Samuel Mouradian
CS 446 – Section 1001
Professor – Papachristos
Assignment Due Date – 12/10/2024

Homework 6

1. What is the responsibility of an OS vendor/distributor in the cases where significant hardware flaws are discovered? What if their product is especially affected when compared to other competitors? What role do you believe an OS software engineer (OS developer/employee/manager) has to play in such a circumstance?

   Should a hardware flaw be discovered, it is the responsibility of an OS vendor/distributor to report the issue to appropriate parties. According to section 2.5 in the *ACM Code of Ethics and Professional Conduct* [I], the system should not be deployed if there is a potential issue – or, the system should be continuously reviewed for risk as the system evolves with use over time.

   If a product will be affected by another competitor's, it is required by professionals to "create opportunities for members of the organization or group to grow as professionals", as detailed in section 3.5 of the *ACM Code of Ethics and Professional Conduct* [I].

   Take the Spectre security vulnerability [II], for example. Since OS developers overlooked the potential issues regarding speculative execution, this caused attackers to gain private information when users interacted with their systems. To fix this issue, software engineers who follow the code of ethics and professional conduct need to contact government officials, as well as OS vendors/distributors about these issues. Furthermore, it is on the developers of those operating systems to innovate their implemented systems in a way that fixes the issue, as well as maintains the public's security.

2. What is the responsibility of an OS vendor/distributor when their platform is exploited (unspecified whether knowingly or not) to launch industry attacks that may jeopardize more than just financial assets? What is the role of the OS engineer?

   It is stated in sections 1.1, 1.2, 2.2, 2.9, 3.1, 3.7, and 4.2 within the *ACM Code of Ethics and Professional Conduct* [I] that the OS vendor/distributor must adhere to the code, and to put public security and usage as the priority of any software design. The role of the OS engineer is to improve the security and usage of the system by everyone, which could potentially mean they must retire the system if its use is not adhering to the code.

3. What is the responsibility of an OS vendor/distributor with respect to safeguarding privacy? If your answer is situation-specific, elaborate. What is the role of the OS engineer? What concerns do you have regarding whether the OS and its safety features are proprietary or open source?

   The responsibility of an OS vendor/distributor is to honor confidentiality and privacy, as stated in Sections 1.6 and 1.7 of the *ACM Code of Ethics and Professional Conduct* [I]. As for the role of the OS engineer, their responsibilities lie in ensuring a system that has been integrated into society is innovated and protected by the code they design. That means systems must be constantly scrutinized for potential risks, regardless if they are currently being used by the public or are about to be retired.

   Some concerns I personally have is when safety features aren't properly implemented in a system, regardless if they are proprietary or open source. The Meltdown security vulnerability [III], for example, had the capability to bypass privilege checks within a system, therefore allowing the attacker to view private information. This failure on the developer's end, whether the Meltdown design was open source or not, could have allowed for a failure in public privacy and confidentiality, should the security vulnerability have been found and used by attackers.

4. What do you believe are the ethics-related questions and principles that apply to an OS-development engineer, from the single-feature development roles, all the way to high-level management? Describe a form of integration between these levels that you believe is long-term sustainable.

   Some ethics related questions I have in mind that, I feel, apply to all levels of OS-development/management reflect the *ACM Code of Ethics and Professional Conduct* [I], one being: how can this benefit the general public? Another question I often ask revolves around team communication and management. Simply put, how will the team support one another with a level of respect and professionalism that not only brings innovation to implemented systems, but innovation to teamwork and the ethical codes all developers, vendors, and distributors follow.

   In short, presence and transparency between all levels of development and management will not only mitigate the risk of overlooking security issues within a system but will also parallel the kind of actions the code of ethics and professional conduct require from all its members.

Works Cited

I. Code of Ethics and Professional Conducts: https://www.acm.org/code-of-ethics#h-2.5-give-comprehensive-and-thorough-evaluations-of-computer-systems-and-their-impacts,-including-analysis-of-possible-risks.

II. Spectre (security vulnerability) Wikipedia Document: https://en.wikipedia.org/wiki/Spectre_(security_vulnerability)

III. Meltdown (security vulnerability) Wikipedia Document: https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)