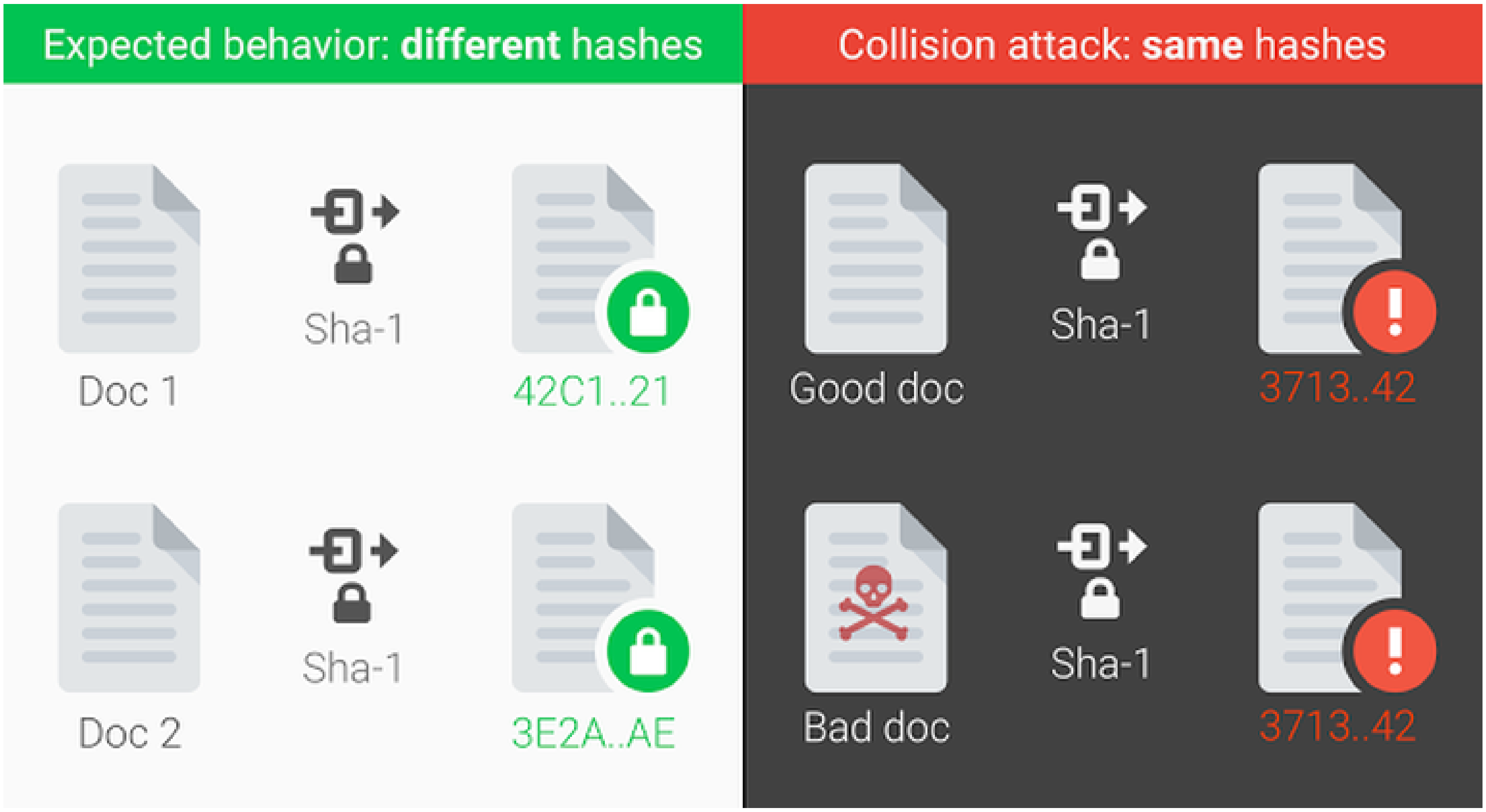
JUST IN WINDOWS EMERGENCY PATCH: MICROSOFT'S NEW UPDATE KILLS OFF INTEL'S SPECTRE FIX

Google breaks SHA-1 web crypto for good but Torvalds plays down impact on Git

Researchers' SHA-1 collision spells the end of the cryptographic hashing algorithm for the web, but Linux kernel creator Linus Torvalds says not to worry about Git's reliance on SHA-1.

By Liam Tung | February 24, 2017 -- 11:53 GMT (03:53 PST) | Topic: Security



Google explains that if two distinct pieces of data have the same hash, an attacker could use this collision to deceive systems into accepting a malicious file as a benign one.

Image: Google

No one considers the 20-year-old SHA-1 hash function secure, and browser makers are well on the way to phasing it out. But until yesterday's revelation by researchers at Google and CWI Amsterdam, there was no known reliable way of causing a SHA-1 collision.

The SHA-1 algorithm produces a 160-bit mathematical representation, or hash value, that should be unique for a given file. It's been used to ensure the integrity of everything from digital certificates for HTTPS websites, to managing commits in code repositories, and protecting users against forged documents.

Now the researchers, using a technique called SHAttered (https://shattered.it), have demonstrated that two PDFs with different content can have the same hash, which should never happen.

"We hope that our practical attack against SHA-1 will finally convince the industry that it is urgent to move to safer alternatives such as SHA-256," the researchers said (https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html).

The two-year effort was led by CWI Amsterdam researcher Marc Stevens and Google head of anti-abuse research Elie Bursztein, and relied on some serious computing power from Google.

The attack required nine quintillion (9,223,372,036,854,775,808) SHA-1 computations and took the equivalent of 6,500 years of single-CPU computations to complete phase one of the collision, and 110 years of single-GPU to finish phase two. Although that process sounds long, it's 100,000 times faster than a brute-force attack on SHA-1.

The researchers note in a paper that the estimated cost of a collision attack has fallen significantly in the past few years, which is why it's being phased out for signing HTTPS certificates.

Microsoft's Edge and Internet Explorer will warn users (https://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-sha1-certificates.aspx) if a site is using a SHA-1 certificate by mid-2017 (https://blogs.windows.com/msedgedev/2016/11/18/countdown-to-sha-1-deprecation/#ykSfITgTLoeOcvcS.97), while Google's Chrome made the move in January. Firefox will do so in early 2017 (https://blog.mozilla.org/security/2017/02/23/the-end-of-sha-1-on-the-public-web/).

Based on a SHA-1 attack developed by Stevens, cryptographer Bruce Schneier in 2012 estimated (https://www.schneier.com/blog/archives/2012/10/when_will_we_se.html) a SHA-1 collision attack would have a processing cost of around $700,000 in 2015 using spot prices for Amazon EC2 instances, which would fall to $173,000 in 2018.

As noted in the SHAttered paper (https://shattered.it/static/shattered.pdf), the second and more expensive phase of the attack, which led to a full SHA-1 collision, was far less costly than the 2012 estimate. This phase relied on a cluster of GPUs hosted by Google. Again, using Amazon Web Services pricing as a yardstick, they write:

"Using a p2.16xlarge instance, featuring 16 K80 GPUs and nominally costing $14.4 per hour would cost $560,000 for the necessary 71 device years. It would be more economical for a patient attacker to wait for low spot prices of the smaller g2.8xlarge instances, which feature four K520 GPUs, roughly equivalent to a K40 or a GTX 970. Assuming thusly an effort of 100 device years, and a typical spot price of $0.5 per hour, the overall cost would be $110,000."

Potentially affected applications include SHA-1 signed digital certificates, email PGP/GPG signatures, and GIT.

Google has released a tool to test if a file is part of a collision attack, and has added protections in Gmail and G Suite to detect its PDF collision technique.

The researchers highlight that Linus Torvald's code version-control system Git "strongly relies on SHA-1" for checking the integrity of file objects and commits.

"It is essentially possible to create two Git repositories with the same head commit hash and different contents, say, a benign source code and a backdoored one," they note.

However, Torvalds said on a mailing list yesterday that he's not concerned since "Git doesn't actually just hash the data, it does prepend a type/length field to it", making it harder to attack than a PDF.

"Put another way: I doubt the sky is falling for Git as a source control management tool. Do we want to migrate to another hash? Yes. Is it game over for SHA-1 like people want to say? Probably not," wrote (http://marc.info/?l=git&m=148787047422954) Torvalds.

"I haven't seen the attack details, but I bet: (a) the fact that we have a separate size encoding makes it much harder to do on Git objects in the first place (b) we can probably easily add some extra sanity checks to the opaque data we do have, to make it much harder to do the hiding of random data that these attacks pretty much always depend on."

MORE ON SECURITY

- Sentinel Labs, SpyChatter, Vir2us settle with FTC over fake security certificate claims (http://www.zdnet.com/article/sentinel-labs-spychatter-vir2us-settle-with-ftc-over-security-certificate-lies/)
- Cloudflare found leaking customer HTTPS sessions for months (http://www.zdnet.com/article/cloudflare-found-leaking-customer-https-sessions-for-months/)
- Hoping for a payrise? Then watch out for this sneaky phishing scam (http://www.zdnet.com/article/hoping-for-a-payrise-watch-out-for-this-sneaky-phishing-scam/)
- Linux's decade-old flaw: Major distros move to patch serious kernel bug (http://www.zdnet.com/article/linuxs-decade-old-flaw-major-distros-move-to-patch-serious-kernel-bug/)
- Cybercriminals start cashing in on vulnerable WordPress websites (http://www.zdnet.com/article/cybercriminals-start-cashing-in-on-vulnerable-wordpress-websites/)
- Think you're safe from hackers offline? This drone steals data from a PC's blinking LED (http://www.zdnet.com/article/think-youre-safe-from-hackers-offline-this-drone-steals-data-from-a-pcs-blinking-led/)

RELATED TOPICS: GOOGLE SECURITY TV DATA MANAGEMENT CXO DATA CENTERS

LOG IN TO COMMENT | Community Guidelines

Join Discussion

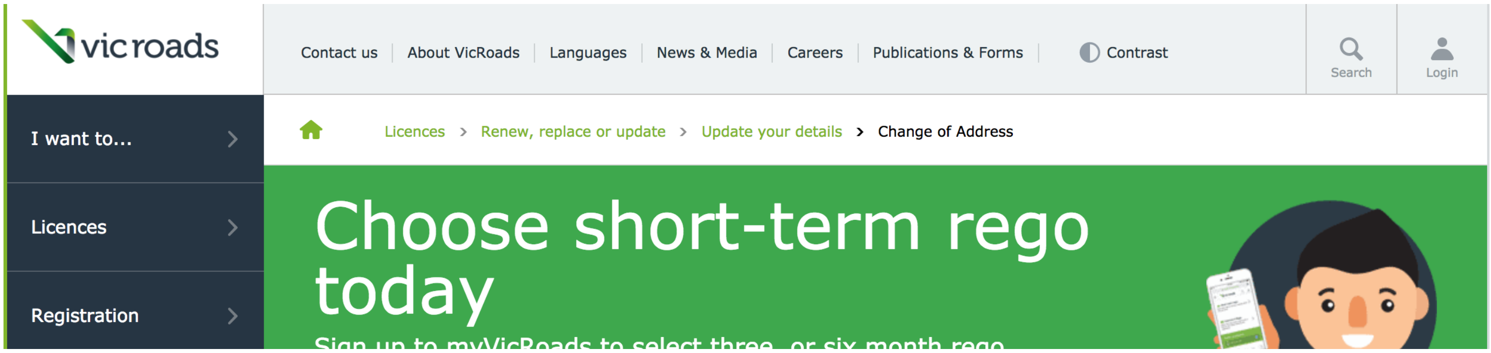
Ghostery blocked comments powered by Disqus.

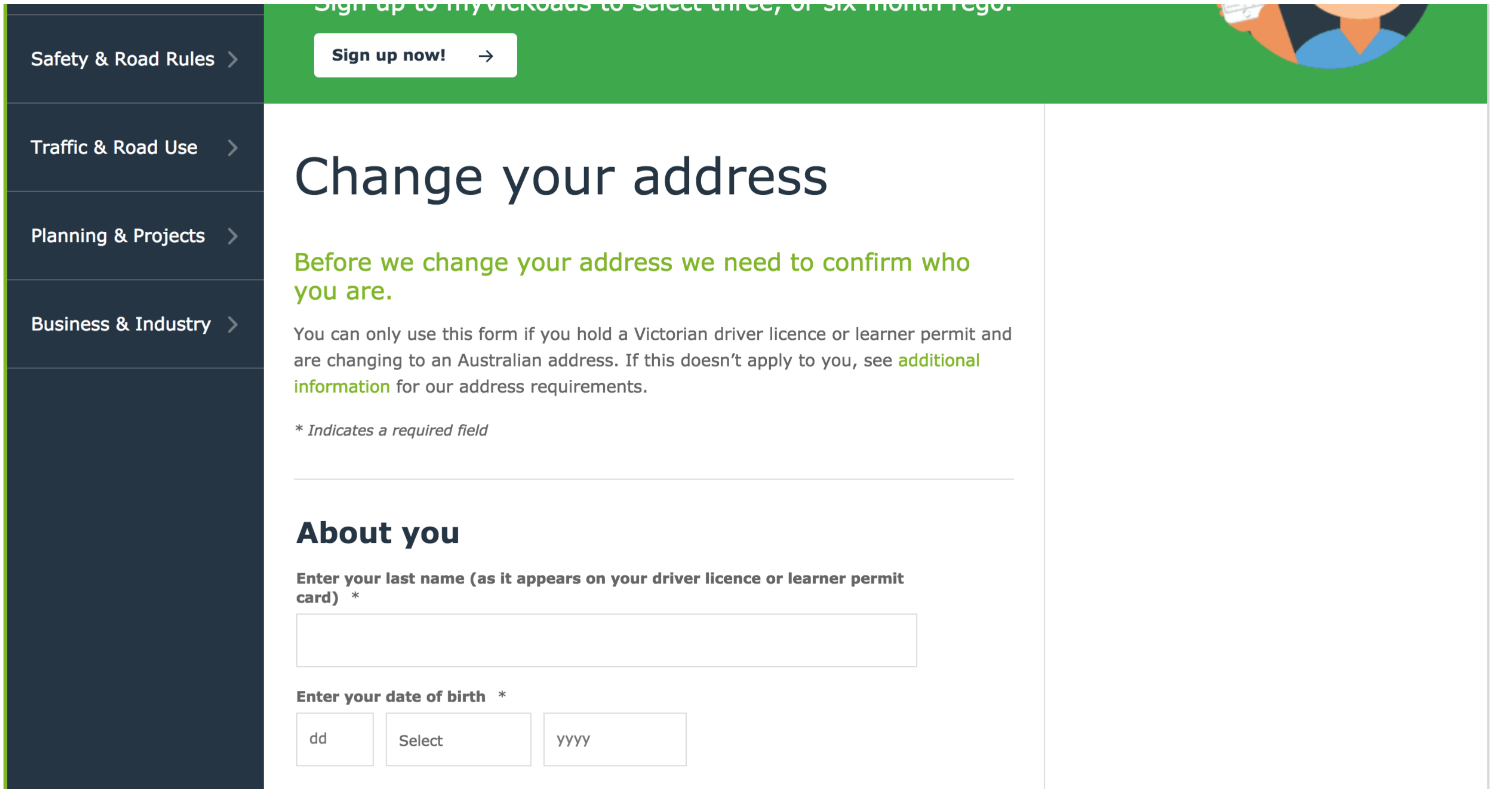
ADD YOUR COMMENT

VicRoads to fill identity theft pothole eventually

A web form lets anyone change the address on a Victorian driver's licence without authentication. The state's licensing authority knows this, they know it's been abused, but the form is still online.

By Stilgherrian for The Full Tilt | January 31, 2018 -- 05:08 GMT (21:08 PST) | Topic: Security


vic roads
Contact us
About VicRoads
Languages
News & Media
Careers
Publications & Forms
Contrast
Search
Login
I want to...
Licences
Registration
Licences > Renew, replace or update > Update your details > Change of Address
Choose short-term rego today
Sign up to myVicRoads to select three, or six month rego



Sign up to myVicRoads to select three, or six month rego.

Change your address

Before we change your address we need to confirm who you are.

You can only use this form if you hold a Victorian driver licence or learner permit and are changing to an Australian address. If this doesn't apply to you, see additional information for our address requirements.

** Indicates a required field*

About you

Enter your last name (as it appears on your driver licence or learner permit card) *

Enter your date of birth *

dd | Select | yyyy

(Screenshot: Stilgherrian/ZDNet)

On November 10, 2017, Melbourne resident Niel Fulton applied for a new driver's licence. It never arrived. Two weeks later, someone used a form on the VicRoads website to change the registered address.

Fulton assumes his licence was stolen from the post, either in transit or from his letter box. The thief would then have had everything they'd have needed to submit the change-of-address form: the licence number, and the driver's name, address, and date of birth. Then, as per standard procedure, VicRoads would have posted them a sticker with the new address, to attach to the physical licence.

As Fulton told ZDNet, the thief is then free to use this licence as a verifiable form of ID, at least until the change is noticed by the legitimate licence holder, particularly with services that don't require a photo -- and that includes many if not most online accounts.

"What does this mean? Anyone in possession of a licence not their own is free to use it as a form of ID, paving the way for deeper identities to be built," Fulton said.

"What's more, once the actual owner of the licence notices the change, and changes the address back, there's nothing to stop the original problem happening again, as the unknown party still has enough details to change the address, thereby still leaving opportunity for fraud."

Fulton eventually contacted VicRoads on January 15, but they seemed unconcerned.

VicRoads can't track the user IP address or any other details of the illegitimate change beyond the date it was made, Fulton said he was told, and VicRoads won't issue a new licence number until they see tangible evidence of fraud having been committed.

"A new licence issued with the same number means the one held by unknown parties is still valid and usable for ... whatever," Fulton said.

VicRoads declined to confirm any of these specifics, but told ZDNet that the agency "takes the security of our customers' personal information very seriously".

"We process more than 24 million licensing and registration interactions each year and the number of licences replaced due to fraudulent activity each year is one in 1 million," said Paul Santamaria, the acting executive director of VicRoads' Registration and Licensing division.

"We encourage customers to set up a myVicRoads account as the most secure way to manage their interactions with VicRoads."

myVicRoads is a password-protected portal allowing customers to complete a range of transactions, including change of address. Once an account is created, the customer is sent a follow-up letter to confirm the accuracy of their details.

The agency currently has 315,000 registered myVicRoads account holders, and said it plans to decommission the change-of-address service from the website as more myVicRoads accounts are created.

However there's no indication on the change-of-address form that a myVicRoads account would be more secure, only that it provided the option of short-term vehicle registration.

"We understand the issues associated with identity theft and we encourage customers to contact police if they believe they are the victim of identity theft ... Licence theft and fraudulent activity is [sic] dealt with as a Victoria Police matter."

Fulton did file a report with Victoria Police, but there was little they could do.

"I get the feeling they deal with it semi-regularly since the constable I spoke to said, paraphrasing, 'We really can't just rock up to the address and ask if they know anything because they'll just deny it', which I completely understand."

Victoria Police was unable to provide any statistics on licence theft. A spokesperson told ZDNet that "isn't a box to tick" in their crime reports.

Victoria's recently-established Crime Statistics Agency (CSA), an independent body along the lines of the highly-respected NSW Bureau of Crime Statistics and Research, was also unable to provide any numbers, as their statistics derive from Victoria Police reporting.

"We don't really have much coming up in the detailed offence codes that isolates fraud and deception offences relating to driver's licences, and if any cases have been recorded by Victoria Police, it is probably hiding in the more generic categories," said the CSA's chief statistician, Fiona Dowsley.

The morning after ZDNet contacted VicRoads, they called Fulton to apologise, reassure him they're looking into it, and confirm that they're issuing him with a new licence number.

"They can't comment about the vulnerability specifically, but they are aware of it from the language they used," Fulton said. But he's still far from happy.

"What makes this worse for me is that I understand the difficulty that all parties have in this matter ... I'm exhausted, worried about my future, pissed off, and wondering how many other people are in the same situation here -- some of whom surely do not know."

PREVIOUS VICTORIAN COVERAGE

Victoria's DHHS digital transformation held back by executives, not ministers (/article/victorias-dhhs-digital-transformation-held-back-by-executives-not-ministers/)

A 'risk averse' leadership culture is preventing the Victorian Department of Health and Human Services form embracing digital transformation, despite the state's ministers demanding change.

Victoria abandons federal mobile blackspots program to go it alone (/article/victoria-abandons-federal-mobile-blackspots-program-to-go-it-alone/)

The state's Minister for Innovation and the Digital Economy said the Commonwealth's blackspot program chooses tower locations based on political interests rather than merit.

Apple to open 'toasted' flagship store in Melbourne's Federation Square (/video/apple-to-open-toasted-flagship-store-in-melbournes-federation-square/)

A proposal for a flagship Apple store in Melbourne has quickly drawn criticism from the public.

Melbourne startup makes STEM more engaging for kids with 'science cookies' (https://www.techrepublic.com/article/melbourne-startup-makes-stem-more-engaging-for-kids-with-science-cookies/) (TechRepublic)

The Project Counter is using interactive gingerbread cookies in an effort to inspire young Australians to take an interest in STEM subjects.

Sleepbus using data to help homeless Australians get back on their feet (https://www.techrepublic.com/article/sleepbus-using-data-to-help-homeless-australians-get-back-on-their-feet/) (TechRepublic)

Sleepbus' founder and CEO has embarked on a project to help Australia's 105,237 homeless people, whilst leveraging data to change the model of a charity to one that also engages the donor.

RELATED TOPICS: SECURITY TV | DATA MANAGEMENT | CXO | DATA CENTERS

LOG IN TO COMMENT | Community Guidelines

Join Discussion

ADD YOUR COMMENT