Deprecation of Vulnerable Encryption Standards

Behind every authentication, online purchase, and email sent to and from your boss, cryptography algorithms are working in the background to secure your information. Data Encryption Standard (DES) has a long history in cryptography advancement from peer review to finding a secure encryption standard for government documents, to furthering education in the field of cybersecurity, but DES is no longer secure. The encryption algorithm’s short key length makes it an easier algorithm to decrypt, thus leaving information open to attack. This paper will be addressing and summarizing why DES is no longer being used, how DES is being deprecated, how successful the deprecation of DES has been, and where the future of algorithmic encryption will be heading to compensate for the loss of readily used standards for encryption protocols.

In need of a reputable guideline for cybersecurity standards, I looked to the world leading institute for creating encryption standards in technology, The National Institute of Standards and Technology (NIST). The National Institute of Standards and Technology (NIST) shares and creates publications from their Information Technology Laboratory in an effort to educate and preserve the cybersecurity industry. There’s been an endeavor to transition encryption algorithms over smoothly through notices of when DES will further be disallowed from protocols such as TLSS, IPsec. NIST’s publications and published guidelines, frameworks, and updates are the only information I could find to effectively move to a more secure encryption algorithm. Although, this transition can take up to a decade at a time and there is lacking research on what is most effective for an encryption protocol change. Understanding a more effective way to transition encryption algorithms and keep up to date on standards in cryptography can help lower the time it takes for new encryption algorithms to come into succession so that your boss won’t be subject to attack.