T-110.4206 Information security technology

Examination 2011-01-13

Lecturer: Tuomas Aura

*Answer **only 5** of the 6 problems. If you answer them all, only problems 1–5 will be marked.*

1. Security terminology

Explain the meaning of the following terms (max 20 words each):

a. Reference monitor
b. Trusted path
c. Pseudo-SSO
d. PCR (in TPM)
e. Cross-site request forgery
f. Cross-site scripting

2. Access control models

Give an example of each of the following types of policies and explain why they may be needed:

a. Separation-of-duty policy in university or city administration
b. Chinese Wall policy in a consulting or accounting company
c. Data sanitization when healthcare data is used for research

3. PKI

A university issues identity cards to its members (students and staff). The cards are used for access control in locked doors and for checking student status in the canteen. The security of the cards is based on public-key authentication and X.509 certificates, which include both the user name and the user's status at the university. When might it be necessary to revoke a certificate?

4. Cryptography

What type of cryptography could be used for

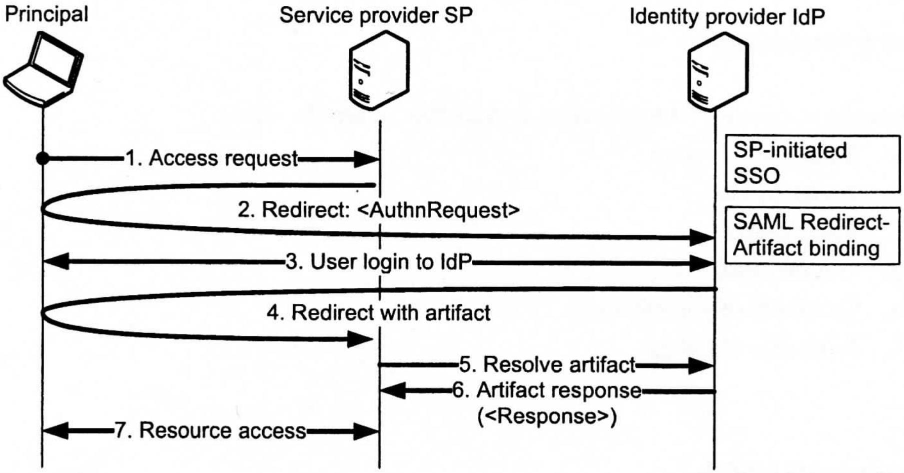
a. publishing software updates for a smart-phone operating system
b. publishing an electronic book in an online bookshop

In each case, explain how and why.

Please turn the paper for problems 5–6.

5. Identity management

The picture below illustrates SAML authentication for web-browser-based SSO (for example, Shibboleth). The Response in message 6 is signed by the IdP. Moreover, SSL is typically used to protect all the connections.



How and why is the security of the protocol affected if SSL is *not* used between

a. the client and the SP
b. the client and the IdP
c. the SP and the IdP

6. Threat analysis

What security threats are there against electricity metering in an apartment building? Prioritize the threats (approximately) from the point of view of the electricity company.