Usability Seminar

Azer Hojlas

February 2, 2023

Chosen articles and main insights

The articles that I have selected to discuss during the seminar are the two listed ones (which are referenced at the bottom of the document) that relate to system administration and the necessity of updating software. Starting with the first article (Security, Availability, and Multiple Information Sources), I will make an account of the main insights that I received while reading the paper:

- Company size matters:
  Larger companies and bigger organisations tend to have formalized protocols for making updates, as well as a higher degree of process automatisation. These organisations however also tend to be more centralised, where system administrators require clearance from higher ups before they are allowed to proceed with updates, i.e precious time is wasted. Furthermore, larger systems can be more negatively affected if a small cog (brought about by the update) suddenly becomes incompatible.

- Third party software:
  In the case of large-scale systems, keeping track of the different software solutions that the organisation uses is difficult without the use of some third party tool that keeps track of updates and informs the administrator of the potential benefits of the update. These tools are great for improving the situational awareness (related to system security) of system administrators.

The following is an account of the main points derived from reading the second paper, Keepers of the Machines: Examining How System Administrators Manage Software Updates:

- System administrator update process:
  Regardless of organisation structure and size, most system administrators follow the same process for updating software. These are (1) Learning about updates, (2) Deciding if the update is worth the deployment risk based on a cost-benefit analysis, (3) Preparing for updates by making backups and configuring machines and installing dependencies, (4) deploying updates and (5) handling post-update issues that might arise.

- Biggest hurdles are aforementioned steps (1) and (2)
  The article states, through a number of suggestions, that organisations should reduce the burden of update information retrieval and decision-making in order to achieve faster update deployment times by administrators. The end result would equate to more secure systems.

Chosen technology and application of insights

My technology of choice is a service that provides encrypted emails, a service called Proton Mail, which uses encryption to protect email communications. The main use of this technology is that it prevents malicious parties from reading said emails, even when intercepted. In a simplified manner, it works through client-side encryption (as opposed to gmail), i.e a user sends an encrypted mail that can only be decrypted with the recipients private key, meaning that only they can decrypt and read the mail. The following points make an account for the aforementioned article insights when applied to proton mail:

- Little need for updates:
  As is the case with most such simple and closed-end technologies, there is little need for serious updates, especially regarding the security kind as the intended outcome of proton mail is confidentiality and integrity, i.e security.

- Clashes with company objectives:
  Large companies tend to want to be able to sometimes monitor employee emails and as such, using Proton Mail might not be the ideal solution.

- Technology size:
  As we are dealing with such a small service there is no considerable cost of conducting update information retrieval, as the updates of such services are rarely security-related in nature. Most often then not, they are cosmetic. Choosing to update Proton or not is therefore an easy straightforward decision. As such, update information retrieval is not such a big hurdle as has been previously described, i.e time spent in the aforementioned steps (1) and (2) are negligent.

- Easily integrated with third party tools:
  Due to the aforementioned small size, Proton migh not be considered a prioritized candidate to keep track of in third party update applications. However, if there was a need to do so, simply acknowledging (logging) an email that states that an update is necessary is enough for said third party application to gather information about a potential proton update.

References

Tiefenau, C. Häring, M. Krombholz, K. Zezschwitz, E. (2020). Security, Availability, and Multiple Information Sources: Exploring Update Behavior of System Administrators. USENIX

Li, F. Rogers, L. Mathur, A. Malkin, N. Chetty, M. (2019). Keepers of the Machines: Examining How System Administrators Manage Software Updates. USENIX