2018 fall, Internet Security, final, 3:35 – 4:30pm

1. In DSA signature, r=(gk mod p) mod q and s=[k-1(H(M)+xr)] mod q. Also, y = gx mod p; w = s-1 mod q; u1 = [H(M)w] mod q; u2 = (rw) mod q; and v = [(gu1 yu2) mod p] mod q. The verifier receives the signature (r, s) and message M. How can he check whether the signature is right? Explain the equation that checks the signature. Note that g, p, q are public parameters for DSA signature; x and k are the secret key and the random number decided by the signer, respectively. H(•) is a hash function.

Y = g^x mod p

r = g^k mod p mod q

s = k^-1 (H(M) + xr) mod q

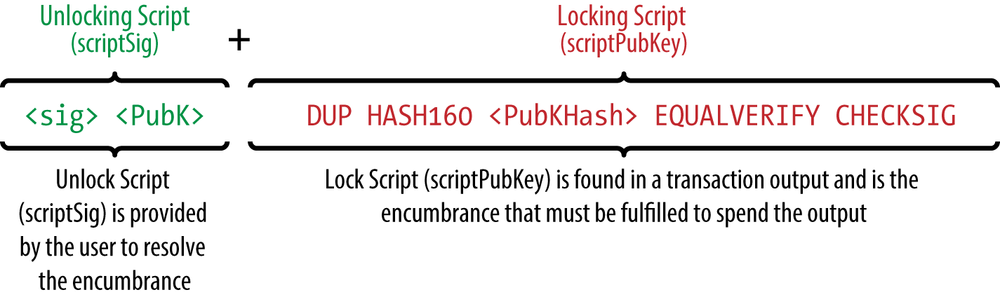
w = s^-1 mod q

u1 = (H(M)w) mod q

u2 = rw mod q

v = g^u1 y^u2 = g^(H(m)w) y^rw = g^(H(M)w) g^xrw = g^w(H(M)+xr) = g^s^-1(H(M)+xr) = g^k mod p mod q = r

v = r 이면 확인

2. What would be in the stack right before the system executes the EQUALVERIFY operation.

Sig pubK pubKHash pubKHash

3. The TCP 3-way handshake can be exploited for DoS attacks. Explain its vulnerability.

3번째 handshake ACK packet 을 보내지 않아 리시버의 SYN cache를 가득 채울 수 있다.

4. Select all the correct statements from below.

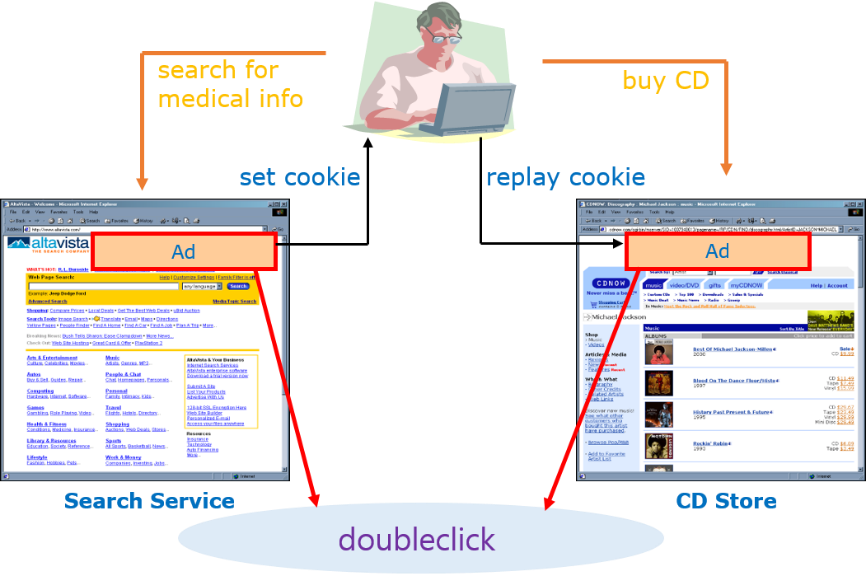
(1) Pharming is related to DNS poisoning attacks.

(2) DNS is a globally distributed database.

(3) Both the stub resolver and the local DNS server cache the responses from DNS servers.

(4) A glue record is the IP address of a DNS server in the DNS hierarchy.

1, 2

5. Explain the picture below with a focus on the user privacy.

광고회사의 서드파티쿠키에 의해 유저가 방문한 사이트 이력이 광고 회사에 노출된다