Jishnu Murali Thampan - 762574
George Sebastian - 762610

Questions & Answers

1. What is a one-way function?
   Ans. Typically, a one-way function as the name indicates is something which is easy to compute but it is very difficult to perform its inverse functionality. For example having data (d) , it is easy or possible to calculate f(d) but extremely difficult to calculate (d) having known f(d). Cryptographic hashes rely on this property of one-way functions and they are a typical real-world example.

2. Define preimage resistance and the second preimage resistance characteristic of a one-way function.
   Ans. Preimage resistance is about the most basic property of a hash function which can be thought. The characteristic of a preimage resistance is that for a given h in the output space of the hash function, it is hard to find any message x with H(x)=h.
   Second Pre-image resistance is another related property of a hash function. The characteristic of a second pre-image resistance is that for a given message x1 it is hard to find a second message $x2 \neq x1$ with H(x1)=H(x2).

3. What is collision and how does it affect the security of a hash function?
   Ans. A collision occurs when two or more input strings of a hash function produce the same hash result. Since hash functions can have infinite input length and a predefined output length, there is inevitably going to be the possibility of two different inputs that produce the same output hash.
   A typical Brute-Force attack where the attacker could try different input combinations to produce the same hash compromises the security of a hash function.

4. Does the Boolean XOR function represent a valid way to verify the integrity of a message. Justify your answer.
   No. In typical integrity verification techniques like checksum calculation, XOR is performed on words which are simply data broken down into fixed n number of bits. Receiver calculates the XOR on all of its words including checksum. The flaw in this technique is that we can only identify a 1-bit error using an XOR function. Error which affects 2 bits, swapping of 2 or more words etc cannot be determined and hence is not reliable.

5. Why do collisions necessarily exist?
   Ans. Hash Collisions occur if we have more items to hash than we have slots. But if we have a poor hashing algorithm, then we'll see collisions even when the slots ratio is very small. A good hashing algorithm (including most of the ones we'll see in the wild) will attempt to spread the resulting hashes over the entire output space as evenly as possible, and thus minimize collisions.

6. Explain the birthday problem and state the relation to hash collisions
   Ans. The birthday problem observes that in a room of 23 people, the odds that at least two people share the birthday is 50%. The same logic that drives the matching birthdays also drives the probability that one can find collisions with a hash function. Real-world applications for the birthday problem include a cryptographic attack called the birthday attack, which uses this probabilistic model to reduce the complexity of finding a collision for a hash function.