This is a collection of past exam questions set by Markus Kuhn in the CST Part IB courses *Security I* and *Introduction to Security* since 2002.

Note that following a rearrangement of the security courses, cryptography material has since moved to the Part II *Cryptography* syllabus. Questions that refer entirely to cryptography material are therefore omitted here.

9 Security I (MGK)

(*a*) Let $\mathsf{Enc}_{K_\mathrm{E}}$ be the encryption function of an encryption scheme that provides indistinguishability under chosen plaintext attack (CPA security). Let $\mathsf{Mac}_{K_\mathrm{M}}$ be a message-authentication-code function that provides existential unforgeability. Named below are three techniques for applying these two functions together to a message M. For each of them

- briefly explain how $\mathsf{Enc}_{K_\mathrm{E}}$ and $\mathsf{Mac}_{K_\mathrm{M}}$ are combined, and
- state whether the resulting construct is likely to provide indistinguishability under chosen ciphertext attack (CCA security):

(*i*) encrypt-and-authenticate [2 marks]

(*ii*) authenticate-then-encrypt [2 marks]

(*iii*) encrypt-then-authenticate [2 marks]

(*b*) How can an attacker calling the C function `parse_text` below cause a buffer overflow? Explain how and why this works. [6 marks]

```
#include <stdlib.h>
#include <string.h>
#define BUFLEN 4096
int check(int n) {
  if (n > BUFLEN) abort();
  return n;
}
void parse_text(char *text, size_t len) {
  char buf[BUFLEN];
  memcpy(buf, text, check(len));
  /* ... */
}
```

(*c*) Many Unix system administrators create a personal group for each of their users with this user as the sole member.

(*i*) What is the purpose of such a group? [2 marks]

(*ii*) Such personal groups typically have the same name and integer identifier as the corresponding user identifier. Is this practice compatible with the Windows NT mechanism for identifying users and groups? [2 marks]

(*d*) Give two examples for resources where an operating system is expected to implement residual information protection and two alternative mechanisms for implementing it. What are their tradeoffs and threat assumptions? [4 marks]

[*Note:* part (*a*) no longer in CST Part IB syllabus]

9 Security I (MGK)

(*a*) Briefly explain *return-oriented programming*: what kind of software vulnerability and countermeasure does this class of attacks target, how does it work, and under what conditions is it applicable? [6 marks]

(*b*) Identify and fix a potential vulnerability in the following C function: [2 marks]

```
#include <stdlib.h>
void *bitmalloc(size_t bits) {
  return malloc((bits + 7)/8);
}
```

(*c*) On a Linux file server, you find this file:

```
$ ls -l
-rw----r-- 1 frank students  13593 May 31 14:55 question.tex
```

User `frank` is a member of group `students`.

(*i*) Based on the POSIX access-control settings shown, illustrate how the server's operating system will authorize access (if-statement pseudo code). [3 marks]

(*ii*) What does an equivalent Windows NTFS access-control list look like? [3 marks]

(*iii*) Does the Windows GUI for manipulating NTFS access-control lists allow users to enter this configuration? [2 marks]

(*d*) Give an example of how POSIX file-system access control can be used to provide the equivalent of password protection for parts of the file space. In particular, show how user `alice` can set up a directory `papers` such that only those members of group `committee` (which includes `alice`) who know the secret string "`SEL-4sB3`" can read a file `restricted.pdf`. Show the setup either as a sequence of shell commands that `alice` can use to create it, or in the form of the metadata of the files and directories involved (as `ls -l` would output it). [4 marks]

8 Security I (MGK)

(*a*) Compare and contrast the security definitions of a *pseudo-random generator* and a *pseudo-random function.* [4 marks]

(*b*) When a Windows NTFS access control entry (ACE) is inherited by a subdirectory, under which circumstances is the "inherit only" flag set or cleared, and why? [4 marks]

(*c*) What is *existential unforgeability* of a message authentication code? [4 marks]

(*d*) Which problem with CBC-MAC is fixed by ECBC-MAC, and how? [4 marks]

(*e*) A C program running on a 32-bit processor contains the following function:

```
void f(int *a, int l) {
  int *b, i;

  b = (int *) malloc(l * sizeof(int));
  if (b == NULL) return;

  for (i = 0; i < l; i++)
     b[i] = a[i];

  [...]
}
```

(*i*) How can a caller cause this function to overwrite unallocated memory? [2 marks]

(*ii*) Modify the function to remove this vulnerability. [2 marks]

[*Note:* parts (*a*), (*c*) and (*d*) no longer in CST Part IB syllabus]

8 Security I (MGK)

(*a*) Windows implements *static inheritance* for the access-control lists of NTFS files and folders.

(*i*) What does *static inheritance* mean here and how does it differ from *dynamic inheritance*? [4 marks]

(*ii*) Five flag bits (`ci`,`oi`,`np`,`io`,`i`) in each NTFS access-control entry (ACE) manage how it is inherited. Briefly describe the purpose of each bit. [5 marks]

(*iii*) User `mike` gives his folder `project` the following access-control list:

```
project
   AllowAccess mike: full-access (oi,ci)
   AllowAccess alice: read-execute (ci,np)
   AllowAccess bob: read-only (oi)
```

It contains one folder and two text files, none of which have any non-inherited access-control entries:

```
project\doc.txt
project\src
project\src\main.c
```

For each of these three objects, list all inherited access-control entries, showing in parentheses the inheritance-control flag bits that are set (using the same notation as above). [5 marks]

(*b*) Describe the purpose and four typical functions of a *root kit*. [6 marks]

9 Security I (MGK)

(*a*) While inspecting the discretionary access-control arrangements on a Unix computer, you find the following setup:

Members of group `staff`: `alex`, `benn`, `cloe`
Members of group `gurus`: `cloe`

```
$ ls -ld . * */*
drwxr-xr-x  1 alex staff    32768 Apr  2  2010 .
-rw----r--  1 alex gurus    31359 Jul 24  2011 manual.txt
-r--rw--w-  1 benn gurus     4359 Jul 24  2011 report.txt
-rwsr--r-x  1 benn gurus   141359 Jun  1  2013 microedit
dr--r-xr-x  1 benn staff    32768 Jul 23  2011 src
-rw-r--r--  1 benn staff    81359 Feb 28  2012 src/code.c
-r--rw----  1 cloe gurus      959 Jan 23  2012 src/code.h
```

The file `microedit` is a normal text editor, which allows its users to open, edit and save files.

(*i*) Draw an access control matrix that shows for each of the above five files, whether `alex`, `benn`, or `cloe` are able to obtain the right to read (R) or replace (W) its contents. [12 marks]

	`manual.txt`	`report.txt`	`microedit`	`src/code.c`	`src/code.h`
`alex`					
`benn`					
`cloe`					

(*ii*) Which users have at least all the access rights of which other users? [2 marks]

(*b*) Explain briefly *three* mechanisms that the operating system kernel of a desktop computer can use to generate unpredictable numbers for use in cryptographic protocols as soon as it has booted. [6 marks]

8 Security I (MGK)

Briefly explain

(*a*) the function of a *salt value* in a password database [3 marks]

(*b*) *two* examples of covert channels in a file system protocol that is restricted to read-only operations under a mandatory access-control policy [2 marks]

(*c*) *three* types of common software vulnerabilities, with examples [9 marks]

(*d*) *two* problems solved by Cipher Block Chaining [2 marks]

(*e*) under which conditions will user U be able to remove a directory D in Berkeley Unix [4 marks]

[*Note:* part (*d*) no longer in CST Part IB syllabus]

2011 Paper 4 Question 8

(Computer Science Tripos Part IB)

Security I (MGK)

(a) In Windows NTFS, each file can have an associated access control list (ACL). Each entry has a type in $\{allow, deny\} \times \{explicit, inherited\}$.

(i) What restriction does the Windows Explorer graphical user interface impose on the order in which these types of access-control entries can appear in an ACL? [4 marks]

(ii) Give *one* example of a POSIX file access-control configuration for which an equivalent NTFS ACL violates this GUI restriction. [4 marks]

(b) Your colleagues used a pseudo-random function $f : \{0,1\}^{64} \to \{0,1\}^{64}$ in order to construct a permutation $g : \{0,1\}^{192} \to \{0,1\}^{192}$. The argument and return values of g are split into three 64-bit registers, respectively: $g(X_1, X_2, X_3) = (Y_1, Y_2, Y_3)$. The output of g is calculated as $Y_2 = f(X_1) \oplus X_2 \oplus f(X_3)$, $Y_1 = X_1 \oplus f(Y_2)$, and $Y_3 = X_3 \oplus f(Y_2)$, where $\oplus$ denotes bit-wise exclusive or.

(i) Show that g is indeed a permutation. [4 marks]

(ii) Show how an attacker who does not know f can efficiently distinguish g from most random permutations, after evaluating g on two different inputs. [4 marks]

(iii) After you point out this shortcoming to your colleagues, they propose an improved variant $g'(X_1, X_2, X_3) = (Z_1, Z_2, Z_3)$ that adds another round to g: $Z_1 = Y_1$, $Z_2 = f(Y_1) \oplus Y_2 \oplus f(Y_3)$, and $Z_3 = Y_3$.

Show how this variant still does not fix the problem of efficient distinguishability from most random permutations. [4 marks]

2009 Paper 5 Question 9

(Computer Science Tripos Part IB)

Introduction to Security (MGK)

(*a*) Make the following statements correct by changing one word or number. (Negating the sentence is not sufficient.)

(*i*) The Advanced Encryption Standard defines a 16-round Feistel cipher. [1 mark]

(*ii*) Files encrypted with Cipher Block Chaining start with a zero initial vector. [1 mark]

(*iii*) Each user on a Unix system is identified by a unique prime number. [1 mark]

(*iv*) The "read" bits associated with a Unix directory affect whether the files in its subdirectory "`foo`" can be accessed. [1 mark]

(*v*) The "real user ID" associated with a Unix process determines its access rights. [1 mark]

(*b*) Name *five* examples of actions for which a Unix application will need to be invoked with *root* privileges. [5 marks]

(*c*) Explain the attack on Double DES that motivates the use of Triple DES. [6 marks]

(*d*) Under which conditions is the Vignère cipher unconditionally secure? [4 marks]

2008 Paper 4/11 Question 7

(Computer Science Tripos Part Ib, Part II (General), Diploma)

Introduction to Security (MGK)

(*a*) The following files are shown by an `ls -l` command on a typical Unix system:

```
-r-xr-sr-x  1 charlie acct    70483 2008-01-04 22:53 accounting
-r--rw----  1 alice   acct   139008 2008-05-13 14:53 accounts
-rwxr-xr-x  1 system  system 230482 1997-04-27 22:53 editor
-rw-r--r--  1 alice   users    7072 2008-06-01 22:53 cv.txt
-r--r-----  1 bob     gurus   19341 2008-06-03 13:29 exam
-r--r-----  1 alice   gurus    6316 2008-06-03 16:25 solutions
```

Unix users `alice` and `bob` are both members of only the group `users`, while `charlie` is a member of only the group `gurus`. Application `editor` allows users to read and write files of arbitrary name and change their permissions, whereas application `accounting` only allows users to append data records to the file `accounts`. Draw up an access control matrix with subjects {`alice`, `bob`, `charlie`} and objects {`accounts`, `cv.txt`, `exam`, `solutions`} that shows for each combination of subject and object whether the subject will, in principle, be able to read (R), (over)write (W), or at least append records (A) to the respective object. [9 marks]

(*b*) A C program uses the line

```
buf = (char *) malloc((n+7) >> 3);
```

in order to allocate an $\lceil \frac{\mathtt{n}}{8} \rceil$-bytes long memory buffer, large enough to receive `n` bits of data, where `n` is an unsigned integer type.

(*i*) How could this line represent a security vulnerability? [2 marks]

(*ii*) Modify the expression that forms the argument of the `malloc()` call to avoid this vulnerability without changing its normal behaviour. [3 marks]

(*c*) Name three types of covert channels that could be used to circumvent a mandatory access control mechanism in an operating system that labels files with confidentiality levels and give a brief example for each. [6 marks]

2008 Paper 3/10 Question 8

(Computer Science Tripos Part Ib, Part II (General), Diploma)

Introduction to Security (MGK)

(*a*) A source of secure, unpredictable random numbers is needed to choose cryptographic keys and nonces.

(*i*) Name *six* sources of entropy that can be found in typical desktop-computer hardware to seed secure random-number generators. [4 marks]

(*ii*) What sources of entropy can a smartcard chip, like the one in your University Card, access for this purpose? [4 marks]

(*b*) As Her Majesty's prime hacker "001", on a mission deep inside an enemy installation, you have gained brief temporary access to a secret chip, which contains a hardware implementation of the DES encryption algorithm, along with a single secret key. You connect the chip to your bullet-proof laptop and quickly manage to encrypt a few thousand 64-bit plaintext blocks of your choice, and record the resulting 64-bit ciphertext blocks. You are unable to directly read out the DES key K used in the chip to perform these encryptions and you will not be able to leave the site without knowing K. But you know that all S-boxes in the last DES round are supplied in this chip via a *separate* power-supply pin. When you create a short-circuit on that pin, the encryption progresses as normal, except that the output of all S-boxes in the last round changes to zero.

(*i*) Explain briefly the role of an S-box and the structure of a single round in DES. [4 marks]

(*ii*) How can you find K, considering that your available time and computing power will not permit you to search through more than 10^9 possible keys? [8 marks]

2007 Paper 4/11 Question 8

(Computer Science Tripos Part Ib, Part II (General), Diploma)

Introduction to Security (MGK)

(*a*) Your colleague wants to use a secure one-way hash function h in order to store h(password) as password-verification information in a user database for which confidentiality might become compromised. For h, she suggests to use an existing CBC-MAC routine based on AES with all bits of the initial vector and the 128-bit AES key set to zero. Is this construct a suitable one-way hash function for this application? Explain why. [8 marks]

(*b*) Explain how and under which circumstances overlong UTF-8 sequences could be used to bypass restrictions regarding which files an HTTP server serves. [8 marks]

(*c*) Name *four* techniques that can be used to make buffer-overflow attacks more difficult. [4 marks]

2007 Paper 3/10 Question 9

(Computer Science Tripos Part Ib, Part II (General), Diploma)

Introduction to Security (MGK)

(*a*) You have received a shipment of hardware random-number generators, each of which can output one 128-bit random number every 10 milliseconds. You suspect that one of these modules has been tampered with and that it actually produces only 30-bit random numbers internally, which it then converts via a pseudo-random function into the 128-bit values that it outputs.

(*i*) How does this form of tampering reduce the security of a system that uses a generated 128-bit random number as the secret key of a block cipher used to generate message authentication codes? [2 marks]

(*ii*) Suggest a test that has a more than 0.5 success probability of identifying within half an hour that a module has been tampered with in this way. [6 marks]

(*b*) Explain briefly

(*i*) the encryption and decryption steps of Cipher Feedback Mode; [3 marks]

(*ii*) why some operating systems ask the user to press a special key combination (e.g., Alt-Ctrl-Del) before each password login; [3 marks]

(*iii*) how a secure hash function h can be used to implement a one-time signature scheme; [3 marks]

(*iv*) what happens if the same private key of the scheme from (*iii*) is used *multiple times*, to sign different messages. [3 marks]

2006 Paper 4 Question 10 / Paper 11 Question 10

(Computer Science Tripos Part Ib, Part II (General), Diploma)

Introduction to Security (MGK)

(*a*) Alice and Bob participate in a public-key infrastructure that enables them to exchange legally binding digital signatures.

(*i*) Name *two* reasons why, for some purposes, Alice might prefer to use a message authentication code, instead of a digital signature, to protect the integrity and authenticity of her messages to Bob. [4 marks]

(*ii*) Outline a protocol for protecting the integrity and authenticity of Alice's messages to Bob that combines the benefits of a public-key infrastructure with those of using a message authentication code. [4 marks]

(*b*) Your colleague proposes a new way for constructing a message authentication code using a block cipher $E : \{0,1\}^{64} \times \{0,1\}^{128} \to \{0,1\}^{128}$. He takes the n-bit input message M, appends $p = 64 \cdot \lceil n/64 \rceil - n$ zero-bits, and splits the result into $k = (n+p)/64$ 64-bit blocks $M_1||M_2||\ldots||M_k = M||0^p$. He then calculates the message authentication code as

$$C_K(M) = E_{M_1}(E_{M_2}(E_{M_3}(\ldots E_{M_k}(K)\ldots)))$$

where K is the 128-bit secret key shared between sender and recipient. Show *two* different ways in which an attacker who observes a pair $(M, C_K(M))$ can, without knowing K, create a new pair $(M', C_K(M'))$ with $M' \neq M$. [6 marks]

(*c*) Show how a 128-bit message authentication code $C_K(M)$ with 64-bit key K can be constructed for an n-bit long message M using

(*i*) a secure hash function $H : \{0,1\}^* \to \{0,1\}^{256}$, such as SHA-256; [2 marks]

(*ii*) a block cipher $E : \{0,1\}^{128} \times \{0,1\}^{256} \to \{0,1\}^{256}$. [4 marks]

2006 Paper 3 Question 9 / Paper 10 Question 12

(Computer Science Tripos Part Ib, Part II (General), Diploma)

Introduction to Security (MGK)

(*a*) Name *three* types of software vulnerability; give an example for each and a brief description of how each could be exploited. [9 marks]

(*b*) Alice wants to attack Bob's computer via the Internet, by sending IP packets to it, directly from her own computer. She does not want Bob to find out the IP address of her computer.

(*i*) Is this easier to achieve for Alice with TCP or UDP based application protocols? Explain why. [3 marks]

(*ii*) For the more difficult protocol, explain *one* technique that Alice could try to overcome this obstacle and *one* countermeasure that Bob could implement in his computer. [3 marks]

(*iii*) Name *three* functions that Alice's Internet service provider could implement to make it more difficult for Alice to achieve her goal? [3 marks]

(*c*) In what way are TCP/UDP port numbers below 1024 special? [2 marks]

2005 Paper 3 Question 9 / Paper 10 Question 11

(Computer Science Tripos Part Ib, Part II (General), Diploma)

Introduction to Security (MGK)

(*a*) A and B play a simple game. A chooses a number $R_A \in \mathbb{Z}_3$ and B chooses a number $R_B \in \mathbb{Z}_3$. Then A and B communicate their respective choice to each other *simultaneously*, meaning that the players cannot change their choice after having seen that of the opponent. These rules decide who wins the game:

$$\begin{aligned} R_A &\equiv R_B + 1 \pmod 3 \quad \Rightarrow \quad A \text{ wins} \\ R_B &\equiv R_A + 1 \pmod 3 \quad \Rightarrow \quad B \text{ wins} \end{aligned}$$

In any other case, the result of the game is a draw.

(*i*) What complication arises when this game is played at a distance, for example via email? [2 marks]

(*ii*) Suggest a cryptographic protocol that prevents cheating when this game is played via email. Your solution should not rely on a trusted third party. [6 marks]

(*iii*) What assumptions do you make about the cryptographic functions used in your solution of (*ii*)? [3 marks]

(*iv*) What assumptions do you make about the amount of computing power available to the opponent in your solution of (*ii*)? [3 marks]

(*b*) Outline briefly the purpose of an organisation's security policy and what steps should be considered in its development. [6 marks]

2004 Paper 3 Question 9 / Paper 10 Question 11

(Computer Science Tripos Part Ib, Part II (General), Diploma)

Introduction to Security (MGK)

(*a*) Explain briefly mechanisms that software on a desktop computer can use to securely generate secret keys for use in cryptographic protocols. [5 marks]

(*b*) Give two different ways of implementing residual information protection in an operating system and explain the threat addressed by each. [5 marks]

(*c*) Consider the standard POSIX file-system access control mechanism:

(*i*) Under which conditions can files and subdirectories be removed from a parent directory? [2 marks]

(*ii*) Many Unix variants implement an extension known as the "sticky bit". What is its function? [2 marks]

(*iii*) On a POSIX system that lacks support for the "sticky bit", how could you achieve an equivalent effect? [2 marks]

(*d*) VerySafe Ltd offer two vaults with electronic locks. They open only after the correct decimal code has been entered. The VS100 – a low-cost civilian model – expects a 6-digit code. After all six digits have been entered, it will either open or it will signal that the code was wrong and ask for another try. The VS110 – a far more expensive government version – expects a 40-digit code. Users of a beta-test version of the VS110 complained about the difficulty of entering such a long code correctly. The manufacturer therefore made a last-minute modification. After every five digits, the VS110 now either confirms that the code has been entered correctly so far, or it asks for the previous five digits again. Compare the security of the VS100 and VS110. [4 marks]

2003 Paper 3 Question 9 / Paper 10 Question 11

(Computer Science Tripos Part Ib, Part II (General), Diploma)

Introduction to Security (MGK)

(a) Explain the difference between mandatory and discretionary access control. [4 marks]

(b) (i) Explain the purpose and operation of cipher-block chaining (CBC). [4 marks]

(ii) Explain how to decrypt a message in CBC. [4 marks]

(c) To protect her interview partners, a journalist needs to ensure that what she records with her digital camera cannot be viewed by anyone before she returns to her home country. You were asked to design for her a camera that encrypts recordings immediately before they are stored on tape. The question arises, how to handle the encryption key. If it is stored in the camera, it could be extracted if the hardware were confiscated and analysed. A key memorised by the user might be obtained using coercion, so this is not a suitable solution either.

Suggest *two* alternative convenient ways of arranging the encryption inside the camera such that decryption of the tape is only possible on the journalist's home computer. [8 marks]