Assignment 5

Ahmed Samir Abdelfattah
8/20

① a) Sectigo ECC Domain Validation Secure Server CA, USERTrust ECC Certification Authority

b) Elliptic Curve Public Key, 2048

c) 1/19/38 1:59:59 AM GMT+2

d) TLS 1.3

e) • yes, you can visit a website the tells you what is your public IP address

• yes, they can monitor the DNS requests i guess, or view a packet and try see where and from where is it going.

② H: MD $\quad MAC(m) = H(K \| m)$ ↑ secret

write $K \| m$ as the seq. of Blocks, $B_1 \dots B_n$

$z_0 = IV$, $z_i = f(z_{i-1}, B_i)$, $H(K \| m) = z_n$ So the tag is $H(K \| m) = z_n$

the attacker after processing $H(k||m)$ will reveal the internal chaining state, he can take this state (the tag) and continue the hash on any extra blocks m_2, producing $H(k||m||\text{padding}||m_2)$. Without knowing k, they only need to guess the key length to compute correct padding.

3. this MAC is insecure cuz it leaks $F_k(m_1)$ directly as half of the tag, so attacker can easily replace m_2 with any value and compute a new tag by reusing $F_k(m_1)$.

4. In CBC-MAC, if length is not fixed, attacker can take the tag of 1 block and use it as the first block of the new 2 block message

$$F_k(t \oplus (t \oplus x)) = F_k(x)$$

5. if padding is only done with zeros, diff msgs will produce same padding. So Merkle-Damgard will hash all messages to the same value, causing collisions.

6. yes, chose random r and a signature on m', $m' = m \cdot r^e \bmod n$, the signer return $s' = (m')^d = r \cdot m^d \bmod n$ the compute $s = s' \cdot r^{-1} \bmod n$ which will output a valid Sign. for m.

So, RSA are still insecure even with 1 query.

7. yes, they are possible if the client sorts the elements before building the merkle tree. Whe the client keeps the root of a sorted Merkle Tree, the Serve can prove non-membership. & Since they are sorted, showing x's neighbours prove its not in the set with only log-size.

8. a) Give key, m, & signature $\sigma = [\sigma_0 \dots \sigma_{n-1}]$

compute $d = H(m)$, d is from $d_0 \dots d_{n-1}$

for each i in d, check that $H(\sigma_i) = h_{i,d_i}$, accept if check for all bits passed

b) n (size of each σ_i) $\times$ n (number of σ) $= n^2$ bits

c) cuz every sign. reveal a primage for a_i.

So if have seen the key on diffrent msgs, i can have a lot of preimages for the same d_i

d) ?