Your PGP Key? Make Sure It's Up to Date

coindesk William Foxley
Coindesk 24 January 2020

Identity thieves now have another tool at their disposal: bitcoin hashing power.

That's the conclusion from a new cryptanalysis paper published earlier this month on SHA-1 (pronounced "shaw"), a once-popular hash function created by the National Security Agency and disapproved in the mid-2000s after failing against theoretical hack attacks.

SHA-1 continues to see use in certain circles, such as on source code program Git and other legacy products for sending secure transmissions on computers, according to Gaetan Leurent of France's National Institute for Research in Digital Science and Technology and Thomas Peyrin of Singapore's Nanyang Technological University, authors of the paper.

Related: Bitcoin's Share of PoW Mining Rewards Now Above 80%

Despite notices in 2006 and 2015 from the National Institute of Standards and Technology (NIST) for federal agencies to stop using the hash function, and other studies warning of SHA-1's flaws, academics are still warning firms to switch hash functions.

"SHA-1 signatures now offers virtually no security in practice," the paper notes.

By renting spare hash power from bitcoin miners – made feasible during bear market lulls – Leurent and Peyrin were able to conduct an impersonation attack by forging a fake key assigned to another's identity.

Hash functions, a one-way cryptographic scrambler comprising the basic security of cryptocurrencies, can also be used for verifying individual identities.

Related: This Metric Suggests Bitcoin Has Bottomed Out

In PGP keys, the intended message (called plain text) is compressed and scrambled through a one-time only "session key." Paired with a public key, users can safely transmit information to someone else. To decrypt the message, recipients match their private key with the session key to recover the plain text.

According to the paper, PGP keys – often used to self-verify users – can be broken with $50,000 worth of rented hash power, a small sacrifice for government agencies, not to mention black hat hackers.

How? Through collision attacks wherein different inputs result in the same random hash. When this occurs, two parties have access to the same key.

"It's so cheap because the GPU computation is nowadays very cheap," Peyrin said in a phone interview. "That's going to go down more in the coming years. Our attack is costing maybe $45,000 now but in, let's say, five to 10 years, it's going to cost like less than $10,000."

While many users have moved on from SHA-1, Leurent and Peyrin noted two popular mainstream self-verification tools, Pretty Good Privacy (PGP) and GnuPG, are at risk of impersonation attacks through hash function collisions for certain legacy applications. The latter is now rejecting SHA-1 based signatures based on the research, the academic said.

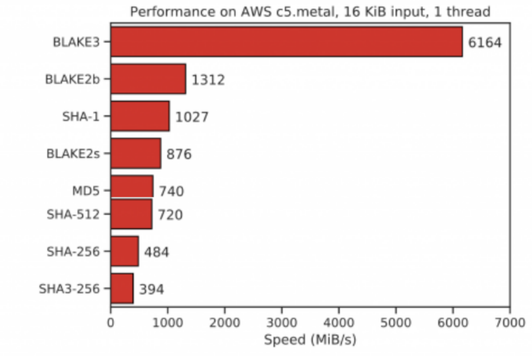
"We don't have the numbers about how many actually Yukis (a popular self-verification device) are using the old versions," Peyrin said. "A lot of people are used to using SHA-1 unfortunately and one of the reasons is because of legacy purposes. It costs a lot of money simply to move away."

A day in the life of a hash function

The same week the vulnerability in SHA-1 was exposed, a new one emerged: BLAKE3. Four cryptanalysts, including zcash creator and cypherpunk Zooko Wilcox, presented BLAKE3 as another alternative to the many hash functions available today for commercial use.

Wilcox told CoinDesk the use of Merkle trees was a motivation for developing a new standard along with his colleagues. First patented in 1979 by Ralph Merkle, Merkle trees – used in cryptocurrencies – efficiently store verified data and allow machines to conduct the same computations simultaneously in what is called "parallelism." As the BLAKE3 paper notes, the use of Merkle trees "supports an unbounded degree of parallelism."

Translation: it's a very fast hash function.



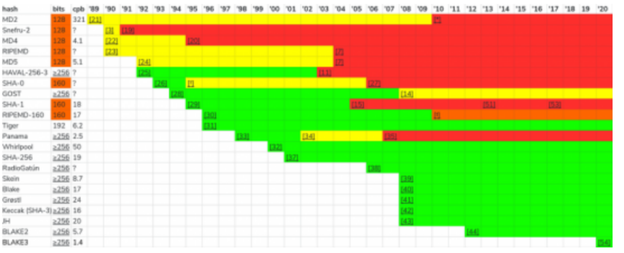
Mostly intended for verifying video streams, the hash function is based on the BLAKE family of functions such as BLAKE1 and BLAKE2.

SHA-1 has its own family members as well: SHA-2 and SHA-3. Unlike its BLAKE cousins, however, the SHA family was created out of the need to fix SHA-1 after a 2004 bombshell paper which broke multiple hash functions. In fact, bitcoin's hash function, SHA-256, is a member of the same family (created as an alternative to SHA-1).

Following the 2004 paper, SHA-2, created three years earlier, was expected to be broken as well as researchers assumed its older brother's failings would be genetic traits.

Still, most security experts at the time thought it was bust leading to a NIST competition for a replacement in 2007. Hence, SHA-3.

Years later, and SHA-2 is still rocking and rolling while its brother continues to take a pounding. The cost of launching an attack on applications utilizing SHA-1 continues to depreciate, starting in the millions of dollars worth of rented GPU equipment to only thousands under Leurent and Peyrin's research.



So what about BLAKE3 and other hash functions such as crypto's SHA-256? While all hash functions go the way of SHA-1? Not quite, said BLAKE3 lead author Jack O'Connor.

"We learned quite a lot about how to build crypto in the 90s. What you might think of as a natural life and death cycle of hash function might be incorrect to assume. Look at SHA-1 and 'say okay, you know born and died, depending on how you count it 2015 or 2005, like a 12 to 15 year life cycle,'" O'Connor said.

"That's probably not the best way to understand how hash functions work because we were learning a lot in the 90s and we are not repeating the mistakes that were made with SHA-1," O'Connor said.

You can paint a landscape a thousand ways, however. It's unfair to extrapolate from SHA-1's demise to other functions as it depends on how future technology counters more secure and powerful hash functions rolling out today such as BLAKE3.

"One story that people tell is 'all secure hash functions eventually fail — they have a finite lifespan.' Another story is 'in the early 2000's, cryptographers learned how to make secure hash functions — before that, they all failed, after that, none of them did,'" Wilcox said.

"It's important to realize that both of these stories are compatible with the data, so anybody who tells you that they know which one is the true story is drawing conclusions beyond the data," he concluded.

UPDATE: (27 January, 15:45 UTC): The Lifetimes of popular hash functions image has been changed to a more up to date image.

Related Stories

- A Russian Nuclear Plant Is Renting Space to Energy-Hungry Bitcoin Miners
- Lawsuit Shows How a Public Firm's $80M Bet on Bitcoin Miners Went Terribly Wrong