Assignment 2 - RSA tunnel

Security

Sébastien Vaucher
sebastien.vaucher@unine.ch

10 October 2017

1 Assignment instructions

Create a secure TCP bridge between two computers in a client-server model. You will develop two components that will work together, an RSA *server* and a *client*. The server will be configured to accept encrypted TCP connections on a configurable port, and forward them in clear to a target computer. The client will accept clear TCP connections on a configurable port, and forward them encrypted to the previously mentioned *server*. Once the connection is established, traffic will flow asymmetrically like in any classical TCP connection. Note that some applications may need to open several connections in parallel. Ideally, your application should be able to tunnel any protocol based on TCP.

RSA will provide a secure connection between the client and the server. You can encrypt all the traffic with RSA or use RSA only to share an initial symmetrical session key (more speed). The RSA algorithm must be implemented manually, and the RSA server application must be able to generate the RSA key-pair.

2 Application layout

A A client application (e.g. browser)

C The RSA client (listening on port X, e.g. 8080)

S The RSA server (listening on port Y, e.g. 20000)

T Target of the TCP connection (e.g. website, google.com) send decrypted output to website, e.g.

`A → C:8080 [encrypt] → (traffic is encrypted here) → S:20000 [decrypt] → google.com:80`

3 Hand-in

The time allotted for this assignment is 2 weeks. The deadline is on 2017-10-25T13:59:59 local time. Late submissions are not accepted.

- To be submitted to Ilias[1]:
  - Source code of **your** assignment
  - Readme file briefly mentioning how to compile and run your program, which dependencies it requires, etc.
  - All the files have to be packed in an archive in a standard format[2], named following this exact pattern (in lowercase letters only):
    `security17-as<assignment number>-<your family name>.<extension>`.
    For example, if your name were to be *Homer J. Simpson*, you would use the following filename for this assignment: `security17-as2-simpson.tar.gz`
- You have to present a demonstration of the program in class (to the TA).
  - It is **mandatory** for each student to demonstrate his or her submission!
  - The sooner you present your assignment, the better (even before the deadline).

Your grade will depend on both the presentation and the code.

4 Notes

You can use your favorite programming language for the assignments of this course, so long as it is a programming language readily available on the GNU/Linux operating system[3]. The suggested language for this assignment is a JVM-based language (Kotlin, Scala, Java).

Should you have additional questions, please direct them to the TA at sebastien.vaucher@unine.ch.

[1] Or sent by e-mail for external students

[2] `.tar, .tar.gz, .tar.bz2, .tar.xz, .zip`

[3] You can use any of the languages in the following list. If you want to use another language, please check with the TA first. List in alphabetical order: Bash, C, C++, Go, Java, Kotlin, Perl, PHP, Python, Ruby, Rust, Scala