Security I: Supervision 2

Daniel Chatfield (dc584)

May 11, 2015

10. In the CBC mode of operation, the initial vector (IV) is chosen uniformly at random, using a secure source of random bits. Show that CBC would not be CPA secure if the initial vector could be anticipated by the adversary, for example because it is generated instead using a counter or a time-stamp.

    If the IV is predictable then an attacker can confirm whether a guessed plaintext (M_{guess}) is correct. Suppose they have some ciphertext, C that they know was encrypted using an IV IV_0, they can check their guess by submitting $M_{guess} \oplus IV_1 \oplus IV_0$, when this gets XORed with the next IV (IV_1) it cancels it out and results in the same bits as if it was XORed with just IV_0.

    This is used in the SSL BEAST attack, an attacker that could get a browser to make requests over https can craft the request such that the block is something like "Cookie: session=X" where X is a character the attacker does not know, with a predictable IV an attacker only has to try each of the possibilities and then adapt the request so that the block is "ookie: session=XY", repeating the process for each character.

12. A sequence of plaintext blocks $M_1, \ldots, M_8$ is encrypted using DES into a sequence of ciphertext blocks. Where an IV is used, it is numbered C_0. A transmission error occurs and one bit in ciphertext block C_3 changes its value. As a consequence, the receiver obtains after decryption a corrupted plaintext block sequence $M'_1, \ldots, M'_8$. For the discussed modes of operation (ECB, CBC, CFB, OFB, CTR), how many bits do you expect to be wrong in each block M'_i?

    Hint: You may find it helpful to draw decryption block diagrams

    ECB The only block that would contain incorrect bits is M_3, the number of bits that would be flipped would be random, and thus the expectation is that half the bits (32) would be flipped.

    CBC The decryption of blocks M_1 and M_2 are independent of the value

of C_3 and thus won't contain any incorrect bits.

In the decryption of block M_3, C_3 goes through a pseudo-random permutation function and thus the expected number of flipped bits is half of them (32 bits).

For M_4, C_3 is XORed with the decryption after being put through the pseudo-random permutation function, and thus a single bit will be flipped.

For M_5 through M_8 the decryption is independent again and thus no flipped bits will occur.

CFB M_1, M_2, and M_5 through M_8 will have no flipped bits. M_3 will have a single flipped bit. M_4 will be expected to have 32 flipped bits.

OFB A single bit will be flipped in M_3, all others will have no flipped bits.

CTR A single bit will be flipped in M_3, all others will have no flipped bits.

13. Your opponent has invented a new stream cipher mode of operation for DES. He thinks that OFB could be improved by feeding back into the key port rather than the data port of the DES chip. He therefore sets $R_0 = K$ and generates the key stream by $R_{i+1} = E_{R_i}(R_0)$. Is this better or worse than OFB?

This is worse, for a start it removes the separate random IV as now the key is set to R_0.

In addition to this, whilst E_x is a pseudo-random permutation function, this scheme limits the possible values it can act on.

Given a key K, $R_1 = E_K(K)$, $R_2 = E_{E_K(K)}(K)$.

15. Show that CTR mode is not CCA secure.

An adversary $\mathcal{A}$ can choose messages $M_0, M_1 \in \{0,1\}^m$. The challenger then computes $C \leftarrow Enc_K(M_b)$. The adversary then XORs C against a random block X and gets the challenger to decrypt it. The result, will be one of the original messages xored with X and thus the adversary can output b.

18. The runtime of the usual algorithm for comparing two strings is proportional to the length of the identical prefix of the inputs. How and under which

conditions might this help an attacker to guess a password?

> If a system uses naïve string comparison to check whether a password is correct then an attacker can try each letter in the alphabet over and over again until one has a statistically significant lower average running time (thus indicating that the comparison moved on to the next character).
>
> This timing attack can be used to recover each character in sequence until the entire password has been recovered.

19. (a) Describe a cryptographic protocol for a prepaid telephone chip card that uses a secure 64-bit MAC function Mac implemented in the card. In this scheme, the public telephone needs to verify not only that the card is one of the genuine cards issued by the phone company, but also that its value counter V has been decremented by the cost C of the phone call. Assume both the card and the phone know in advance a shared secret K. There is no encryption or decryption function on the phone or card and the protocol must be performed without contacting the phone company.

    Hint: Protocol equations may make your answer clearer.

    > Every card has a unique ID which is not writeable, all communication to and from the card except the initial handshake includes this ID.
    >
    > To prevent replay attacks, every time the phone attempts to read or write the card it must first get a challenge from the card that it has to include in the request.
    >
    > The machine debits the card at the start of each minute, if the debit fails then the call is terminated.
    >
    > If the restriction on being able to contact some central system is relaxed then the system can be designed in a way that is resilient even in the presence of a leaked key. At a fixed time interval (could be every minute or once a day) the telephone synchronizes with a central system, the central system checks that the balance on all cards seen in the time period is consistent with what it has seen before. If it is not consistent then it blacklists the card ID. This is how Oyster cards work, if you boost your oyster balance on the card using a compromised key then the card will be blacklisted before you reach your destination.

    (b) Explain the disadvantage of using the same secret key K in all issued

phone cards and suggest a way around this.

> The disadvantage is that if someone compromised the key on their card, by bruteforce or other means then they have compromised all other cards as well. You could get around this by having a pseudo-random function that generates a key from an ID and then each card will have a unique key.

24. Which of the Unix commands that you know or use are setuid root, and why?

> - traceroute
> - sudo
> - crontab
> - login
>
> They need to access resources that are only available to root.

25. What Unix mechanisms could be used to implement capability based access control for files? What is still missing?

> *Not sure about this*
>
> Can use groups, each group corresponds to a capability.

27. How can you implement a Clark-Wilson policy under Unix?

> *Not sure at all*