Avoiding The Top 10 Software Security Design Flaws

Lasse K. Brun & Håvard Rustad Olsen
(Group 5)

lkbrun@gmail.com & haavard.olsen@live.com

INF226 - Software Security, Fall 2014

13. November 2014

- Test 1
- Test 2

1. Earn or Give, but never assume, Trust

2. Use an authentication mechanism that cannot be bypassed or tampered with

- One goal of secure design: prevent unauthenticated access
- Prevent changing of identity without re-authenticate
- Authenticating requires one or more factors
  - Something you know (Password)
  - Something you are (Biometric signature)
  - Something you have (Smartphone)
- Authenticate machines as well as humans

2. Use an authentication mechanism that cannot be bypassed or tampered with

- Don't use forgeable session tokens
- Use time-tested mechanisms such as Kerberos
- Specify time limit for the session if user is inactive
- Handle passwords properly!
- It's preferable to use on component responsible for authentication

3. Authorize after you authenticate

4. Strictly separate data and control instructions, and never process control instructions received from untrused sources

5. Define an approach that ensures all data are explicitly validated

6. Use cryptography correctly

7. Identify sensitive data and how they should be handled

8. Always consider the users

9. Understand how integrating external components changes your attack surface

10. Be flexible when considering future changes to objects and actors