**Name: Talha Abdullah Punjabi QUID: 201903446**

**Computer Security L01**

**BONUS RESEARCH**

1. **Attack on CBC-MAC**

The use of the same key for encryption and authentication is one of the most prevalent vulnerabilities exposed when employing the CBC-MAC approach. Although it is bad practice to reuse a key for several applications, these errors can lead to serious attacks. Another attack is MAC forging, in which an unauthorized person obtains a legitimate MAC on a message that was not produced by the secret key holders, senders, or receivers. To obtain forgeries, the attacker will likely require many genuine MACs and associated messages. The attacker uses a key recovery attack to retrieve the secret key required to generate one or more MACs. These are successful recovery attacks that allow for the creation of an unlimited number of forgeries.

A basic method of calculating an attack's effectiveness. The attacker accomplishes this using a four-tuple that indicates the size of the resources required by the attacker. The attacker specifies the tuple [a, b, c, d] for each attack, where a determines the number of off-line block cipher decipherments, b determines the number of known data string/MAC pairs, c determines the number of chosen data string/MAC pairs, and d determines the number of on-line MAC verifications. The rationale for the distinction between the integers c and d is that in some situations, obtaining MAC verifications may be easier than obtaining the true MAC value for a given message.

1. **Attack on HMAC**

One of the attacks are Related-key attacks. It was proposed at Asiacrypt 2012 [14], a new type of generic distinguishing (distinguishing H) and forgery attacks for HMAC was proposed. These attacks are in the related-key model and can apply even to wide pipe proposals, but they only work for HMAC, and only when a special restrictive criterion is verified: the attacker must be able to force a specific difference between the inner and the outer keys (with the predefined values of opad and ipad in HMAC, this criterion is verified when k = b). The idea is to compare the cycle length when iterating the HMAC construction on small messages with a key K, and the cycle length when iterating with a key K0 = K ⊕opad ⊕ ipad.

Another attack is on instantiations with concrete hash functions because of its widespread use in many security applications, HMAC has also been scrutinized when instantiated with a concrete hash function, exploiting weaknesses of some existing hash function. In parallel to the recent impressive advances on hash function cryptanalysis, the community analyzed the possible impact on the security of HMAC when instantiated with standards such as MD4-19, SHA-1-22, or MD5-20. Key-recovery attacks have been found on HMAC-MD4-9,24 and HMAC-HAVAL-27.

The complexity of generic attacks, which work even with good hash functions, must be considered to put these attacks into perspective.

**References:**

1. Bellare, M.: New Proofs for NMAC and HMAC: Security without CollisionResistance. In Dwork, C., ed.: CRYPTO. Volume 4117 of Lecture Notes in Computer Science., Springer (2006) 602–619
2. Wikipedia contributors. (2022, February 10). HMAC. In *Wikipedia, The Free Encyclopedia*. Retrieved 07:58, March 7, 2022, from <https://en.wikipedia.org/w/index.php?title=HMAC&oldid=1071016735>
3. ISO/IEC 9797-1. Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher. International Organization for Standardization, Gen`eve, Switzerland, 1999.
4. Wikipedia contributors. (2020, September 28). CBC-MAC. In *Wikipedia, The Free Encyclopedia*. Retrieved 07:59, March 7, 2022, from <https://en.wikipedia.org/w/index.php?title=CBC-MAC&oldid=980797008>