Proposal to Write About Whether Security Problems Should Always Be Publicly Disclosed

Over the past two decades, software has become a very integral part of our lives and it is going to be embedded into them a lot more in the future. However, with software, there will always be the issue of safety and security, no matter how important or seemingly unimportant that software is. This issue will always exist. This existence leads us to wonder if security problems should always be disclosed publicly. This is a question that needs a lot of research and depends on many variables. On one hand, public disclosure of security problems might result in a solution from a third party; however, it can be very damaging to the organization by diminishing the trust of its clients, for instance. Public disclosure of security problems can cause havoc which can be even more detrimental to the clients and the organization. When it comes to public disclosure of security problems, a decision can literally change people's lives: clients, employees, and employers. On the other hand, solving security problems without public disclosure makes the organization avoid many problems that it might face in the case of public disclosure. However, if the problem that has been solved were to be proven to exist, the trust of the clients will be diminished. One thing to think about, if a problem is not disclosed publicly, is do we want to put a deadline to solve it before public disclosure. If so, how long from now? Public disclosure of security problems is a very sensitive and influential decision.

The previous paragraph has been inspired by the referenced technical paper.[i]

[i] Anbalagan, Prasanth. *A Study of Software Security Problem Disclosure, Correction and Patching Processes*, North Carolina State University, Ann Arbor, 2011. *ProQuest*, https://login.proxy.hil.unb.ca/login?url=https://www.proquest.com/dissertations-theses/study-software-security-problem-disclosure/docview/881634816/se-2.