takes an average of 150 seconds to run the server test
- We ran 10 EC2 Instances for ~ 1 week
- Only 8,422 sites could be analyzed
 - Reasons include:
 - Unable to resolve domain name
 - Unable to connect to the server
 - Connection timed out
 - Connection reset
 - Handshake failure
 - Incomplete results





2a.

Overall Breakdown: Grade

B

Frequent Rating

Grade	A+	A	A-	B	C	F
# of sites	550	1614	12	5818	151	277
% of sites	6.53	19.16	0.14	69.08	1.79	3.29



2b.

Overall Breakdown: Supported Protocols



2.48%

Any SSL



6.22%

SSL 2.0

Released in 1995
Superseded in 1996
Deprecated in 2011

100%

SSL 3.0

Released in 1996
Deprecated in 2015

99.92%

Any TLS



61.88%

TLS 1.0

70.6%

TLS 1.1

Released in 1999 and 2006

Deprecated* in 2020

*by major browsers like Firefox and Google

99.56%

TLS 1.2

Released in 2008

29.3%

TLS 1.3

Released in 2018

Highest Protocol Supported

2,466
TLS 1.3

1
TLS 1.1

0
SSL 3.0

5,913
TLS 1.2

35
TLS 1.0

0
SSL 2.0

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in blue and others in grey.

2c.

Overall Breakdown: Vulnerabilities

534

Vulnerable Websites

165

Poodle

7

Poodle TLS

1

Heartbleed 

17

Freak

68

ZombiePoodle

21

GoldenDoodle

44

OpenSSL
LuckyMinus20

12

Drown

8

SleepingPoodle

68

Bleichenbacher

15

OpenSSL CCS

8

Logjam

Other Security Findings

1802

**Support
Heartbeat
Extension**

48

0-LengthPaddingOracle

369

**Support RC4
Ciphers**

223

**Don't Support
TLS_FALLBACK_SCSV**

Still Vulnerable to Heartbleed

```
CY4740-FinalProject : bash — Konsole
File Edit View Bookmarks Settings Help
martin@martin-X1C7:~/NortheasternUniversity/CY4740/CY4740-FinalProject$ nmap -p 443 --script ssl-heartbleed weiyangx.com

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-12 03:21 EDT
Nmap scan report for weiyangx.com (211.144.130.162)
Host is up (0.41s latency).

PORT      STATE SERVICE
443/tcp   open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.
|   State: VULNERABLE
|   Risk factor: High
|   OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.
|
|   References:
|   http://cvedetails.com/cve/2014-0160/
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|   http://www.openssl.org/news/secadv_20140407.txt
|_

Nmap done: 1 IP address (1 host up) scanned in 16.66 seconds
martin@martin-X1C7:~/NortheasternUniversity/CY4740/CY4740-FinalProject$
```

Interesting Results

- Sites that scored an A+ (twitter.com, wikipedia.org)
- Sites that scored an F (apple.com)
- SSL v2.0 & v3.0 still in use
- >50% of sites still use TLS 1.0 & 1.1
- Heartbleed being present in the top 10,000 sites



2d. **Overall Breakdown:** Logarithmic

Overview

~10,000 were scanned, broken logarithmically into 4 buckets:

- ⊙ Ranks 1-10
- ⊙ Ranks 11-100
- ⊙ Ranks 101-1000
- ⊙ Ranks 1001-10000

Overview of Results

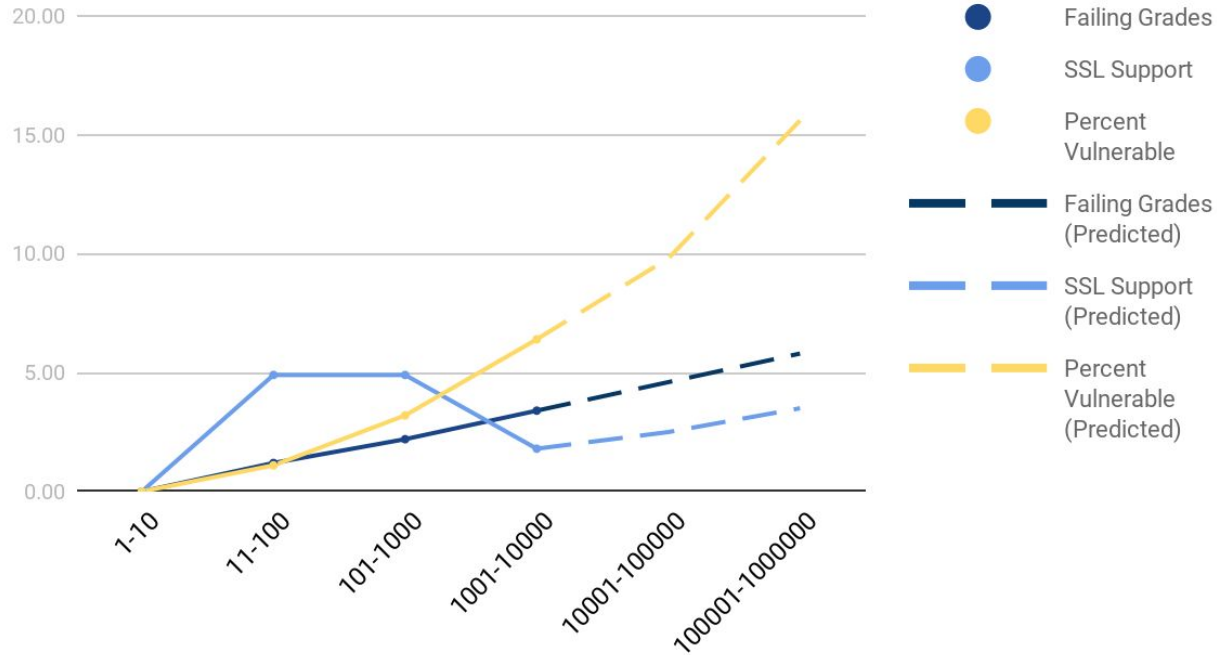
Bucket	Avg Grade	Failing Grades	SSL Support	% of TLS 1.3	% vulnerable	Major Vulnerabilities
Ranks 1-10	B	0%	0%	50%	0%	None!
Ranks 11-100	B	1.2%	4.9%	33%	1.1%	ZombiePoodle & Poodle
Rank 101-1000	B	2.2%	1.8%	28.5%	3.2%	8 Different Vulnerabilities*
Rank 1001-10000	B	3.4%	2.5%	29.3%	6.4%	13 Different Vulnerabilities**

*OpenSSLCcs, OpenSSLLuckyMinus20, Bleichenbacher, ZombiePoodle, GoldenDoodle, 0-LengthPaddingOracle, Poodle, Drown

**Heartbleed, OpenSSLCcs, OpenSSLLuckyMinus20, Bleichenbacher, ZombiePoodle, GoldenDoodle, 0-LengthPaddingOracle, SleepingPoodle, Poodle, PoodleTLS, Freak, Logjam, Drown

Logarithmic Predictions

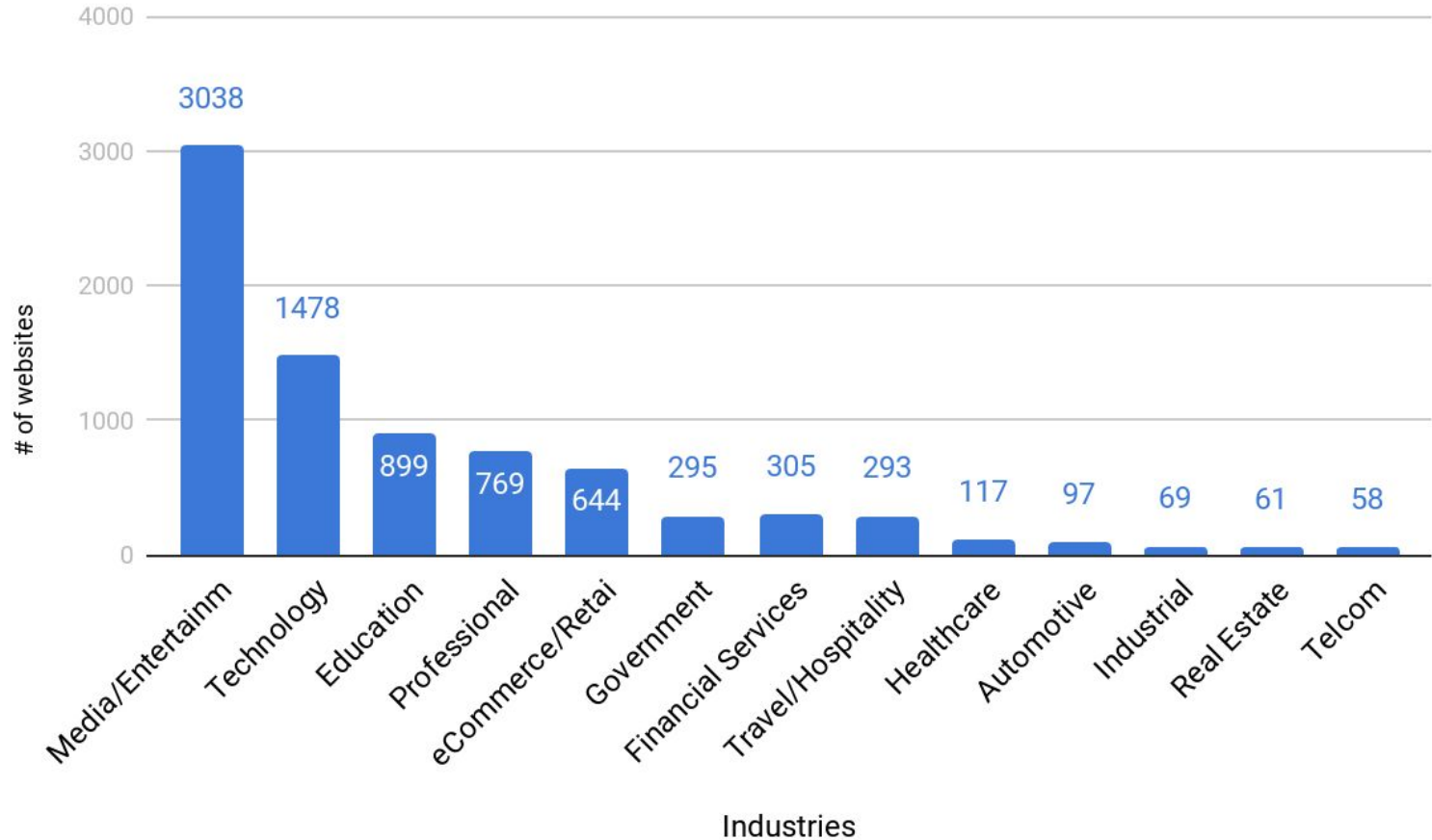
Logarithmic Breakdown w/ Predictions



A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting different levels of connectivity or importance. The lines are thin and gray, creating a mesh-like structure.

3. **Industry Breakdown**

Industry Breakdown





3a.

Industry Breakdown: Grade

Findings

- All industries were dominated by B ratings
- Industrial, Automotive, Financial, and Government had the highest percentage of A ratings
 - Along with Education and E-Commerce, these industries each had over 30% of sites with A+/A-
- Telecom had the lowest percentage of A ratings, at 13.7%
- Automotive and E-commerce had the highest number of F ratings while Healthcare had the least



3b.

Industry Breakdown: Supported Protocols



Findings

- Real Estate is more likely to still support SSL, with nearly 5% of sites supporting either 3.0 or 2.0
 - Automotive follows with 4% of sites supporting SSL
- 99.9% or 100% of sites within each industry support some version of TLS
 - 100% of Telecom sites support TLS *only*
- TLS 1.3 is least adopted in the Telecom industry
- TLS 1.3 is more widely adopted in the Entertainment, Healthcare, and Technology industries

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines, with some nodes highlighted in blue and others in grey.

3c.

Industry Breakdown: Vulnerabilities



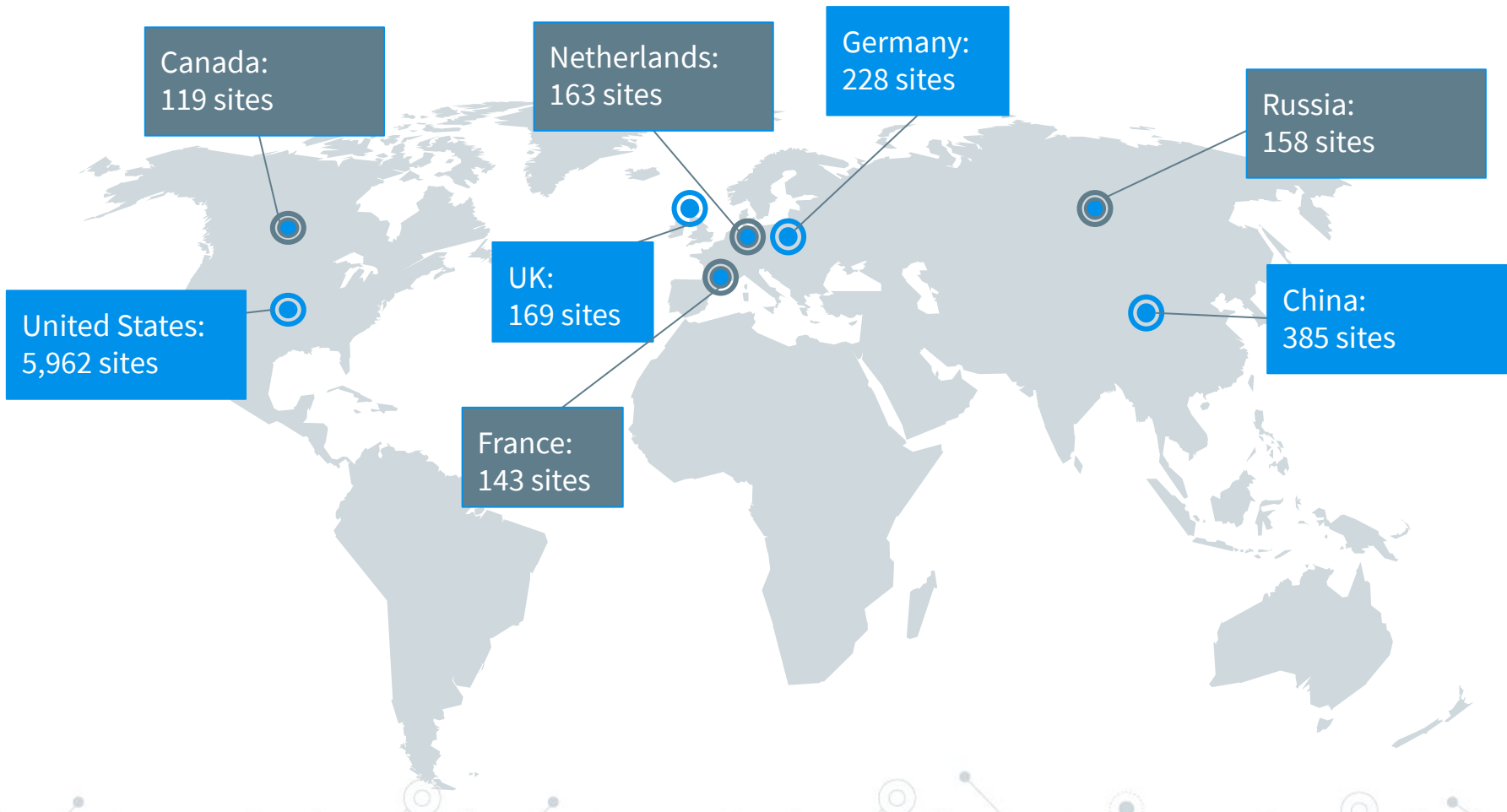
Industry	% of Vulnerable Sites
Automotive	9.23
Government	7.46
E-Commerce/Retail	7.45
Industrial	7.25
Education	7.23
Travel & Hospitality	6.83
Real Estate	6.56
Financial Services	6.55
Media/Entertainment	5.89
Technology	5.89
Professional Services	4.55
Healthcare	3.42

Vulnerability	Susceptible Industries	Not Vulnerable
Poodle	Automotive (3.09%), Industrial (2.90%), Education (2.34%), Media (2.21%), Travel & Hospitality (2.05%), Professional Service (1.69%), Technology (1.55%), Financial (1.64%), Real Estate (1.64%), Government (1.36%), E-Commerce/Retail (1.09%)	Telecom, Healthcare
Zombie Poodle	Telecommunications (3.45%), Industrial (2.90%), Financial (2.29%), Automobile (2.06%), E-Commerce/Retail (1.09%), Travel & Hospitality (1.02%), Others (<0.90%)	Real Estate
Sleeping Poodle	Industrial (1.45%), Professional Service (0.26%), Media/Ent (0.07%)	Technology, Education, Retail, Financial, Government, Travel, Healthcare, Automotive, Real Estate, Telecom
Poodle TLS	Industrial (1.45%), Professional Service (0.13%), Media/Ent (0.10%)	Same as above
Golden Doodle	Automotive (2.06%), Financial (1.64%), Industrial (1.45%), Travel (0.34%), Retail (0.31%), Professional Service (0.26%), Media/Ent (0.16%), Education (0.11%), Technology (0.07%)	Government, Healthcare, Real Estate, Telecom
Logjam	Professional Service (0.26%), Technology (0.20%), Media (0.10%)	Above, Education, Financial, Travel, Automotive, Industrial
Freak	Automotive (1.03%), Professional Service (0.39%), Government (0.34%), Technology (0.27%), Media/Entertainment (0.26%)	Education, Financial, Travel, Industrial, Real Estate, Telecom, Healthcare, Retail
Bleichenbacher	E-Commerce/Retail (2.64%), Automotive (2.06%), Travel (1.71%), Education (1.00%), Media (0.79%), Others (<=0.65%)	Financial, Healthcare, Industrial, Real Estate, Telecom



4.

Geographic Breakdown



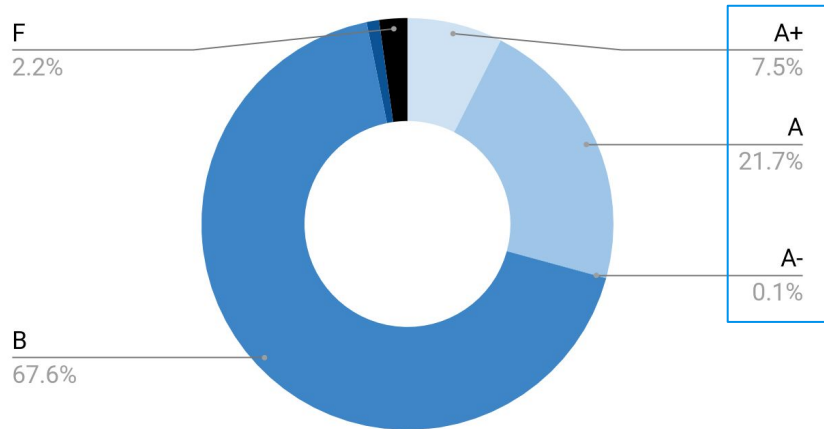
Remaining countries: Japan, Ireland, Iran, Singapore, India, and 63 others



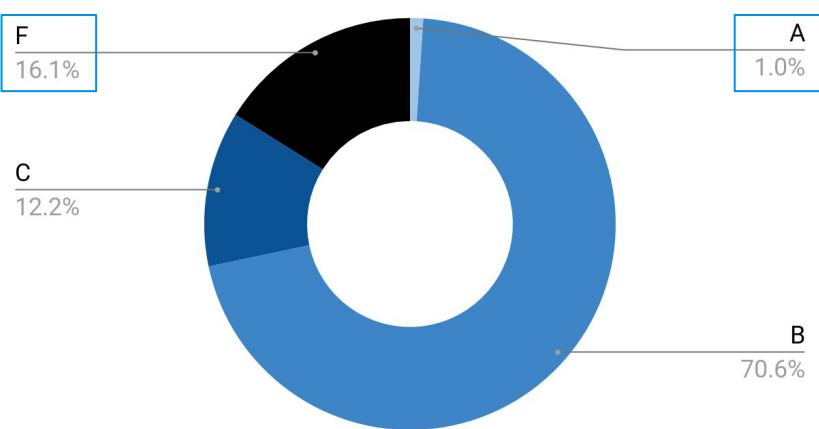
4a.

Geographic Breakdown: Grade

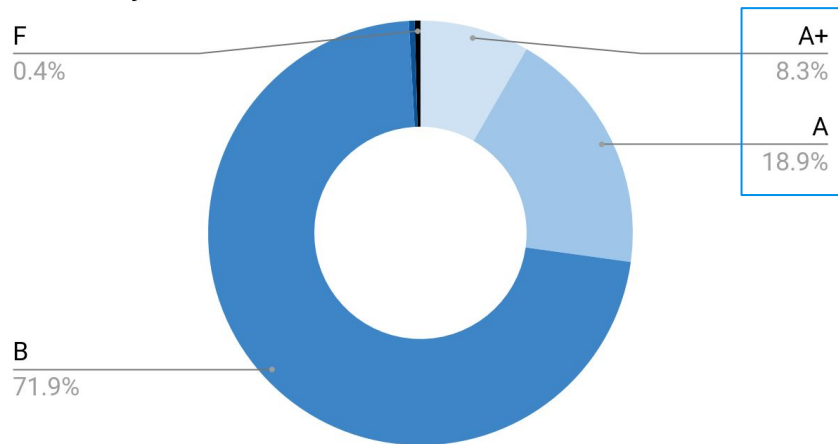
United States



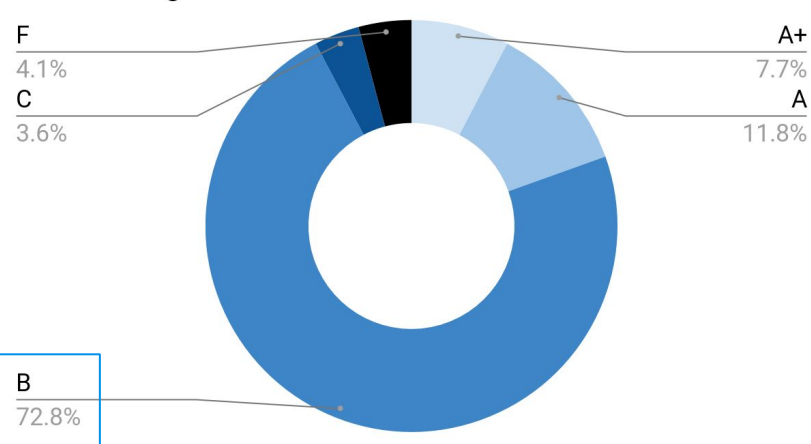
China



Germany



United Kingdom





4b.

Geographic Breakdown: Supported Protocols



Findings

- China and Netherlands sites have the most support for SSL
 - 17.14% and 4.9%, respectively
- TLS 1.3 is more widely supported by US and Russian sites at 35.8% and 31%, respectively
 - It is least supported by Chinese sites at 4.4%
- Aside from US and Russia, TLS 1.2 is the highest supported protocol for over 82% of sites within each country

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines, rendered in a light gray color.

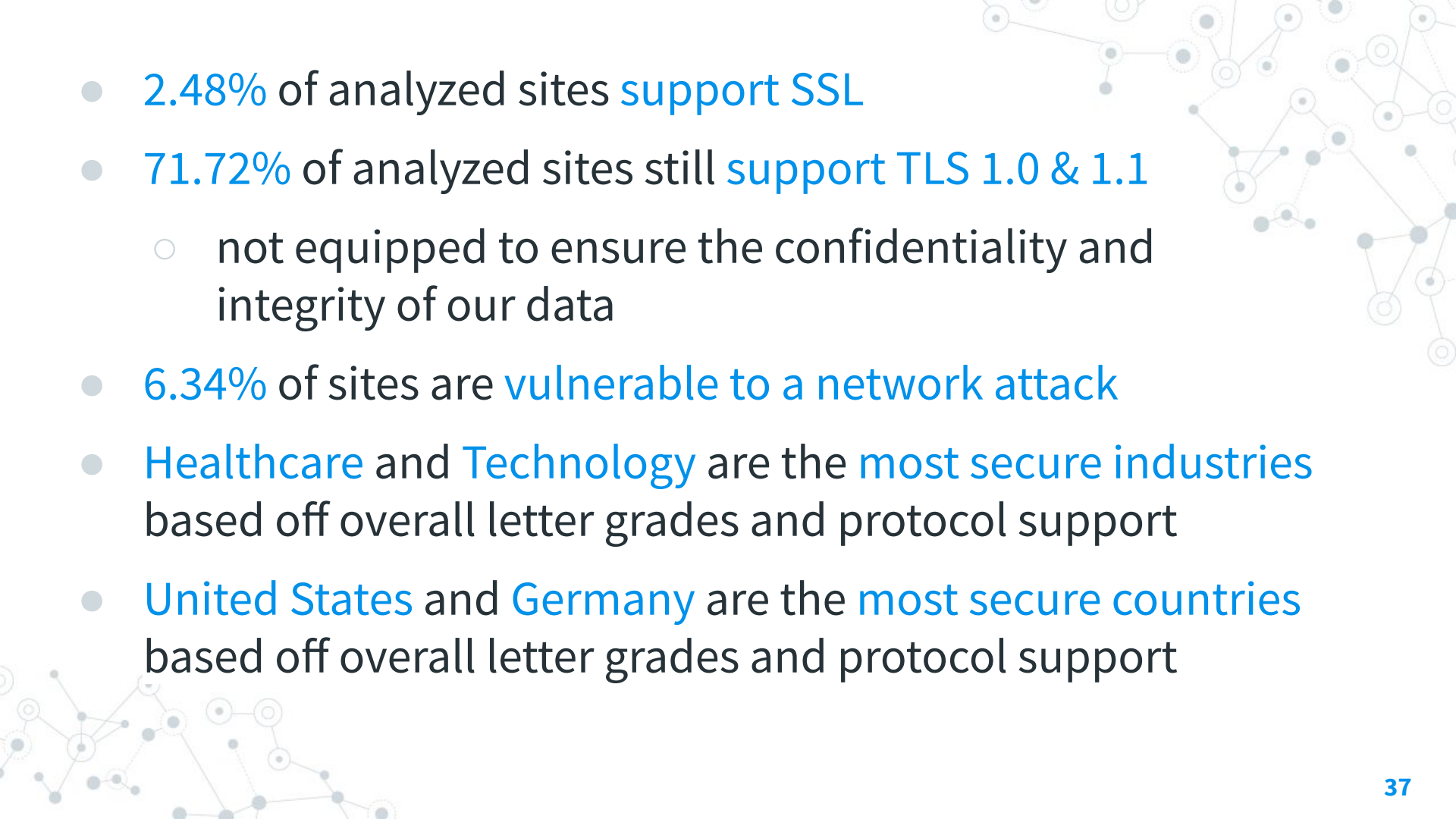
4c.

Geographic Breakdown: Vulnerabilities

Country	% of Vulnerable Sites
China	27.53%
United Kingdom	10.06%
Canada	8.40%
Netherlands	7.97%
France	7.69%
Russia	7.59%
United States	4.27%
Germany	1.32%

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric rings, suggesting a hierarchical or central structure. The lines are thin and gray, connecting the nodes in a non-linear fashion.

5. **Key Takeaways**

- 
- 2.48% of analyzed sites support SSL
 - 71.72% of analyzed sites still support TLS 1.0 & 1.1
 - not equipped to ensure the confidentiality and integrity of our data
 - 6.34% of sites are vulnerable to a network attack
 - Healthcare and Technology are the most secure industries based off overall letter grades and protocol support
 - United States and Germany are the most secure countries based off overall letter grades and protocol support



A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting a hierarchical or multi-layered structure. The lines are thin and gray, connecting the nodes in a non-linear fashion.

6. **Future Research**

Some Further Considerations

- Re-evaluate sites that returned a grade of NA
- Use updated SSL Labs API (currently underworks)
- Develop comprehensive industry classification
 - e.g. “Technology” → social media, productivity tools, cloud services, data analytics, ad services, etc.
- Get more granular with the geographic breakdown
- Scan sites again over the next year to observe TLS 1.0/1 phase-out time and potential TLS 1.3 adoption
- Conduct a Proof of Concept on vulnerable sites
- Consider the top 1 million sites (after pandemic, of course)

Sources

- ◎ Top 10,000 list retrieved from [Tranco](#)'s top 1 million
- ◎ Analysis conducted with [SSL Labs API](#)
- ◎ [Global Industry Classification Standard](#)
- ◎ [Analysis](#) of 450,000 sites from Alexa's top 1 million
- ◎ This Project's GitHub Repo:
<https://github.com/MartinLPetrauskas/TLSMeasurement>



Thanks!

Any questions?

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, while others are smaller. The lines are thin and gray, connecting the nodes in a non-linear fashion. The overall style is minimalist and technical.

Appendix

Lots of charts and clarifying info!

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It shows a cluster of nodes connected by lines, with some nodes being larger and more prominent than others. The lines are thin and gray, creating a web-like structure.

Resource Guide

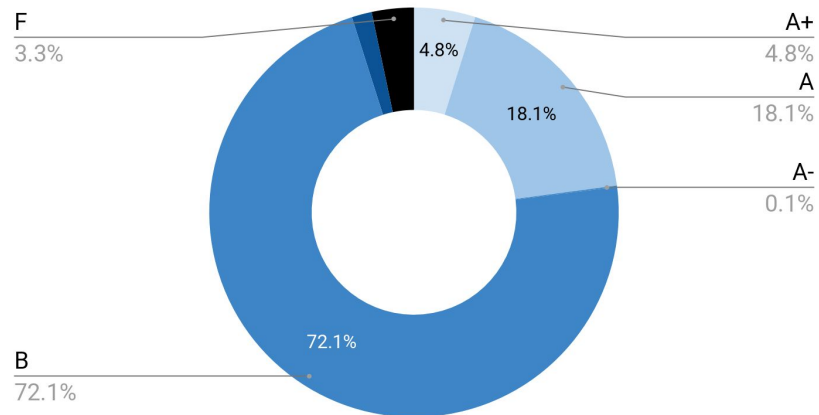
- ◎ [SSL Labs API v3 Documentation](#)
- ◎ [Understanding the SSL Labs Letter Grades](#)

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, while others are smaller and solid. The lines are thin and gray, connecting the nodes in a non-linear fashion.

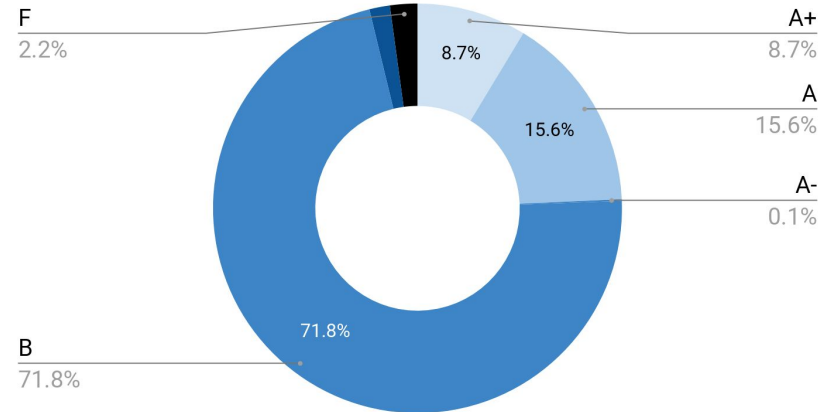
Industry Grade Breakdowns

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It shows a cluster of nodes connected by lines, with some nodes being larger and having concentric circles, and others being smaller and solid. The lines are thin and gray.

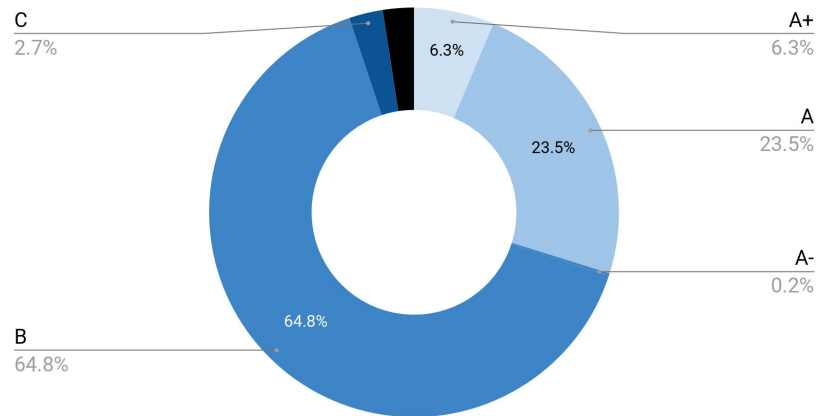
Media/Entertainment



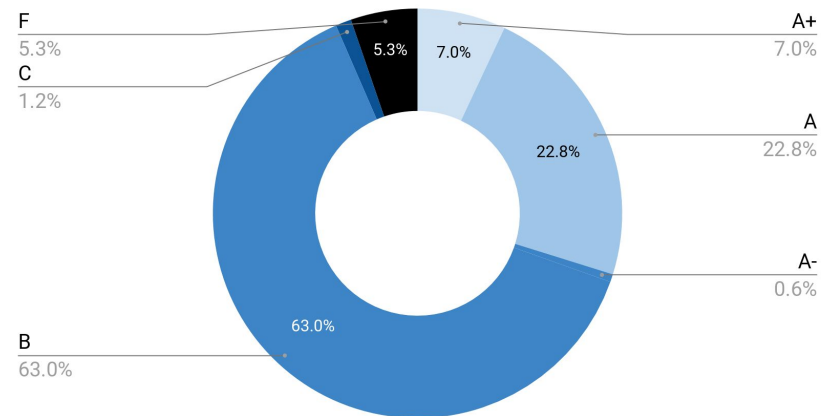
Technology



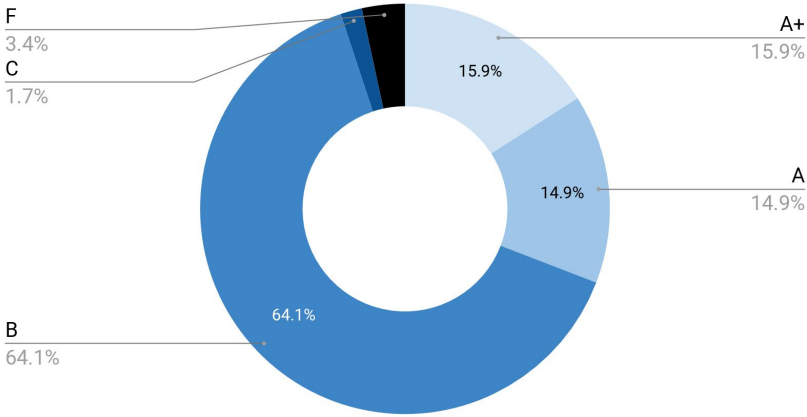
Education



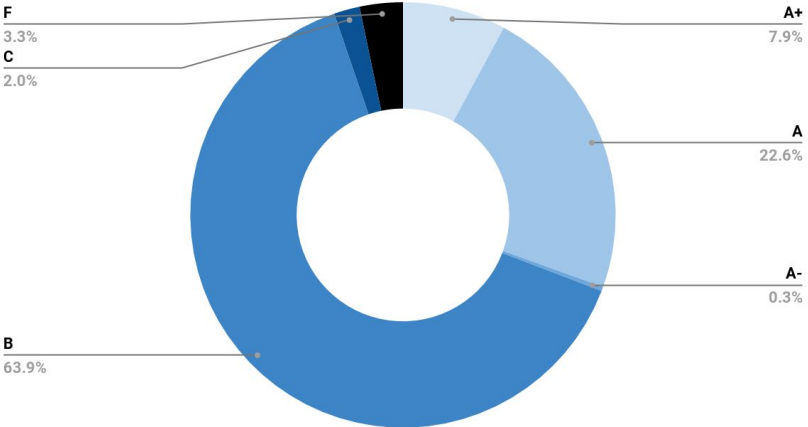
e-Commerce/Retail



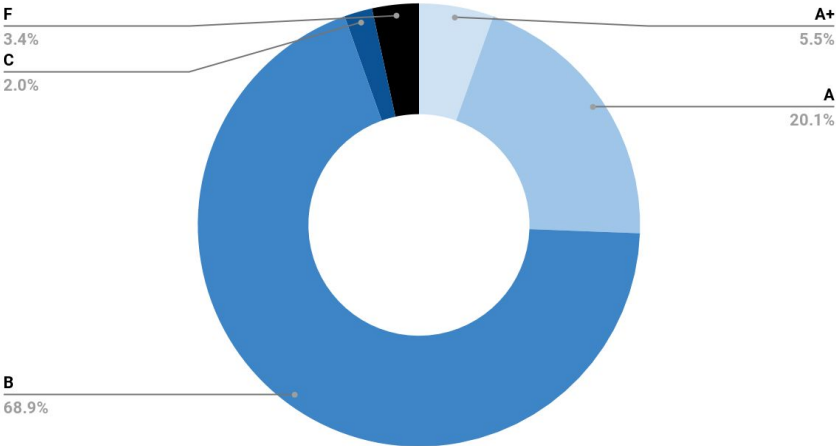
Government



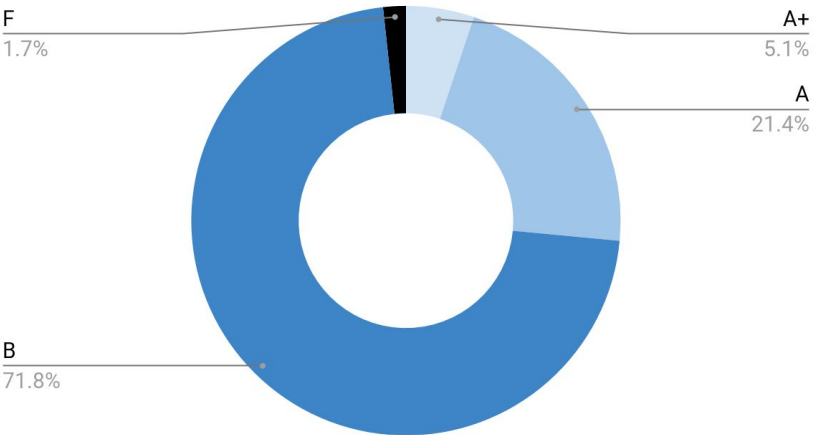
Financial Services



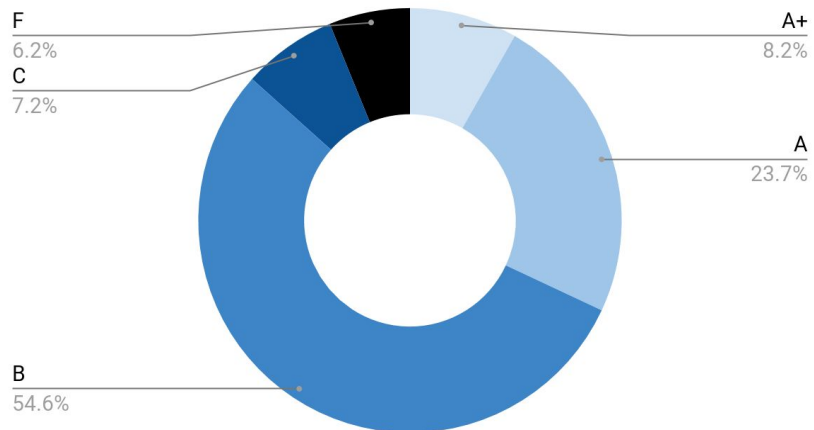
Travel & Hospitality



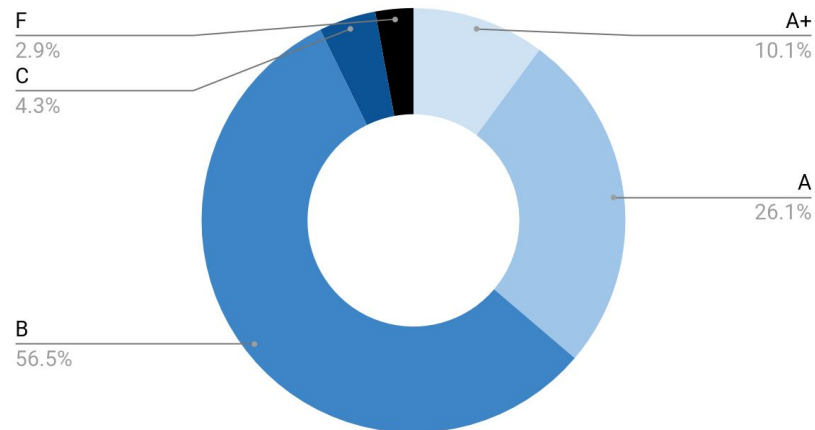
Healthcare



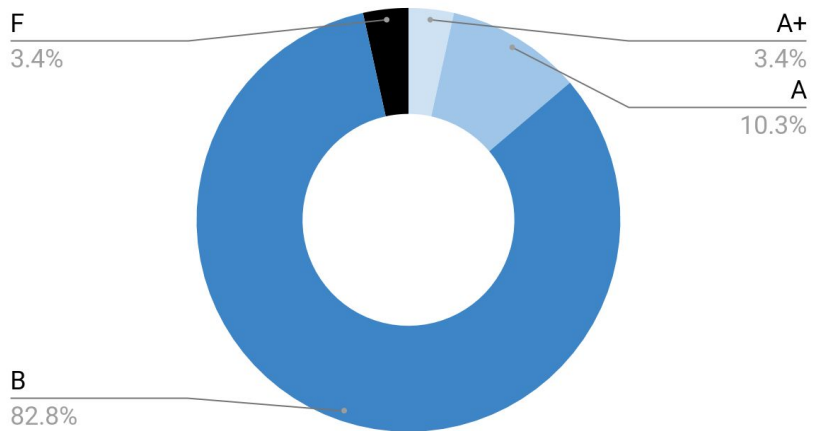
Automotive



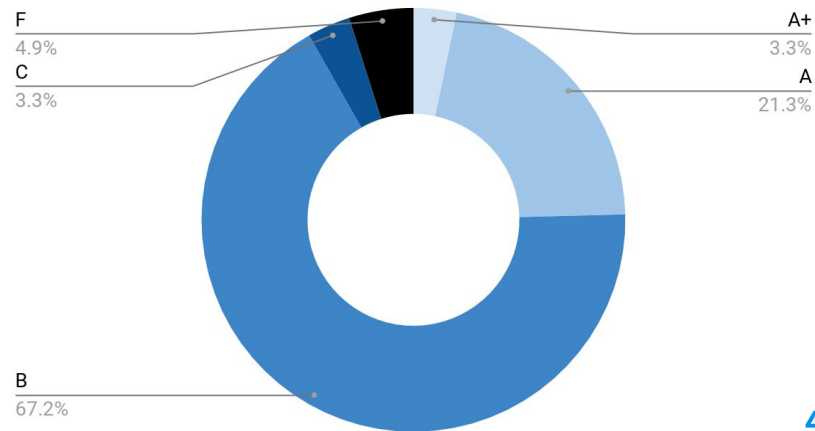
Industrial



Telecom



Real Estate

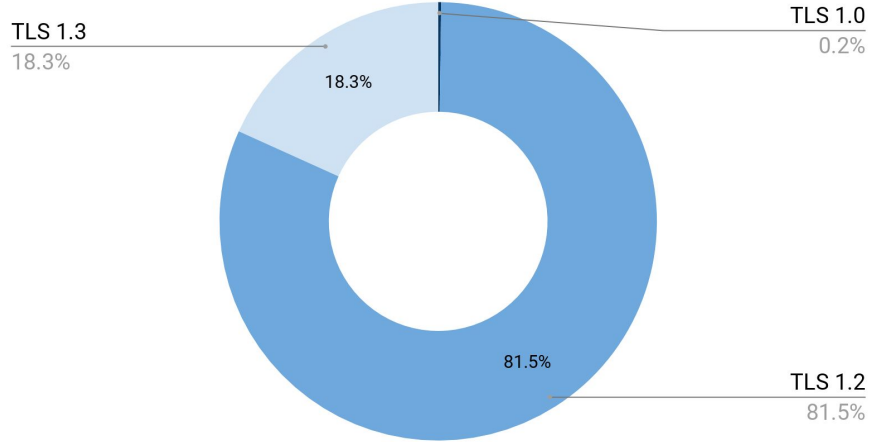


A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting different levels of connectivity or importance. The lines are thin and gray, creating a mesh-like structure.

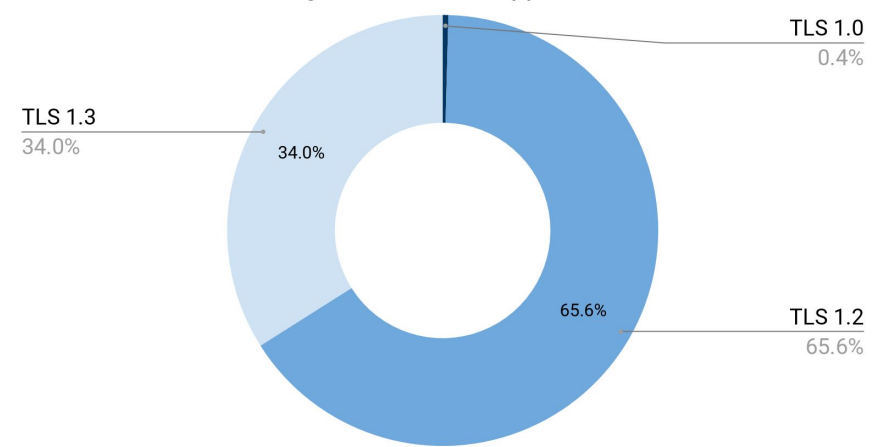
Industry Protocol Breakdowns

A decorative network diagram in the bottom-right corner, similar to the one in the top-left, showing a cluster of interconnected nodes and lines, with some nodes highlighted by concentric circles.

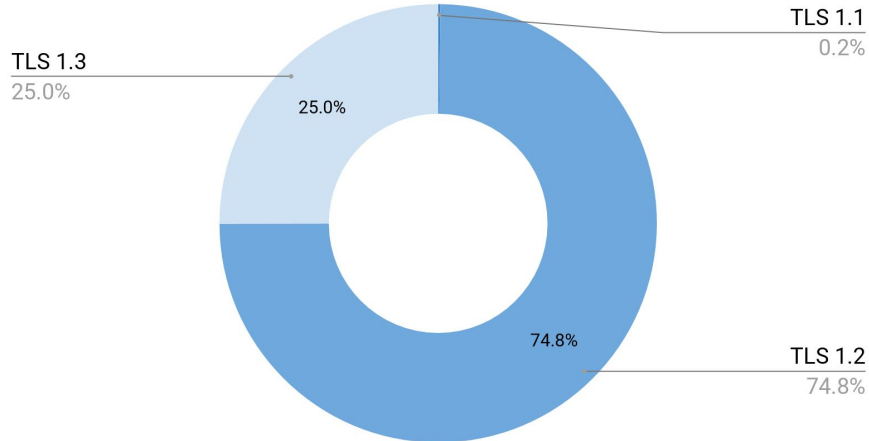
Education: Highest Protocol Supported



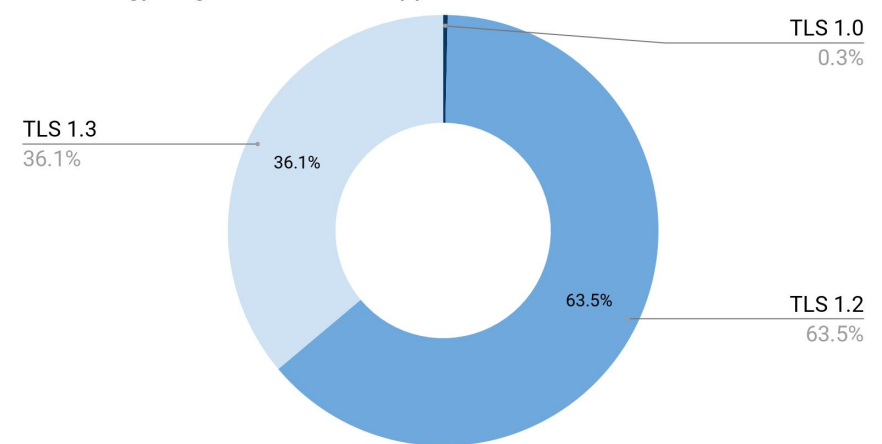
Media/Entertainment: Highest Protocol Supported



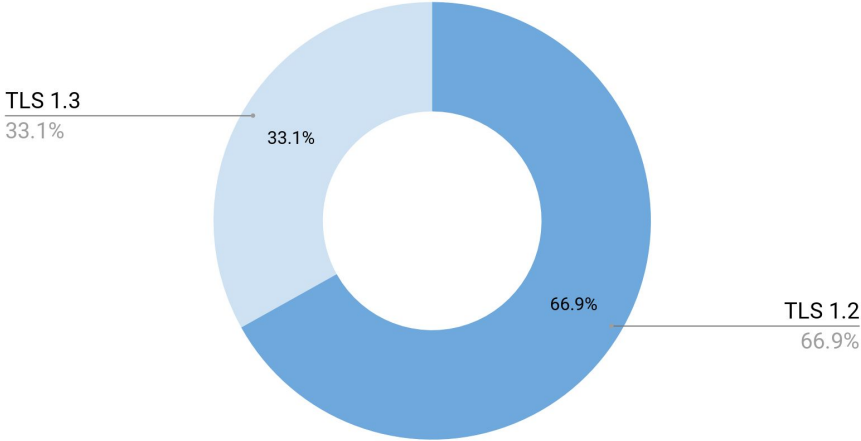
e-Commerce/Retail: Highest Protocol Supported



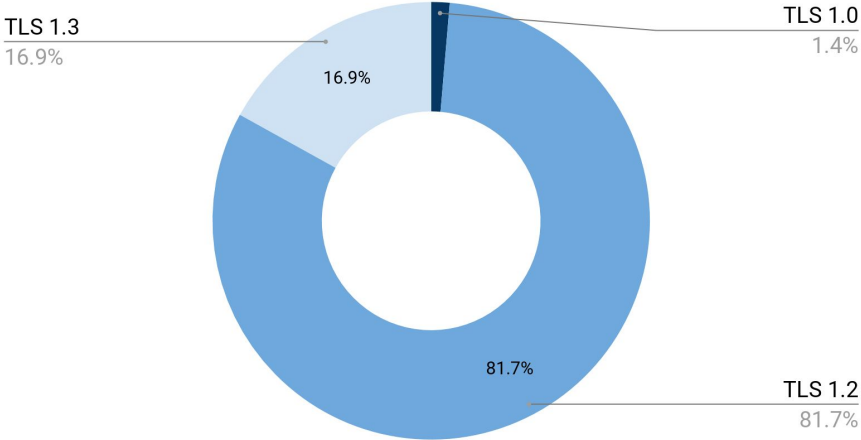
Technology: Highest Protocol Supported



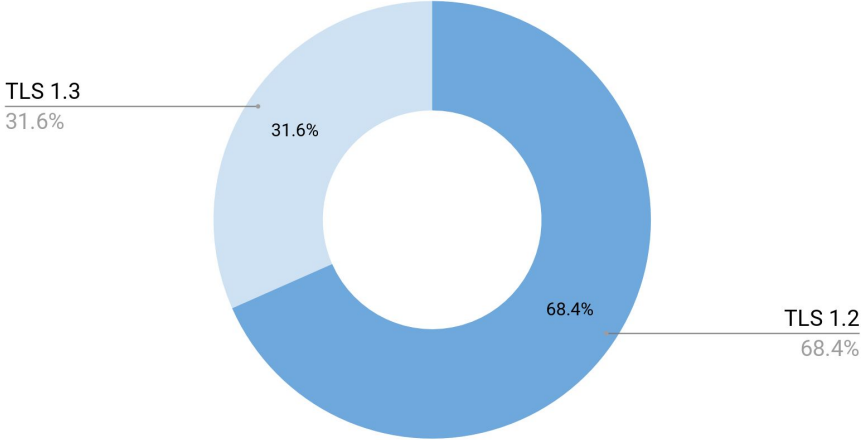
Travel & Hospitality: Highest Protocol Supported



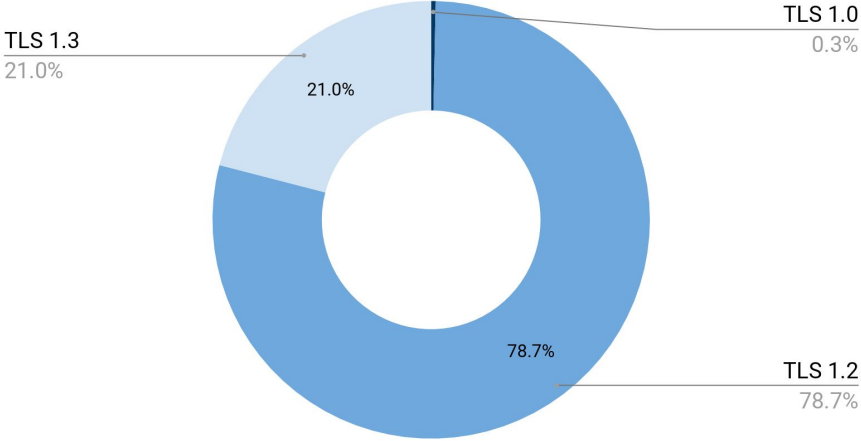
Government: Highest Protocol Supported



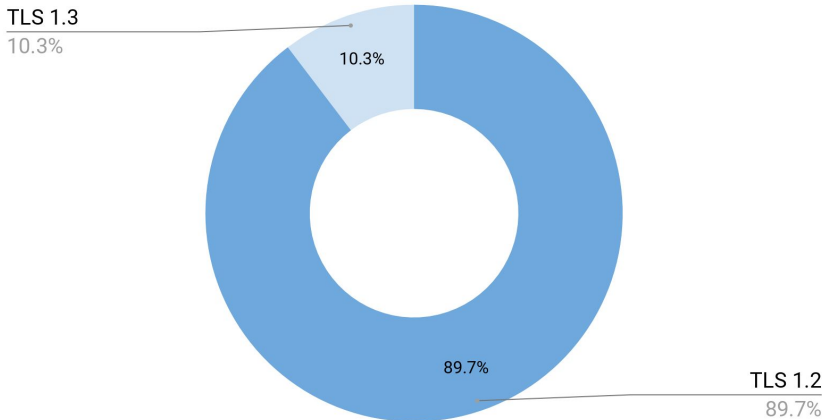
Healthcare: Highest Protocol Supported



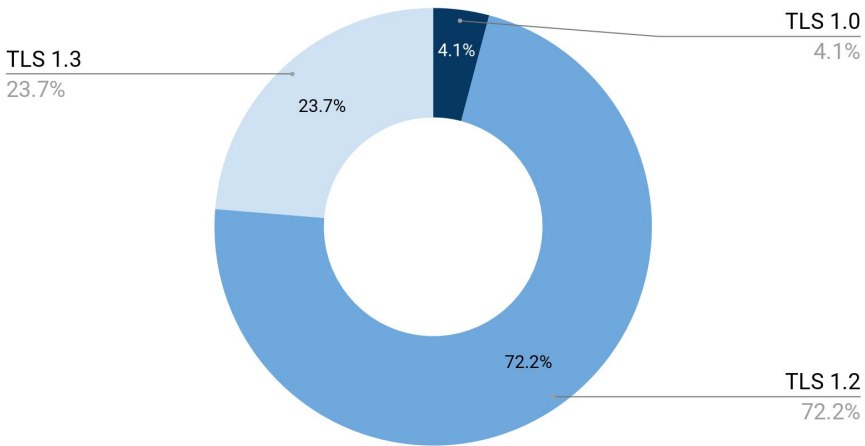
Financial Services: Highest Protocol Supported



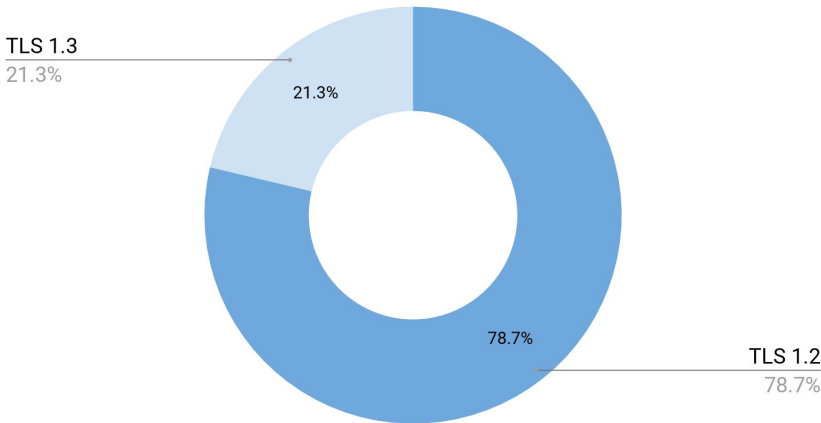
Telecom: Highest Protocol Supported



Automotive: Highest Protocol Supported



Real Estate: Highest Protocol Supported



Industrial: Highest Protocol Supported

