K

Kerckhoffs' Principle

Fabien A. P. Petitcolas
Smals Research, Brussels, Belgium

Synonyms

Kerckhoffs' law; Shannon's maxim

Definition

Kerckhoffs' Principle states that the security of a cryptosystem must lie in the choice of its keys only; everything else (including the algorithm itself) should be considered public knowledge.

Background

Dr. August Kerckhoffs, a Dutch linguist trained at the University of Liège, became a professor at *École des Hautes Études Commerciales* in Paris, where he taught German. He was also a keen supporter of volapük, a constructed language. His strong interest in cryptography led him to publish in 1883 an article entitled *La Cryptographie Militaire* ("Military Cryptography") in which he surveyed the state of the art in cryptography and proposed six fundamental principles for any cryptosystem alongside rules of the thumb and general practical advice. At the time, the main goal of cryptographers was to set up a secure telegraphic system.

The six principles enunciated by Kerckhoffs are as follows:

1. The system must be substantially, if not mathematically, undecipherable.
2. The system must not require secrecy and can be stolen by the enemy without causing trouble (what is nowadays referred to as Kerckhoffs' Principle).
3. It must be easy to communicate and remember the keys without requiring written notes, and it must also be easy to change or modify the keys with different participants.
4. The system ought to be compatible with telegraph communication.
5. The system must be portable, and its handling or usage must not require more than one person.
6. Finally, considering the circumstances in which such system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.

The second and third principles can be interpreted more generally: in any security system, a secret is a potential source of breakage and should therefore be kept to a minimum and should be easily replaceable.

Later Shannon established a theoretical basis for the understanding of cryptosystems and proposed this other formulation: "the enemy knows the system," known as Shannon's maxim.

S. Jajodia et al. (eds.), *Encyclopedia of Cryptography, Security and Privacy*,
https://doi.org/10.1007/978-3-642-27739-9_487-2

Kerckhoffs' Principle and Shannon's maxim are in sharp contrast with "security through obscurity" and remain one of the main design principles of modern cryptosystems.

Cross-References

- ▶ Cryptosystem Security
- ▶ Security Through Obscurity

Recommended Reading

Caraco J-C, Géraud-Stewart R, Naccache D (2020) Kerckhoffs' legacy, Cryptology ePrint archive, Report 2020/556. https://eprint.iacr.org/2020/556

Kahn D (1996) The codebreakers: the comprehensive history of secret communication from ancient times to the internet, chapter 8. Scribner, New York. ISBN 0684831309

Kerckhoffs A (1883) La cryptographie militaire. J Sci Mil IX:5–38 and IX:161–191. http://www.petitcolas.net/kerckhoffs/