Arnav Surve

CNIT 270

02/09/23

Kerckhoff’s Principle

According to Kerckhoff’s principle, a cryptosystem should be secure even if every aspect of the system is public knowledge. In other words, a system should be secure even if an attacker has complete knowledge of the system. Security by obscurity is an implementation of security that focuses on confidentiality of the system’s inner details. It relies on concealing any security flaws in the hope that they are not found by malicious actors. This contrasts with Kerckhoff’s principle, as it relies on keeping information of a system secret instead of relying on the strength of the system and its protocols to keep it secure.

Given Kerckhoff’s principle, security by obscurity is bound to fail because it relies on the hope that attackers won’t eventually discover and exploit hidden vulnerabilities. This is flawed, as given enough time and resources hackers are bound to find vulnerabilities through enumeration. As a result, any security measures taken through security by obscurity are rendered useless in the long run.