Determinism within Cybersecurity & Computer Hacking

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 201S: Cybersecurity & Social Science, Professor Trinity Woodbury

February 3, 2025

Discussion Board Topic #2, Assignment Question:

How does the principle of determinism relate to computer hacking?

Definition: Computer Hacking

Computer hacking is, “whoever willfully and knowingly with the intent to defraud, access a protected computer without authorization, or exceeds authorized access and by means of such conduct furthers the intended fraud and obtains anything of value” (Legal, 2024).

What is determinism?

Determinism, in philosophy, argues that all events—including human thoughts, decisions, and actions—are "preordained" or "premeditated." It suggests that human behavior is causally predictable, inevitable, and dictated by prior events and external conditions beyond an individual's free will. As the University of Stanford Department of Philosophy (2023) explains, determinism is "the idea that every event is necessitated by antecedent events and conditions together with the laws of nature," much like executing a linear computer program or web browser script. This perspective implies that computer hackers' motivations, knowledge, skills, and external influences, including childhood upbringing or socio-economic status, shape their actions. For example, suppose security teams gather sufficient information about a hacker's behavior, routines, and mannerisms. In that case, they can use this knowledge to strengthen network defenses, anticipate future threats, and potentially track the hacker's location.

One’s past does not absolutely dictate the future.

Determinism does not necessarily preclude free will, individual responsibility, or accountability (Carneades.org, 2021). It does not serve as a justification for illegal activities such as computer hacking. While internal and external influences may shape decisions, the choice to engage in unlawful computer hacking remains intentional. Hackers may face duress or threats from more powerful, nefarious forces compelling them to continue their activities. However, such pressures do not eliminate free will like deterministic computer programs or natural laws do (i.e., gravity or Newton's Laws of Motion).

Philosopher Hans-Georg Gadamer, in his work on hermeneutics, argues that prejudices (in the neutral sense) or prior knowledge are essential sources of understanding. They shape beliefs,

claims, and actions but do not eliminate the freedom to decide how they are applied (Malpas, 2022). We cannot function without these preconceptions; however, their application determines whether they lead to right or wrong, good or evil, usefulness or harm. Thus, computer hacking—particularly by "Black Hat" hackers—is a deliberate and premeditated act that violates universal societal principles, including privacy, security, and the integrity of computer networks and data.

How does determinism assist with understanding and fortifying cybersecurity by preventing computer hacking?

Systems are typically deterministic, meaning they operate based on programs or algorithms that produce the same output when given the same input, consistently following the same sequence of states. However, some systems are non-deterministic, generating different outputs or state sequences from identical inputs due to factors such as randomization or multithreading. However, even randomness follows a form of determinism, as it operates within a predefined set of possibilities within a given environment. Examples include "Choose Your Own Adventure" books from brands like Goosebumps or role-playing video games such as Baldur's Gate 3 and World of Warcraft.

When a security team has sufficient knowledge of a network system—how it functions and where its vulnerabilities lie—it can predict a hacker's behavior with a certain degree of accuracy. By reducing vulnerabilities, such as closing unnecessary open ports, the team can "shore up" access points, making it easier to anticipate where and when an attack might occur. Honeypots serve as both a defensive tool and a way to study hacker behavior within a closely monitored proxy network.

However, hackers can apply the same deterministic approach when attempting unauthorized access. For instance, they may analyze recent CVE reports to exploit newly patched software vulnerabilities before updating systems. Additionally, by reverse-engineering patches, hackers can uncover core software structures, backend code, and weaknesses, targeting similar programs and anticipating future vulnerabilities in upcoming software updates.

Conclusion

While determinism can provide insight into the factors contributing to someone becoming a hacker, it does not justify or condone the illegal and unethical nature. It is important to focus on prevention, education, and promoting ethical behavior in cybersecurity.

References

Carneades.org. (2021, March 7). *What is Determinism? (Free Will)*. Retrieved from Youtube: https://www.youtube.com/watch?v=cXWmgcXaHAI

Legal, U. (2024, June 18). *Computer Hacking Law and Legal Definition*. Retrieved from US Legal: https://definitions.uslegal.com/c/computer-hacking/

Malpas, J. (2022, August 22). *Hans-Georg Gadamer*. Retrieved from The Stanford Encyclopedia of Philosophy: https://plato.stanford.edu/entries/gadamer/

Stanford, U. o. (2023, September 21). *Casual Determinism*. (D. o. Philosophy, Producer) Retrieved from Stanford Encylopedia of Philosophy: https://plato.stanford.edu/entries/determinism-causal/