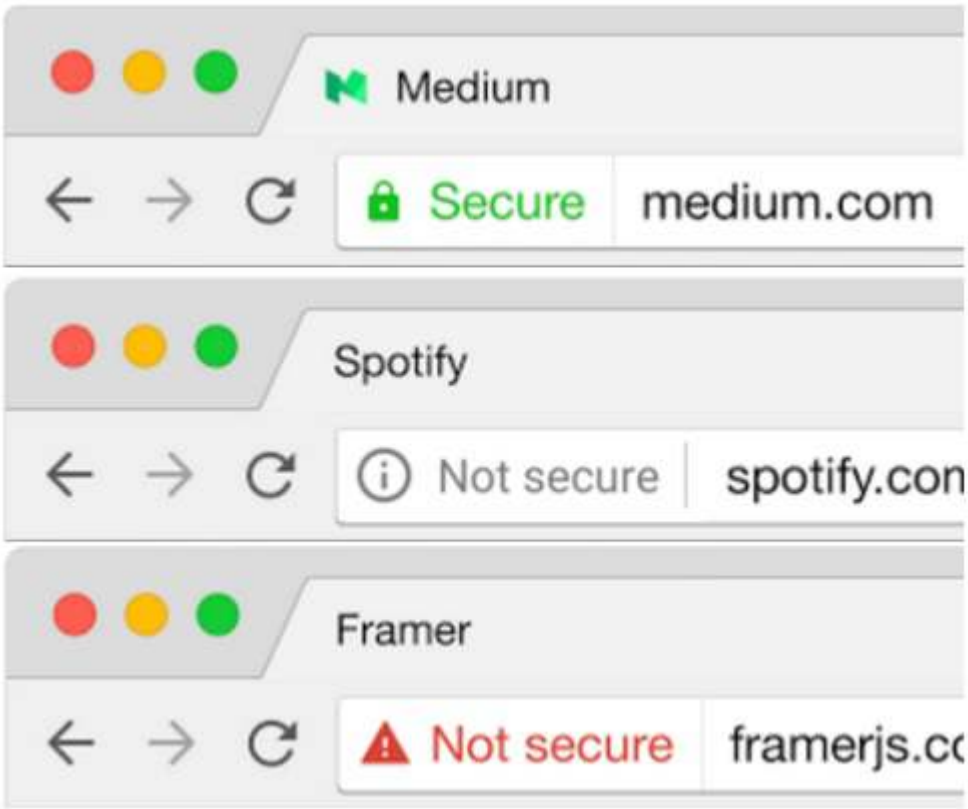
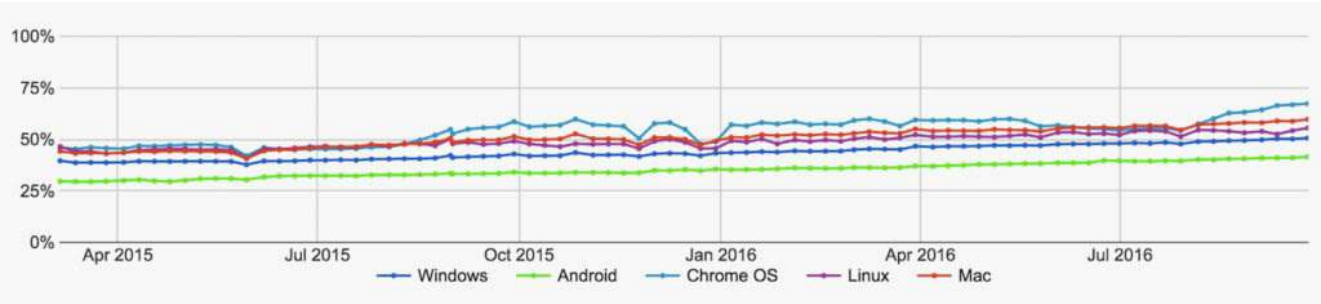
Google's Chrome Hackers Are About to Upend Your Idea of Web Security

Caption: Parisa Tabriz, center, and the Chrome security team. Amy Harrity for WIRED

Slide: 2 / of 6 . Caption: Parisa Tabriz.Amy Harrity for WIRED



Slide: 3 / of 6 . Caption: Google's new warning scheme for Chrome, indicating an HTTPS-encrypted site (top) a non-HTTPS site (middle) and a site with faulty HTTPS. (bottom)Google



Slide: 4 / of 6 . Caption: Percentage of HTTPS pages viewed in Chrome over time.Google

Slide: 5 / of 6 . Caption: Adrienne Porter Felt.Amy Harrity for WIRED

Slide: 6 / of 6 . Caption: Some of the security indicators Google considered to represent a site's encryption (top row) or lack of encryption. (bottom row)Google/Berkeley

Skip Article Header. Skip to: Start of Article.

In a show of hacker team spirit in August of last year, Parisa Tabriz ordered hoodies for the staff she leads at Google, a group devoted to the security of the company's Chrome browser. The sweatshirts were emblazoned with the words "Department of Chromeland Security," along with Chrome's warning to users when they visit insecure websites that leave them open to surveillance or sabotage: a red padlock crossed out with an X.

But when one of Tabriz's team members, Adrienne Porter Felt, donned the hoodie later that month, her sister looked at that lock icon—a simple rectangle with an arch over it—and asked an innocent question: Why did the sweatshirt have a red purse on it?

For Tabriz's team, the mistaken assumption that an average person on the internet can tell the difference between the symbol for a purse and a padlock has come to represent a fundamental problem with modern browsers.

Google's head of Chrome security Parisa Tabriz.Amy Harrity for WIRED

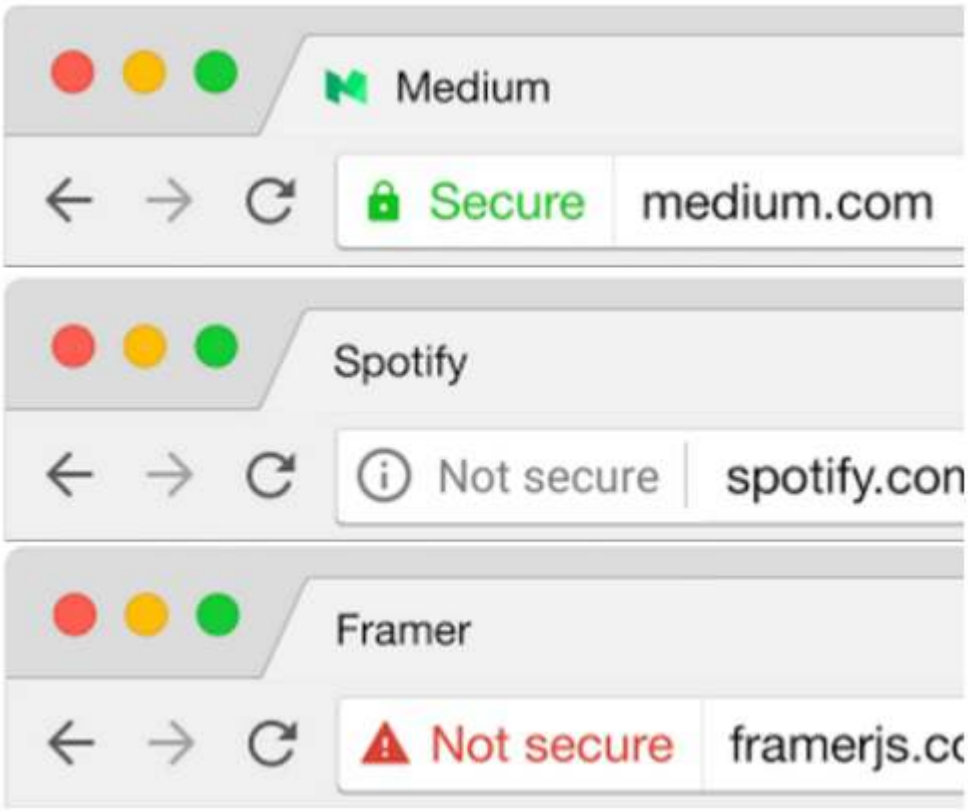
They're responsible for helping billions of people gauge the security of the sites they visit, but there's only an inscrutable icon to signal the difference between an encrypted site that locks its connections and unprotected sites that leave them vulnerable to threats—which can range anywhere from a hacker sniffing passwords at the next Starbucks table to a hacked home router eavesdropping on emails to an internet provider surreptitiously injecting ads. The confusing collection of hieroglyphics used by most browsers today to draw that line are misleading at best; at worst they're negligently silent or even dishonest about a site's lack of security.

That's why, for the first time, the Chrome team is about to start naming and shaming the nearly half of the world's websites that don't use strong encryption, putting a clear "Not secure" warning next to thousands of popular online destinations that use unencrypted HTTP connections rather than encrypted HTTPS connections. In the process, they may just change the standard for security online.

"People say we can't make half the web look scary, that people will be afraid of it," Tabriz says. "But for us, it's a problem of trying to be honest with users. Without HTTPS, a user or web service can have no expectation that anything on a site hasn't been tampered with or eavesdropped. And that's crazy."

Tightening the Crypto Ratchet

Starting in January, Chrome will flip the web's security model: Instead of warning users only about HTTPS-encrypted sites with faulty or misconfigured encryption, as Chrome currently does, it will instead flag as "not secure" any unencrypted sites that accept a username and password or a credit card. That unmistakable alert will appear to the left of Chrome's address bar.



Google's new warning scheme for Chrome, indicating an HTTPS-encrypted site (top), a non-HTTPS site (middle), and a site with faulty HTTPS (bottom). Google

Soon after, the team also plans to announce another category of sites that will be flagged for not using HTTPS by a deadline later in 2017. Among the candidates they're considering: any unencrypted page visited through Chrome's Incognito mode and any non-HTTPS site that offers downloads. Check your daily tour of web forums, download sites, and registration-enabled media outlets for the telltale lack of a green padlock, and you'll see many are set for an unpleasant wakeup call when they fail those tests. And over the coming years, Chrome plans to hold more and more types of sites to that HTTPS standard.

"This is really important," says Josh Aas, the founder of the HTTPS-focused nonprofit Let's Encrypt. "There's no more effective motivator for websites to switch to HTTPS than the browser's user interface."

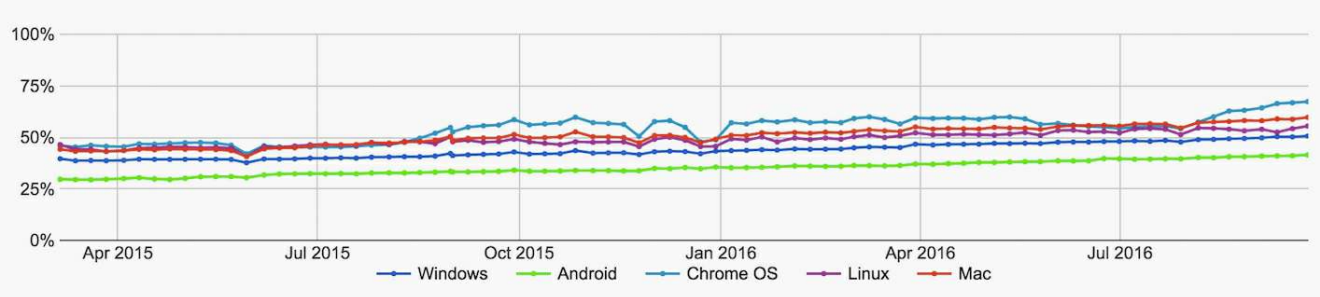
For many web administrators, Google's encryption-shaming may not be so welcome. Turning on HTTPS isn't quite as easy as flipping a switch: Many complex media sites with elements like ads and video, for instance, are dependent on those outside data sources to encrypt every piece of content before they can meet Google's bar. WIRED, for instance, announced in April that it would be turning on HTTPS for all of Wired.com, but it took five months to iron out issues like insecure third-party content and, ironically, maintaining the site's high rankings in search results while changing all of its web addresses. *The New York Times*, for its part, issued a challenge in late 2014 to news sites to switch to HTTPS by the end of 2015, but still hasn't achieved that standard itself.

Riling web admins, however, is a small price to pay for the security benefits HTTPS will bring, says Aas. "There are going to be people who feel like they're forced into this too early," he concedes. "But that's true of every change on the web. And this is the direction we need to go."

Google has solid business reasons to be aggressive in its HTTPS campaign. In contrast to closed-off environments like Apple's App Store, Google loves the open web, where its search engine reigns supreme and its ads rake in the vast majority of the company's $80 billion a year in revenue. To compete with mobile apps, Tabriz explains that Google wants web pages to be able to reach deeper into your computer's resources, accessing the same sensitive information, like location and offline data, that apps routinely use. But if the web's tendrils are going to extend further into our private lives, they first need to be secure. "You wouldn't want a man-in-the-middle to be able to access those things," says Tabriz, using the cryptographer's term for hackers who intercept and eavesdrop on HTTP data as it's traveling from your computer to a web server and back.

As a kind of progress bar for the web's security evolution, Tabriz's team today released a new set of data on Google's website that displays the exact fraction of sites visited through Chrome that are encrypted, broken down by country and operating system. It shows that around 51 percent of Windows' Chrome traffic is encrypted and 60 percent for MacOS. Android lags behind at 43 percent, perhaps because many of users' most sensitive smartphone connections are made through apps instead of the web. The report also breaks down encryption on a country-by-country basis and shows that while 60 percent of Windows users' Chrome connections are encrypted in the US, only 47 percent are protected in Turkey and only a third in Japan.

Until their graphs near 100 percent across global operating systems, Tabriz says, they'll keep ratcheting up Chrome's HTTPS requirements. Eventually they aim to make web encryption so ubiquitous that a lock icon symbolizing HTTPS is hardly necessary—that users can rightly assume their traffic is encrypted unless they see an alert to the contrary. "I'm determined to make the web go there," Tabriz says. "Because if we can't have HTTPS, we can't have real security."



Percentage of HTTPS pages viewed in Chrome over time.Google

Fixing Human Problems

Since she started as a security engineer at Google nearly a decade ago, Tabriz has approached her job as a white-hat hacker with an understanding that security problems are not merely technical but human. After repeatedly finding and fixing the same bugs in the company's code, for instance, she says she became determined to instead fix Google's coders. So in 2010 she and a fellow Googler started Google's "Resident Hacker" program, a crash course in information security training for programmers so they could learn to find, exploit, and patch bugs in their own work.

Tabriz's interest in HTTPS in particular was piqued in 2011, when her colleagues on the security team discovered that the certificate authority DigiNotar—one of the companies tasked with handing out the certificates that authenticate the identity of an HTTPS website—had been breached by hackers. The attackers then used their access to fake encrypted connections to Google sites like Gmail and eavesdropped on visitors. The attack appeared to be the work of the Iranian government, affecting more than 300,000 mostly Iranian victims. For Tabriz, whose father is an Iranian who periodically returns to his hometown of Tehran, the attack carried personal resonance. She remembers reading a comment from one Iranian on a blog post about the incident: "For you guys, a fake certificate means a stolen password or personal information," he wrote. "For me and thousands of other Iranians, it leads to jail, torture or even death sentence."

So when Tabriz took over the Chrome security team in 2014, she put a new focus on not just locking down Chrome but the entire web that users see through it. Google has long fought to advance Chrome's security beyond that of other browsers. Chrome was the first popular browser to implement a rigorous "sandbox"—a security measure that limits how deeply a malicious web page can reach into a user's computer—to automatically install security updates, and to pay bounty rewards in the hundreds of thousands of dollars for information about the browser's security flaws. But Tabriz's HTTPS push meant looking beyond Chrome's own code and pulling up the rest of the web's security to meet its standards.

Adrienne Porter Felt, who's leading the Chrome security team's push for HTTPS.Amy Harrity for WIRED

The Chrome team's most powerful lever to move the web's security is arguably the trusty padlock you see by the URL, which signals a site's encryption. But Chrome and other browsers today use a counterintuitive and even perverse system to guide users towards secure web sites, issuing a warning only if an encrypted connection looks suspect; for example, if a site's certificate—the data proving it is who it claims —is invalid or expired. But if you visit a completely unencrypted site—no matter what credit cards, passwords, or other sensitive data the page asks for—your browser shows no warning at all as you spill your guts to eavesdroppers.

As Tabriz's team considered how to redesign that faulty system, they started from scratch. Porter Felt took the lead on Chrome's encryption push, and along with fellow Googlers and researchers at Berkeley, surveyed more than 1,300 people about how they perceive security warnings in web browsers. Over two years, they went so far as to travel to India, Brazil, and Indonesia to test people's understanding of security indicators like the red lock icon that confused Porter Felt's sister. In India, for instance, Porter Felt interviewed more than a dozen internet newcomers, and the majority couldn't even guess what the lock symbol meant. "This goes beyond cryptography," Tabriz says. "Trying to present this to users who are colorblind or don't speak English or think a lock is a purse is a very *human* problem."

No More Red Purses

Porter Felt and her fellow researchers presented the survey results at the USENIX Symposium on Usable Privacy and Security last summer, showing how Chrome's security symbology was failing. When users viewed an unencrypted HTTP page in Chrome, only about one in five interpreted the white page icon to the left of the address bar as "not secure." When they were asked to choose a symbol to indicate that a site was secure, they chose a red lock just as often as they chose a green one. But when users were shown a black circle with an exclamation point in it, accompanied by the word "HTTP," 38 percent regarded the site as unsafe and said they'd leave the page immediately. Change that symbol to a red triangle with an exclamation point and "HTTP" to "not safe," and over two-thirds of respondents said they'd flee.

Some of the security indicators Google considered to represent a site's encryption (top row) or lack of encryption. (bottom row) Google/Berkeley

Ultimately, Porter Felt and the Chrome team settled on a system that tries to educate users without alarming them into a state of numbness. For now, when someone lands on a typical unencrypted site, Chrome shows a white circle with an "i" in it rather than the exclamation point, meant to serve as an invitation to click for more information. Starting in January, the "i" will in many cases be accompanied by the blunt words "Not secure." In a few years, Tabriz says, she hopes HTTPS will have progressed to the point that they can unleash the red triangle exclamation point icon on all remaining HTTP sites. "In our impatient moments, we just want to mark everything as insecure," Tabriz says. "A huge fraction of the web isn't HTTPS, and that's embarrassing to me. It's not going to solve itself."

The team, however, is taking a carrot-and-stick approach: Punishing laggards with its revamped security warnings while also working to make HTTPS easier to adopt. It's created tools for assessing the components of an HTTPS site, digging up and explaining to developers the flaws that trigger Chrome's warnings. And it's donated $350,000 to the non-profit Let's Encrypt, which has distributed millions of encryption certificates for free, rather than charge annual fees like other certificate authorities.

Even so, Porter Felt and Tabriz say they've gotten emails and developer forum comments accusing them of moving too fast, breaking sites, and even "ruining lives." But Tabriz has resolved to stick to Chrome's timeline of a slow, inexorable push towards greater security for all.

"It's easy to convince yourself not to do something, to not move forward," says Tabriz. "But I've developed a thick skin." If the world's websites don't want to get left behind, they'd better toughen up, too.

Go Back to Top. Skip To: Start of Article.Skip Social. Skip to: Latest News.

- Share
- Share
- Tweet
- Pin
- Email

Skip Comments. Skip to: Footer.