Making the web more secure with Let's Encrypt

David Calavera

Netlify
Making the web more secure with Let's Encrypt

David Calavera
Netlify
Vegan Grasshopper Cake

This vegan Grasshopper Cake is an organic chocolate cake with vanilla mint buttercream frosting, chocolate ganache, and mint chocolate hello kitty candies. This was Isabelle's birthday cake since she specifically requested fried mac-n-cheese hearts for dinner and a chocolate mint birthday cake for dessert. This is a must-make for any chocolate and mint lover.
Moving towards a more secure web

September 8, 2016

Posted by Emily Schechter, Chrome Security Team

[Updated on 12/5/16 with instructions for developers]

Developers: Read more about how to update your sites here.

To help users browse the web safely, Chrome indicates connection security with an icon in the address bar. Historically, Chrome has not explicitly labelled HTTP connections as non-secure. Beginning in January 2017 (Chrome 56), we’ll mark HTTP pages that collect passwords or credit cards as non-secure, as part of a long-term plan to mark all HTTP sites as non-secure.
Dear XFINITY Customer,

You have reached 90% of your 1024 GB monthly data plan for your XFINITY Internet Service. As of 12-29-2016, you have 102 GB remaining for this calendar month.

Click to close
Last I checked, Stanford doesn’t hawk fashion accessories or telecom service. And it definitely doesn’t run obnoxious ads that compel you to wait.

Some ad-supported websites, like the Wall Street Journal, were also emblazoned with extra marketing material.
SSL Certificates

Want customers to come back? Protect them.

- Safely accept credit cards on your website
- Make sure your customers feel safe
- 24/7 support (480) 463-8887

Get Started
Write frontend code. Push it. We handle the rest.

CDN, Continuous deployment, 1 click HTTPS, and all the services you need. From instant prototypes to huge global enterprises.

Get Started with Netlify
HTTPS configuration

Free on all Netlify plans. Set a custom domain and enable secure connections instantly.

1. Configure a custom domain
2. Enable HTTPS

Enable HTTPS

This site's subscription allows Let's Encrypt TLS certificates for your domain.

Let's Encrypt is a fully automated install. We'll provision a TLS certificate from Let's Encrypt and install it on our CDN.

Let's Encrypt Certificate
Let’s Encrypt is a **free, automated, and open** Certificate Authority.

- Get Started
- Donate
HTTPS Everywhere: Encryption for All WordPress.com Sites

We’re proud to support a more secure web — now for all custom domains on WordPress.com.

Barry

Apr 8, 2016 @ 5:10 pm

Today we are excited to announce free HTTPS for all custom domains hosted on WordPress.com. This brings the security and performance of modern encryption to every blog and website we host.

Best of all, the changes are automatic — you won’t need to do a thing.

As the EFF points out as part of their Encrypt the Web initiative, strong encryption protects our users in various ways, including defending against surveillance of content and communications, cookie theft, account hijacking, and other web security flaws.
Implementing SSL/TLS for All Squarespace Sites

FRANKLIN ANGULO
How Etsy Manages HTTPS and SSL Certificates for Custom Domains on Pattern

Posted by Andy Yaco-Mink and Omar on January 31, 2017

In April of 2016 Etsy launched Pattern, a new product that gives Etsy sellers the ability to create their own hosted e-commerce website. With an easy-setup experience, modern and stylish themes, and guest checkout, sellers can merchandise and manage their brand identity outside of the Etsy.com retail marketplace while leveraging all of Etsy’s e-commerce tools.

The ability to point a custom domain to a Pattern site is an especially popular feature; many Pattern sites use their own domain name, either registered directly on the Pattern dashboard, or linked to Pattern from a third-party registrar.

At launch, Pattern shops with custom domains were served over HTTP, while checkouts and other secure actions happened over secure connections with Etsy.com. This model isn't ideal though; Google ranks pages with SSL slightly higher, and plans to increase the bump it gives to sites with SSL. That’s a big plus for Pattern sellers.
Sites with custom domain on Netlify use secure connections.
Automatic Certificate Management Environment (ACME)

github.com/letsencrypt/boulder
Message Transport

JWS payloads

A JWS is represented as a JSON object containing some or all of these four members:

- "protected": \`BASE64URL(UTF8(JWS Protected Header))\`
- "header": \`JWS Unprotected Header\`
- "payload": \`BASE64URL(JWS Payload)\`
- "signature": \`BASE64URL(JWS Signature)\`
Replay protection

HEAD /acme/new-nonce HTTP/1.1
Host: example.com

HTTP/1.1 204 No Content
Replay-Nonce: oFvn1FP1wIhRlYS2jTaXbA
Cache-Control: no-store
Request URI Integrity

{ "protected": base64url({
   "alg": "ES256",
   "jwk": {...},
   "nonce": "6S8IqOGY7eL2lsGoTZYifg",
   "url": "https://example.com/acme/new-account"
}),
"payload": base64url({
   "terms-of-service-agreed": true,
   "contact": ["mailto:admin@example.com"]
})
"Signature": "RZPOnYoPhjszF...-nh6X1FPB519I" }
Certificate Management

Account creation

{ "protected": base64url({...}),
  "payload": base64url(
    "terms-of-service-agreed": true,
    "contact": ["mailto:admin@example.org"]
  ),
  "Signature": "RZPOnYoPhjszF...-nh6X1FPB519I" }
Certificate authorization

{  "protected": base64url({...}),
  "payload": base64url(
    "identifier": {
      "type": "dns",
      "value": "example.org"
    }
  ),
  "signature": "nuSDISbWMgE7H...QyVUyzf3Zawps" }

Certificate authorization

{  "status": "pending",
  "expires": "2018-03-03T14:09:00Z",
  "identifier": {
    "type": "dns",
    "value": "example.org"
  }
}
"challenges": [
    {
      "type": "http-01",
      "url": "https://example.com/authz/1234/0",
      "token": "DGyRejmCefe7v4NfDGDKfA"
    },
    {
      "type": "tls-sni-02",
      "url": "https://example.com/authz/1234/1",
      "token": "DGyRejmCefe7v4NfDGDKfA"
    },
    {
      "type": "dns-01",
      "url": "https://example.com/authz/1234/2",
      "token": "DGyRejmCefe7v4NfDGDKfA"
    }]}
HTTP-01 Challenge

GET /well-known/acme-challenge/token
Host: example.org

{  "protected": base64url({...}),
    "payload": base64url({
        "keyAuthorization": "evaGxfADs...62jcerQ"
    }),
    "signature": "Q1bURgJbD1c5...3pYdSMLioNN4" }

DNS-01 Challenge

_acme-challenge.example.org.
300 IN TXT "gfj9Xq...Rg85nM"

{
  "protected": base64url({...}),
  "payload": base64url(
    {
      "keyAuthorization": "evaGxfADs...62jcerQ"
    }
  ),
  "signature": "Q1bURgJbD1c5...3pYdSMLioNN4"
}
TLS-02 Challenge

CLIENTHELLO example.org:443

ServerName: gfj9Xq.Rg85nM.token.acme.invalid

```
{
  "protected": base64url({...}),
  "payload": base64url(
    
    "keyAuthorization": "evaGxfADs...62jcerQ"
  
    
  ),
  "signature": "Q1bURgJ bD1c5...3pYdSMLioNN4"
}
```
Certificate request

GET /acme/cert/asdf HTTP/1.1
Host: example.org
Accept: application/pkix-cert

HTTP/1.1 200 OK
Content-Type: application/pkix-cert
Certificate request

...
Certificate request

-----BEGIN CERTIFICATE-----
[End-entity certificate contents]
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
[Issuer certificate contents]
-----END CERTIFICATE-----
How can I interact with an ACME Authority?
Automatically enable HTTPS on your website with EFF's Certbot, deploying Let's Encrypt certificates.

To get instructions for Certbot, choose your server software and the system it is running on from the dropdown menus above. You can then pick 'advanced' if you want less automation and more control.
letsencrypt.org/docs/client-options
How does Netlify's Certificate Engine work?
http://example.com/.well-known/acme-challenge/token

Token response

Token response
Lessons learned after provisioning thousands of certificates
Nobody knows how DNS propagation works
DNS resolution

As a domain may resolve to multiple IPv4 and IPv6 addresses, the server will connect to at least one of the hosts found in A and AAAA records, at its discretion.
Beware of the rate limits
Rate limits

20 SAN Certificates per registered domain per week.
- example.org
- staging.example.org
- [PUT YOUR GIT BRANCH HERE].example.org

5 Duplicate Certificates per week.
The network is still not reliable

https://aphyr.com/posts/288-the-network-is-reliable
How will Netlify's Certificate Engine work in the future?
User facing API for DNS propagation verifications
Certificate request batching and lazy provisioning
Based on message bus with better delivery guarantees
Open Source, independent service
HTTPS adoption has reached the tipping point

https://www.troyhunt.com/https-adoption-has-reached-the-tipping-point/
Let's Encrypt → @letsencrypt · 14 Oct 2016

Yesterday, for the first time, @Mozilla telemetry shows more than 50% of page loads were encrypted with HTTPS.

pic.twitter.com/kADcLOLsQ7
Thank you for listening!

David Calavera
Netlify