Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 22-28 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

TLS 1.3 ახალი პროტოკოლი ახალი შესაძლებლობებით
TLS 1.3 NEW PROTOCOL WITH NEW POSSIBILITIES

ლუკა ნაჭყებია, კიბერუსაფრთხოების მეცნიერთა ასოციაცია (SCSA)
L. Nachkebia Scientific Cyber Security Association(SCSA)
ნოდარ უგლავა, კიბერუსაფრთხოების მეცნიერთა ასოციაცია (SCSA)
N. Uglava Scientific Cyber Security Association(SCSA)
ქეთევან გრძელიძე, კიბერუსაფრთხოების მეცნიერთა ასოციაცია (SCSA)
Q.Grdzelidze, Scientific Cyber Security Association(SCSA)

აბსტრაქტი: დღესდღეობით TLS პროტოკოლები გამოიყენება თითქმის ყველა აპლიკაციაში. ის წარმოადგენს ვებ ბრაუზერს (კლიენტი) და ვებგვერდს (სერვერი) შორის მონაცემთა გადაცემის უსაფრთხოების უზრუნველყოფის ყველაზე ხშირად გამოყენებად მეთოდს. წინამდებარე სტატიაში განხილულია TLS 1.2-ის და TLS 1.3-ის ძლიერი და სუსტი მხარეები, მათი უსაფრთხოების სისუსტეები. სტატიის დასკვნითი ნაწილი შეეხება TLS 1.3-ის ნაკლოვანებების თავდამსხმელების მიერ გამოყენების შესაძლებლობებს.

ABSTRACT: Nowadays, TLS protocols are being used in almost every application. It is the most used method for ensuring secure communication and transfer of data between web-browser (client) and web-page (server). In the present paper the strentghs and weaknesses of TLS 1.2 and TLS 1.3 and their security concerns are discussed. The final part of the paper addresses the matter, how the hackers can use TLS 1.3 shortcomings for their advantage.

საკვანძო სიტყვები: *TLS 1.3, უსაფრთხოების პროტოკოლი, TLS 1.2, უსაფრთხო კომუნიკაცია*
KEYWORDS: *TLS 1.3 security protocol, TLS 1.2 secure communication*

Transport Layer Security (TLS) წარმოადგენს კრიპტოგრაფიულ პროტოკოლს, რომელიც შექმნილია ვებ-ბრაუზერებსა და სერვერებს შორის კომუნიკაციის უსაფრთხოების უზრუნველსაყოფად. დღესდღეობით TLS პროტოკოლები გამოიყენება თითქმის ყველა აპლიკაციაში. მეორეს მხრივ, SSL წარმოადგენს პროტოკოლს, რომელიც გამოიყენება ვებ-ბრაუზერებსა და სერვერებს შორის დაშიფრული კომუნიკაციის დასამყარებლად. SSL გადაცემული მონაცემების დასაშიფრად იყენებს.
ის წარმოადგენს ვებ ბრაუზერს (კლიენტი) და ვებგვერდს (სერვერი) შორის მონაცემთა გადაცემის უსაფრთხოების უზრუნველყოფის ყველაზე ხშირად გამოყენებად მეთოდს. ის უზრუნველყოფს რომ კომუნიკაციის ორივე მხარეს არსებული მხარეები იყვნენ ავთენტურები და ასევე, უზრუნველყოფს მონაცემთა მთლიანობას მათი დაშიფვრის გზით.

არსებობს TLS-ის 1.0, 1.1., 1.2 და 1.3 ვერსიები:

- TLS 1.0 გამოქვეყნდა 1999 წელს RFC 2246-ის სახელით.
- TLS 1.1 გამოქვეყნდა 2006 წელს RFC 4346-ის სახელით.
- TLS 1.2 გამოქვეყნდა 2008 წელს RFC 5246-ის სახელით[1].
- TLS 1.3 ოფიციალურად გამოქვეყნდა 2018 წელს RFC 8446-ის სახელით.
-

ცნობილია, რომ TLS 1.0 და TLS 1.1 წარმოადგნენ ადვილად მოწყვლად პროტოკოლებს, ამასთან 1.2 და 1.3 ითვლება ბევრად უსაფრთხო პროტოკოლებად და შესაბამისად,

[1] "TLS 1.2 vs TLS 1.1 - KeyCDN Support," October 4, 2018. https://www.keycdn.com/support/tls-1-2-vs-tls-1-1.

რეკომენდებულია მათი გამოყენება. მიუხედავად იმისა, რომ 1.2-ს გააჩნია უსაფრთხოების პრობლემები, მისი გავრცელებადობის და სისტემებთან თავსებადობის გათვალისწინებით, დღესდღეობით მას არსებულ პროტოკოლებს შორის ყველაზე მეტი მომხმარებელი ყავს.

ამასთანავე, უსაფრთხოების საკითხებიდან გამომდინარე, 2020 წლიდან Apple, Google, Microsoft და Mozilla-მ შეწყვიტეს TLS 1.0 და TLS 1.1-ის გამოყენება და მხარდაჭერა.

დღეს TLS 1.3-ის სრული და ნაწილობრივი გამოყენების მაჩვენებელი მსოფლიოში დაახლოებით 89.02%-ია[2], ხოლო TLS 1.2-ის მაჩვენებელი 97.91%-ს უტოლდება[3].

გრაფიკი 1. TLS 1.2 და TLS 1.3-ის გამოყენების შესახებ მონაცემები[4]

TLS 1.2

როგორც ზემოთ აღვნიშნეთ, TLS 1.2 დღესდღეობით წარმოადგენს ყველაზე გავრცელებულ პროტოკოლს. თუმცა, ეს არ ნიშნავს, რომ მას არ აქვს პრობლემები. TLS 1.2 კვლავაც აქვს შედარებით მოძველებული კრიპტოგრაფიული ალგორითმების მხარდაჭერა, რაც უფრო მოწყვლადს ხდის მას სხვადასხვა ტიპის თავდასხმებისათვის. მაგალითისთვის *Zombie POODLE attack.* ამ თავდასხმის დროს მეცნიერებმა გამოავლინეს ორი ახალი სისუსტე, რომელიც TLS 1.-2ზე POODLE-ს ტიპის განხორციელების საშუალებას. ამ შემთხვევაში, თავდამსხმელი იყენებს CBC-დაშიფვრის მეთოდის სისუსტეს, რომელიც იძლევა Man-in-the-middle თავდასხმის განხორციელების შესაძლებლობას იმ სისტემებზე, რომლებიც ჯერაც იყენებენ დაშიფვრის მოძველებულ მეთოდებს.

2 Can I use... Support tables for HTML5, CSS3, etc, September 24, 2020, https://caniuse.com/#feat=tls1-3
3 Can I use... Support tables for HTML5, CSS3, etc, September 24, 2020, https://caniuse.com/#search=1.2
4 Can I use... Support tables for HTML5, CSS3, etc, September 24, 2020, https://caniuse.com/#search=1.2, Can I use... Support tables for HTML5, CSS3, etc, September 24, 2020, https://caniuse.com/#feat=tls1-3

POODLE და სხვა ტიპის თავდასხმების შემდგომ, გარკვეულწილად მოხდა ამ ნაკლოვანებების აღმოფხვრა. თუმცა, მომხმარებელთა გარკვეული ნაწილს კვლავაც აქვს ძველი პროტოკოლების მხარდაჭერა, ვინაიდან ეს ხელს უწყობს ძველი ვებ-გვერდების შენარჩუნებასა და თავიდან ირიდებს ვებ-გვერდებიდან ძველი მომხმარებლების დაბლოკვას. ეს, თავის მხრივ, ნიშნავს, რომ პრობლემები და სისუსტეები კვლავას რჩება სისტემებში და შესაძლებელია მათი გამოყენება.[5]

გარდა კოდში არსებული პრობლემებისა, TLS 1.2 მის შემდგომ ვერსიასთან შედარებით არის უფრო ნელი. უმეტეს შემთხვევაში მონაცემთა დაშიფვრა გამოიყენებოდა კონკრეტულ სისტემაში ავტორიზაციის ან საკრედიტო ბარათის მონაცემების გადაგზავნისთვის. ამავდროულად, სხვა ტიპის მონაცემები რჩებოდა ღიად ხელმისაწვდომი. შესაბამისად, ბოლო პერიოდში უფრო აქტუალური გახდა ინტერნეტის ტრაფიკის სრულად HTTPS-ში გადატანა, რაც მოხმარებლებს მეტად იცავს ე.წ. „eavesdropper“-ების და ინექციური თავდასხმებისაგან, თუმცა, როგორც ზემოთ აღინიშნა, ამ პროტოკოლის და შესაბამისად განხორციელებული პროცესების მინუსს წარმოადგენს მისი სიჩქარე.

კერძოდ, იმისათვის, რომ ბრაუზერი და სერვერი შეთანხმდნენ დაშიფვრის გასაღებზე, მათ სჭირდებათ კრიპტოგრაფიული მონაცემების გაცვლა. გაცვლა, იგივე „ხელის ჩამორთმევა“ TLS-ში მცირედად არის შეცვლილი 1999 წლის შემდეგ (მას შემდეგ რაც მოხდა სტანდარტიზება). „ხელის ჩამორთმევისათვის“ საჭიროა ბრაუზერსა და სერვერს შორის ორი დამატებითი წრის გავლა, მანამ სანამ მოხდება დაშიფრული მონაცემების გადაგზავნა (ან სანამ გაგრძელდება წინა კომუნიკაცია). შესაბამისად, აღნიშნულიდან გამომდინარე HTTP-სთან შედარებით HTTPS არის უფრო ნელი. ამ შეფერხებამ კი შესაძლოა ნეგატიური გავლენა იქონიოს იმ აპლიკაციებზე, რომელთა ორიენტირსაც წარმოადგენს სისწრაფე.

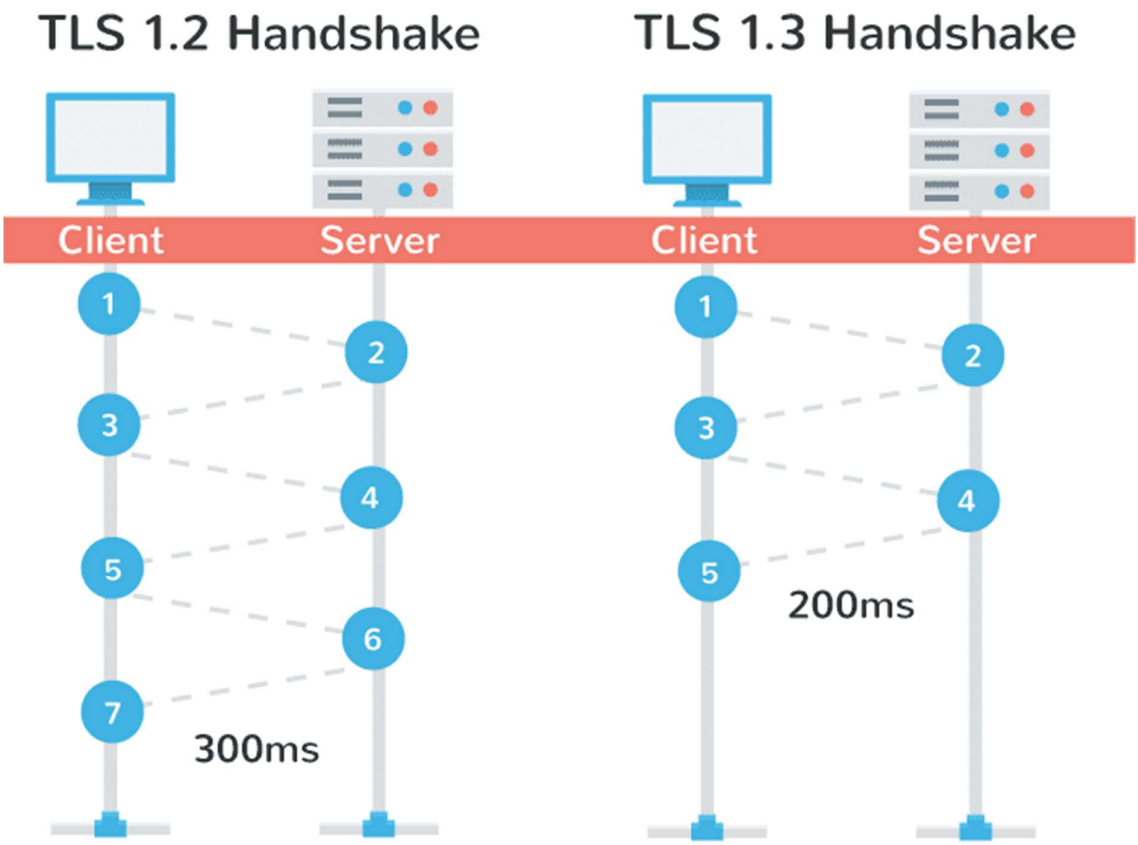
TLS 1.3-ს უპირატესობები TLS 1.2-თან შედარებით:

სისწრაფე

როგორც უკვე აღინიშნა, TLS 1.2 კავშირის დამყარებისას იყენებს უკვე მოძველებულ პროტოკოლს და არის შედარებით ნელი. მისგან განსხვავებით, TLS 1.3 პროტოკოლის მიხედვით, პირველადი კომუნიკაციის დამყარებისას საჭიროა მხოლოდ 1 წრის გავლა, რაც ბევრად ასწრაფებს და აადვილებს პროცესს. გარდა ამისა, TLS 1.3-ის პირობებში, თუ ვებ-გვერდი არის ახალი დახურული, ბევრად სწრაფად ხდება მასთან კავშირის გაგრძელება, რადგან აღარ არის საჭირო ხელახლა კომუნიკაციის დამყარება და „ხელის ჩამორთმევის“ პროცედურის გავლა, რადგან შესაძლებელია უკვე შეთანხმებული გასაღების გამოყენებით კომუნიკაციის გაგრძელება.

შესაბამისად, პროცესის გასაუმჯობესებლად TLS 1.3 კომუნიკაციიდან სრულად იღებს ხელის ჩამორთევის 1 წრეს. უმრავლეს შემთხვევაში, ახალი TLS 1.3 კავშირები მყარდება 1 წრის შემოვლით[6].

[5] Pollack Keren, “Leaving TLS 1.2 and Moving to TLS 1.3,” September 2, 2020, https://calcomsoftware.com/leaving-tls1-2-using-tls1-3/.
[6] “TLS 1.3,” EZ, accessed September 26, 2020, https://www.hcc-embedded.com/tls-1-3.



გრაფიკი 1: TLS 1.2 და TLS 1.3 პროტოკოლების „ხელის ჩამორთმევის“ პროცესი[7]

დაშიფვრის ახალი სქემა

მნიშვნელოვანია, რომ TLS 1.3 აღარ იყენებს იმ ალგორითმებს, რომლებიც TLS 1.2-ის პირობებში მიჩნეული იქნა თავდასხმებისადმი მოწყვლადად. შესაბამისად, გამოიყენება მხოლოდ ყველაზე უსაფრთხო ალგორითმები, როგორიცაა, მაგალითად ეფემერული დიფი-ჰელმანის (DHE) ალგორითმი.

გარდა ამისა, TLS 1.3-ის პირობებში 1.3-ის პირობებში „ხელის ჩამორთმევის“ მოლაპარაკების უფრო დიდი ნაწილი იშიფრება, რაც მონაცემთა გადაცემისათვის უფრო მეტ უსაფრთხოებას უზრუნველყოფს. ეს ხელს უწყობს კომუნიკაციის მონაწილე მხარეების საიდენტიფიკაციო მონაცემების დაცვას და ართულებს ტრაფიკის ანალიზის შესაძლებლობას.

Forward Secrecy არის ავტომატურად უზრუნველყოფილი. ეს გულისხმობს, რომ იმ შემთხვევაში, თუ TLS 1.3-ის პირობებში დაშიფრულ ინფორმაციას შეექმნება საფრთხე/მოხდება მისი განშიფვრა, შეუძლებელი იქნება ამ ინფორმაციის გამოყენებით გადაცემული მონაცემების/კომუნიკაციის განშიფვრა. ეს გულისხმობს, იმ შემთხვევაშიც კი,

[7] “Advantage of TLS 1.3 over TLS 1.2,” November 25, 2019, https://dev.to/https_india/advantage-of-tls-1-3-over-tls-1-2-6ig.

თუ სამომავლო კომუნიკაციები არ იქნება უსაფრთხო, ეხლანდელ კომუნიკაციას მაინც არ ემუქრება საფრთხე.

TLS 1.3-ის შესაძლო საფრთხეები

სესიის სისწრაფე წარმოადგენს TLS 1.3-ის ერთ-ერთი ყველაზე დიდ მიღწევას, რადგან ის აუმჯობესებს მომხმარებლის გამოცდილებას. თუმცა, არსებობს 0-RTT-ს საშუალებით სესიის „გაგრძელებასთან“ დაკავშირებული უსაფრთხოების საკითხები - მაგალითად, ის რომ ეს შესაძლებელს ხდის „replay“ შეტევას. აღნიშნულიდან გამომდინარე, ბევრი კრიპტოგრაფი და ორგანიზაცია თვლის, რომ TLS 1.3-ის გაშვებისას/გამოყენებისას გათიშავს პროტოკოლის ამ ნაწილს[8].

TLS 1.3-ს აქვს ახალი ტიპის შიფრები, რომელიც იყენებს თანამედროვე AEAD ალგორითმებს, რომლებიც შეიქმნა სპეციალურად ამ პროტოკოლისთის. ეს არის დაშიფვრის იმგვარი ფორმა, რომელიც TLS-ის უსაფრთხოებისა და სანდოობის გაზრდის მიზნით ქმნის შემდეგ მახასიათებლებს:

- კონფიდენციალურობა: უზრუნველყოფს, რომ ვერავინ ვერ შეძლოს კლიენტსა და სერვერს შორის გაზიარებული მონაცემების დეშიფრაცია.
- ავტენთიფიკაცია: უზრუნველყოფს, რომ კლიენტი რეალურად ესაუბრებოდეს მხოლოდ რეალურ სერვერს. ასევე შესაძლებელია, რომ სერვერმა მოახდინოს კლიენტის ავტენთიფიკაცია, მაგრამ ეს არის იშვიათი შემთხვევა.
- მთლიანობა: უზრუნველყოფს რომ გაგზავნილი ინფორმაცია და კომუნიკაცია არ შეიცვალოს და არ მოხდეს მისი მთლიანობის დარღვევა[9'10].

რატომ გამოიყენება უფრო მეტად 1.2 ვიდრე 1.3

ვინაიდან, TLS და SSL არის ღია სტანდარტებზე დაფუძნებული, მათი ეფექტური განვითარებისთვის საჭიროა პროტოკოლის მასობრივი დანერგვა აღჭურვილობის მწარმოებლების, ვებ-ბრაუზერების, აპლიკაციების (მაგ: Facebook და მისი სერვერები), მხრიდან მათი დანერგვა და იმისი უზრუნველყოფა, რომ არ იყოს გარკვეული ტიპის ჩავარდნები.
აქედან გამომდინარე, მიუხედავად იმისა, რომ TLS 1.3 უკვე არსებობს 2018 წლიდან, დღემდე, როგორც ზემოთ აღინიშნა, TLS 1.2 არის უფრო ფართოდ გამოყენებადი, რადგან ეს უკვე არის დე ფაქტო დანერგილი და აპრობირებული სტანდარტი[11].

TLS 1.2-ს საფრთხის იდენტიფიცირების მიზნით გააჩნდა გარკვეული ხილვადობა, რომელიც ფართოდ იყო გავრცელებული. TLS 1.3-მა ამ ხილვადობის დიდი ნაწილი დაფარა. მისი მუშაობის და უსაფრთხოების უფრო მეტად უზრუნველსაყოფად განხორციელდა გარკვეული ცვლილებები, რამაც ასევე ხელი შეუწყო გარკვეული კომპლექსურობების და სიმარტივეების პროტოკოლიდან ამოღებას. თუმცა, ისეთი

8 Gigamon, “What Do You Mean TLS 1.3 Might Degrade My Security?,” Gigamon.com (Gigamon, 2020), https://www.gigamon.com/content/dam/gated/wp-what-do-you-mean-tls1.3-might-degrade-my-security.pdf.
9 Pecanek Michal, Improving web performance & security with TLS 1.3, September 24, 2018, https://blog.cdn77.com/latest-tls-improving-https/
10 Gigamon, “What Do You Mean TLS 1.3 Might Degrade My Security?,” Gigamon.com (Gigamon, 2020), https://www.gigamon.com/content/dam/gated/wp-what-do-you-mean-tls1.3-might-degrade-my-security.pdf.
11 Martin Rudd and April 6, “TLS 1.3: Slow Adoption of Stronger Web Encryption Is Empowering the Bad Guys,” April 5, 2020, https://www.helpnetsecurity.com/2020/04/06/tls-1-3-adoption/.

კორპორაციებისთვის, რომლებიც იყენებენ ქსელუს უსაფრთხოებაზე დაფუძნებულ გადაწყვეტებს, არსებობს შესაბამისობის, რისკების მართვისა და საფრთხეების მოკვლევისათვის გარკვეული მითითებები[12].

როგორ შეუძლიათ კიბერკრიმინალებს 1.3-ის დანერგვაში არსებული ხარვეზების/ნაკლოვანებების გამოყენება

ერთ-ერთი ტიპის თავდასხმა, რომელსაც ხშირად ახსენებენ არის „Bleichenbacher"-ის თავდასხმა. ის ძირითად სამიზნეს წარმოადგენს RSA განშიფვრის ალგორითმი. მანამ, სანამდე TLS-ის ავტორები ცხდილობდნენ რომ გაერთულებინათ RSA-ის განშიფვრის გასაღების ამოხსნა, Bleichenbacher-ის თითოეული ახალი ვერსია ამას ახერხებს. შესაბამისად, ნებისმიერი მოწყობილობა რომელიც იყენებს TLS-ზე დაფუძნებულ მახასიათებლებს არის მოწყვლადი. TLS 1.3 ზღუდავს RSA-ს გამოყენებას, მაგრამ კონკრეტული შემთხვევისთის მასზე უარის თქმა ნიშნავს TLS 1.2-ზე დაბრუნებას და მასზე თავდასხმები უკვე ხშირია.

არსებობს მოსაზრება, რომ DNS over HTTPS ხელს უწყობს კიბერუსაფრთხოების მხრივ გადადგმული ნაბიჯების შესუსტებას, რადგან უფრო მეტი ბოტნეტი იყენებს მისი დაშივრის შესაძლებლობას DNS-ის გვერდის ასავლელად. დაშიფრული მოთხოვნები ნიშნავს, რომ ისინი ხვდება ტიპიური ღონისძიებების სიაში და ხელს უშლის კორპორაციულ კიბერუსაფრთხოების საშუალებებს, რომლებიც დაფუძნებულია DNS სერვერებსა და DNS მონიტორინგზე, რომ დაბლოკონ კონკრეტულ მოთხოვნებზე წვდომა. შესაბამისად, ამას შეუძლია საშუალება მისცეს თანამშრომლებს რომ მოხვდნენ სახიფათო/დავირუსებულ საიტებზე[13].

გამოყენებული ლიტერატურა:

1. "Advantage of TLS 1.3 over TLS 1.2," November 25, 2019. https://dev.to/https_india/advantage-of-tls-1-3-over-tls-1-2-6ig.

2. Gigamon. "What Do You Mean TLS 1.3 Might Degrade My Security?" Gigamon.com. Gigamon, 2020. https://www.gigamon.com/content/dam/gated/wp-what-do-you-mean-tls1.3-might-degrade-my-security.pdf.

3. Keren, Pollack. "Leaving TLS 1.2 and Moving to TLS 1.3," September 2, 2020. https://calcomsoftware.com/leaving-tls1-2-using-tls1-3/.

4. Pecanek, Michal. "Improving Web Performance & Security with TLS 1.3: CDN77.Com." CDN77. CDN77, September 24, 2018. https://blog.cdn77.com/latest-tls-improving-https/.

5. Rudd, Martin, and April 6. "TLS 1.3: Slow Adoption of Stronger Web Encryption Is Empowering the Bad Guys," April 5, 2020. https://www.helpnetsecurity.com/2020/04/06/tls-1-3-adoption/.

12 Gigamon, "What Do You Mean TLS 1.3 Might Degrade My Security?," Gigamon.com (Gigamon, 2020), https://www.gigamon.com/content/dam/gated/wp-what-do-you-mean-tls1.3-might-degrade-my-security.pdf.
13 Martin Rudd and April 6, "TLS 1.3: Slow Adoption of Stronger Web Encryption Is Empowering the Bad Guys," April 5, 2020, https://www.helpnetsecurity.com/2020/04/06/tls-1-3-adoption/.

6. "TLS 1.2 vs TLS 1.1 - KeyCDN Support," October 4, 2018. https://www.keycdn.com/support/tls-1-2-vs-tls-1-1.

7. Can I use... Support tables for HTML5, CSS3, etc, September 24, 2020, https://caniuse.com/#search=1.2

8. TLS 1.3. Can I use... Support tables for HTML5, CSS3, etc, 25AD. https://caniuse.com/.

9. „TLS 1.3." EZ. Accessed September 26, 2020. https://www.hcc-embedded.com/tls-1-3.