Ethics of Security

The idea of responsible disclosure is highlighted in research articles 1 and 2 which describe it as: “[1] researchers who uncover a flaw don't go public until the system's developer has had a chance to fix it”. This is of note as this not only provides the developer’s with time to patch their system, but also to prevent the public from losing trust in said system. Responsible disclosure is a “[1] community accepted” protocol, so while it may not be mandatory for researchers and developers to follow through, it is in the best interest of most companies to align themselves by it.

A growing ethical concern is the phenomenon of social networks. With the group project being involved with music apps, which are commonly linked to users’ social media accounts, this is of important note. The issue comes in the place of a lack of “[1] central command” which is compounded by anonymity, as well as virtual/multiple personalities. This brings in a wide range or social and ethical issues with the use of social networking, examples of this being cyberbullying, cyberstalking, and cyber-harassment. According to a survey taken by i-SAFE, more than 53% of children admit to having been abusive over the internet, with 42% having admitted to being victims of said abuse [4]. In addition to this, the use of social networking has led to internet addiction being a clinical disorder. Users that are extroverted/unselfconscious, shy, or narcissistic [3] tend to have higher usages of social networking applications.