Knaur Robin

Problem iden: A_ Sending of the whole users list
Severity: low
Practicability: potential flaw
Description: server can reveal information about all the users
Proposed solution: friend list

Problem iden: A_AES_128b
Severity: medium
Practicability: easy
Description: aes128 can be cracked by brute force
Proposed solution: aes256b

Problem iden: C_storing of public keys on client
Severity: low
Practicability: n/a
Description: for every change of server and ca public keys store on client you need to issue a program code update instead of simple change in configuration
Proposed solution: configuration files

Problem iden: A_Registracia klienta u CA
Severity: low
Practicability: n/a
Description: request for registration message cannot be encrpypted by private key, because CA does not know public key yet which is encrypted in this message, probably only misstype
Proposed solution: encrypt by public key of CA

Problem iden: C_Some functions in public interacea are useless
Severity: low
Practica: n/a
Description: function server_verifyUser, server_generateRSAKeys
Proposed solution: remove them

Problem iden: C_Some functions in public interacea of client
Severity: low
Practica: n/a
Description: functions generateRSAKeys, generateAESKey, encrpyt, decrypt, login should not be public
Proposed solution: make them private

Plch Matej

Problem iden: C_Some functions in public interacea of client
Severity: low
Practica: n/a
Description: functions sendRequest, sendData should not be public
Proposed solution: make them private,

Problem iden: A_ Sending of the whole users list
Severity: low
Practicability: potential flaw

Description: server can reveal information about all the users
Proposed solution: friend list

Garai Mainak

Problem iden: A_Sending of the whole users list
Severity: low
Practicability: potential flaw
Description: server can reveal information about all the users
Proposed solution: friend list

Problem iden: C_Server overload
Severity: depends
Practicability: easy
Description: trade of for pricing but can cause delays fo communication when many clients are connected
Solution: you cant do much with this tradeof