THREAT MODELING BASICS

Bug Hunting Praktikum 2019

23-Oct-2019

Philipp Holzinger

Fraunhofer SIT

AGENDA

- Introduction
- Assets
- Security goals
- Attackers
- Attack surface
- Attack vector

AGENDA

- **Introduction**
- Assets
- Security goals
- Attackers
- Attack surface
- Attack vector

INTRODUCTION – WHY THREAT MODELING?

- There is no absolute notion of „secure“ or „insecure“
- Security must be considered in the context of a reference point
- Threat model can be used as a reference to determine
  - What is a valuable asset?
  - What are security goals?
  - Who would attack the system?
  - What are possible entry points for attackers?
  - How would they attack the system?
- Can be used reason about countermeasures, severities of vulnerabilities, etc.

INTRODUCTION

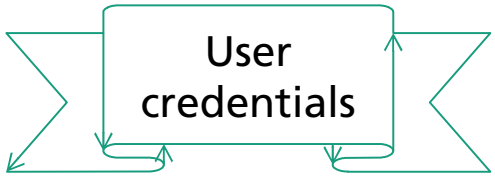
- In our context
  - What is a valuable target?
  - What are possible attacks?
  - How severe is an attack?
  - How to document attack vectors?

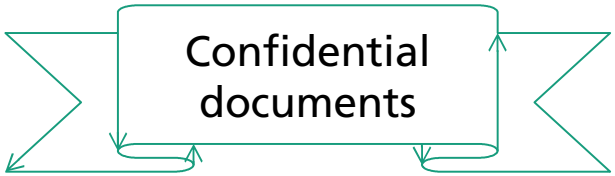
AGENDA

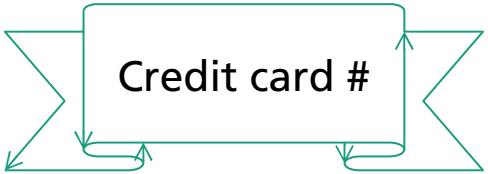
- Introduction
- **Assets**
- Security goals
- Attackers
- Attack surface
- Attack vector

ASSETS

- **Asset:** Anything of value to a stakeholder of the system







AGENDA

- Introduction
- Assets
- **Security goals**
- Attackers
- Attack surface
- Attack vector

SECURITY GOALS

- Assets are associated with security goals
- Security goals may include
  - Confidentiality
  - Integrity
  - Availability
  - Non-repudiation
  - Authenticity
  - …

AGENDA

- Introduction
- Assets
- Security goals
- **Attackers**
- Attack surface
- Attack vector

ATTACKERS

- Who wants to attack the system? For what purpose?
- In which assets are they interested?
- Which security goals do they threaten?

Property	Value
Identifier	Online criminal
Read source code	Yes
Write source code	No
Goals	• Unauthorized read access to credit card # • Unauthorized read access to user credentials • Unauthorized read/write access to confidential documents

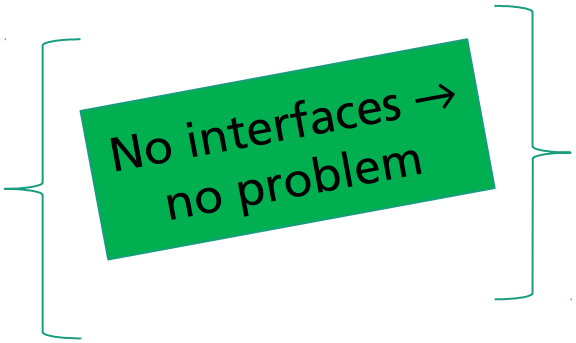
Capabilities & permissions

AGENDA

- Introduction
- Assets
- Security goals
- Attackers
- **Attack surface**
- Attack vector

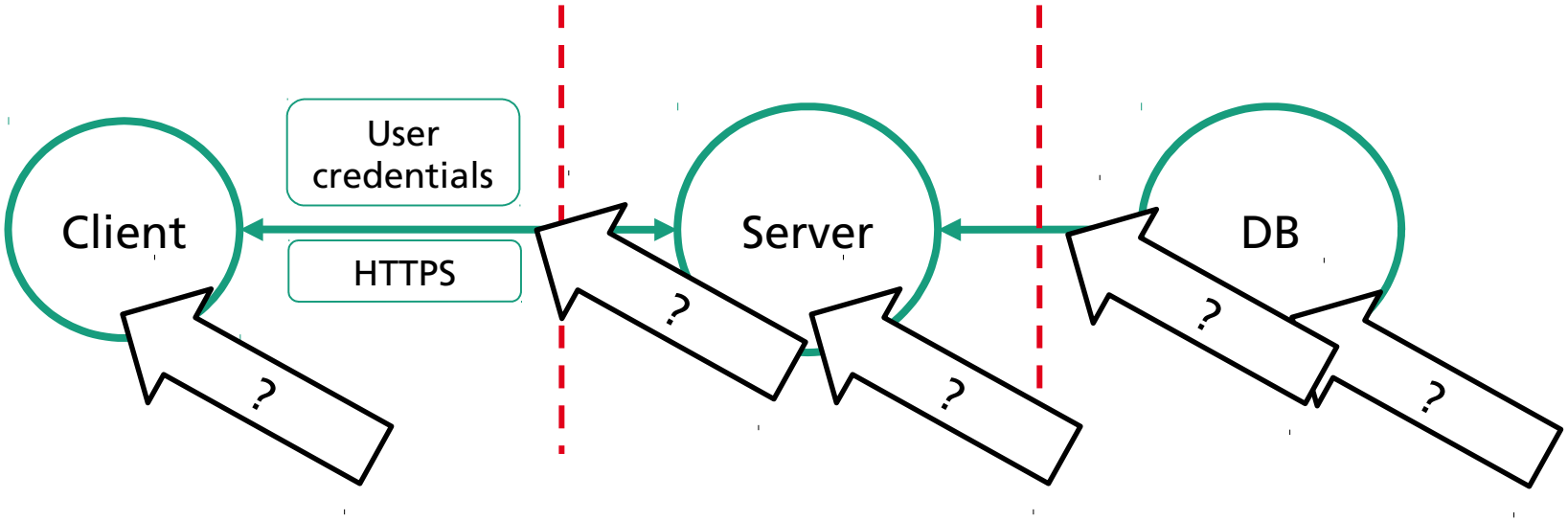
ATTACK SURFACE

- Attack surface: The set of all entry points and data extraction points of the target system
- Attackers must interact with the target system to execute an attack
- Interfaces may include
  - User interface
    - Text input/output
  - HTTP Get/Post parameters
  - Configuration files
  - Cookies
  - Socket connections
  - …



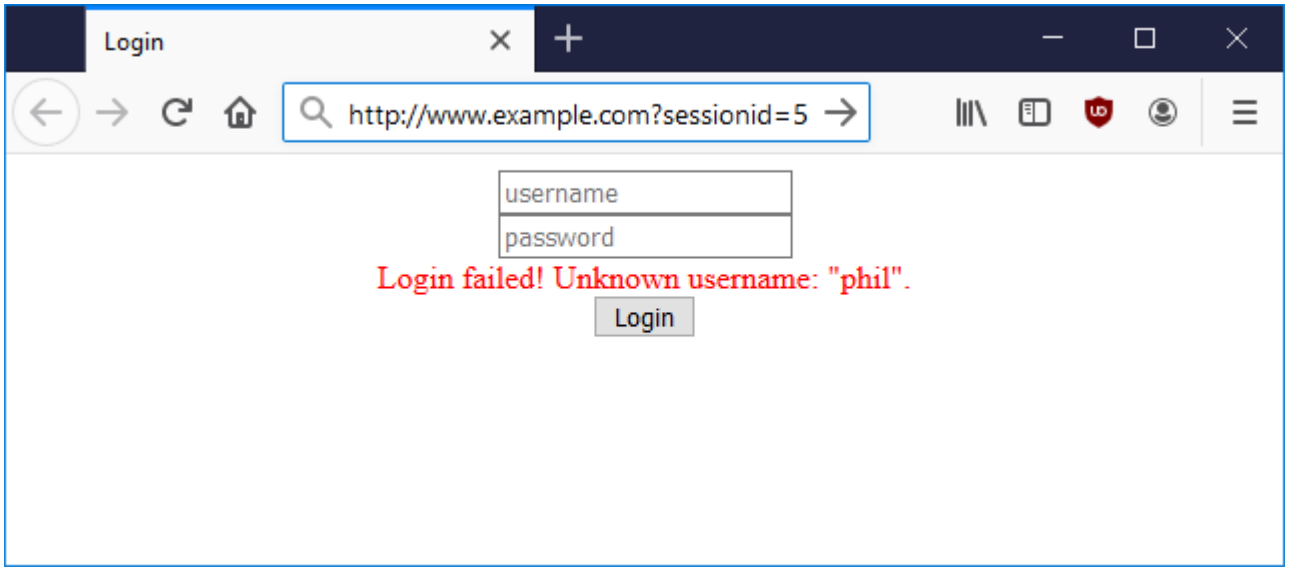
ATTACK SURFACE

- Architectural view: data flow diagram



ATTACK SURFACE

- User interfaces

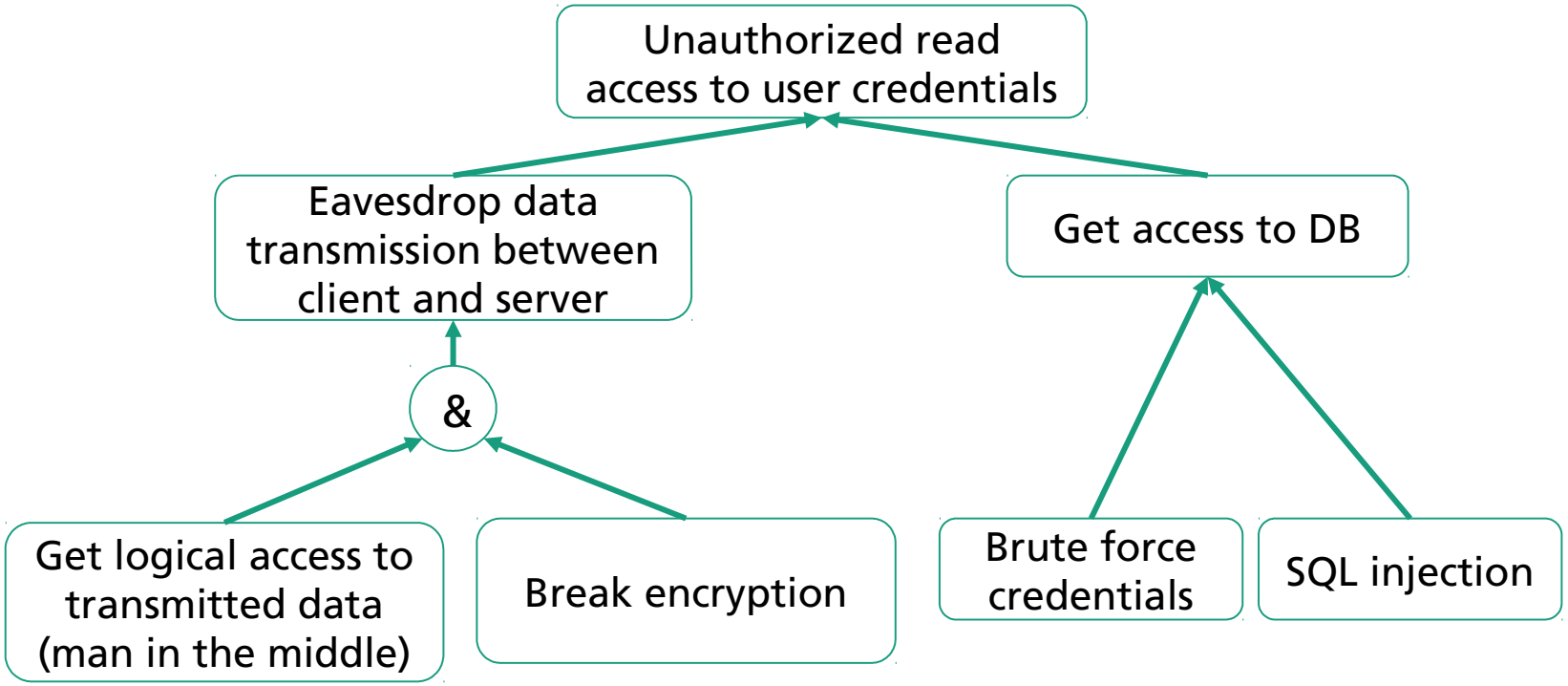


AGENDA

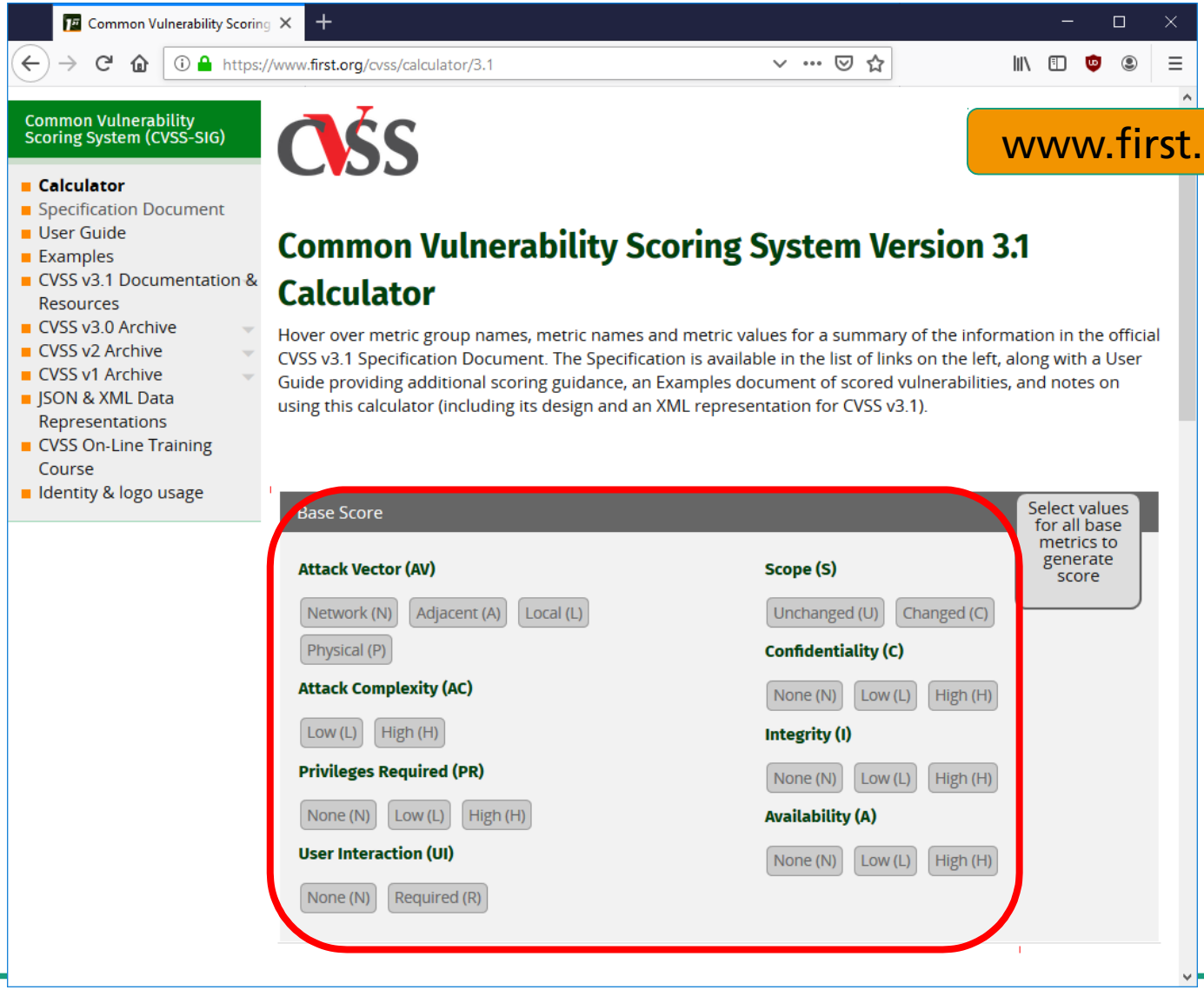
- Introduction
- Assets
- Security goals
- Attackers
- Attack surface
- **Attack vector**

ATTACK VECTOR

- How can attackers execute an attack?



CVSS


Common Vulnerability Scoring
https://www.first.org/cvss/calculator/3.1
Common Vulnerability Scoring System (CVSS-SIG)
Calculator
Specification Document
User Guide
Examples
CVSS v3.1 Documentation & Resources
CVSS v3.0 Archive
CVSS v2 Archive
CVSS v1 Archive
JSON & XML Data Representations
CVSS On-Line Training Course
Identity & logo usage
CVSS
www.first.org/cvss
Common Vulnerability Scoring System Version 3.1 Calculator
Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.1 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.1).
Base Score
Select values for all base metrics to generate score
Attack Vector (AV)
Network (N) Adjacent (A) Local (L) Physical (P)
Attack Complexity (AC)
Low (L) High (H)
Privileges Required (PR)
None (N) Low (L) High (H)
User Interaction (UI)
None (N) Required (R)
Scope (S)
Unchanged (U) Changed (C)
Confidentiality (C)
None (N) Low (L) High (H)
Integrity (I)
None (N) Low (L) High (H)
Availability (A)
None (N) Low (L) High (H)

SUMMARY

- Threat modeling supports systematic reasoning about
  - **Assets** – What is considered valuable by stakeholders?
  - **Security goals** – Which properties of assets are important?
  - **Attackers** – Who threatens assets and what are their capabilities?
  - **Attack surface** – Which interfaces can attackers use?
  - **Attack vectors** – How can attackers execute attacks?