CMSC389R Week 10 Alternative Essay

Kerckhoffs’ Principle vs. Security through Obscurity and Moving Target Defense

Auguste Kerckhoffs wrote in 1883 two articles in a french cryptographic journal dictating six principles under which military ciphers should operate. While the bulk of the principles are outdated or irrelevant to modern cryptography, the second of these is an axiom by which modern systems are developed. This principle said that a cipher shouldn’t create problems by falling into enemy hands. In modern terms, a system or cipher’s code should be treated as public knowledge, with private keys being the main point of failure if leaked. This makes it easier to adjust after a breach or leak, since keys are easier to change than a full system. Hash algorithms operate under this principle, with source code publicly available but private keys are protected by the mathematical difficulty of prime factorizations.

By contrast, security through obscurity relies uses the secrecy of a system to provide security. The enigma machines used in WW2 are an example, where the machines remained fully secure from 1926 to December 1932 when Marian Rejewski broke the message keys. However, while he was able to figure out the patterns in the keys through analysis of the cipher permutations in November 1932, it wasn’t until December when the French military intelligence leaked message keys that the wirings of the rotors within the enigma were solved, and the enigma machine (mostly) compromised.

Although security through obscurity has mostly been discredited as a primary design axiom, modern “moving target defense” works on similar principles. The broad concept is to mutate code over time in order to move potential vulnerabilities around within the system, limiting the amount of time that any given vulnerability can be exploited. While modern systems are in effect vulnerable inversely proportional to computational power, (see the evolution of hash algorithms over time), moving target defense provides a novel workaround for defending against brute force attacks.