CS/Analytics Breakout Assignment 5
Due: Oct. 25
To be done only by CS and Analytics majors

There are many communication apps that promise absolute privacy for their users, but Signal and Telegram stand out as leaders in the field. Within the past year the security of both applications has been called into question. It has been alleged that Signal has a security flaw and that the security of Telegram has been compromised since the arrest of one of its founders.

For this assignment, you are to find at least two recent (within the past year) articles (for each app, so minimum 4 articles total) describing the issues leading people to question these app's security and the response to the issues. You are to summarize the issues and responses for each app (separately) and provide clickable links to the articles.

I expect this assignment to be 1-2 pages long and reference at least 4 articles.

Assignment Follows on Next Page

Telegram and Signal are two popular messaging platforms that have become wildly popular in recent years for their data policies and the security they boast. In recent years, however, the security of both applications has been called into question. This short paper will examine the issues that have arisen with both apps, and the response to those issues that have been taken by each company.

After the CEO, Pavel Durov, of Telegram was arrested at the end of august this year, several issues and concerns have been brought forth about the application. The first main issue that has arisen is that end to end encryption is not enabled by default. This means that data is encrypted during the transmission of the message to another person but is not encrypted on Telegram's servers. The server side code is also completely in house so outside individuals are not able to analyze what is being done with data. Additionally, it's stated in each article about Telegram that metadata is another issue as this data can still be collected even if the end user has enabled end to end encryption.

Another main issue that has been brought to light about Telegram is a large amount of illegal activities are being carried out on the app and not much is being done to combat it. Most notably it is cited that these activities include, "selling stolen data, distributing malware, and engaging in hacktivism." This has led to further issues being brought forth about Telegram's lack of moderation, and their unwillingness to work with law authorities. Telegram will often process reports on public content, and remove it if it breaks their terms of service, however, its noted that "private chats" are often where illegal activities occur and is an unmoderated feature of the application.

Shortly after the arrest of the CEO, Telegram went on in response to claim that their privacy standards were equivalent to many other applications and conformed with European law where the CEO was arrested. Telegram also added to their FAQ page how people can report content for removal. Many individuals do not believe this response was good enough and the illegal activities will continue to occur on the platform.

Signal is another online messaging platform used by many, but has recently come into the light with reports of a major security flaw in its design. By design Signal stores a local text file to a user's device which holds the encryption key for all their messages. Since this file is stored locally, anyone with access to the device, or a hacker with access to the device, can easily access this key and make all encryption done by signal completely useless. The issue was first reported in 2018, but was swept under the rug by Signal, until Elon Musk recently made a Tweet about the issue.

In response to both occasions of the issue being brought up, Signal has committed to fixing the issue. The change was largely due to the influence of Musk's tweet gaining lots of traction and the company coming under fire because of it. Signal plans to fix the issue by implementing the "Electron safeStorage API" which will allow the OS of the device to encrypt the key and add another layer of protection to the security of peoples messages.

Both Telegram and Signal have seen issues in the past few years, and both have taken a response to this in some way. The response from Telegram might not end up being enough to stop some or any of the activities on the platform, and the response from Signal took considerable time to occur from the initial reporting of the major security flaw which may be indication of how future incidents could be handled. As future issues arise, we can only hope that each company will learn from these issues and their responses, and provide better transparency in the future.

Telegram Sources

https://spectrum.ieee.org/telegram-security

https://www.techtarget.com/searchsecurity/feature/Infosec-experts-detail-widespread-Telegram-abuse

Signal Sources

https://www.bleepingcomputer.com/news/security/signal-downplays-encryption-key-flaw-fixes-it-after-x-drama/

https://gizmodo.com/signal-is-working-to-close-a-security-vulnerability-in-its-desktop-app-2000469908