

Secure Software Development

Threat Modelling, Design and Implementation of a Secure Website



April 8, 2015

Wayne Caruana

1BSC2S

Table of Contents

[Task 1 – Definition of requirements, Threat Modelling and Design (P2.1, P2.2) 2](#_Toc417920242)

[Assets 2](#_Toc417920243)

[Trust Levels 2](#_Toc417920244)

[Architecture Overview 2](#_Toc417920245)

[DFD Level 0 2](#_Toc417920246)

[Threats (At least 10) 2](#_Toc417920247)

[STRIDE 2](#_Toc417920248)

[Mitigation Strategy 2](#_Toc417920249)

[Task 2 – DFDs in Threat Modelling Document (M1.4) 3](#_Toc417920250)

[Task 3 – Implementation of Secure Website (P3.1) 3](#_Toc417920251)

[Task 4 – Documentation of security patterns and practices (P3.2, P4.3) 3](#_Toc417920252)

[Task 5 – Implementation of Further security techniques in website (M1.5) 3](#_Toc417920253)

[Task 6 – Documentation of alternative security patterns (M1.3) 3](#_Toc417920254)

[Task 7 – Security Patterns – Argue on what you cannot protect against (D1.2) 3](#_Toc417920255)

[Task 8 – Testing and Reviewing a 3rd Party application (P4.1, P4.2, P4.4) 3](#_Toc417920256)

[Task 9 – Perform Attacks on a third party application and document them (D1.3) 3](#_Toc417920257)

# Task 1 – Definition of requirements, Threat Modelling and Design (P2.1, P2.2)

## Assets

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Description | Trust Level |
| A1 | User | Assets that relate to a website user |  |
| A1.1 | User’s Login data | Users’ credentials username and password. This asset needs protection because if it is stolen another user would be able to do anything which the user can do. | T2 Authenticated user  T3 Database server admin |
| A1.2 | User’s Personal Data | User’s personal data including contact information. This needs protection because some personal data might be important such as telephone number. | T2 Authenticated user  T3 Database server admin |

## Trust Levels

|  |  |  |
| --- | --- | --- |
| ID | Name | Description |
| T1 | Remote anonymous user | A user who has not yet authenticated to the website |
| T2 | Authenticated user (Buyer) | A registered user who has valid credentials has only the right to buy certain items. |
| T3 | Website administrator | User who can do any operations on the website such as updating, deleting and inserting any products. |
| T4 | Authenticated user (Seller) | A registered user who can upload, edit or delete his own items in order to put them on the market. |

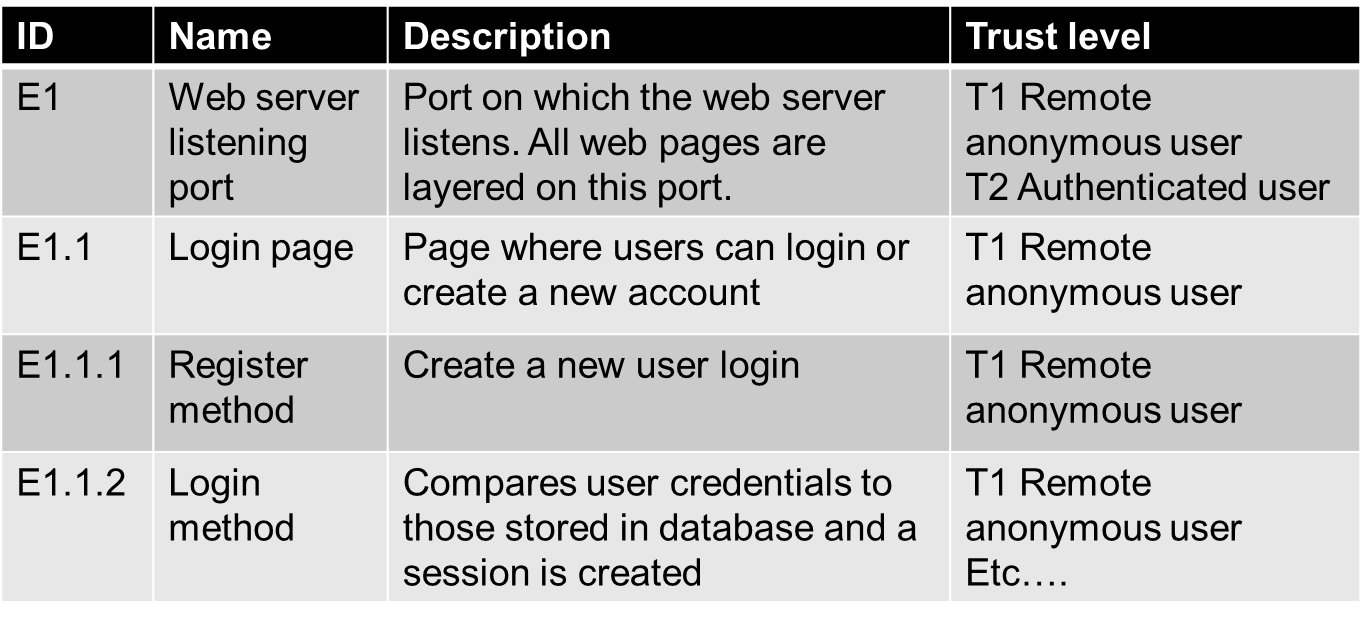
## Architecture Overview

|  |  |
| --- | --- |
| ID | Description |
| U1 | The website will be installed on a Web server that has been secured to current industry guidelines. Current security patches for the web server must be maintained. |
| U2 | Web Server should be protected from direct access. |
| U3 | Communication between the web server and the database server should be over a private network. |

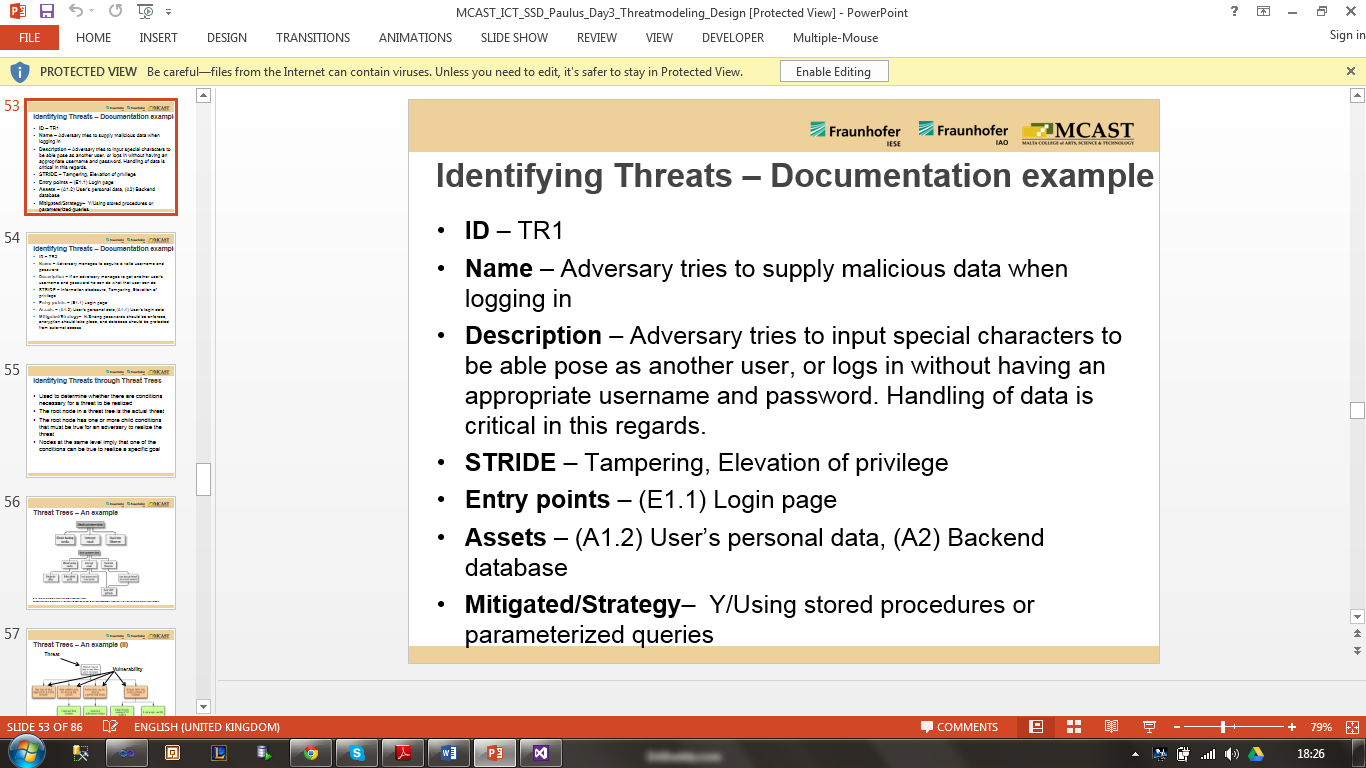
## DFD Level 0

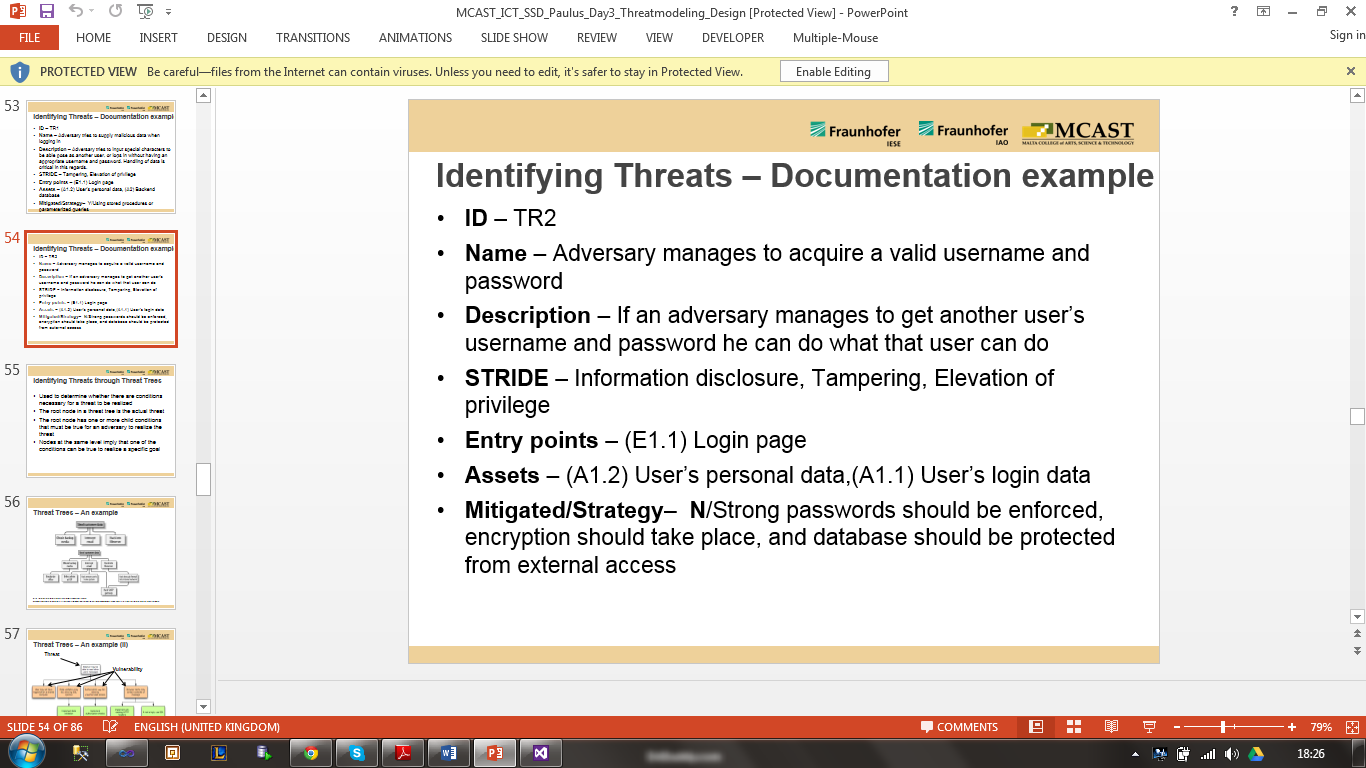
## 

## Entry Points

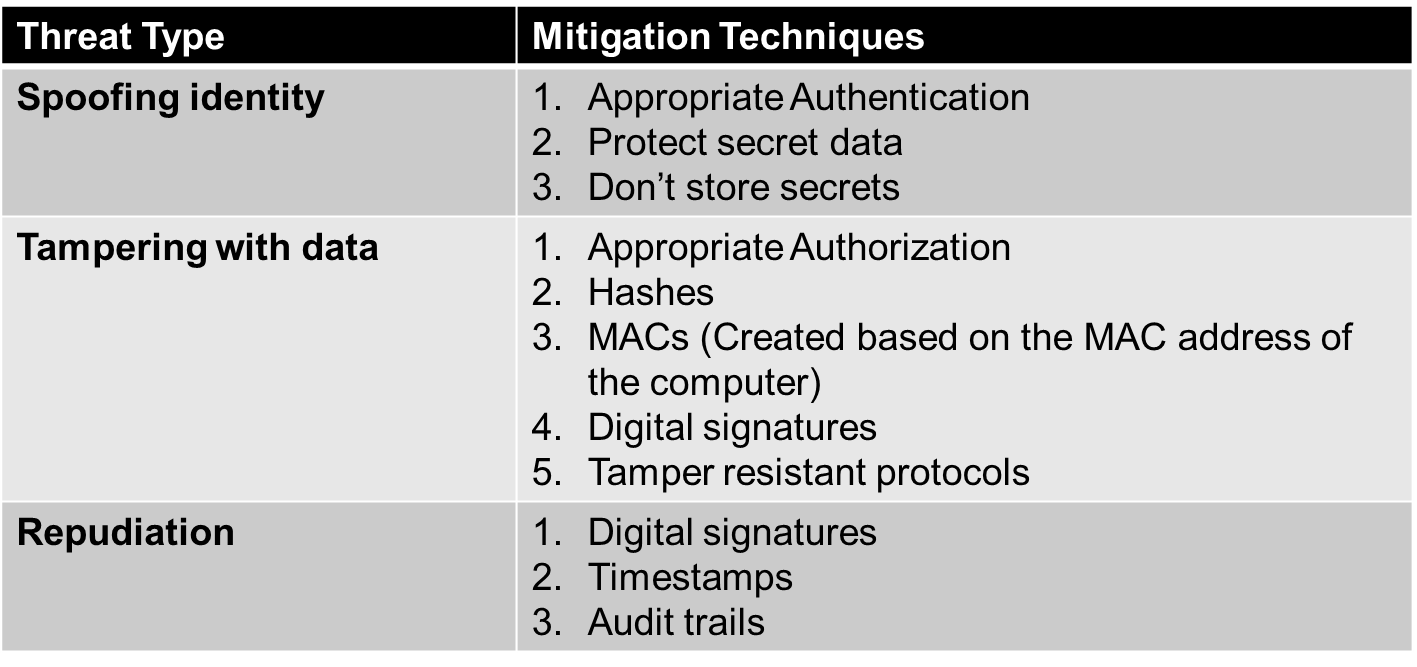


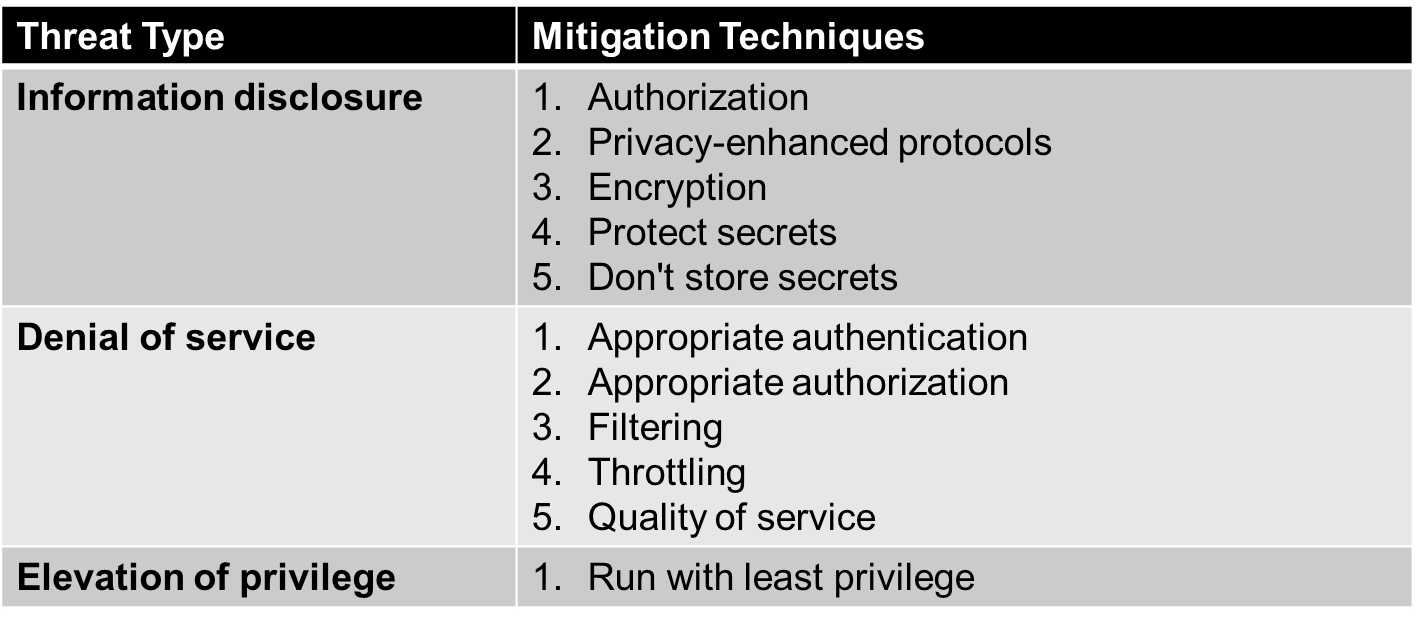
## Threats (At least 10)





## STRIDE





## Mitigation Strategy

# Task 2 – DFDs in Threat Modelling Document (M1.4)

# Task 3 – Implementation of Secure Website (P3.1)

# Task 4 – Documentation of security patterns and practices (P3.2, P4.3)

# Task 5 – Implementation of Further security techniques in website (M1.5)

# Task 6 – Documentation of alternative security patterns (M1.3)

# Task 7 – Security Patterns – Argue on what you cannot protect against (D1.2)

# Task 8 – Testing and Reviewing a 3rd Party application (P4.1, P4.2, P4.4)

# Task 9 – Perform Attacks on a third party application and document them (D1.3)