Critical Thinking:

Another fundamental tradeoff in computer science could be the tradeoff between usability and security. This tradeoff involves the need of user-friendliness on the application and ease of use with the need for software, hardware, servers, or any other system to be secure and protect user data and systems from unauthorized access or attacks. A developer can use the following factors when faced with this dilemma:

User feedback: The developer can take advantage of user feedback. User feedback can provide valuable information on the usability of software. By collecting feedback from users, developers can find areas of the software that may be difficult to use, misleading or confusing. User feedback , though, may not always provide a complete picture of the usability of software, and developers may need to supplement user feedback with other metrics. Additionally, some may believe that their security is being infringed upon by answering these questions about the product or by collecting data automatically.

Vulnerability assessments: Vulnerability assessments can help identify potential security vulnerabilities in software, hardware, and systems. By assessing the product for potential security weaknesses, developers can identify areas where additional security measures may be needed. However, vulnerability assessments may not always be comprehensive, and it may be difficult to identify all potential security threats. Plus, vulnerability assessments usually result in loss of usability or functionality on the short term while the test is going on, and in the long term if the fix for the security limits the usability of the application or system.

Compliance with standards: Compliance with industry standards and regulations can provide a baseline for security requirements in software. By ensuring that software meets industry standards and regulations, developers can help ensure that the software is secure. On the other hand, some standards, such as two factor authentication, are upsetting to end users because they believe it is ‘annoying’ to have to go through the whole process of validation and authentication in order to use your application, when all you are trying to do is make your product more secure.