GDAŃSK UNIVERSITY
OF TECHNOLOGY

Security of Computer Systems
Project rules

dr inż. Piotr Rajchowski

- Project task are realised individually or in groups of two.
- In the first two weeks it advised to select the algorithm and data base access method.
- During submission of the project there is a need of using own computer. In a case a computer room can be booked.
- A control and submission terms were pointed:
  - Control term – **21-23.04.2020.**
  - Project submission: **2.06-10.06.2020** (2nd correction term: **14-18.06.2020** – positive mark with a maximum of 60% of points).
  - It is possible to obtain 30 points from 1st and 10 points from 2nd project.

- Submission of the project:
  - Present a project,
  - Briefly present a report in an electronic version,
  - Send the report to the website no later than the deadline (10.06.2020). **In a case of a delay 1 point per day is subtracted from the ”documentation points”.**

	Selection		Realization						Control term			Realization				Submission			2nd term	
Month	II		III						IV			V				VI			IX	
Mo		24	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	14	
Tu		25	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	15	
We		26	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	16	
Th		27	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	17	
Fr		28	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	18	

Holidays | Exams | Control Term | Submission | 2nd term | Introduction

GDAŃSK UNIVERSITY
OF TECHNOLOGY

Project 1
Data encryption with session key transfer - a protocol for sending messages with a session encryption key

Block Ciphers:

- **AES** (Rijndael) – block size: 128 bits, key: 128/192/256 bits; realized in rounds

- DES – block size: 64 bits, key: 56 bits; realized in 16 rounds

- **3DES** – triple DES, three realizations: EEE, EDE (3 independent keys), EDE (2 independent keys)

- Blowfish – block size: 64 bits, key up to 448 bits; realized in 16 rounds

Modes of Block Ciphers:

- **ECB** – *Electronic Code Book* – splitting the message to a sub blocks with a length fitted to the algorithm.
- **CBC** – *Cipher Block Chaining* – input of the next block is dependent from the output of the previous block. The block of cryptogram is only dependent from the input plain text. The plain text is also mixed with initialize vector.
- **CFB** – *Cipher Feedback Mode* – input of the next block is dependent from the output of the previous block and the plain text. The plain text is not mixed with initialize vector but with a cryptogram.
- **OFB** – *Output Feedback Mode* – input of the next block is dependent from the output of the previous block. The input data of the next block are dependent from the output of the previous block, the input is not dependent from the plain text..

- The main task of the project is to design and program an application to cipher text messages and data files and then send them by using the Ethernet network. In general, the application must take a form of a network secure communicational tool. The application must allow sending and receiving the ciphered data and messages on both sides of communication. It means that user A have the application, and so does the user B. They can send each other ciphered text messages and files.

- Before the transmission user A and B must exchange their public keys, they will be used for secure session key exchange.

- During project realization and submission presentation the application must be executed on two physical computers, or on a physical computer and a virtual machine. For the communication purposes the network should be configured as the host-only adapter in the VirtualBox. The IP addresses should be configured by the user manually from a reasonable range.

- The GUI interface must allow to type and send a text message to the other user. Besides the text also an ability of sending any files (e.g. *.txt, *.png, *.mp3, *.avi, itp.), with any size (from 1kB to more that 100 MB) must be implemented. A test files are given by the teacher.

- It is obligatory to implement one of the block ciphers (AES or 3DES).

- It is obligatory to implement all four modes of operation of the block ciphers (ECB, CBC, CFB, OFB), one mode will be selected by the user in the GUI.

- For the CFB and OFB modes the size of the size of the subblock must be the power of 2.

- It is obligatory to implement a progress bar presenting the progress of sending the large files.

- For large files a method of data division must be implemented before sending them via the Ethernet interface.

- A UDP (User Datagram Protocol) or TCP (Transmission Control Protocol) communication protocol must be used to send the data between the mashines.

- When the UDP protocol was used a data loss exceptions must be handled.

- A pseudorandom generator must be used to generate the session key. The input data for the generator must be taken “from the environment” (system time, HDD disk sector, mouse position)..

- The session key must be encrypted by using the RSA public key of the receiving person and send to the receiving person.

- The public and private keys must be stored separately (e.g. in a different directories). The keys must be encrypted by using the block cipher operating in the CBC mode. The encryption key is the hash (generated by using the SHA-1, SHA-256 function) of the user-friendly password.

- It is allowed to use the available implementations of the block ciphers, RSA encryption.

- In a case of unauthorized decryption (e.g. using an incorrect password) the decryption process should be done with no notification to the user and as a result of the decryption process a pseudorandom data will be obtained.

- In the report the results of performer tests must be included (ciphering time, usage scenarios).

During realization of the project it is obligatory to generate the following keys:

- session key (used for data encryption),
- private and public keys of the users (used for secure transmission of session keys),
- access key (typed by the user) which hash will be used to encrypt the private RSA key to store it on the hard disk.

- The project report must contain a description of the applications' GUI interface, description of communication protocol and results of performed tests. Additionally, an algorithmic description of the program must be done. The report must be based on a given template.

- One submission term is assumed for the project task. If there will be a need to correct the project task, it is possible to obtain a maximum 60% of total points (24/60).

GDAŃSK UNIVERSITY
OF TECHNOLOGY

Project 2
Implementation of Data Base Access Control Methods

Main rules of permissions allocation:

- **Minimum / maximum permissions** – usually the rule of minima permissions is used (minimum permissions for normal activity).

- **Open / closed access control** – the system must verify each request for access generated by the subject. All requests may be discretionary unless they are prohibited - so-called open access control. In the case of closed access control, requests are not considered unless explicitly provided.

- **Gradation of access control**– each object has a defined scope of permissions and it is assumed that if the subject has the permission higher than the object's permissions, it also has lower-level permissions to this object.

Access control models

- **DAC** – *Discretionary Access Control* – each object has one owner. The owner is responsible for access granting.

- **MAC** *Mandatory Access Control* – the objects are classified in the hierarchy of security levels. Access level is assigned to the users. The access is granted or denied with respect to the access level of the user and the subject.

- **RBAC** – *Role Based Access Control* – permissions are connected not with objects but with roles acted by users. The user always acts a role and receives come access to the objects.

Discretionary Access Control – DAC

- Assumptions:
  - Users protect owned information,
  - Users can grant an access to other users,
  - Users can define the access level granted to others,
  - Users are responsible for the security policy.

- Permissions:
  - Read,
  - Add, insert,
  - Modify (delete),
  - Execute program,
  - Manage the permissions,
  - Manage permissions owned to the object.

Mandatory Access Control – MAC

- Basis of many security models.
- A labels are assigned to the objects (*Classification level*) i users/subject (*Clearance level*).
- Level of confidentiality: subject: *clear*(***S***), object: *class*(***O***).
- The security policy can be understood as a *label* control.
- User ***S*** has access to object ***O*** (same access for reading and writing?) when: *clear*(***S***) ≥ *class*(***O***).

  No control of data leakage and consistency.
- Rule:
  - *Read Down Access* **when** *equal or less Clearance*
  - *Write Up Access* **when** *equal or higher Clearance*

Role Based Access Control – RBAC

- **Basic rules**
  - A role is a group of permissions to the set of objects.
  - RBAC defines which users (subjects) have access to the objects on the basis of their roles.
  - Users get permissions not directly but by the role. The role is strictly related to the workplace / function in the company.
  - Roles should be separable.

- In most cases the RBAC is based on DAC.
- The RBAC model should be consistent with the structure of workplaces.
- High administration costs.
- Users have permissions directly related to their role in the company – minimum permissions.

- Any technology, limited by the DBMS,

- The database should be simple - several, at most a dozen of relationships, eg. DVD rental, doctor's office, announcements, members of associations, etc. (the aim is to demonstrate the operation of the access control model – not the database),

- It is necessary to implement the full functionality of the access control model, including basic SQL operations on objects (tables),

- Access to the database should be possible by using a web browser and a SSL tunnel. Dedicated client applications are also allowed.

- In the case of the DAC model with delegation of permissions, the presence of cycles in the graph of permissions delegation should be controlled (eliminated), and the possibility of granting the same right to the same object by more than one user should be eliminated. In addition, for a takeover right, it should be assumed that the previously assigned rights of the object are deleted and replaced with the permissions taken from the donor, while the donor is deprived of all possessed permissions - even when he transfers only one.

- In the case of the MAC model, one should remember the rules of data flow control (rule: no-read-up, no-write-down),

- In the case of the RBAC model, it is necessary to take into account static separation of roles during work, i.e. during the session you can only act one role (having many), despite opening e.g. multiple connections to the database and using different browsers.

- The selection of access control method should be made during the first two project classes.

- One submission term is assumed for the project task. If there will be a need to correct the project task, it is possible to obtain a maximum 60% of total points.