New Collision Attack Lowers Cost of Breaking SHA1

By Eduard Kovacs on October 08, 2015

A team of researchers has demonstrated that the cost of breaking the SHA1 cryptographic hash function is lower than previously estimated, which is why they believe the industry should accelerate migration to more secure standards.

The SHA1 algorithm, designed in 1995 by the NSA, has become an important Internet security standard as the cryptographic fingerprints it generates are used to compute the digital signatures in HTTPS connections. SHA1 is also commonly used these days for signing software and documents.

One of the main threats against SHA1 are collision attacks. Under normal circumstances, hashing different messages should result in unique hashes, but collisions can lead to the same hash value being produced for different messages, which can be exploited to forge digital signatures.

Researchers started finding weaknesses in SHA1 in 2005 and in 2012 cryptography experts estimated that a practical collision attack against the algorithm would cost roughly $700,000 by 2015. The same experts estimated that the cost would drop to approximately $173,000 by 2018, which, they argued, would be well acceptable for an organized crime syndicate.

However, a team of international experts from the Centrum Wiskunde & Informatica in the Netherlands, Inria in France, and the Nanyang Technological University in Singapore have showed that the costs can be significantly reduced by using graphics cards.

In a type of attack they call a "freestart collision," researchers managed to break the full inner layer of SHA1. Using this method, experts estimate that the cost of an SHA1 collision attack is currently between $75,000 and $120,000 using computing power from Amazon's EC2 cloud over a period of a few months.

Furthermore, the experts have warned that large corporations and governments may possess even greater resources than those provided by Amazon. Researchers said they managed to perform an attack in 10 days by conducting computations on a 64-GPU cluster.

The world renowned cryptography expert Bruce Schneier and others have been urging the industry to migrate to the much more secure SHA2 or SHA3 for years. In 2012, the National Institute of Standards and Technology (NIST) recommended that SHA1 certificates should not be trusted starting with 2014, but SHA1 is still widely present even today.

Microsoft was among the first to take action. In November 2013, the company announced its intention to deprecate the use of the SHA1 algorithm in code signing and SSL certificates in favor of SHA2. Google and Mozilla announced in September 2014 that Chrome and Firefox would stop accepting SHA1-based certificates after January 1, 2017.

Service providers argue that the migration must be conducted gradually to avoid a negative impact. However, the researchers behind the freestart collision attack believe the industry should speed up migration to SHA2 and kill off SHA1 as soon as possible.

“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,” said Ronald Cramer, head of the cryptology group at Centrum Wiskunde & Informatica. “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.”

Previous Columns by Eduard Kovacs:

New Collision Attack Lowers Cost of Breaking SHA1
Iranian Attackers Use Fake LinkedIn Profiles to Target Victims
Developers of Mysterious Wifatch Malware Come Forward
Malicious Android Adware Infects Devices in 20 Countries
Amazon Launches Web Application Firewall for AWS

Tags:
NEWS & INDUSTRY Vulnerabilities

Subscribe to SecurityWeek

Enter Your Email Address Subscribe

Most Recent Most Read

- New Collision Attack Lowers Cost of Breaking SHA1
- Iranian Attackers Use Fake LinkedIn Profiles to Target Victims
- Developers of Mysterious Wifatch Malware Come Forward
- Changes in Control System Standards Ease Procurement: IEC 62443-2-4 Updates
- Malicious Android Adware Infects Devices in 20 Countries
- Microsoft Leaks User Account Identifiers in Clear Text
- Amazon Launches Web Application Firewall for AWS
- Long-Term Strategy Needed When Analyzing APTs: Researcher
- Cisco Disrupts Major Ransomware Operation Powered by Angler EK
- Winnti Spies Use Bootkit for Persistence, Distributing Backdoors

Popular Topics

Information Security News
IT Security News
Risk Management
Cybercrime
Cloud Security
Application Security
Smart Device Security

Security Community

- IT Security Newsletters
- IT Security White Papers
- Suits and Spooks
- ICS Cyber Security Conference
- CISO Forum
- InfosecIsland.Com

Stay Intouch

- Twitter
- Facebook
- LinkedIn Group
- Cyber Weapon Discussion Group
- RSS Feed
- Submit Tip
- Security Intelligence Group

About SecurityWeek

- Team
- Advertising
- Events
- Writing Opportunities
- Feedback
- Contact Us