Tor upgrades to make anonymous publishing safer

March 20 2017, by Philipp Winter

Credit: AI-generated image (disclaimer)

In the coming months, the Seattle-based nonprofit The Tor Project will be making some changes to improve how the Tor network protects users' privacy and security. The free network lets users browse the internet anonymously. For example, using Tor can reduce the risk of being identified when dissidents speak out against their governments,

whistleblowers communicate with journalists and victims of domestic abuse seek help.

In its most common, and best-known, function, a person using the free Tor Browser – essentially a privacy-enhanced version of Firefox – uses the internet mostly normally. Behind the scenes, the browser and the network handle the web traffic by bouncing the communications through a chain of three randomly chosen computers from all over the world, called "relays." As of March 2017, the Tor network counts almost 7,000 of these relays. The goal of leveraging these relays is to decouple a user's identity from her activity.

But those users are still, generally speaking, using others' websites, which can be shut down or pressured into censoring online activity. My own work as a scholar and volunteer member of The Tor Project also looks at the network's way of allowing people to host websites privately and anonymously, which is where most of the upgrades to the system will come.

Called "onion services," this element of the Tor network makes it possible for a person to run a website (or filesharing site, or chat service or even video calling system) from a dedicated server or even her own computer without exposing where in the world it is. That makes it much harder for authorities or opponents to take down. The upcoming changes will fix flaws in the system's original design, and employ modern-day cryptography to make the system future-proof. They will improve security and anonymity for existing Tor users and perhaps draw additional users who were concerned the prior protections were not enough when communicating and expressing themselves online.

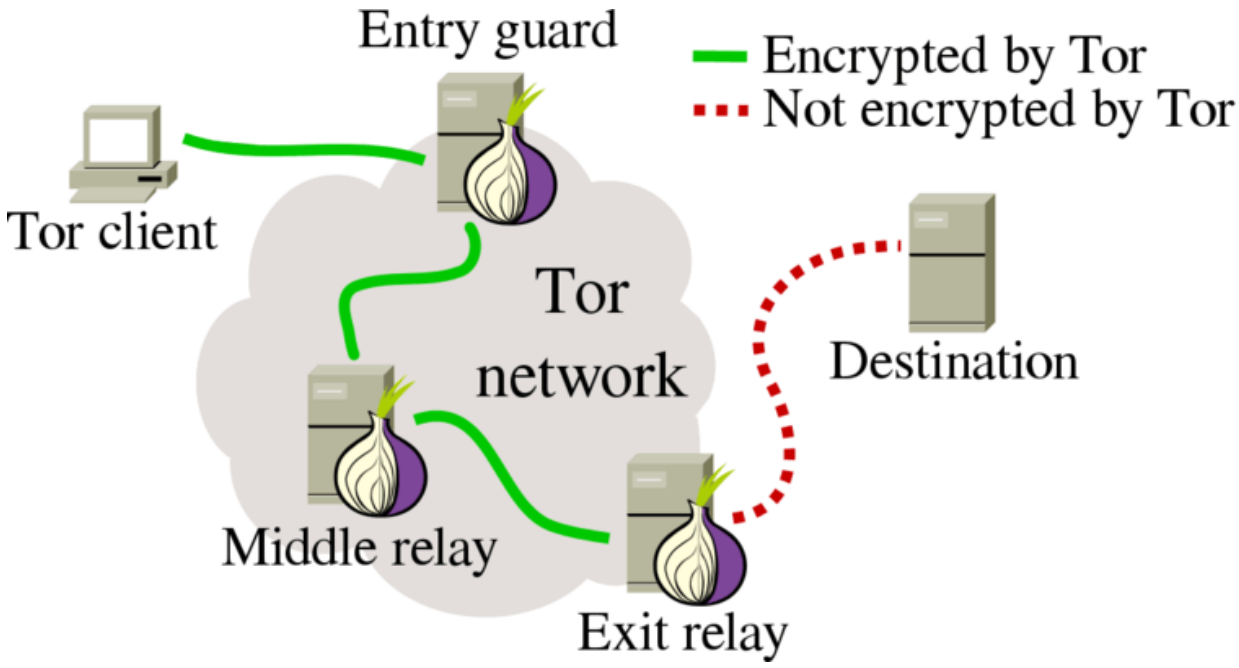
Understanding onion services

As of March 2017, an estimated 50,000 onion services are operating on

the Tor network. Onion services continuously come online and offline, though, so it is difficult to obtain exact numbers. Their name comes from the fact that, like Tor users, their identities and activities are protected by multiple layers of encryption, like those of an onion.

While criminals are frequently early adopters of anonymitytechnology, as more people use the system, legal and ethical uses become far more common than illegal ones. Many onion services host websites, chat sites and video calling services. We don't know all of what they're doing because The Tor Project designs privacy into its technology, so it does not and cannot keep track. In addition, when new onion services are set up, their very existence is private by default; an operator must choose to broadcast a service's existence publicly.

Many owners do announce their sites' existence, however, and the Ahmia search engine provides a convenient way to find all publicly known onion services. They are as diverse as the internet itself, including a search engine, a literary journal and an archive of Marxist and related writing. Facebook even has a way for Tor users to connect directly to its social media service.



Tor bounces web traffic over three randomly selected Tor relays out of a total of around 7,000 relays.

Creating an onion site

When a privacy-conscious user sets up an onion service (either manually or with a third-party tool such as onionshare), people who want to connect to it must use the Tor Browser or other Tor-enabled software; normal browsers such as Chrome and Firefox cannot connect to domains whose names end in ".onion." (People who want to peek at onion sites without all of the network's anonymity protections can visit Tor2web, which acts as a bridge between the open web and the Tor network.)

Originally, a new onion service was supposed to be known only to its creator, who could choose whether and how to tell others of its existence. Of course, some, like Facebook, want to spread the word as widely as possible. But not everyone wants to open their Tor site or

service to the public, the way search and social media sites do.

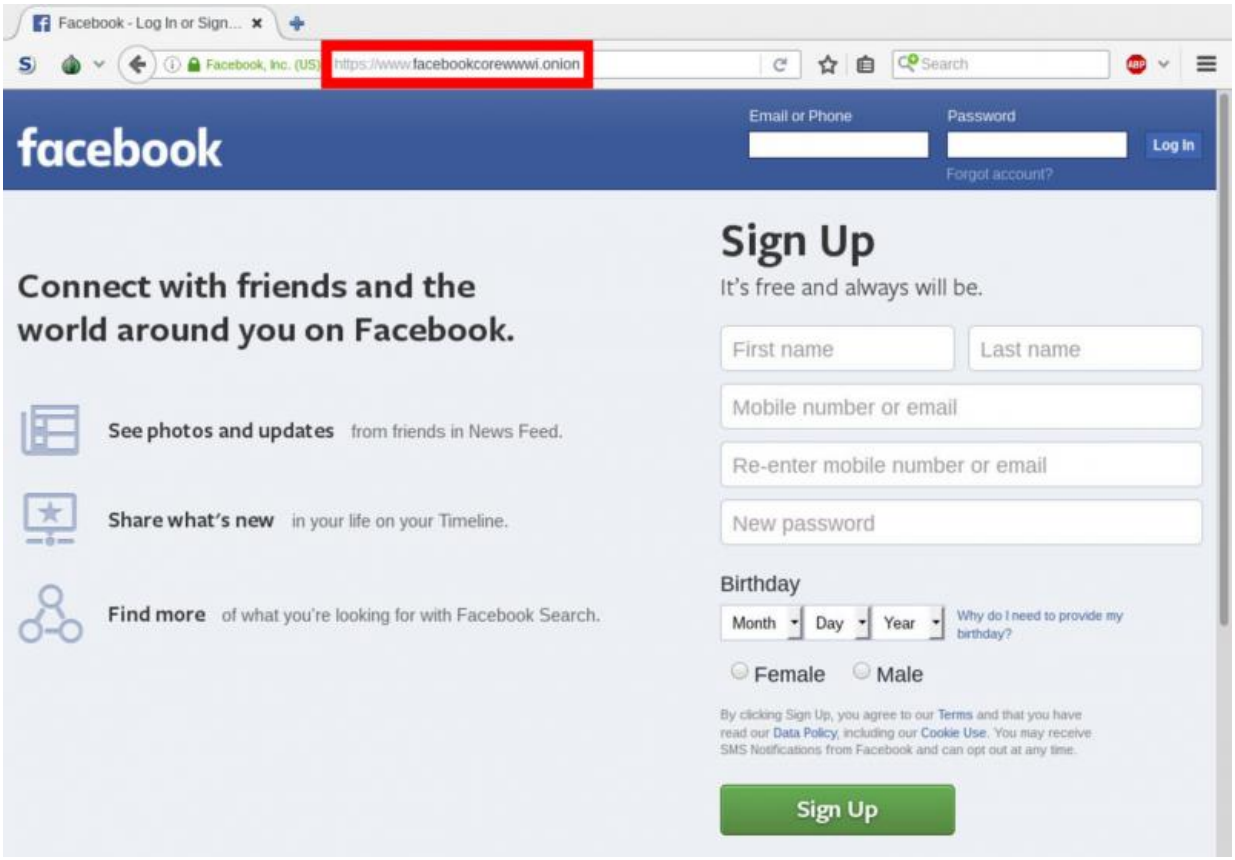
However, a design flaw made it possible for an adversary to learn about the creation of a new onion service. This happened because each day, onion services announce their existence to several Tor relays. As happened in 2014, an attacker could potentially control enough relays to keep track of new service registrations and slowly build up a list of onion sites – both secret and public – over time.

The same design flaw also made it possible for an attacker to predict what relays a particular service would contact the following day, allowing the adversary to become these very relays, and render the onion service unreachable. Not only could someone wanting to operate a private, secret onion service be unmasked under certain circumstances, but their site could effectively be taken offline.

The updates to the system fix both of these problems. First, the relays each service contacts for its daily check-in will be randomly assigned. And second, the check-in message itself will be encrypted, so a relay can follow its instructions, but the human operator won't be able to read it.

Naming domains more securely

Another form of security causes the names of onion services to be harder to remember. Onion domains are not named like regular websites are: facebook.com, theconversation.com and so on. Instead, their names are derived from randomly generated cryptographic data, and often appear like expyuzz4wqqyqhjn.onion, which is the website of The Tor Project. (It is possible to repeatedly generate onion domains until a user arrives at one that's a bit easier to recognize. Facebook did that and – with a combination of luck and raw computational power – managed to create facebookcorewwwi.onion.)



Facebook's onion service, facebookcorewwwi.onion, when accessed through the Tor Browser.

Older onion services had names made up of 16 random characters. The new ones will use 56 characters, making their domain names look like this: l5satjgud6gucryazcyvyvhuxhr74u6ygigiuyixe3a6ysis67ororad.onion.

While the exact effects on users' ability to enter onion services' addresses haven't been studied, lengthening their names shouldn't affect things much. Because onion domain names have always been hard to remember, most users take advantage of the Tor Browser's bookmarks,

or copy and paste domain names into address fields.

Protecting onion sites

All this new design makes it significantly harder to discover an onion service whose operator wants it to remain hidden. But what if an adversary still manages to find out about it? The Tor Project has solved that problem by allowing onion services to challenge would-be users to enter a password before using it.

In addition, The Tor Project is updating the cryptography that onion services employ. Older versions of Tor used a cryptosystem called RSA, which could be broken by calculating the two prime factors of very large numbers. While RSA is not considered insecure yet, researchers have devised several attacks, so The Tor Project is replacing it with what is called elliptic-curve cryptography, which uses keys that are shorter, more efficient and understood to be at least as secure.

The developers are also updating other basic elements of the encryption standards used in Tor. The hash function, which Tor uses to derive short and constant-length text strings from arbitrarily long data, will change from the troubled – and partially broken – SHA-1 to the modern SHA-3. In addition, secret keys for the Advanced Encryption Standard cryptosystem will be twice as long as before – and therefore significantly harder to break. These don't address specific immediate threats, but protect against future improvements in attacking encryption.

With these improvements to the software that runs Tor, we're expecting to be able to prevent future attacks and protect Tor users around the world. However, better anonymity is only one aspect in the bigger picture. More experimentation and research are necessary to make onion services easier to use.