Homework 1

Part 1 - Ethical Analysis

(1a)

The consequentialist will weigh the harms against benefits. There will be significant harms to a large percentage of the users after the adversaries exploit and before the company patches the vulnerability, if the researchers decide not to disclose the vulnerability to Company D. Additionally, disclosing the vulnerability to Company D will not harm the researchers in any way, since Company D is believed to be a responsible company and the researchers are tenured professors who don't need publications to advance their careers. Therefore, the morally correct action is for the researchers to disclose the vulnerability to Company D.

(1b)

The researchers may feel a sense of duty to protect the users' rights over their personal savings, as well as the Company D's rights to know and address the vulnerability in their product. If the researchers decide to disclose the vulnerability to Company D, they will be fulfilling their duty to protect both parties rights since Company D will be able to address the vulnerability and the users will be protected from the adversaries. Moreover, if the researchers decide not to disclose the vulnerability to Company D, they will be failing to protect the users' rights to their personal savings as Company D will not be able to address the vulnerability in time to protect the users. Therefore, from a deontological perspective, the morally correct action is for the researchers to disclose the vulnerability to Company D.

(2a)

The consequentialist will weigh the harms against benefits. Disclosing the vulnerability to Company D will not only harm the researchers' reputation and ability to publish in the next three years, but also the users who will be exploited by the adversaries by 6 months. However, not disclosing the vulnerability to Company D will not cause harm to the researchers themselves, and the users will only be exploited by the adversaries for 3 months. Therefore, the morally correct action is for the researchers to not disclose the vulnerability to Company D, since this will cause less harm to the researchers and the users.

(2b)

Similar to 1b, the researchers may feel a sense of duty to protect the users' rights over their personal savings, as well as the Company D's rights to know and address the vulnerability in their product. However, even thought the researchers could protect their own rights and reduce the harm to the users by not disclosing the vulnerability to Company D, they could not form a maxim that allowed them to violate the rights of Company D and use it as means to protect themselves as well as the users' rights. Therefore, from a deontological perspective, the morally correct action is for the researchers to disclose the vulnerability to Company D.

(3)

Reference: 1. Presentation 2. Paper
Communicants: 1. Tony Zhang, 2. Sebastian Liu

Security Review: Google Docs

1 Summary

Google Docs is a web-based text editor that can be shared to collaborate with others. Users can create their Google account and log in to access Google Docs, which can be created in users' web browsers with no special software required, allowing documents stored in Google Drive. The owner of the document can share the link with others identified by their Google account by controlling their roles (viewer, commenter, editor). And each account that gets the link can interact with the document concerning their roles. The documents on Google Docs are encrypted in transit and at rest.

2 Benefits

2.1 Stakeholder: Google Docs users

Users can effortlessly create, edit, and access documents online via their browser without the need for application downloads or concerns about system compatibility. Storing documents on the cloud makes sure that users do not need to worry about local storage capacity for their files. Documents can be shared with groups, allowing members to edit and comment simultaneously or asynchronously, which makes group work a lot easier.

2.2 Stakeholder: Google (the company)

Although Google Docs is free, it is part of Google's huge ecosystem of productivity software. Increased adoption of Google Docs leads to more users for Gmail (as many of Google Docs' features require a Google account), Google Drive, Google Meet, and even Google Search, among others. Many of these products offer additional subscription-based features or generate revenue through advertising. A positive user experience with Google Docs also helps in building a good brand image, which benefits Google's long-term profitability.

3 Harms

3.1 Stakeholder: Google Docs Users

Documents stored in the cloud require reliable internet access for retrieval and updates, disproportionately affecting users in areas with poor internet infrastructure. Moreover, based on past experiences, Google Docs has a soft collaboration limit; exceeding which can result in slow performance and reliability issues, which can cause editing mistakes or conflicts. This is particularly problematic for important documents that are used as important references.

3.2 Stakeholder 2: Google (the company)

Google does not directly profit from Google Docs (as far as we know), which can consume significant storage and computing resources considering the number of users it has, especially when users create and store excessively long documents. This resource allocation decision might be a significant opportunity cost for Google, since these resources could be directed towards more directly profitable products, like expanding storage for Google Drive or Google Cloud users.

4 Assets

4.1 The contents inside the documents

Security Goal: Ensure that document access is strictly controlled: only accounts with appropriate permissions from the document owner can view, edit, or comment. Unauthorized accounts should not access the document in any capacity. In the event of a security breach, the owner or an authorized party should be able to move or delete the documents to mitigate damage. This is important for protecting potentially sensitive information stored in Google Docs, like passwords, banking details, Social Security numbers, and proprietary corporate data. Unauthorized access could lead to serious consequences, like identity theft.

4.2 User's account information

Security Goal: Make sure the account owner has exclusive access to the account information which includes login credentials, personal and payment information, document access details, etc. If an account is compromised, the account owner or authorized party should be able to lock or disable the account to reduce harm. This is important because a user's Google account gives the user access to all associated documents and services. When a user's account is compromised, all user's documents are no longer secure.

5 Threats

5.1 Impersonation

An adversary may gain access to sensitive documents by impersonating an authorized user and requesting access from the owner. For instance, in the case of documents containing a company's sensitive information, the adversary could pose as an executive and email an employee to gain access.

5.2 Phishing Attacks

An adversary could obtain a user's credentials through phishing attacks, thereby accessing the user's account information and all associated documents. For example, the adversary might impersonate Google, email a user claiming their account is compromised, prompting them to reset their password and trick the user into revealing their current credentials, which will give the adversary access to the account.

6 Weaknesses

6.1 Single Factor Authentication

The password-based user authentication method is not sufficient (Note: here we assume 2FA is not mandatory for Google Docs). Weak or overly reused passwords could allow adversaries to compromise user credentials and gain access to sensitive account information and documents.

6.2 User Misuse

A lack of awareness and misunderstanding of Google Docs' features can lead to security vulnerabilities. Users may unintentionally grant access to unauthorized individuals if they are unfamiliar with the Google Docs' access levels (view, comment, edit). Google Docs' ease of sharing might lead to accidental oversharing and related issues. For example, edit privileges may be inadvertently given to users who should only view documents. Moreover, a general lack of security awareness could make the user an easy target for phishing attacks.

7 Potential defenses

Implement multifactor authentication or passkeys as the default setting to reduce the risk of compromised passwords. When users attempt to disable this feature, display warnings about the risks associated with storing important information in Google Docs. Additionally, consider deploying a machine learning algorithm to identify unusual activity based on device and location. Send alert emails to users or temporarily limit certain actions, like file downloads or sharing access whenever abnormalities are detected. Create a brief tutorial and periodically educate users on how to securely manage documents, identify phishing attempts, and protect account information. It could also be beneficial to prompt warnings about the implications of sharing documents each time users initiate sharing (while this could be a problem for UX).

8 Risk Evaluation

In our case, the risks tied to the identified assets, threats, and vulnerabilities vary depending on the sensitivity of the documents and the significance of the user accounts. For documents with sensitive data and accounts holding many such documents, the risks are higher because of the greater potential gains for attackers, which could raise serious concerns about identity theft, unauthorized access to confidential company information, data breaches, etc. However, for users who, for example, create a new Google account just to practice typing with nonsensical information, the risks are low. Nevertheless, from the perspective of Google Docs developers, it's important to prepare for the worst case scenario and have the highest security standards. The effectiveness of defenses in mitigating these risks largely relies on their correct implementation and users following recommended security measures.

9 Conclusion

Google Docs, as it is today, has many benefits in terms of collaboration, accessibility, and productivity, while having robust security measures to protect user data and documents. However, overcoming the challenges of phishing attacks and feature misuse is a delicate dance between enhancing security and maintaining a good user experience. For example, enforcing multifactor authentication or passkeys and educating users about secure practices, can significantly reduce the risks. Yet, these measures introduce additional steps for users and jeopardize user experiences. In essence, Google has to keep on improving its product to make sure users have good experiences overall and their safety online when they're using Google Docs. Adopting and maturing new security frameworks to keep users using Google products safely will also expand Google's competitive advantage and gain users' trust.