Virtual
Software
Systems

Kaleidoscope Abstract and Characteristics

Kaleidoscope Abstract:

Kaleidoscope (K) is a probabilistic state, injected entropy, stream cipher. It is a novel algorithm, like its namesake, it constantly “shape-shifts” i.e. changes its operating characteristics, alters its footprint, and injects entropy to deny a solid foothold to any attacker. It has potentially quantum resistant properties that provide secrecy, continuous authentication, and message integrity. K can improve and extend the life of existing ciphers, enhance the security of other communication channels (e.g. VPNs), and be adapted to meet specific mission requirements.

Kaleidoscope takes plaintext, pre-processes it with the K-Engine into extended-ciphertext then encrypts the extended-ciphertext into channel-ciphertext for transmission. It manages the creation and use of dynamic keys through state synchronization. The extended-ciphertext is comprised of both commands and data that increase entropy and change the state of the K-secure channel that it creates.

During each processing cycle, the K encoder *dynamically and randomly changes* its own operating characteristics, data structures, and other parameters of the K-Secure channel. The K decoder automatically synchronizes with the K encoder. Changes can include swapping encryption algorithms on the fly, altering the cipher’s mode or its inputs (e.g. key, Initialization Vector), and continually adding entropy.

The K-Engine can be shaped to meet specific mission needs through the addition of custom operations and commands without impacting the K cipher operation.

©2020 Virtual Software Systems, Inc.

Kaleidoscope Paper: A paper describing the details of its operation, "**Kaleidoscope: A Probabilistic State, Injected Entropy, Stream Cipher"**, is available under mutual NDA. The purpose of the paper is to provide a starting point for further discussion. Topics such as provisioning, implementation, properties, features, and potential benefits are presented. User benefits will vary based upon each user's objectives and their implementation of the algorithm. They are therefore best discussed in the context of the user's specific needs.

Early versions of the algorithm have been reviewed positively by US Government and academic experts. The intent of the paper is to seek input and feedback based on your requirements and your thoughts about the potential benefits you might realize from these inherent features and characteristics of the Kaleidoscope technology. The primary architectural themes, prominent features, and characteristics are briefly outlined below.

Features and Characteristics:

- **Quantum Resistance:**
  We have been told by those associated with the fields of quantum physics and cryptography that K's non-number theoretic approach should provide quantum resistant properties.
- **Dynamic Probabilistic Encryption:**
  K implements probabilistic encryption, including not only multiple alphabets, but also the ability to change and create alphabets dynamically as well as providing the ability to select or create cipher alphabets randomly at or during runtime.
- **Diffusion and Confusion:**

  K can be paired with AES and potentially other ciphers to provide additional diffusion and confusion properties. K's apparatus provides a stream of random keys and initialization vectors (IV's) that can enhance AES and other ciphers.
- **Side Channel Attack Resistance:**
  K includes a Random Program Generator (RPG), that creates a "shape shifting" effect, including the ability to use multiple, programmatically different copies of the same opcode. This capability could blunt the ability of an attacker to capture meaningful data.

©2020 Virtual Software Systems, Inc.

- **Nature of the attacker's challenge:**
  K presents new attacker challenges vs. classical ciphers: With a classical cipher (RSA or AES) an attacker must break a static "hard problem" (a one-way function for which solutions seem to be getting easier). K, on the other hand, presents a more difficult challenge, forcing the attacker to solve not only a hard, but many constantly changing hard statistical problems.
- **Tamper Detection:**
  In addition to being able to add a MAC to a message, K provides streaming tamper detection.
- **Common Reference Strings:**
  K provides the properties of a one-time pad through a random common reference string using its History Buffer.
- **Manufacturing K at Scale:**
  K endpoints (in code or silicon) can be "manufactured" at scale and distributed. With appropriate security, these endpoints pairs can be activated easily as needed.
- **Small footprint:**
  The small size of the K algorithm should make it useful in IoT and other low latency applications where speed/size/strength can be optimized to fit the application.
- **Entropy:**
  K's method of harvesting and injecting entropy is constantly changing because its key is constantly changing. On the other hand, classical ciphers, such as AES, have a deterministic method for harvesting entropy (e.g. an algorithm and a fixed key).
- **Avoiding vulnerabilities in deterministic encryption schema:**
  Classical ciphers (RSA, AES) are deterministic - by having knowledge at any intermediate state of processing, it is possible to gain information related to the key. In contrast, K's key (and state) is dynamic and is applicable to only that moment before it changes randomly. We believe that there is little the attacker can glean about the prior or future state by knowing the current one.

Let us know if you are interested in receiving a copy of the Kaleidoscope Paper.

©2020 Virtual Software Systems, Inc.