PRESS RELEASE

From: Centrum Wiskunde & Informatica (CWI) in the Netherlands, Inria in France and Nanyang Technological University in Singapore (NTU Singapore)

Thursday 8 October 2015

RESEARCHERS URGE: INDUSTRY STANDARD SHA-1 SHOULD BE RETRACTED SOONER

An international team of cryptanalysts urges the industry today that SHA-1 internet security standard should be retracted sooner, since the cost of breaking it is significantly lower than previously thought. This industry standard is used for digital signatures, which secure credit card transactions, electronic banking and software distribution. Currently, Internet browsers will mark SHA-1 signatures as insecure in favour of its secure successor SHA-2 only by January 2017. Marc STEVENS (CWI, the Netherlands), Pierre KARPMAN (Inria, France and NTU Singapore) and Thomas PEYRIN (NTU Singapore) now estimate that fake digital signatures plausibly can be made much sooner than that. STEVENS says: “We just successfully broke the full inner layer of SHA-1. We now think that the state-of-the-art attack on full SHA-1 as described in 2013 may cost around 100,000 dollar renting graphics cards in the cloud. ”

Graphics cards

On 22 September, the joint effort by STEVENS, KARPMAN and PEYRIN led to a successful so-called freestart collision attack on the industry standard SHA-1. This is a cryptographic algorithm designed by the NSA in 1995 to securely compute message fingerprints. These fingerprints are used in the computation of digital signatures, which are fundamental to Internet security, such as for HTTPS (SSL) security, electronic banking, signing documents and software. Collisions – different messages with the same message fingerprint – can lead to forgeries of digital signatures. A freestart collision breaks the inner layer of SHA-1. “We just showed how graphics cards can be used very efficiently for these kinds of attacks. Now we can use this to also make the state-of-the-art collision attack for SHA-1 significantly more cost efficient,” explains Karpman.

International policy

The research team says: “In 2012, security expert Bruce SCHNEIER estimated the SHA-1 attack costs to be around 700,000 dollar in 2015. This would decrease by 2018 to about 173,000 dollar, which he deemed to be within the resources of criminals. However, we showed that graphics cards are much faster for these attacks and we now estimate that a full SHA-1 collision will cost between 75,000 and 120,000 dollar renting Amazon EC2 cloud over a few months today, in early autumn 2015. This implies that collisions are already within the resources of criminal syndicates, almost two years earlier than previously expected, and one year before SHA-1 will be marked as unsafe in modern Internet browsers. Therefore we recommend that SHA-1 based signatures should be marked as unsafe much sooner than current international policy prescribes. In particular, we strongly urge against a recent proposal to extend issuance of SHA-1 certificates with another year in the CA/Browser Forum, for which the discussion closes tomorrow, on 9 October.”

Sinking ship

“Although this is not yet a full attack, the current attack is not the usual minor dent in a security algorithm, making it more vulnerable in the far future,” adds Ronald CRAMER, head of CWI’s Cryptology group. “Compare SHA-1 to a ship that hit an iceberg and is making water fast. We know how large the hole is, how fast the water will enter and when it will sink: soon. It’s time to jump ship to SHA-2.” Thomas PEYRIN, head of SYmmetric and Lightweight cryptography Lab (SYLLAB) at NTU, explains: “SHA-1 was already broken theoretically, but now a very practical cost efficient implementation is in sight. SHA-1’s successors SHA-2 and SHA-3 are unaffected by these recent cryptanalytic advances and remain secure.” Daniel AUGOT, head of team Grace at Inria Saclay - Ile-de-France, the group to which Pierre KARPMAN is affiliated, says: “The impact of actual future SHA-1 collisions might not be as severe as was the case with the HTTPS break in 2008 and the Flame malware in 2012. However, collisions herald the end of trust in SHA-1 based digital signatures.” Huaxiong WANG, head of NTU’s Division of Mathematical Sciences, says: “Certification Authorities (CA’s), browser vendors, and the industry in general are recommended to speed up the migration to SHA-2. Regrettably, even a single insecure CA threatens the security of all HTTPS websites worldwide, as clearly shown by the 2008 HTTPS break. Nevertheless, websites are also advised to migrate to SHA-2 soon, to avoid warnings for visitors when Internet browsers stop trusting SHA-1." STEVENS: "We hope the industry has learned from the events with SHA-1's predecessor MD5 and in this case will retract SHA-1 before examples of signature forgeries appear in the near future."

The group described their recommendations in a technical report, which is available online: https://sites.google.com/site/itstheshappening/. This research was partially funded by the Netherlands Organization for Scientific Research Veni Grant 2014 for Marc STEVENS, the Direction Générale de l'Armement for Pierre KARPMAN, and by the Singapore National Research Foundation Fellowships 2012 for both Pierre KARPMAN and Thomas PEYRIN.

About CWI

Founded in 1946, Centrum Wiskunde & Informatica (CWI) is the national research institute for mathematics and computer science in the Netherlands. It is located at Amsterdam Science Park and is part of the Netherlands Organisation for Scientific Research (NWO). The institute is internationally focused and renowned. Over 150 researchers conduct pioneering research and share their acquired knowledge with society. Over 30 researchers are also employed as professors at universities. The institute has generated twenty-two spin-off companies. More information: http://www.cwi.nl.

About Inria

Inria, the French National Institute for computer science and applied mathematics, promotes "scientific excellence for technology transfer and society". Graduates from the world's top universities, Inria's 2,700 employees rise to the challenges of digital sciences. With its open, agile model, Inria is able to explore original approaches with its partners in industry and academia and provide an efficient response to the multidisciplinary and application challenges of the digital transformation. Inria is the source of many innovations that add value and create jobs. More information: http://www.inria.fr.

About Nanyang Technological University, Singapore (NTU Singapore)

A research-intensive public university, Nanyang Technological University, Singapore (NTU Singapore) has 33,500 undergraduate and postgraduate students in the colleges of Engineering, Business, Science, Humanities, Arts, & Social Sciences, and its Interdisciplinary Graduate School. It has a new medical school, the Lee Kong Chian School of Medicine, set up jointly with Imperial College London. NTU is also home to world-class autonomous institutes – the National Institute of Education, S. Rajaratnam School of International Studies, Earth Observatory of Singapore, and Singapore Centre on Environmental Life Sciences Engineering – and various leading research centres such as the Nanyang Environment & Water Research Institute (NEWRI), Energy Research Institute @ NTU (ERI@N) and the Institute on Asian Consumer Insight (ACI). A fast-growing university with an international outlook, NTU is putting its global stamp on Five Peaks of Excellence: Sustainable Earth, Future Healthcare, New Media, New Silk Road, and Innovation Asia. The University's main campus has been named one of the Top 15 Most Beautiful in the World. NTU also has a campus in Novena, Singapore's medical district. For more information, visit www.ntu.edu.sg

----

Notes for the press, not for publication:

Scientific announcement / technical report: see https://sites.google.com/site/itstheshappening/ (including the link to the CA / Browser Forum meeting on 9 October 2015).

Contact information:

- Dr.ir. Marc Stevens: stevens@cwi.nl
- Pierre Karpman MSc: pierre.karpman@inria.fr
- Asst. Professor Thomas Peyrin: thomas.peyrin@ntu.edu.sg

- Covered by: Annette Kik, Annette.Kik@cwi.nl, phone +31 (0)6-51574891 (Mon, Wed, Thu, Fri-afternoon), or 0031 20-5924181 (Peter Hildering). Centrum Wiskunde & Informatica, Science Park 123, 1098 XG Amsterdam, the Netherlands, http://www.cwi.nl.