COSC 4760
Networking

Name: Jacob Tuttle

Homework 12

November 18, 2019

1. Checksums provide only the most basic form of error checking. For instance, as we discussed in earlier homeworks, even with a two dimensional form of checksum checking, collisions are very simple to find even for a human. Since it is only summing different locations, multiple different pieces of data can produce the same checksum; however, a hash such as MD5 does more than simply operate on the given data. The padding and block processing for hashing means that there is a much, much lower chance of two pieces of data hashing to the same value than two pieces of data checksumming to the same value. This indicates that hashing gives better message integrity checks than a checksum.

2. Encrypting an entire message can be a costly endeavor. Since encryption utilizes math that requires very large prime numbers, it is costly both in terms of time and processing power. If a message is large, this time can be a considerable amount of time. This colleague is correct in this assessment: it may be cheaper to simply send a digital signature rather than a fully encrypted message if the information isn't of a truly sensitive nature. This could still provide a way to validate that the contents of the message were correctly received, but it wouldn't provide the security of information that is a major concern when discussing encryption.

3. No, you can't convert a hash back into the original message. By the definition of a hash, it is a one-way function making use of modulus operations in order to create a one-way form of encoding; however, it is theoretically possible to compute a message that hashes to the same value. In practice, this is virtually impossible, and so there is no effective way to convert a hashed value back to its original value.

4. The purpose of a nonce is to defend against the replay attack, an attack where a transmission is captured and then retransmitted at a later time. A nonce is a value that will only be used a single time by a transmitting host, so a receiver knows that if it receives the same nonce value again, the trasmission has been replayed.

5. Since a cipher block chaining method of encryption is, at the most basic level, a repeated XOR process, it can be implemented effectively in hardware. One of the most expensive parts of encryption is in the time and processing power required to encrypt data, and if encryption could be handled in the hardware, it could cut down on these required resources.

6. One of the biggest concerns with sharing a ”secret” comes in sharing it. It needs to be transmitted in a way that both end points of the transmission can know that a third party can't spoof a communication. Using a Diffie-Hellman key exchange. The Diffie-Hellman key exchange is the method by which private cryptographic charing

can occur on private channels. This will allow both parties in this example to compute a shared secret such that any further transmissions can encrypt a message authentication code to be included by the participants.

7. (a) When you send out a PGP message, before the message is sent out, it is ”signed” using your private key. This generates a PGP signature, which appears at the bottom of a message and can be used to verify the sender of the email. After exchanging PGP keys in some secure way, such as a Diffie-Hellman key exchange, you can use the signature and the keys to validate that the sender of a PGP message is who they claim to be.

   (b) Yes. The PGP signature is a form of a message authenitcation code. It provides authentication that the information being received is truly what was intended to be received.