Security I
– exercises

Markus Kuhn

Easter 2015 – CST Part IB

1 Cryptography

Exercise 1: Decipher the shift cipher text
LUXDZNUAMNDODJUDTUZDGYQDLUXDGOJDCKDTKKJDOZ

Exercise 2: How can you break any transposition cipher with $\lceil \log_a n \rceil$ chosen plaintexts, if a is the size of the alphabet and n is the permutation block length?

Exercise 3: Show that the shift cipher provides unconditional security if $\forall K \in \mathbb{Z}_{26} : \mathbb{P}(K) = 26^{-1}$ for plaintexts $M \in \mathbb{Z}_{26}$.

Exercise 4: Show that an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is *perfectly secret* if and only if

(a) for every probability distribution over $\mathcal{M}$, every message $M \in \mathcal{M}$, and every ciphertext $C \in \mathcal{C}$ with $\mathbb{P}(C) > 0$ we have

$$\mathbb{P}(C|M) = \mathbb{P}(C).$$

(b) for every probability distribution over $\mathcal{M}$, every message pair $M_0, M_1 \in \mathcal{M}$, and every ciphertext $C \in \mathcal{C}$ with $\mathbb{P}(C) > 0$ we have

$$\mathbb{P}(C|M_0) = \mathbb{P}(C|M_1).$$

Exercise 5: How can you distinguish a Feistel cipher from a random function if it has only (a) one round, (b) two rounds?

Exercise 6: If the round function f in a Feistel construction is a pseudo-random function, how many rounds r are at least necessary to build a pseudo-random permutation? What test can you apply to distinguish a Feistel structure with $r - 1$ rounds (with high probability) from a random permutation?

Exercise 7: Using a given pseudo-random function $F : \{0,1\}^{100} \to \{0,1\}^{100}$, construct a pseudo-random permutation $P : \{0,1\}^{300} \to \{0,1\}^{300}$ by extending the Feistel principle appropriately.

Exercise 8: What happens to the ciphertext block if all bits in both the key and plaintext block of DES are inverted?

Exercise 9: Given a hardware implementation of the DES encryption function, what has to be modified to make it decrypt?

Exercise 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.

Exercise 11: Explain for each of the discussed modes of operation (ECB, CBC, CFB, OFB, CTR) of a block cipher how decryption works.

Exercise 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.)

Exercise 13: Your opponent has invented a new stream-cipher mode of operation for 128-bit key AES. He thinks that OFB could be improved by feeding back into the key port rather than the data port of the AES 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?

Exercise 14: A programmer wants to use CBC in order to protect both the integrity and confidentiality of network packets. She attaches a block of zero bits M_{n+1} to the end of the plaintext $M_1||\ldots||M_n$ as redundancy, then encrypts with CBC. At the receiving end, she verifies that the added redundant bits are still all zero after CBC decryption. Does this test ensure the integrity of the transferred message?

Exercise 15:

Show that CTR mode is not CCA secure.

Exercise 16: Your colleagues have invented a new authenticated encryption scheme that they call AES-CBC+CMAC. Their key generating function outputs a 128-bit AES key K, and their encryption function outputs $C\|T = \mathsf{Enc}_K(M)\|\mathsf{Mac}_K(M)$, where $\mathsf{Enc}_K(M)$ shall be the AES-CBC encryption of M with key K (with random IV each time), and $\mathsf{Mac}_K(M)$ shall be the AES-CMAC of M with key K. Show that this construct lacks CPA security.

2 Entity authentication

Exercise 17: Users often mix up user-ID and password at login prompts. How should the designer of a login function take this into consideration?

Exercise 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?

Exercise 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.)

(b) Explain the disadvantage of using the same secret key K in all issued phone cards and suggest a way around this.

3 Operating-system security

Exercise 20: Read

> Ken Thompson: *Reflections on Trusting Trust*, Communications of the ACM, Vol 27, No 8, August 1984, pp 761–763
> `http://doi.acm.org/10.1145/358198.358210`

and explain how even a careful inspection of all source code within the TCB might miss carefully planted backdoors.

Exercise 21: You are a technician working for the intelligence agency of Amoria. Your employer is extremely curious about what goes on in a particular ministry of Bumaria. This ministry has ordered networked computers from an Amorian supplier and you will be given access to the shipment before it reaches the customer. What modifications could you perform on the hardware to help with later break-in attempts, knowing that the Bumarian government only uses software from sources over which you have no control?

Exercise 22: The Bumarian government is forced to buy Amorian computers as its national hardware industry is far from competitive. However, there are strong suspicions that the Amorian intelligence agencies regularly modify hardware shipments to help in their espionage efforts. Bumaria has no lack of software skills and the government uses its own operating system. Suggest to the Bumarians some operating system techniques that can reduce the information security risks of potential malicious hardware modifications.

4 Access control

Exercise 23: Which Unix command finds all installed setuid root programs?

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

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

Exercise 26: If a multilevel security OS has to run real-time applications and provides freely selectable scheduling priorities at all levels, how does that affect security?

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

Exercise 28: How can you implement a Clark-Wilson policy under Windows?

Exercise 29: How can the *GNU Revision Control System (RCS)* be set up to enforce a Clark/Wilson-style access control policy? (Hint: `man ci`)

5 Software security

Exercise 30: Suggest a mandatory access control policy against viruses.

Exercise 31: How can you arrange that an attacker who has gained full access over a networked machine cannot modify its audit trail unnoticed?

Exercise 32: The log file of your HTTP server shows odd requests such as

```
GET /scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+C:\
GET /scripts/..%u002f..%u002fwinnt/system32/cmd.exe?/c+dir+C:\
GET /scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir+C:\
```

Explain the attacker's exact flaw hypothesis and what these penetration attempts try to exploit.

(Is there a connection with the floor tile pattern outside the lecture theatre?)