

Application Security

Exercise Set 4, Tigers

1. Investigate the OCSP:

- Check out the current stage of deployment OCSP on the market, find out what main certificates' providers prefer (CRL vs. OCSP) and what is the trend on the market.
- Find a certificate with OCSP referenced and perform a manual verification by making an appropriate call to the OCSP service. Check other main capabilities of the service.
- Check and explain what OCSP stapling is.

Create a report of the findings.

[6p]

2. Install a CA based on the OpenCA and create a small classic application for any operating system. Generate a certificate for application signing and sign the application with it. How the signature influences the application execution? What makes such a solution more secure?

[4p]

Pawel Rajba