(Approx. 1036 words)

Internet Security – Once over easy, with Hash

By Phil Sorrentino, Secretary, and APCUG Rep

Sun City Center Computer Club, FL

<https://www.scccomputerclub.org/>

philsorr \*\* yahoo.com

The Internet is essential to so many things we do, like shopping, investing, and banking, that you may have wondered how secure the Internet is. And additionally, how secure is my private information during an Internet transaction? And now that we're thinking about it, how is the Internet made secure? If knowing a little about how the Internet is kept secure is interesting, read on; if not, jump to the next article.

The Internet provides essential communications between tens of millions of people and has become an essential tool for commerce; therefore, security has become a tremendously important issue. Internet security has many facets, ranging from keeping communications private to protecting passwords and guaranteeing secure commerce transactions and payments.

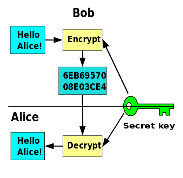
Computers are an integral part of the Internet, and when it comes to computers, security is a concern on many different levels. There is physical security that keeps your computer hardware from being stolen. There is software security that keeps people out of our private files. There is "malware" security that keeps your computer software from being infected with viruses, spyware, worms, and the like. And finally, there is "network" security that keeps private data protected as it goes from one computer (or client) to another computer (or server) on the Internet. These security concerns are important, but the subject here is network security. Network Security is implemented by applying cryptography to messages sent on the Internet.



Remember the "s" in "https://" and the little lock icon on the browser when you go to a "secure" website? Well, cryptography is behind all that security. Cryptography is used to secure telephone, Internet, and email communications (as well as to protect software and other digital property). Cryptography is nearly as old as written language itself. It was invented to address the age-old question: How can I communicate with my friend so that no one else listening will know what was shared? Cryptography becomes necessary when communicating private information over a public or "un-trusted" medium, such as the Internet. Typically, you can be sure that the message you send over the Internet will get to the destination you expect, but you cannot guarantee that intermediaries (computers along the way) will not be able to see and/or read your message if it is not protected. With a collection of not-so-expensive equipment and a good deal of knowledge, a message on the Internet can be intercepted (sniffed), and if it is "plain text," it can be read. For mundane email messages, this is not much of a concern; for messages that contain private information, such as personal information such as bank account or social security numbers, this could be an invitation for Identity Theft.

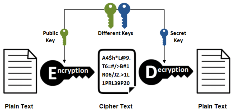
To get a bit technical here (here's the once over, with hash), we need to address the following four security concerns to guarantee messages are secure on the Internet. 1) *Privacy:* Ensuring that no one can read the message except the intended receiver. 2) *Integrity:* Assuring the receiving party that the received message has not been altered from the original. 3) *Authentication:* The process of proving one's identity. 4) *Non-repudiation:* A mechanism to prove that the expected sender sent this message.

There are, in general, three types of cryptographic schemes typically used to accomplish these goals: Secret-key cryptography, Public-key cryptography, and Hash functions, each of which can be researched in great detail by doing a Google search on the subject and settling in for some rigorous mathematics and explanations.



Secret-key Cryptography

However, here is a brief summary. Secret-key cryptography, sometimes called symmetric cryptography because the sender and receiver use the same key, is the more traditional form of cryptography where the (same) key is used to encrypt and decrypt a message.



Public-key cryptography

On the other hand, public-key cryptography uses algorithms to create two asymmetric keys, a public, and a private key. (Unlike secret-key cryptography, it does not require a secure initial exchange of secret keys to both sender and receiver.) The asymmetric keys are a mathematically related key pair: a secret private key and a published public key. These keys protect a message by creating an encrypted message using the public key, which can be decrypted only by using the private key, providing "privacy," the first security concern.

Hash functions are mathematical transformations used to irreversibly encrypt data, meaning that the Hash results cannot be reversed to recover the original message. Hash functions are well-suited for ensuring data "integrity," the second security concern, because any change made to the contents of a message will result in the receiver calculating a different hash value than the one sent by the sender. Since it is doubtful that two different messages will yield the same hash value, data *integrity* is ensured to a high degree of confidence.

"Authentication," the third security concern, is accomplished in nearly all modern computer systems using passwords that authenticate users attempting to access computer resources. For security reasons, passwords are not typically kept on a server in plaintext. Hash functions are commonly used to convert passwords to an irreversible data pattern. When you type in your password, a Hash function converts it to a data pattern and compares it to the data pattern previously stored for your password. Your password is never stored on your machine or your server's machine; only the hash function results are stored. There is no way of going backward from the Hash function data pattern to the password (remember, the Hash function is irreversible). So now you know how the passwords are protected and why when you forget a password, the server can't tell you what it was; they can only reset it to a new password.



Digital Signature

The fourth security concern, "non-repudiation, " ensures the message was sent from the expected sender. This is accomplished by a digital signature which ensures that the sender cannot deny the authenticity of its signature or later deny sending the message. A digital signature is created using the private key of an asymmetric key pair. The signature can be verified by the corresponding public key of the asymmetric key pair, thus proving that the document was "electronically signed" by the private key owner, thus guaranteeing the message's source. So with all of these four concerns met my take, it looks like the Internet is pretty secure.