Assignment 2

INF-2301 Computer Communication & Security

Introduction

- Security will be the focus of this assignment
  - Cryptography
  - Security Principles
  - Types of attack
- Contact same as before
  - morten.gronnesby@uit.no - Office A123
  - fredrik.h.rasch@uit.no - Office A040

Part A - File sharing

- Implement a server
  - Start with a filename as argument
  - Generate a fresh AES key and wait for connections
  - Upon connection encrypt and transmit the file
- Implement a client
  - Start with the IP-address of the server as argument
  - Generate an RSA key-pair and request the AES key from the server
  - Request the file
  - Decrypt the file and save it to disk

Part B - Analyze and Redesign

- Pure report assignment
- Discuss your solution with regards to:
  - CIA
    - Confidentiality
    - Integrity
    - Availability
  - AAA
    - Assurance
    - Authenticity
    - Anonymity

Implementation Details

- Socket level operation
  - Use of high level implementations is not allowed
  - No need for HTTP
- Use a cryptographic library
  - Pycrypto - Python 2.6 or 2.7
  - PyOpenssl - Python
  - OpenSSL - C
  - Cryptography - C#
  - crypto - Go

Implementation Details

- You can use any AES encryption mode
  - ECB - Electronic Code Book, unsafe
  - CBC - Cipher Block Chaining, need IV
  - CFB - Cipher Feedback, very similar to CBC
- We recommend you try using ECB and CBC both, but only ECB is required

Report

- DO NOT just explain your program step by step
- Explain why
- Discussion part
  - Alternative solutions? Improvements?
  - Test results
- Use in text citations
- Use more than just Wikipedia
- Submit your assignment on time
  - Extension? Tell us BEFORE the deadline