Tampere University – Department of Computing Sciences

Security Protocols: Helping Alice and Bob to Share Secrets (COMP.SEC.220)

Tutorial 3: Cryptography II

Antonis Michalas antonios.michalas@tuni.fi

Mindaugas Budzys mindaugas.budzys@tuni.fi

Hossein Abdinasibfar hossein.abdinasibfar@tuni.fi

August 19, 2024

Submission Deadline: 23.09.2024 at 23:00

Tutorial Description

This tutorial is devoted to helping you understand the basics of Public Key Infrastructure (PKI) and building on your knowledge acquired in tutorial 2. This will give you a hands-on experience on the following tasks:

- Digital signing of messages and verification of signatures;
- Setup and deployment of a certificate authority (CA);
- Generation and use of digital certificates;
- Leverage digital certificates to secure applications.

Exercise 1 – Digital Signatures

In this exercise, you will be building on what you learnt from the last tutorial (i.e. SHA-256). Digital signatures work the same way normal signatures work in the physical world. Digital signatures provide non-repudiation. As described in lecture 3a, to digitally sign a message: i) a user hashes a message, and ii) signs the hashed message with his/hair private key.

To complete this task;

- Extend your program from Exercise 2 of Tutorial 2 with digital signing and verification functions;
- To sign a message, the program should take as input a .txt file and the private key of the user;
- Generate a SHA-256 hash digest of the .txt file;
- Sign the generated digest with the user's private key;
- To verify the signature tag of a received message, the program should take as input the signature tag (signed digest), the message and the public key of the message sender. Explain how the verification process works.

Exercise 2 – Certificate Authority (CA)

The CA is a trusted entity that issues digital certificates and performs key management of public keys. The CA is well known and trusted by all principals in a communication instance. In this exercise, you are tasked with creating your own root CA to issue and sign certificates for your use.

Once you have created the root CA, you will be ready to sign digital certificates. To do so:

- Generate a private and public key pair for a user;
- Generate a Certificate Signing Request (CSR). In a real world scenario, the CSR will be sent to the CA for verification and digital signature creation.
- Generate a certificate based on the CSR. The certificate is generated by the CA signing the CSR.

Hint: Use the linux command line for this task.

Exercise 3 – Digital Certificates for Websites

In this exercise, you will explore how websites are typically secured using public-key certificates. You are required to launch a simple web server and secure it with your generated certificated (generate a certificate with a simple domain name in the previous exercise). Then you are required to use a packet analyzer tool (for example Wireshark) to capture the traffic between the web server and your browser, and observe the encrypted traffic.

To complete this exercise:

- Configure your computer to recognize the self created domain name;
- Launch the web server with the generated certificate;
- Import the self-signed certificate into the browser of your choice (any observations?);
- Take a screenshot of web server page with information on the certificate displayed.
- Write a short report on your observations with the packet analyzer tool.

Exercise 4 - Email Security

In this exercise, you will learn how to use digital certificates to secure online communication. You need to create and generate your own personal certificate and use it to secure your e-mail messages (You can use either OpenPGP, OpenSSL, or any service of choice). Once you have generated the certificate, bind it to your e-mail account and send the following to either Hossein or Mindaugas (emails provided above);

- A signed e-mail message;
- An encrypted e-mail message – what do you need to know in order to send and decrypt the encrypted messages?