RISOFTDEV inc. Encryption and related technologies

Vincent L Gilbert MCSE MCSA MCP

Abstract

In this paper we will provide a brief overview of the various technologies in the field of crypto logic which have been developed at RISOFTDEV inc., and the types of commercial products that might be developed from those technologies.

RISOFTDEV inc. obfuscated key technology

R.I. Keys represents a leap forward in Black Key technology. Instead of a master KEK, environmental and other factors create a KEP, or Key Extraction Pattern. This KEP is used to extract the key from a Keyfield. (See ‘Keyfield’ above) Because the key itself is not visible, any attempts to back engineer the algorithm will arduous at best. However we acknowledge that relying on this fact is not in keeping with accepted cryptographic practices. Kerckhoffs' principle — "only secrecy of the key provides security", or in Shannon's maxim, "the enemy knows the system" simply states that any encryption system has to accept that given enough time and access to the system, a dedicated group will be able to discern its mechanics. With this in mind, most encryption algorithms are made public and depend on mathematical complexity . In this case we seem to be, and are in fact violating this principle. To do so we are introducing what we are calling Extensible Obfuscated Algorithm Encryption technology. In EOAE the algorithm which creates the key is hidden, but it is accepted that given access to enough keys a dedicated effort will be able to discern it according to the foregoing principles. This is expressed as the value T. However elements of the algorithm are extensible, that is they can be altered simply, and without changing the fundamental mechanics of the algorithm. Since the algorithm is meant to be used by a known group, the updated version of the algorithm can be made available to this group within the time T, or upon a determination that the algorithm is compromised. The existing key is exported and a new key using the updated algorithm is sent to the user. Anyone attempting to crack it is forced to start over. The design allows for a nearly limitless number of patterns. This technology will NEVER be obsolete. From a business model perspective, it is ideal as the provider has a service that they can offer in perpetuity.

Encryption algorithms

Details regarding RISOFTDEV inc. encryption technologies must be considered proprietary and therefore to a large degree they are only available upon request and under strict non-disclosure arrangements. However there are (2) main areas where our technologies may be considered superior.

[1] With the advent of readily available super computing speed through the use of distributed processing via networked computers, we can expect to see the amount of time necessary to brute force a key of a particular length decrease dramatically. RISODTDEV inc. encryption algorithms are highly resistant to this type of attack.

[2] RISOFTDEV inc. encryption algorithms offer significant advances in the area of speed when encrypting video and other media files.

Summary

The field of crypto logic is facing a crisis brought about by increased computing speeds using existing technologies, as well as threats brought about by the possibility of emerging technologies such as Quantum computing. RISOFTDEV inc.'s encryption technologies offer unsurpassed resistance to these threats in a comprehensive manner.

.