LNMIIT/B. Tech/CSE/CORE/2019-20/ODD/CSE329

The LNM Institute of Information Technology

Department of Computer Science & Engineering

Computer Security (CSE329)
Mid-term Examination

Time: 3 hours(11:00-12:30PM) Date:03/10/2019 Maximum Marks: 30

1. Suppose, a user applies the following MAC scheme for construction of a `Cryptographic check sum` or Tag.

Consider a block cipher

$$E : \{0,1\}^{32} \times \{0,1\}^{32} \rightarrow \{0,1\}^{32}$$

where $E_k(m) = E(k, m)$ denotes the encryption of the plaintext m under the key k. The Tag of a given message $m \in \{0,1\}^*$ is constructed as:
Let the message $m = m_1 \| m_2 \dots m_n$, where $m_1, m_2 \dots m_n$ are n blocks.
$\mathrm{MAC}_k(m) = c_1 \oplus c_2 \cdots c_n$, where $c_i = E_k(c_{i-1}) \oplus m_i$ for $i = 2 \dots n$ and $c_1 = E_k(IV) \oplus m_1$ being an initialization vector. Assume that all messages have a length multiple of 32 bits. Where $\|$ denotes concatenation operation and $\oplus$ is the XOR operation.

(a) Let the adversary is allowed to access the oracle that computes the MAC. Prove that the adversary can recover $E_k(IV)$ by submitting query on a message to the oracle. [3]

(b) Given a message m of n blocks and the code $h = \mathrm{MAC}_k(m)$, show that it is possible to generate a new message $\tilde{m}$ of n blocks and a $\tilde{h} \in \{0,1\}^{32}$ such that $\tilde{m} \neq m$ and $\mathrm{MAC}_k(\tilde{m}) = \tilde{h}$. [5]

2. Let $H_1 : \{0,1\}^* \rightarrow \{0,1\}^n$ and ~~$H_2 : \{0,1\}^* \rightarrow \{0,1$~~$\}^n$ are two collision resistant hash functions.
Let $G : \{0,1\}^* \rightarrow \{0,1\}^n$ be hash function constructed as $G(0^n 1 \| m) = H_1^n(m)$,
where $H_1^n(m) = H_1(H_1^{n-1}(\dots H_1(m))$. Prove that G is not collision resistant. [5]

3. Let the user is allowed to construct his alphanumeric password with special characters according the following policies. Also this uses **SHA-II** as the hash function. [5]
↳ |h| = 256 bit

- at least 7 characters and at most 9 characters long.
- compose of characters of lower case letter $(a \dots z)$, uppercase letter $(A \dots Z)$ and digits $(0 \dots 9)$
- special chatterers/symbols of size 32.

The adversary mounts **Dictionary Attack** and is allowed to access system password file. The dictionary maps every possible password to its hash values, so that the adversary simply can lookup that he wants to crack. Assume that every character stores in the dictionary requires one byte. What would be the require storage size for his dictionary. Note that the passwords are unsalted.

*** PTO ***

4. How does the Proactive Password checker approach based on Bloom filter can improve the password security? Show that the probability P of false positive is

$$P \simeq (1 - e^{\frac{-km}{n}})^k$$

where k is the number of independent hash functions, n is number of bits in the hash table, m is the number of words in dictionary. [5]

5. Consider the following protocol use to authenticate the user U to server S. But not not vice versa.

- $U \rightarrow S : ID_u$ i.e (U sends his identity ID_u to S)
- $S \rightarrow U : n_S$ i.e (S select a nonce n_S a number used once and sends to U).
- $U \rightarrow S$: $E_k(n_S)$ i.e (U sends the cipher of n_S to S), where k is the secret shared key and E is the symmetric key encryption algorithm.

(a) What kind of attack is applicable when the same n_S is reused ? Justify your answer in 1-2 lines. [2]

(b) Modify the given protocol to achieve mutual authentication between U and S. Hint: the user U chooses a nonce n_u. [5]

****END***