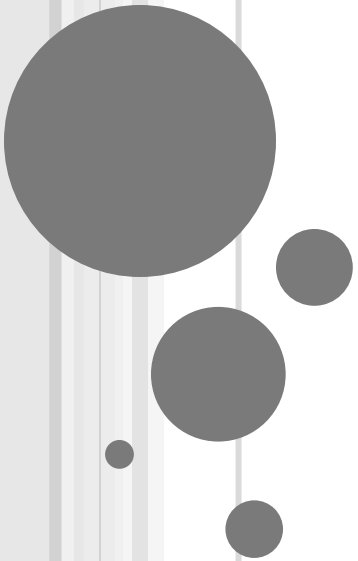
Framework "A" Tutorial



ABC Material
G. Almashaqbeh et al. 2019

Outline

- Threat modeling framework “A” steps.
- Example scenario.
- Running example application.

Overview

- In this tutorial we will explore the steps of a threat modeling framework, we refer to it as framework “A”.

- You will use this framework to build a threat model of a simplified resource-backed cryptocurrency system in the study.

- For ease of reference when working on the study, this tutorial is given to you in the form of handout as well.

Example Scenario

- We will demonstrate the steps of framework "A" by applying them to the following example:

Social Network 2.0:

- *Alice is a registered user of a social network.*
- *Each time she connects with a new friend she first connects to the social network's web portal.*
- *The portal communicates with the social network's server and the friendship information of Alice and her friend is updated in the database.*

Framework "A" Steps

- Consists of three steps:
  1. System Model Characterization.
  2. Threat Identification.
  3. Threat Scenario Enumeration.

1. System Model Characterization

- **First,** define the use scenarios, any external dependencies on other systems, and all assumptions.

  List assumptions and external dependencies:

  - the server that manages the users' information database and provides the social network website (or portal) is trusted.
  - End users are not trusted.

1. System Model Characterization

- **Second,** break the system into components based on its functionality. For each component identify its entry points, the participants, the assets, etc.

List of components: update friendship information.

List of participants: server and users.

List assets of value: database of user's personal information.

1. System Model Characterization

- **Third,** model the components as data flow diagrams (DFDs).
  - A DFD contains the following elements: data flows , data stores, processes, external entities.

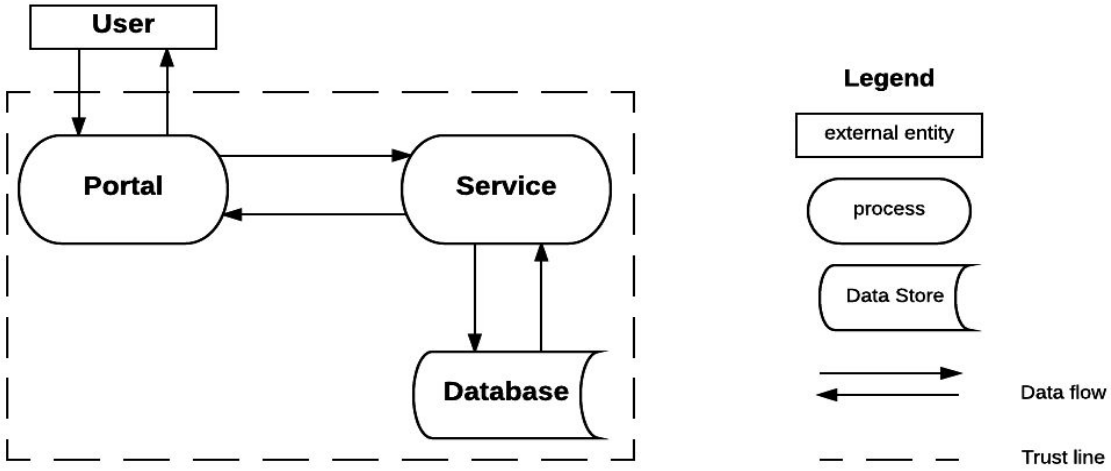


Figure 1: Social network example DFD

2. Threat Identification

- Identify the threats that may take place in the system.
- It might be helpful to use the following threat categories (Table 1) beside the mapping of these categories to each element in the DFD (Table 2).

Threat	Threat Definition	Examples
Spoofing	Spoofing threats involve an adversary creating and exploiting confusion about who is talking to whom. Spoofing threats apply to the entity being fooled, not the entity being impersonated. Thus, external elements are subject to a spoofing threat when they are confused about what or whom they are talking to.	• Accounts.contoso.com is spoofed when it thinks that a user is giving it authorized credentials. • An adversary may have poisoned the DNS cache so accounts.contoso.com now points at a malicious system that looks exactly like the real accounts.contoso.com.
Tampering	Tampering threats involve an adversary modifying data, usually as it flows across a network, resides in memory, on disk, or in databases.	• An adversary tampers with network packets, and changes commands after the user has logged in. • An adversary tampers with a registry key, making us run any program they choose.
Repudiation	Repudiation threats involve an adversary denying that something happened.	• Joe denies that he clicked on that link, for example to deny that he has benefited from a financial transaction. • Amy receives an email from Joe in which he agrees to a contract between the two. Later, Joe denies ever having sent that email.
Information disclosure	Exposing information to someone not authorized to see it.	• Examples include passwords for known or unknown users, copies of emails, and names and social security numbers in a database.
Denial of service	Deny or degrade service to users.	• An adversary prevents customers from connecting to a website. • An adversary prevents the client from getting a DNS response.
Elevation of privilege	Gain capabilities without proper authorization.	• An adversary who starts as an anonymous internet user can send commands to an application that execute as the web server. • An adversary with a web server can make code run as the local user.

Table 1: Threat categories.

Table 2: Mapping of DFD elements to threat categories.

Threat	Data Flow	Data Store	Process	External Entity
Spoofing			✓	✓
Tampering	✓	✓	✓	
Repudiation		✓	✓	✓
Information disclosure	✓	✓	✓	
Denial of service	✓	✓	✓	
Elevation of privilege			✓	

Running Example Application

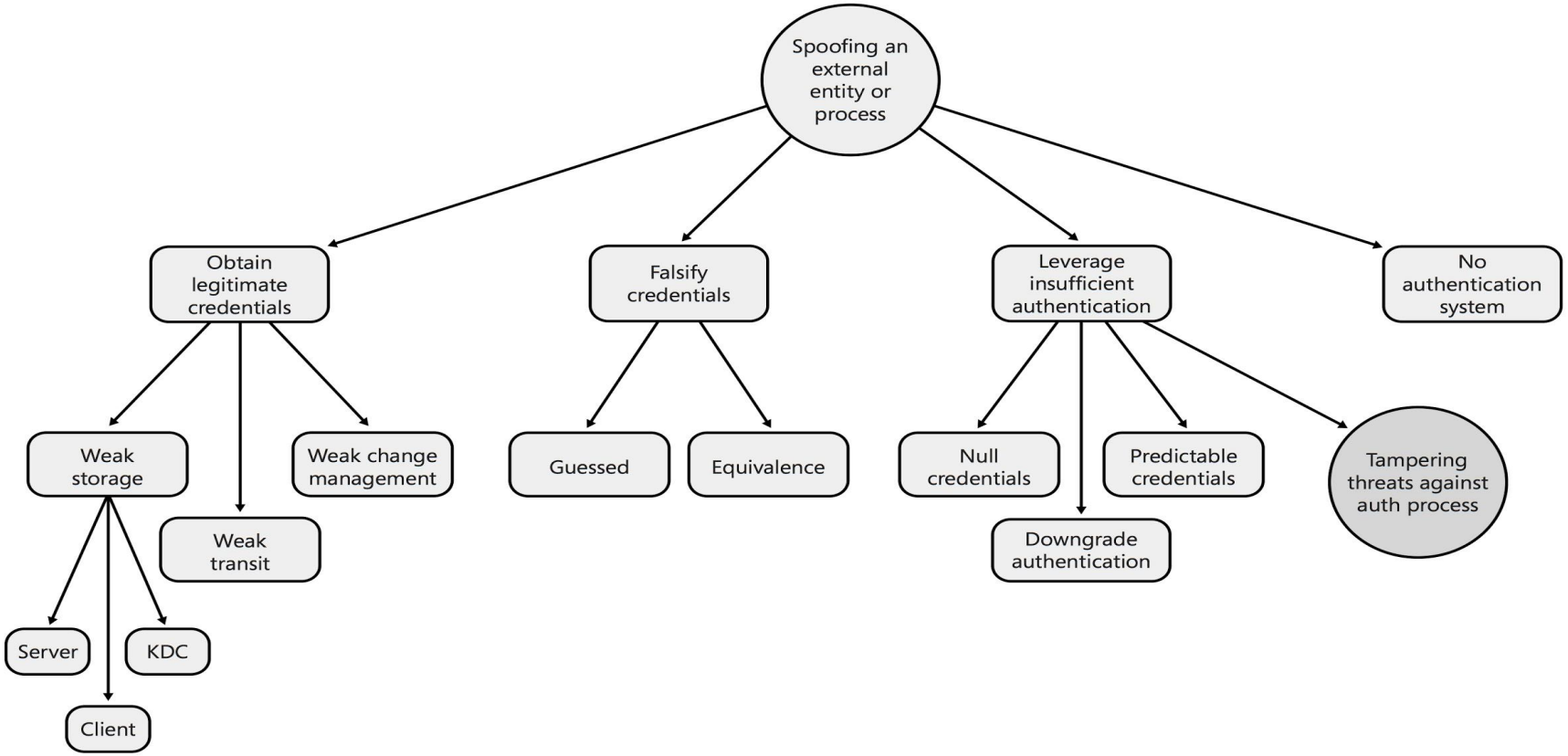
- **Threats:**
  - Tampering with the data flow between the user and the portal,
  - spoofing the server,
  - denial of service against the social network server,
  - etc.

3. Threat Scenario Enumeration

Elicit the threats in the system as follows:

- Examine each threat and enumerate all its possible scenarios.
- Write down a brief description of each threat scenario.
- You may find the threat tree patterns useful in this process.

Threat Tree Pattern Example - Spoofing



NOTE

- Due to time constraints, you will be asked to examine only one threat in the study.

STOP AFTER STEP 2 AND ASK THE MONITOR TO HAND YOU THE REST OF THE STUDY THAT DETERMINES WHICH THREAT TO WORK ON.

Running Example Application

Threat scenarios: Spoofing the server.

1. The portal does not implement any authentication service, an attacker can pretend to be Alice and manipulate her information through the server.

2. The portal implements a weak authentication service, an attacker is able to obtain the credentials or downgrade the authentication.

3. Alice stores her credential in an insecure location, an attacker is able to access this location and steal her credentials and spoofed her.

4. Alice is using weak credentials, an attacker is able to guess them and access the portal.