WRAP-UP 2

Introduction to Computer and Network Security

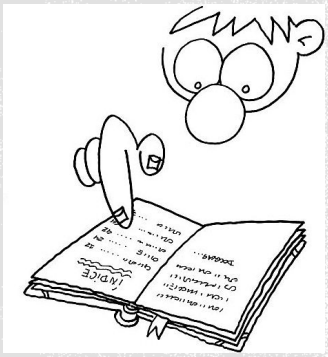
Silvio Ranise [silvio.ranise@unitn.it or *ranise@fbk.eu*]

UNIVERSITÀ DI TRENTO

FONDAZIONE BRUNO KESSLER

CONTENTS

- Authentication II
- Access Control I & II
- Web app security
- Privacy and Data Protection



2

AUTHENTICATION II

AUTHENTICATION II

- Define the notion of Single Sign On and its main properties
- What is SAML?
- Describe the high-level SAML authentication flow
- Explain the following concepts of SAML:
  - Assertion
  - Protocol
  - Binding
  - Profile
  - Authentication context
  - Metadata
- Describe the two scenarios for the Web Single Sign On profile:
  - Identity provider initiated
  - Service provider initiated
- In SAML, how is it possible to
  - guarantee trust in the assertions consumed by the relying party?
  - avoid man-in-the-middle attacks?
  - use pseudonyms and provide some privacy?
- Briefly describe how SPID uses the SAML standard?
- What is eIDAS? Explain with an example its utility

3

4 ACCESS CONTROL I

ACCESS CONTROL I (1)

- Describe the general architecture of an access control enforcement mechanism (including subjects, requests, guard, policy, isolation boundaries, audit log, and the role of authentication and authorization)
- Explain the role of access control in the context of an operating system explaining what are the problems with
  - multiple users
  - multiple tasks
- Give the definition of access control by explaining what is an authorization requests and how it is evaluated to grant or deny
- Explain what is the structured approach to access control including the notions of
  - policy
  - model
  - enforcement

  and how this supports separation of concerns
- Describe the notions of
  - Access Control Matrix
  - Access Control Lists (ACLs)
  - Capabilities

  and their relationships
- **Exercise**: given an access control matrix derives equivalent ACLs and capabilities

5

ACCESS CONTROL I (2)

- Explain what is a confused deputy possibly with the help of an example and how capabilities allows for avoiding it
- Explain the notions of
  - Discretionary Access Control (DAC)
  - Mandatory Access Control (MAC)

  and their relative advantages and disadvantages
- Explain the notion of Multi-level security by illustrating it with the Bell-La Padula model; in particular
  - security level
  - need-to-know
  - dominance relation
  - no-read-up rule
  - no-write-down rule
  - which properties among C, I, and A can be enforced by this model?
- Explain
  - the attack by trojans in the context of the Discretionary Access Control (DAC) model
  - the covert channel attack in the context of the Mandatory Access Control (MAC) model
- **Exercise**: given the security levels, subjects with clearance levels, and resources with sensitivity levels, answer authorization requests by using the no-read-up and no-write-down-rules of the Bell-La Padula model

ACCESS CONTROL I (3)

- Describe the Role Based Access Control (RBAC) model; in particular
  - User-role assignment relation
  - Permission-role assignment relation
  - Role hierarchy
  - how to answer if a user has a permission or not without/with role hierarchy
- In the context of RBAC, describe the following notions
  - sessions
  - static/dynamic separation of duty constraints
- **Exercise**: given a user-role assignment relation, permission-role assignment relation, and role hierarchy, answer authorization requests

8 ACCESS CONTROL II

ACCESS CONTROL II (1)

- Explain the notion of Attribute Based Access Control (ABAC) and the reasons for which it has been introduced with respect to previous models (such as RBAC)
- Describe the XACML standard including
  - the policy language (rules, policies, and policy sets, obligations, and rule combining algorithms)
  - request/response protocols
  - reference architecture (including PEP, PDP, context handler, PAP, PIP)
- What is the purpose for which OAuth 2.0 has been introduced and explain the problem is meant to solve
- What is the role of the main entities involved in the OAuth 2.0 protocol, namely
  - Resource owner
  - Client
  - Protected resource
  - Authorization server
  - OAuth token (and explain what is a JSON Web Token and its relation with the OAuth token)

9

ACCESS CONTROL II (2)

- Describe the steps of the Authorization Code Flow of OAuth 2.0
- In the context of OAuth 2.0, explain the notions and the roles of
  - refresh tokens
  - authorization codes
- Explain why it is a bad idea to use OAuth 2.0 for authentication and justify why another standard (OpenID connect) has been introduced for that purpose
- What is the role of TLS in the context of the standards OAuth 2.0 and SAML 2.0?

WEB & IOT APP SECURITY

WEB & IOT APP SECURITY (1)

- Which types of attackers are relevant in the context of web application security? Briefly describe each one of them together with the assets that they target.
- What are the threats in the application and user layer?
- Describe an SQL injection attack. Which are the mitigations to an SQL injection attack?
- Describe a XSS attack. Which are the mitigations to a XSS attack?
- Describe the problem of Unvalidated input and possible mitigations.
- Describe the problem of broken authentication and possible mitigations.
- Explain the notion of phishing attack and possible mitigations.
- Explain how access control can be crucial to mitigate the impact of attacks on web applications even against unknown vulnerabilities. Use an example to illustrate your reasoning

12

WEB & IOT APP SECURITY (2)

- Explain the publish-subscribe pattern and how it differs from the client-server pattern. What are the advantages of using the publish-subscribe pattern for IoT applications?
- Explain how MQTT implements the publish-subscribe pattern
- What are the main security issues of MQTT?
- Why it may be problematic to use TLS to secure the communication between the MQTT broker and the IoT devices?

13

14

PRIVACY & DATA PROTECTION

PRIVACY & DATA PROTECTION (1)

- Give two complementary definition of privacy and briefly comment them.
- Explain the linkage attack on anonymized data set with an example.
- Describe the technique of k-anonymity and explain how it can mitigate linkage attacks.
- Explain the trade-off between anonymity and utility in the context of realizing data sets.
- Explain the notion of pseudo anonymization function, describe possible implementations together with their pros and cons.
- Explain the use of persistent and transient identifiers in SAML together with their pros and cons for the privacy of users.
- Explain the properties of the LINDDUN approach, namely
  - Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance

15

PRIVACY & DATA PROTECTION (2)

- In the context of the GDPR, define the following notions:
  - Data subject, Data Controller, Data Processor, personal data, consent, and data breach
- Describe the notion of Data Protection Impact Assessment (DPIA, Art. 35 of the GDPR)
- Define the notion of risk as a combination of likelihood and impact in the context of cybersecurity and in the context of the GDPR.
- Explain the notion of risk matrix and the various level of risks from negligible to very high.
- Briefly describe two examples of data breach and describe the impact on the data subjects in terms of fundamental rights and freedom.