Faculty of Engineering and Information Technology

Computer Science Department

COMP438 Assignment #1

Title: Case Study: SSL Warnings - example user

Objectives: 1. Enhance user understanding of security alerts.
2. Promote informed decision-making.
3. Design a Usable Security alerts that prioritizes both usability and privacy.

Description:

Part A:

In an increasingly interconnected digital world, online security and privacy have become paramount concerns for users. When browsing the web, you may have encountered SSL (Secure Sockets Layer) warnings—those messages that pop up in your web browser, often making you pause and wonder about their meaning and implications. This assignment delves into the realm of usable security and privacy, challenging you to analyze and understand these SSL warnings. As a starting point, please examine the provided SSL warning figure below. Then, answer the following series of questions and scenarios. We aim to assess your ability to interpret these messages.

1. What do you think that message means?
2. What do you think the risks are if you see an error like this?
3. What would you do if you got this error?
4. Do you know what that means when it says someone is tampering with the connection?
5. If the site is your bank account, what you do?
6. **Design a usable user interface for this warning?**

This Connection is Untrusted

You have asked Firefox to connect securely to **www.youtube.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

This site uses HTTP Strict Transport Security (HSTS) to specify that Firefox only connect to it securely. As a result, it is not possible to add an exception for this certificate.

[Get me out of here!]

▶ **Technical Details**

Part B:

1. Find **two warning messages (one from a browser and one from a desktop application)** other than the one provided in this question. In two lines, explain why you believe each warning message is not usable (i.e., difficult for users to understand or respond to). **Your answer should be related to the material you have learned in this course.**

2. Design a usable user interface for the warning messages you found. You can use any online tool or any tool you are familiar with to design these messages

Please note the Followings:

I. This is an **individual assignment**. Disciplinary action will be taken against those who **cheat**. Additionally, the use of **AI tools** for generating solutions or **copying from websites** is strictly prohibited. Students found in violation of these policies will face severe consequences. It is crucial to ensure that all work submitted is **your own** and adheres to the **guidelines provided for this assignment**.

II. Please submit your answers by replying to the message **on Ritaj by Saturday, 12/10/2024**. **Only PDF format is acceptable for submission**. If you submit any file in a non-PDF format, it will not be graded, and you will receive a zero.

All the Best