Hash Chaining: A Theoretical Model Using Salted Hashes to Generate Ethereal Keys

Berkley, Samuel (School: The Governor French Academy)

As technology becomes more widespread, the possibilities hackers have to access our data grows exponentially. People's personal information is put at risk most often by frail security protocols or predictable encryption keys. Given the increasing number and severity of cyber-attacks, it is more important than ever to safely and securely encrypt private data. This project proposes a technique incorporating existing, secure methods of encryption in an innovative way to generate secure encryption keys, called “Hash Chaining”. Unless a user's encryption key is secure, their information is at risk for being attacked by hackers. Hash Chaining generates secure encryption keys by utilizing the unique, secure output of hashes as a form of key generation. This generated key is secure because it is obscured by multiple hashes and determined by a series of completely random secret values shared securely between the two communicating entities. Through a process I call “modulation”, a new encryption key can be generated comprised of secret values used to create the previous encryption key. In this way, two communicating entities only need a single instance of communication between them in order to agree upon secret values, after which they will be able to generate secure encryption keys on their own. Surface-level investigation and probabilistic analysis suggests that Hash Chaining is a secure method for data encryption, verified by an industry expert in cyber security.

Awards Won: