Extended Validation Is Broken

By @iangcarroll

Extended validation ("EV") certificates are a unique type of certificate issued by certificate authorities after more extensive validation of the entity requesting the certificate. In exchange for this more rigorous vetting, browsers show a special indicator like a green bar containing the company name, or in the case of Safari completely replace the URL with the company name.

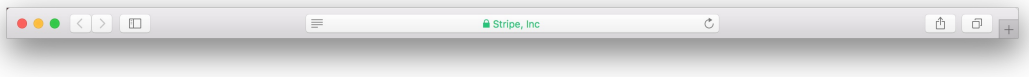
Generally, this process works fairly well, and there are few misissuances. There are not a lack of problems, however. Extended validation certificates include information about the legal entity behind the certificate, but not much else. What a legal entity can be turns out to be quite flexible; James Burton, for example, recently obtained an EV certificate for his company "Identity Verified". Unfortunately, users are simply not equipped to deal with the nuances of these entities, and this creates a significant vector for phishing.

Today, I will demonstrate another issue with EV certificates: **colliding entity names**. Specifically, this site uses an EV certificate for "Stripe, Inc", that was legitimately issued by Comodo. However, when you hear "Stripe, Inc", you are probably thinking of the payment processor incorporated in Delaware. Here, though, you are talking to the "Stripe, Inc" incorporated in Kentucky. This problem can also appear when dealing with different countries.

Edit (April 29th, 2018): This site no longer uses an EV certificate. Comodo arbitrarily revoked — without any notice — the first certificate, saying this site was made with the intent to mislead. GoDaddy issued us a new one on 04/11/2018, but revoked it later that day, stating that the site was fraudulent. It is notable that neither company believes they mis-issued the certificate.

How can a user tell which one you're talking to? Browsers hide this information at first glance, at most showing the **country** of incorporation. Obviously, here, both the real and fake Stripe are in the same country. With enough mouse clicks, you may be able to open a system certificate viewer, or get your browser to show you the city and state. But neither of these are helpful to a typical user, and they will likely just blindly trust the bright green indicator.

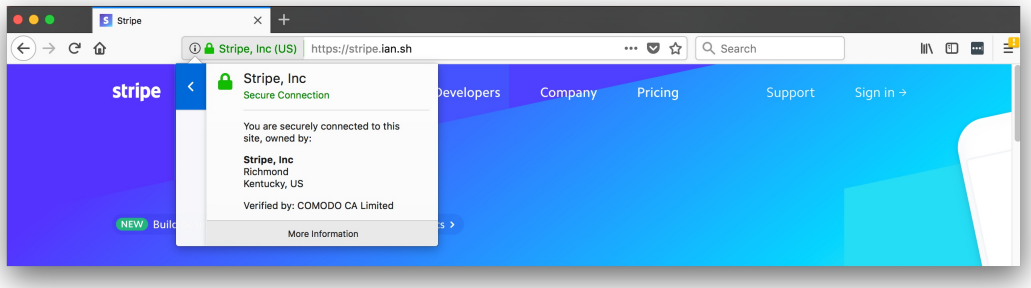
Let's look at the user interfaces of browsers. On Safari, the URL is **completely hidden**! This means the attacker does not even need to register a convincing phishing domain. They can register anything, and Safari will happily cover it with a nice green bar. The below screenshot is from this site. Hard to tell, right?



With Chrome, the story is slightly better, but only if you bother to look at the full URL. Chrome has no native way to view anything other than the company name and country of the certificate. Newer versions of Chrome will open the system certificate viewer with two mouse clicks (older versions completely removed viewing the certificate), but the system certificate viewer is useless for any

normal user.

Firefox is about the same as Chrome, but does allow users to view the city and state of incorporation after two mouse clicks. This is still fairly useless; even if a typical user bothered to check, they would need to know where the company they're ordering from is headquartered and ensure it matches up.



One question may be how practical this attack is for a real attacker who desires to phish someone. First, from incorporation to issuance of the EV certificate, I spent less than an hour of my time and about $177. $100 of this was to incorporate the company, and $77 was for the certificate. It took about 48 hours from incorporation to the issuance of the certificate.

The primary point raised by advocates of extended validation is that obtaining EV certificates would leave behind a signifigant paper trail of the bad actor's identity. However, there is minimal **individual** identity verification in the process. Dun & Bradstreet[1] is the only entity who attempted to verify my identity, and did so with a few trivial identity verification questions. Purchasing identities with answers to common verification questions is neither hard nor expensive.

Otherwise, there was no attempt at identity verification from the state of Kentucky or the registered agent I used in the process. This is typical of company formation in the United States. In summary, it would be trivial for bad actors to obtain these certificates. Some types of attackers may be more inclined to spend the effort on this, like those sending out SMS phishing messages. Mobile Safari on iOS would hide the URL once it's opened and likely drastically increase the success rate of collecting credentials. And, of course, there is no way to view the certificate with Mobile Safari.

After James Burton obtained a certificate for "Identity Verified", a discussion on the CA/Browser Forum's public mailing list, cabfpub, ensued. Some ideas were tossed around, mainly centered around adding a stronger tie to the individual requesting the certificate in order to deter criminals from obtaining these certificates. However, these are all band-aids that maybe, hopefully, will stop criminals from trying to get an extended validation certificate.

One of the solutions proposed was to require some form of face-to-face validation, either virtually or in real life, with the applicant and have them present identification to confirm their identity. While this may stymie some bad actors, those engaging in more targeted or high-profile attacks will have no problem taking a little extra time to invest in fake identification, or generally try to defeat other

verification methods.

It is worth noting that the Baseline Requirements, a set of standards for which all publicly trusted certificates are supposed to adhere to, contain a bit about High Risk Certificate Requests. However, the definition for a High Risk Certificate Request is not well defined, and not very useful. It "may include names at higher risk for phishing", but it relies on certificate authorities to reliably maintain a list of phishing targets, and generally be competent.

There will undoubtedly be many proposed solutions to this issue. Ultimately, though, any method that ends up giving users a legal entity is fatally flawed. As a result of how extended validation certificates work, browsers have few options to fix this. Having said that, they can take steps to ensure EV certificates do not override other critical parts of the user interface, like Safari does.

Thanks to Ryan Hurst, Eric Mill, and Filippo Valsorda for their feedback prior to publication.

[1] Amusingly, Dun & Bradstreet explicitly said they would deny any applications using third-party addresses, and then happily accepted my third-party agent's address.