NOVEMBER 5, 2019

Legaltech news

ONLINE

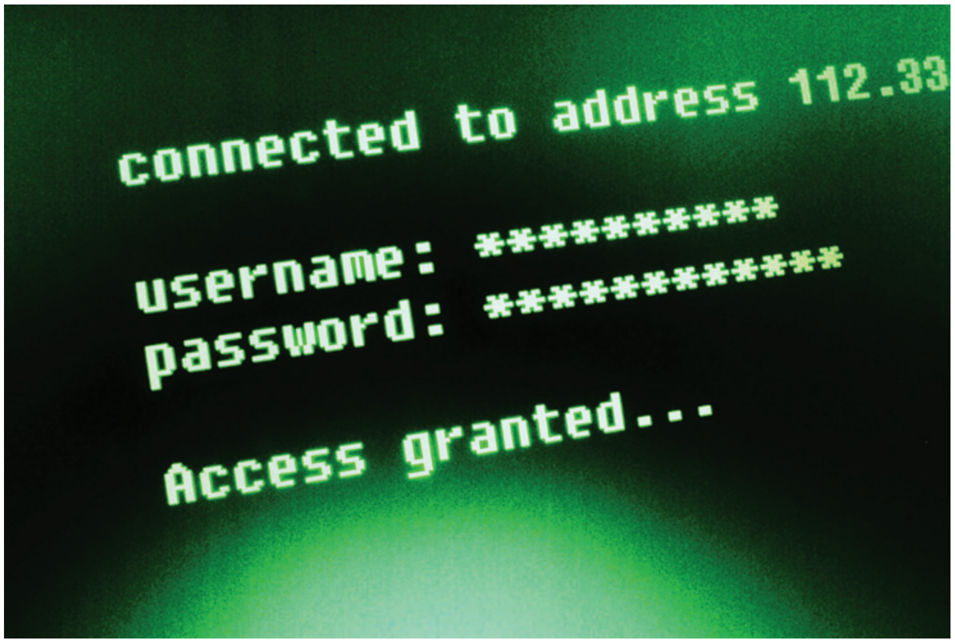
An ALM Publication

Nervous System: Passwords Became More Secure By Adding a Pinch of Salt

Forty years ago this month, Robert Morris and Ken Thompson published an article in Communications of the Association for Computing Machinery and created something that computer users still benefit from almost every day.

BY DAVID KALAT, BRG

With the aggressive pace of technological change and the onslaught of news regarding data breaches, cyber-attacks, and technological threats to privacy and security, it is easy to assume these are fundamentally new threats. The pace of technological change is slower than it feels, and many seemingly new categories of threats have actually been with us longer than we remember. ***Nervous System*** *is a monthly blog that approaches issues of data privacy and cybersecurity from the context of history—to look to the past for clues about how to interpret the present and prepare for the future.*



Credit: Michael H Jones/Shutterstock.com

Forty years ago this month, Robert Morris and Ken Thompson published an article in the monthly journal *Communications of the Association for Computing Machinery*. With those four pages, they created something that computer users still benefit from almost every day.

Passwords have long been a fundamental insecurity at the front door of any computer system. The use of passwords for account management and security dated back to the earliest days of time-sharing computer systems in the early 1960s. One lesson had been taught over and over: Storing all passwords in a single file is a recipe for disaster. That file can be too easily stolen, accidentally deleted or mistakenly broadcast. Data scientists had engineered an attempted solution, but Morris and Thompson discovered serious flaws with that approach.

Although the clever innovation they pioneered worked for, and would be implemented on, all manner of computer systems, the UNIX time-sharing system at Bell Laboratories particularly occupied Thompson and Morris' attention. Thompson had helped invent UNIX, and Morris was the network administrator maintaining it. Every day, Bell Labs' many researchers, inventors, and scientists logged into that system using passwords.

To protect the security of those passwords, Bell's UNIX system did not actually store them internally—at least not in a recognizable form. Instead of storing the passwords in a file vulnerable to being leaked or stolen, each password was *hashed* first. The term "hash" comes from cooking—the practice of transforming something by slicing and dicing it. A mathematical hash takes a chunk of electronic data—such as a password—and processes it through a complex algorithm to reduce it into an encrypted slug of data. This transformation is strictly one-way. There is no way to "un-hash" that encrypted slug back into the original password, any more than a cook can turn hash browns back into a raw potato.

Hashes have many useful functions in computer science, but in terms of password security the value proposition presents a way to store passwords in a form supposedly impervious to attack. When a user attempts to log-on and enters their password into the system, the interface hashes that input and compares it against the stored list of password hashes. If the two hashes match, the user is authenticated into the system. If that list of password hashes were ever to be leaked or stolen, no one could reverse them back into the users' passwords.

At least, that was the idea.

The problem was not the hashing algorithm, which was an impervious piece of encryption technology. To quote Bruce Schneier's book *Applied Cryptography*, no one could hope to reverse a hash until "computers are built from something other than matter and occupy something other than space."

Instead, the problem was human nature. In his work as a network administrator, Morris had discovered fatal flaws in how users choose their passwords—routine human habits that make for catastrophic security lapses.

For one thing, users had a tendency to gravitate toward real English words. Although easy to remember, such passwords opened up an opportunity for an attack. Whereas reversing a hash was inconceivable, running the algorithm to hash a new input was trivial. A foresighted attacker could, for example, grab an electronic dictionary and hash every word in it. If any hash matched one of the hashes in a stolen password list, the attacker would have cracked that password easily, without ever having to even attempt to reverse a hash.

Further, most users chose the same password. A small selection of possible passwords ("password," "qwerty," "1234") accounted for the vast majority of the passwords in use at any given time. Consequently, these duplicate passwords shared duplicate hashes. An attacker would not even have to bother hashing a dictionary to guess that numerous instances of the same hashed password were likely instances of the most commonly used passwords.

Fixing human behavior is hard, so Morris and Thompson opted to fix the technology. In a process that would become known as "salting a hash," they mixed random data into the systems that process user passwords. Now, a hundred users who used the same password would correspond to a hundred *different* hashes, each distinguished by a unique piece of random "salt." An attacker who pre-hashed a dictionary would find it useless, because each word would transform into a different hash depending on what salt was applied.

It was a simple solution, applied almost invisibly at the back-end of the system, that substantially improved the security of the overall system without solving the user error that led to it. After a remarkable career as a researcher at Bell Labs, in 1986 Morris began serving as the lead scientist at the National Security Agency's National Computer Center, where he pioneered standards for cybersecurity. Thompson continued to innovate new technologies, and since 2006 has worked at Google. Their system of "salted hashes" remains in use today, forty years after it was first published, and continues to be recognized as the gold standard of password security systems.

David Kalat is Director, Global Investigations + Strategic Intelligence at Berkeley Research Group. David is a computer forensic investigator and e-discovery project manager. Disclaimer for commentary: The views and opinions expressed in this article are those of the author and do not necessarily reflect the opinions, position, or policy of Berkeley Research Group, LLC or its other employees and affiliates.