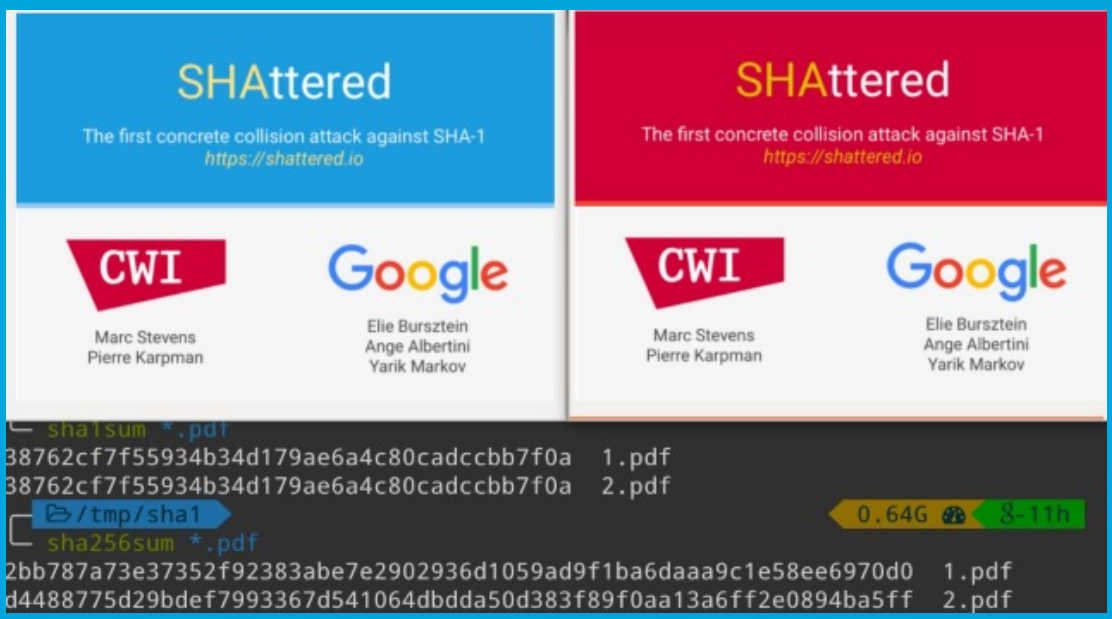
kindred

Security Newsletter

24 February 2017

Security researchers just "shattered" SHA-1 hashing algorithm



This industry cryptographic hash function standard is used for digital signatures and file integrity verification, and protects a wide spectrum of digital assets, including credit card transactions, electronic documents, Git commits, and software updates.

For example, by crafting the two colliding PDF files as two rental agreements with different rent, it is possible to trick someone to create a valid signature for a high-rent contract by having him or her sign a low-rent contract.

Researchers hope their practical attack on SHA-1 will increase awareness and convince the industry to quickly move to safer alteratives, such as SHA-256.

Read More

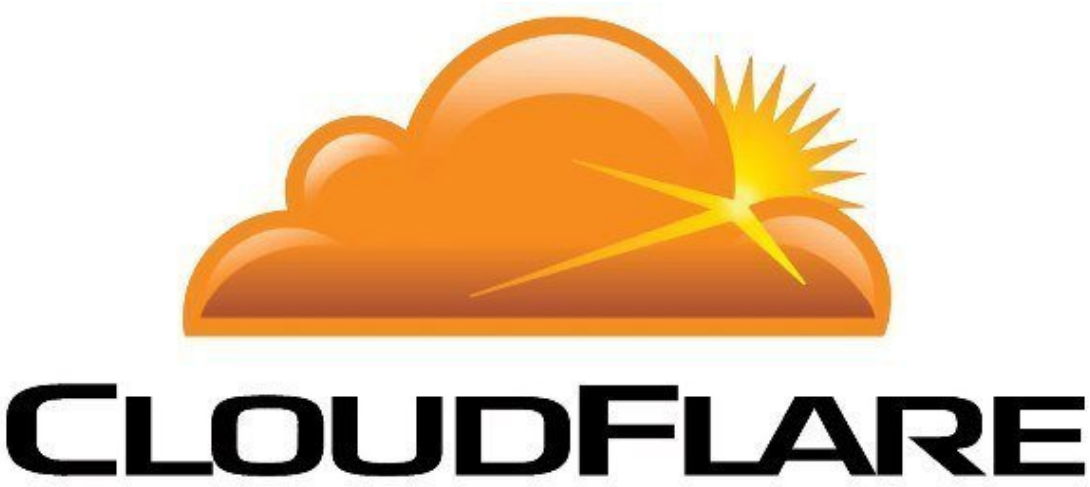
PHP Becomes First Programming Language to Add Modern Cryptography Library in Its Core

The PHP team has unanimously voted to integrate the Libsodium library in the PHP core, and by doing so, becoming the first programming language to support a modern cryptography library by default.

The proposal to embed Libsodium (also known as Sodium) into the PHP standard library came from Scott Arciszewski, Chief Development Officer at Paragon Initiative Enterprises, a man that has campaigned for stronger cryptography in PHP CMSes in the past.

Read More

Cloudflare server errors blamed for leaked customer data



While working on something completely unrelated, Google security researcher, Tavis Ormandy, recently discovered that Cloudflare was leaking a wide range of sensitive information, which could have included everything from cookies and tokens, to credentials.

Cloudflare moved quickly to fix things, but their postmortem downplays the risk to customers, Ormandy said. The problem on Cloudflare's side, which impacted big brands like Uber, Fitbit, 1Password, and OKCupid, was a memory leak. The flaw resulted in the exposure of "HTTP cookies, authentication tokens, HTTP POST bodies, and other sensitive data," Cloudflare said.

Read More

s2n, Amazon's open-sourced TLS implementation, is now handling 100% of SSL traffic for Amazon S3

In June 2015, Amazon introduced s2n, an open-source implementation of the TLS encryption protocol, making the source code publicly available under the terms of the Apache Software License 2.0 from the s2n GitHub repository. One of the key benefits to s2n is far less code surface, with approximately 6,000 lines of code (compared to OpenSSL's approximately 500,000 lines).

Today, we've achieved another important milestone for securing customer data: we have replaced OpenSSL with s2n for all internal and external SSL traffic in Amazon Simple Storage Service (Amazon S3) commercial regions.

Read More

The new "SameSite" cookie headers enables new way to fight against CSRF (Cross-Site Request Forgery)

Cross-Site Request Forgery, also known as CSRF or XSRF, has been around basically forever. It stems from the simple capability that a site has to issue a request to another site.

Essentially, Same-Site Cookies completely and effectively neutralise CSRF attacks.Enabling this attribute on the cookie will instruct the browser to afford this cookie certain protections. There are two modes that you can enable this protection in, Strict or Lax. Strict forbids the browser to attach cookie for any cross-site request, while lax allows it for "safe" requests such as GET.

Read More

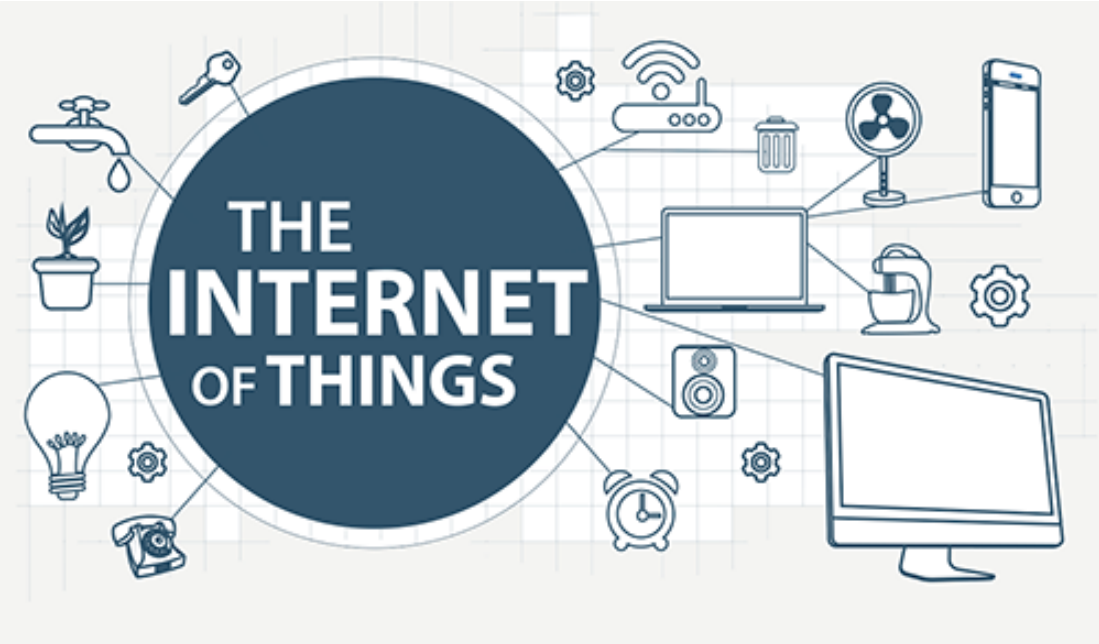
Data Selfie reveals how Facebook's AI tracks and studies your activity

Have you ever wondered how Facebook collects all the data it has to feed you with the content it presumes you'll like and keep you coming back for more? Well, now there's an app that can answer these questions.

Available for free, Data Selfie is an open-source Chrome extension that helps you discover how machine learning algorithms track and process your Facebook activity, and gain insights about your personality and habits. To prevent ill-intended individuals from obtaining the information it collects about you, Data Selfie keeps your data locally – only on your own machine – and never stores anything on external servers.

Read More

How Cyber attacks work



Cyber attacks are malicious Internet operations launched mostly by criminal organizations looking to steal money, financial data, intellectual property or simply disrupt the operations of a certain company.

In this article, the author explores the types of attacks used by cybercriminals to drive up such a huge figure, and also helps you understand how they work and affect you.

Read More

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.