Ryan Ponstein

Dr. Walter Schilling

SE-4930 –Secure Software Development

14 December 2011

Article Review #1: The First 10 Years of Advanced Encryption

In October 2000, after a three-year study period, the United State National Insitiute of Standards and Technology (NIST) announced that the block cipher Rijndael would become the Advanced Encryption Standard (AES). The article, "The First 10 Years of Advanced Encryption", discusses the design of Rijndael, the block cipher's advantages and disadvantages, and its acceptance across the world as the AES. It also explains the importance of having the AES. The article was written by Joan Daeman, a cryptographer at STMicroelectronics, and Vincent Rijmen, a professor in the Electrical Engineering Department of the University of Leuven (Katholieke Universiteit Leuven), in the November/December 2010 issue of IEEE Security and Privacy.

Block ciphers belong to the field of symmetric cryptography, which has existed for thousands of years. The authors explain that Rijndael was designed as a key-iterated cipher $S[k_i](x) = S(x) + k_i$, with + denoting the addition over GF(256) (the Galois field of 256 elements). Rijndael's design philosophy focused on three main principles: simplicity, performance, and well-understood components. According to the authors, Rijndael's strong point was its simplicity, as the algorithm is easily understood and implemented efficiently. It also "facilitates understanding the mechanisms that give the algorithm its high resistance against differential cryptanalysis and linear cryptanalysis, to date the most important general methods of cryptanalysis in symmetric cryptography." The short-comings of Rijndael include the finite-field

operations which appeal to mathematically oriented minds, but can be a burden for programmers. In addition, the mapping from finite-field elements to bit strings utilizes a suboptimal basis, which makes the substitution more costly in hardware than is strictly necessary. In the article, the authors also address how many standards and commercially available products have adopted AES, and researchers are adopting its strategy to design hash functions and other cryptographic primitives both here, in the United States, and internationally. Over the years, AES researchers have analyzed both statistical and algebraic attacks to break through the encryption. The results pointed out both weakness in the AES key schedule and strength in the related-key attack model.

Through reading this article, I learned of the importance of cryptology in developing secure software. As the Advanced Encryption Standard, a review of Rijndael is helpful in understanding the role of encryption in software development and its relation to data confidentiality, data integrity, and authentication. The authors expect that AES will "proliferate further and will replace DES and 3DES in products, designs, and cryptography textbooks." This summarizes the importance of having background knowledge of Rijndael and the progression of advanced encryption.