Security I – exercises

Markus Kuhn

Lent 2013 – Part Ib

1 Cryptography

1.1 Some mathematical prerequisites

1.2 Historic ciphers

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?

1.3 Unconditional security

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

1.4 Block ciphers

Exercise 4 How can you distinguish a Feistel cipher from a random function if it has only (a) one round, (b) two rounds?

Exercise 5 If the round function f in a Feistel construction is a pseudo-random function, how many rounds n are at least necessary to build a pseudo-random permutation? What test can you apply to distinguish a Feistel structure with $n-1$ rounds (with high probability) from a random permutation?

Exercise 6 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 7 What happens to the ciphertext block if all bits in both the key and plaintext block of DES are inverted?

Exercise 8 Given a hardware implementation of the DES encryption function, what has to be modified to make it decrypt?

1.5 Modes of operation

Exercise 9 Explain for each of the discussed modes of operation (ECB, CBC, CFB, OFB, CTR) of a block cipher how decryption works.

Exercise 10 A sequence of plaintext blocks $P_1, \ldots, P_8$ 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 $P'_1, \ldots, P'_8$. For the discussed modes of operation (ECB, CBC, CFB, OFB, CTR), how many bits do you expect to be wrong in each block P'_i?

Exercise 11 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?

Exercise 12 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 P_{n+1} to the end of the plaintext as redundancy, then encrypts with CBC. At the receiving end, she verifies that the added redundant bits are after CBC decryption still all zero. Does this test ensure the integrity of the transferred message?

1.6 Secure hash functions

Exercise 13 Explain the collision resistance requirement for the hash function used in a digital signature scheme.

Exercise 14 Show how the DES block cipher can be used to build a 64-bit hash function. Is the result collision resistant?

1.7 Applications of secure hash functions

1.8 Secret sharing

1.9 Public-key cryptography

Exercise 15 Popular HTTPS browsers come with a number of default high-level certificates that are installed automatically on client machines. As a result, most certificate chains used on the Web originate near the top of a CA tree. Discuss the advantages and disadvantages of this top-down approach for the different parties involved compared to starting with bottom-up certificates from your local system administrator or network provider.

1.10 Software tools

Exercise 16 Generate a key pair with PGP or GnuPG and exchange certificates with your supervisor. Sign and encrypt your answers to all exercises. Explain the purpose of the PGP fingerprint and the reason for its length.

2 Entity authentication

2.1 Passwords

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?

2.2 Protocols

Exercise 19 (a) Describe a cryptographic protocol for a prepaid telephone chip card that uses a secure 64-bit hash function H 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.

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

Exercise 20 Read

> Gus Simmons: *Cryptanalysis and protocol failures*, Communications of the ACM, Vol 37, No 11, Nov. 1994, pp 56–67.
> `http://doi.acm.org/10.1145/188280.188298`

and describe the purpose and vulnerability of the Tatebayashi-Matsuzaki-Newman protocol.

3 Access control

3.1 Discretionary access control

Exercise 21 Which Unix command finds all installed setuid root programs?

Exercise 22 Which of the Unix commands that you know or use are setuid root, and why?

Exercise 23 What Unix mechanisms could be used to implement capability based access control for files? What is still missing?

3.2 Mandatory access control

Exercise 24 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 25 How can you implement a Clark-Wilson policy under Unix?

Exercise 26 How can you implement a Clark-Wilson policy under WinNT?

Exercise 27 How can the *GNU Revision Control System (RCS)* be set up to enforce a Clark/Wilson-style access control policy? (Hint: `man ci`)

4 Operating-system security

Exercise 28 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 29 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 30 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.

Exercise 31 Read in the Common Criteria "Controlled Access Protection Profile" the "Security Environment" section. Was this profile designed to evaluate whether a system is secure enough to be connected to the Internet?

`http://www.commoncriteriaportal.org/files/ppfiles/capp.pdf`

5 Software security

Exercise 32 Suggest a mandatory access control policy against viruses.

Exercise 33 How can you arrange that an attacker who has gained full access over a networked machine cannot modify its audit trail unnoticed?

5.1 Common vulnerabilities

Exercise 34 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?)