Yuqing Zhai

10/30/2024

In July 2024, CrowdStrike pushed an update to their security suite called Falcon Sensor, which resulted in the shutdown of millions of computers. [1, 2, 3, 4] This essay will analyze the risk involved in Falcon Sensor by Sommerville's Risk Triangle and how CrowdStrike failed to mitigate such risks. It will argue that CrowdStrike violates ACM Code Ethics using rule utilitarian ethics.

To provide more context, on July 18th, 2024, CrowdStrike released a flawed updated configuration file to their Falcon Sensor. This flawed configuration file triggered a kernel panic in the operating system, resulting in repeated reboots with blue screens. To detect potential security vulnerabilities, the Falcon Sensor has to be run at the kernel level, the same level as other core components of Windows, and that is the reason why this error cannot be recovered by Windows itself—this complete shutdown of millions of computers disrupted transportation, commerce, emergency services, and medical facilities. [1, 2, 3, 4]

Sommervilles' Risk Triangle categorizes risk into three categories: Acceptable, As low as reasonably practical (ALARP), and Intolerable. As we have seen from the consequences, a single failure in Falcon Sensor could result in a shutdown of millions of computers. While some of the computers are used in transportation and commerce, a shutdown of them is still tolerable, the shutdown of computers used for medical facilities or 911 services [1] is certainly **intolerable**, as that could cause potential death. Therefore, the risk is associated with Falcon Sensor in the Intolerable region.

As any person with minimal understanding of software knowledge, we could probably imagine a simple solution that could prevent such an accident. Since this shutdown happened to every computer, if they have run some internal testing, there is a high chance that it could catch the problem before releasing the update. As some media noted, CrowdStrike might have done some internal testing, but maybe they released the update problematically, which resulted in the accident. [1] Yet, an evident solution could be provided. They could have made the update in batches at different times, which could have made them detect the problem earlier. Also, from the media, we know that Microsoft has a policy where software like Falcon Sensor must be tested in their lab before release, but CrowdStrike has dynamic configuration files that are independent of the software. These files could dynamically change the behavior of their software, essentially bypassing Microsoft's policy. This might make CrowdStrike quickly respond to zero-day attacks, yet it makes their update process more prone to unintended mistakes. Moreover, Windows has its protection mechanism, which will unload the software that triggers a system error when rebooted, but Falcon registers itself as a "boot driver", essentially invalidating this mechanism. [4] From all these

analyses, **we could see that CrowdStrike failed to design a safe product**, even if it had good intentions to do so.

As an afterthought, it seems obvious that there are intolerable consequences associated with such accidents, and it is questionable why CrowdStrike failed to identify these risks. As a security company who have large market share, it is reasonable to assume that they have the expertise to understand the widespread usage of its product and the potential risk associated with it. On the other hand, as noted by multiple media, when sued by Delta, CrowdStrike shifted the problem to Delta rather than their own product. [6] From their response to Delta, we could see the mindset of blaming others and shifting the responsibilities in the company. It is reasonable to suspect that considering that the operating system security involves many entities (**problem of many hands**), they might think they could probably shift their legal liability and moral responsibility to Microsoft or to the end user like Delta in this case, and this mindset made them become negligent and careless in accessing the risk in their standard development process which eventually backfires. **CrowdStrike probably has developed a negligent mindset in the "problem of many hands" of the security industry**, which eventually resulted in their flaws in the risk analysis.

ACM's code of ethics specifies the code of conduct that every computing specialist should adhere to. Rule-based utilitarian ethics argues that we should follow a fixed set of rules that maximize utility (happiness). Using utilitarian ethics, we could see why these ACM code ethics make sense, and why CrowdStrike failed several of them. In sections 2 and 3, ACM code ethics mentioned that "Design and implement systems that are robustly and usably secure" and "Recognize and take special care of systems that become integrated into the infrastructure of society", [5] from the disastrous consequences that happened in few weeks after that notorious update from CrowdStrike, it should be self-evident that failure to adhere rules resulted in huge negative consequences, and therefore we should follow such ACM code. As we see that Falcon Sensor has been shipped into so many industries in our society, **it is evident that not only CrowdStrike failed to robust system, but also failed to take special care of software integrated into the infrastructure of the society.**

Reference

[1]

Newman, L. H., Burgess, M., Greenberg, A. (2024, July 19). How One Bad CrowdStrike Update Crashed the World's Computers. *Wired*. https://www.wired.com/story/crowdstrike-outage-update-windows/

[2]

Davis, W., (2024, July 20). CrowdStrike's faulty update crashed 8.5 million Windows devices, says Microsoft. *The Verge*. https://www.theverge.com/2024/7/20/24202527/crowdstrike-microsoft-windows-bsod-outage

[3]

Roth. E., (2024, July 19). What is CrowdStrike, and what happened? *The Verge*. https://www.theverge.com/2024/7/19/24201864/crowdstrike-outage-explained-microsoft-windows-bsod

[4]

Dave, (2024, July 21). CrowdStrike IT Outage Explained by a Windows Developer?. *YouTube*. https://www.youtube.com/watch?v=wAzEJxOo1ts

[5]

Association for Computing Machinery. (2024, October 30). Code of Ethics. https://www.acm.org/code-of-ethics

[6]

Sato, M., (2024, July 19). CrowdStrike and Microsoft: all the latest news on the global IT outage. *The Verge*. https://www.theverge.com/24201803/crowdstrike-microsoft-it-global-outage-airlines-banking