Security of Distributed Software

SS 2019 – 6. Tutorial

Valentin Siegert M.Sc.

Dang Vu

VSR.*Informatik*.TU-Chemnitz.*de*

Task 1

3 subjects want to communicate over an unsecure channel using a) a **symmetric** and b) an **asymmetric** encryption method.

How one can establish confidential, integrity and authenticity of mutual communication?

Consider a situation for b), where no data exchange over other channels is possible.

2

Task 2

1. Which information is stored in X509 certificates?
2. What is a Certificate Signing Request (CSR)?
3. Using openssl create a self-signed X509 certificate.
4. Using openssl start a fictitious web server on port 12345 and test the page https://localhost:12345/ in your browser.

   Why do you see a warning?

Task 3

1. Using openssl create a certificate for a fictitious certification authority (CA) (see 2.3)
2. Import the CA certificate into your browser (area: certification authorities)
3. Create an X509 certificate on the name localhost, but now signed using the CA-key from 3.1.
4. Restart the web server and open the same page. Why no warning is shown anymore?

Questions?

valentin.siegert@informatik.tu-chemnitz.de

VSR.*Informatik*.TU-Chemnitz.*de*