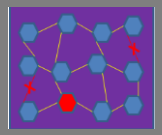
Virtual Software Systems

Value Proposition and Platform Overviews

Kaleidoscope Secure Channel (KSC)

&



Extended Resilience Architecture (xRA)

Table of Contents

VS² Value Proposition

Virtual Software Systems (VS²) technologies provide high reliability, self-protection, and enhanced security for existing hardware and software systems

- ***xRA™* (E*x*tended *R*esilience *A*rchitecture) Platform:**
  Based on fault tolerant computing principles, xRA protects applications and hardware by detecting and correcting deviations in operational execution due to system failures, unpredictable events, or attacks… before harm occurs.

- **Kaleidoscope Secure Channel (KSC) Platform:**
  A breakthrough algorithm-based security technology with potentially quantum resistant properties that provides secrecy, continuous authentication, and message integrity. The KSC can extend the life of existing ciphers, enhance the security of other communication channels (e.g. VPNs), or be shaped to meet specific mission requirements.

The broad applicability of VS² software tools provides a logical upgrade path for a firm's existing systems and products and opens the door for the creation of entirely new solutions to help organizations achieve product differentiation, improve productivity, increase operational resilience, improve security and generate meaningful ROI.

Kaleidoscope Secure Channel ("KSC") Platform

KSC is a breakthrough security algorithm, potentially quantum resistant, consisting of the *K-Engine* and a cipher (i.e. AES, RSA and/or the VS^2 *K-Cipher*)

OPPORTUNITIES:

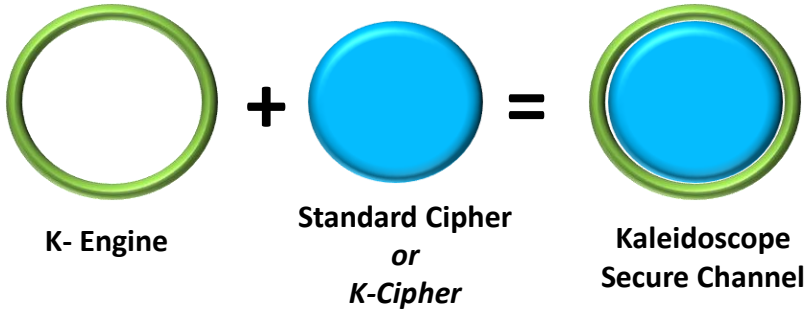
- Potentially protect against quantum-based cipher attacks
- Increase the strength and extend the life of existing cipher algorithms (and meet FIPS 140-2 and related requirements)
- Shape the KSC to specific security missions using its extensible, innovative architecture
- Deploy high entropy, dynamic Common Reference String
- Implement the KSC algorithm in hardware to create mission-specific, ultra-high security chips
- Manufacture KSC kernels (software or hardware) for distribution and uniquely secure activation as needed.
- Protect against side channel attacks on the communications stack

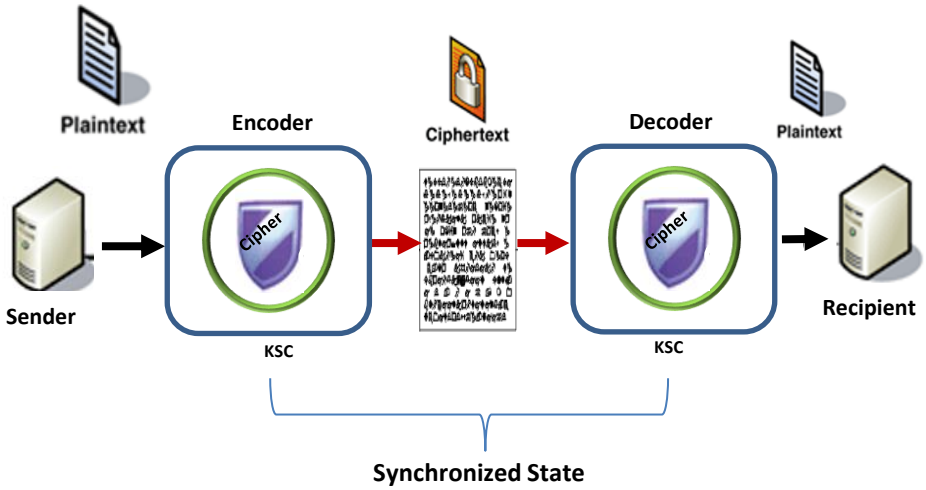
The *K- Engine* injects entropy, randomly changes its own operating characteristics, provides mission-specific capabilities, offers a randomized, common reference string, and offers a block cipher streaming mode-equivalent. The *K-Cipher* is a streaming, symmetric, dynamic-key, polyalphabetic substitution cipher with randomized (i.e., non-linear, time-varying, probabilistic) encryption capability with continuous authentication and tamper resistance.

Kaleidoscope Secure Channel ("KSC") Platform

KSC is a breakthrough, best in class security algorithm. It consists of the *K-Engine* and a cipher algorithm. The platform can use any standard cipher algorithm (i.e. AES, RSA) or the VS² *K-Cipher.*

OPPORTUNITY: Increase communications security with ground-breaking potentially quantum resistant secrecy that extends the life of existing ciphers, provides message integrity, and ensures continuous end point authentication.





The **Kaleidoscope Secure Channel** is composed of two parts:

1) **The K-Engine**, an outer pre-and post-processing "wrapper" that surrounds an inner encryption cipher.
2) **The cipher** can be any standard cipher algorithm (e.g. AES) or VS2's streaming, dynamic key, probabilistic **K–Cipher.**

Kaleidoscope components can be embedded in hardware, software, or in combinations thereof.

Kaleidoscope takes plaintext, pre-processes it with the K-Engine into extended-ciphertext then encrypts that into channel-ciphertext for transmission.

Kaleidoscope manages the dynamic key through state synchronization. The extended-ciphertext comprises commands and data that increase entropy and change the state of the K-Secure Channel.

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

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

Kaleidoscope Secure Channel ("KSC") Platform

Enhances and extends the life of existing encryption algorithms (e.g. AES) and secure communication protocols (e.g. VPN's) and adds operational flexibility

OPPORTUNITY: Increase communications security with ground-breaking potentially quantum resistant secrecy that extends the life of existing ciphers, provides message integrity, and ensures continuous end point authentication.

Business Challenges

- **Current state-of-the-art attacks render existing ciphers (AES, RSA) vulnerable**
- **Today's approved ciphers are known to be vulnerable to quantum-based attacks**
- **Replacing existing ciphers is expensive, and will take years**

VS² Contribution

- **KSC enhances existing ciphers with no alteration of their algorithm or operation (ensuring NIST compliance)**
- **K-Engine and K-Cipher offer extensible, flexible options to securing communications**

Usage

- **Blockchain-based application using KSC to secure on-line voting transmissions**
- **"Communications as a service" solutions provider evaluating the KSC to enhance VPN security**

Benefits Include…

- **Enhances existing encryption algorithms and extends their useful life**
- **Dynamic keys reduce cost of key management**
- **Increased security from resistance to side-channel attacks and potentially from quantum computer attacks**

xRA (eXtended Resilience Architecture) Platform

xRA provides tools for developers to create applications that self-replicate, detect anomalies and divergences, identify and remove offending replicas before harm occurs, and continue operation without losing state.

OPPORTUNITIES:

- Enables new or existing applications to become fault tolerant in heterogenous operating environments using commercial, off-the-shelf (COTS) hardware and software
- Implement applications where availability, reliability, safety, and resilience of mission and life-critical operations are a top priority
- Deploy xRA in a dispersed IoT environment by leveraging its small code footprint
  - ✓ Our IoT prototype clearly demonstrates how xRA can protect a process control application monitoring and controlling a high-value industrial operation
- We believe that xRA enhances the ability of cloud services providers to monitor, detect and recover from “Gray Failure”

At its heart, the xRA platform is a stateful, multi-element comparison engine and therefore ideally suitable to many different functions, from autonomous IoT process control resilience to cloud and edge computing fault tolerance to simultaneous, multi-platform software or circuit testing.

xRA (eXtended Resilience Architecture) Platform

xRA allows developers to create applications that detect anomalies, identify and remove offending elements before harm occurs, and continue operation without losing state.

OPPORTUNITY: Increased availability, reliability, safety, and resilience of mission and life-critical applications using commercial, off-the-shelf (COTS) hardware and software

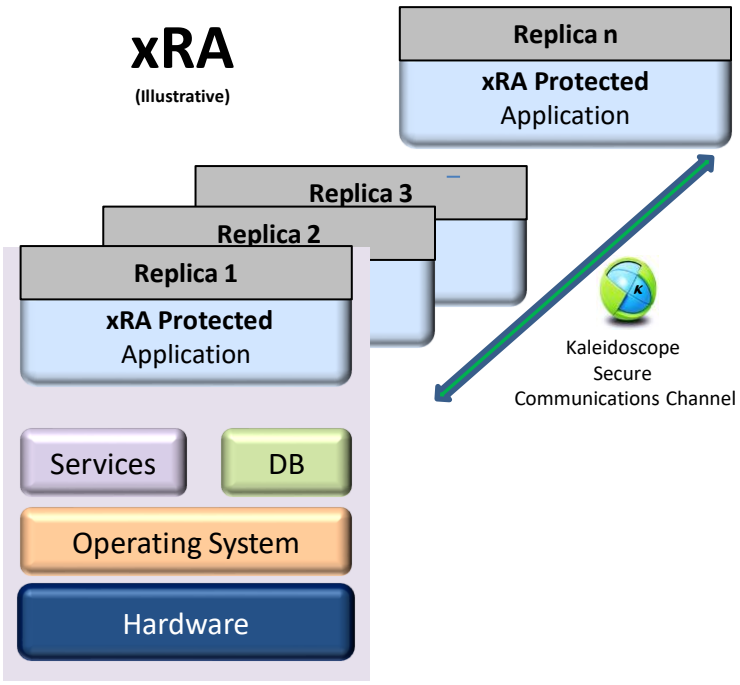


Illustration of a generic xRA replicated application

How xRA works:

- *Creates "n" multiple application replicas of a single, logical application*
- *Provisions and distributes independent, autonomous replicas on designated computer hosts*
- *Once started, all application replicas continually compare execution results*
- *If there is a difference in execution, the offending replica is removed and the application continues operating without loss of state.*
- *Facilitates fault root cause isolation via its fault handler and forensic analysis tools*
- *Leverages VS²'s unique Kaleidoscope secure channel for inter-replica communications*

Each replica retains the complete application state, so they each operate independently providing autonomy and continued operation without loss of transactions in the event of failure or attack.

xRA (eXtended Resilience Architecture) Platform

xRA allows developers to create applications that detect anomalies, identify and remove offending elements before harm occurs, and continue operation without losing state.

OPPORTUNITY: Increased availability, reliability, safety, and resilience of mission critical applications using commercial, off-the-shelf (COTS) hardware and software

Business Challenge

- **Maintain business continuity and safety by maximizing systems availability and reliability**
- **Isolate system failures and avoid performance degradations in complex systems**

VS² Contribution

- **xRA enabled applications detect execution divergence, provide continued operation and aid in the isolation and diagnosis of failures *regardless of their cause***
- **xRA facilitates fault root cause isolation via its fault handler and forensic analysis tools**

Usage

- **Developers employ the xRA SDK and xRA library to 1) create new applications, or 2) modify existing applications, or 3) create xRA agents to monitor and measure application performance and behavior**

Benefits Include…

- **Reduced loss due to application availability issues, improved safety of operational systems, and higher levels of disaster tolerance and recovery**
- **Increased speed and reduced cost of problem isolation reducing operations and maintenance costs**

Our Technology "DNA"

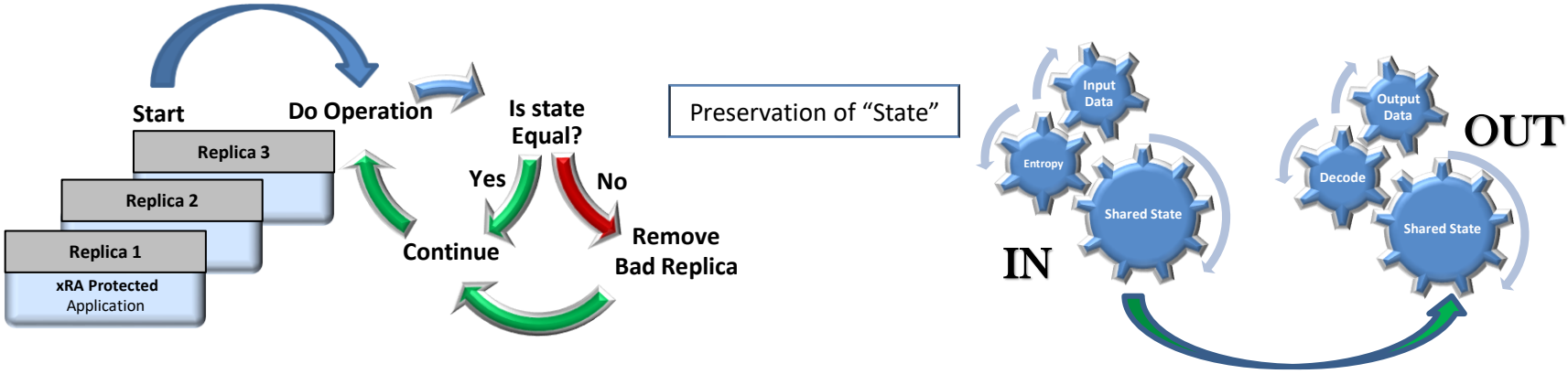
Our technologies uniquely apply the computer concepts of "state[1]" and "determinism[2]" to both user applications and the transfer of information between computing devices. We have incorporated these simple ideas into powerful tools that work either together or independently.

Fault Tolerance/Resilience
(xRA)

xRA creates application replicas that are deterministic and stateful. Replicas run independently, comparing their evolving state with each other to guarantee that the application continues to "do the right thing". Errant replicas are removed; others continue executing.

Authentication/Secrecy/ Integrity
(Kaleidoscope)

Kaleidoscope Secure Channel (KSC) endpoints are created with a shared state (their secret). They each travel a random, but synchronized, path through the state space. This shared state authenticates, secures, and ensures integrity of any data sent over the channel.



[1] In computer science, the state of a machine (or computer program) comprises the condition of its stored inputs, similarly to how the state of an object, for instance, as a gas, liquid or solid, shows its current physical makeup, the state of a computer program shows its current values or contents

[2] In computer science, a deterministic algorithm is an algorithm which, given a particular input, will always produce the same output, with the underlying machine always passing through the same sequence of states

Example Use Cases

Kaleidoscope: Mobile Voting

Kaleidoscope: Blockchain I/O

Kaleidoscope: Enhancing VPN Security

Kaleidoscope: Securing The Software Supply Chain

Kaleidoscope: Securing Autonomous Vehicle Updates

Kaleidoscope: Securing and Authenticating Remote Application Communications

xRA: Process Control Protection

xRA: Autonomous Control Systems

xRA: Simultaneous Multi-Platform Software Testing

xRA: Hardware Testing

xRA: Gray Failure Analytics

For More Information Please Contact:

Tom Wetmore
CMO and co-founder
Virtual Software Systems, Inc.
twetmore@vs-2.com
C: (781) 424-4899