Absolute Security *does not* Exist

Some people believe that absolute security is possible, using advanced technologies such as embedded solutions, one-time pad, or quantum tech. However, such a view is unrealistic and ignores the human factor, the complexity of systems, and the unpredictability of threats. Absolute security does not exist, because there is always a trade-off between security and usability, a possibility of human error or malicious insider, and a risk of unknown vulnerabilities or zero-day attacks[3]. **Security is continuous process, not a final state.**

Achieving absolute security has been a longstanding and contentious topic. This paper delves into the contrasting perspectives on this matter, scrutinizing the arguments both in favor of and against absolute security.

Pursuit of Absolute Security: Proponents of absolute security argue that through advanced technologies and stringent protocols, it is possible to create systems impervious to unauthorized access. This viewpoint relies on the assumption that a combination of cutting-edge encryption algorithms and robust defenses can lead to an invulnerable state.

The Inherent Fallacy: Absolute Security as an unattainable Ideal. The dynamic nature of threats and the continual evolution of malicious tactics make achieving complete security an elusive goal.

Example: An illustrative example of the fallacy of absolute security is found in the concept of the one-time pad (OTP). While celebrated for its theoretical security, the OTP is not immune to practical challenges. Its effectiveness hinges on assumptions regarding the secrecy of the key and the impossibility of repetition. However, maintaining absolute key secrecy is a formidable task, and the logistical challenges of securely generating and distributing truly random keys on a large scale opens many opportunities of attack.

The discussion about absolute security is like finding a balance between what we dream about and what's really possible. The above example teaches us that even the best security ideas can have challenges. In the world of keeping things safe online, it's important to understand these hidden assumptions. So, while we dream of perfect security, we need to be practical. As technology gets better, and new threats come up, the best way to stay safe is to understand weakness of our tools. Perfect security might be a dream, but security risk management is indeed pragmatic way of doing business.

The more you seek it, the more you lose it. The only way to be secure is to be aware, and pursue the path of risk management.

Ji-Won (지원) is a cryptography researcher and volunteer in PakCrypt outreach program.