Title: A Novel Approach to the Tokenization of Credit Card Numbers

Bart Preneel, COSIC, Katholieke Universiteit Leuven, Belgium,
Bart.Preneel@esat.kuleuven.be
Ulf Mattsson, Protegrity, USA, ulf.mattsson@protegrity.com

Abstract

Encryption techniques are used to ensure the confidentiality of sensitive data. They are typically defined as mappings on bitstrings; they can be defined as a mode of operation of a block cipher (a keyed random permutation on strings of 64 or 128 bits) or based on a stream cipher (that typically operates at the level of bits, bytes or 32-bit words). In order to satisfy strict security definitions, encryption schemes need to be randomized, which means that the ciphertext is larger than the plaintext. For some applications, such as the protection of credit card numbers in certain contexts, both constraints are undesirable: the plaintext space consists of digits rather than bits and the mapping from plaintext to ciphertext has to be a permutation, hence there is no room for randomization. The encryption operation is also called *tokenization*. It is definitely possible to define a secure tokenization based on a block cipher such as triple-DES or AES. In this submission, we present a completely new approach, in which a highly efficient block cipher is designed from scratch by using S-boxes defined on strings of n digits (n is typically 5 to 7), that can be interpreted as large keys. We will show that if the number of plaintexts encrypted with a single key is limited, a very high security level can be obtained using this approach. It can be proven that under realistic constraints, the security of the scheme is equal to an "ideal" tokenization scheme.