Virtual Software Systems

Kaleidoscope Secure Channel (KSC)

Use Cases

Kaleidoscope Use Cases: Table of Contents

Kaleidoscope Use Case Descriptions (For Business Summary Deck)

- **Mobile Voting Application**
  Kaleidoscope secures and enhances communications between a remote application and a server: in this example, the KSC ensures the secrecy and integrity of each ballot, from the voting device to a secure voting database repository.
- **Blockchain I/O**
  Kaleidoscope protects blockchain “on- and off-ramps” where data is vulnerable to attack or compromise.
- **Enhancing VPN Security**
  Kaleidoscope enhances and extends the security of both software and hardware-based VPN technologies.
- **Securing the Software Supply Chain**
  Kaleidoscope securely transfers software updates or other changes ensuring that they are only sent to the device for which they are intended, whether the device is a computer, a vehicle, a device, or an appliance.
- **Securing Autonomous Vehicle Updates**
  Kaleidoscope locks down all autonomous vehicle software updates and ensures that the intended vehicle (or subsystem) is the only one that can receive the update, that the update is encrypted, and that no tampering has occurred.

Kaleidoscope: Mobile Voting

APPLICATION : Kaleidoscope Secure Channel (KSC) protects ballot data

Kaleidoscope enables secure transmissions of a ballot from a remote device into a blockchain-based voting system

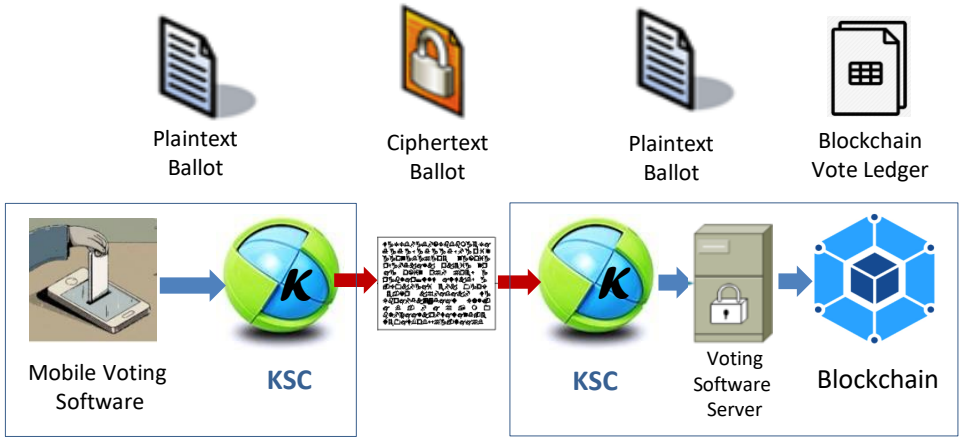
Tamper-Resistant, Secure Mobile Voting

(Illustrative)

A voter uses voting software on a remote device to fill out a ballot which is then transmitted to the server and added to the blockchain.

The KSC is embedded in the device software and used to protect the transmission of the vote.

KSC secures the content of the vote (secrecy), ensures that the vote comes from that device (authentication), and prevents tampering or alteration of the vote in transmission (integrity).



Kaleidoscope: Mobile Voting

APPLICATION : Kaleidoscope Secure Channel (KSC) protects ballot data

Kaleidoscope enables secure transmissions of a ballot from a remote device into a blockchain-based voting system

Business Challenge

- **Existing ciphers are vulnerable**
- **Suspected "backdoors" exist which could allow adversaries to corrupt voting results**

VS² Contribution

- **KSC API enables easy integration with voting software application**
- **K-Engine with K-Cipher can be tailored to the meet the unique needs of voting jurisdiction**

Usage

- **On-line voting application developer is using KSC to address concerns about backdoors**
- **K secures ballot transmission to blockchain**

Benefits Include…

- **Secure data communications, by embedding it into existing applications**
- **Provides developer with competitive advantage**
- **Secrecy, integrity, continuous authentication**

Kaleidoscope: Blockchain I/O

APPLICATION: Defending Blockchain On-Ramps and Off-Ramps

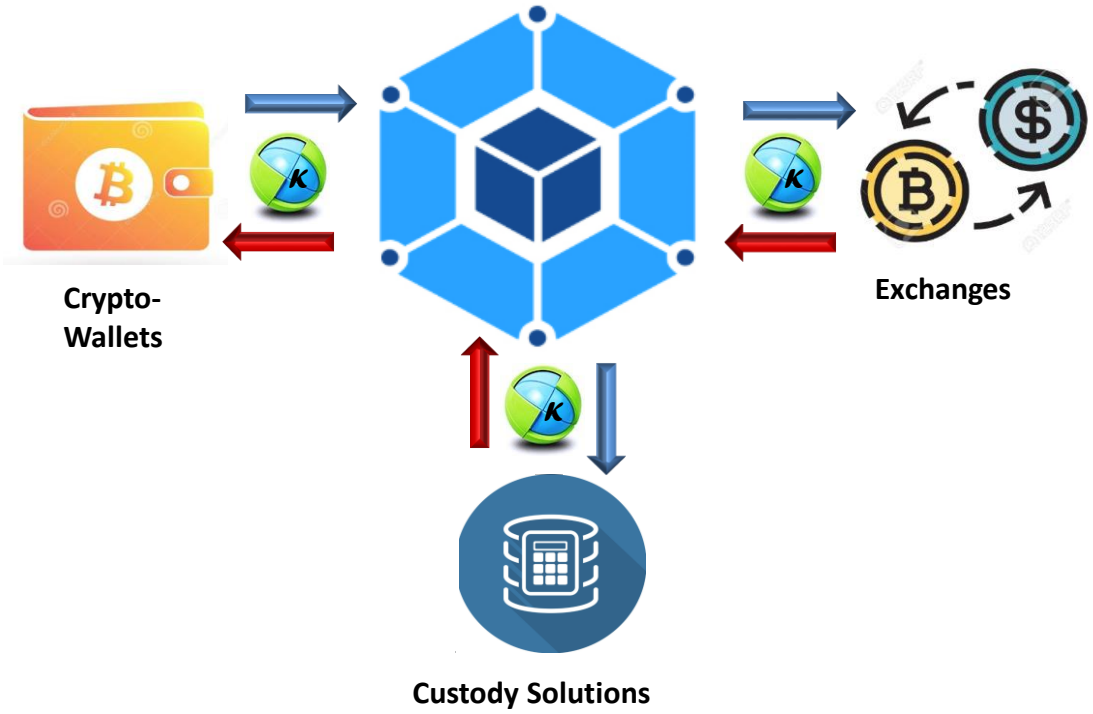
Protecting Blockchain-based custody solutions, wallets, and exchange data transfers

Enhanced Blockchain Communications

(Illustrative)

Kaleidoscope provides additional levels of device authentication and security for data and devices being used to transfer data between applications and a blockchain.

Often referred to as referred to as blockchain “on-and off-ramps”, these are currently vulnerable areas of the blockchain ecosystem.



Kaleidoscope: Blockchain I/O

APPLICATION: Defending Blockchain On-Ramps and Off-Ramps

Protecting Blockchain-based custody solutions, wallets, and exchange data transfers

Business Challenge

- **Data being transferred into or out of the blockchain is vulnerable**
- **NIST (National Institute of Standards and Technology) warns that existing ciphers may be vulnerable to quantum attacks**

VS² Contribution

- **KSC enhances existing security technologies, increases secrecy, integrity, and continually authenticates**
- **Kaleidoscope is potentially quantum resistant**

Usage

- **Enhances storage custody solutions, protects exchanges, secures wallets**
- **Enforces endpoint-to-endpoint authentication, adds to existing blockchain privacy & security**

Benefits Include…

- **Blockchain solution providers can differentiate their offerings by delivering improved security and the possibility of quantum resistance**

Kaleidoscope: Enhancing VPN Security

APPLICATION: Kaleidoscope enhances and extends protection of Virtual Private Networks (VPNs)

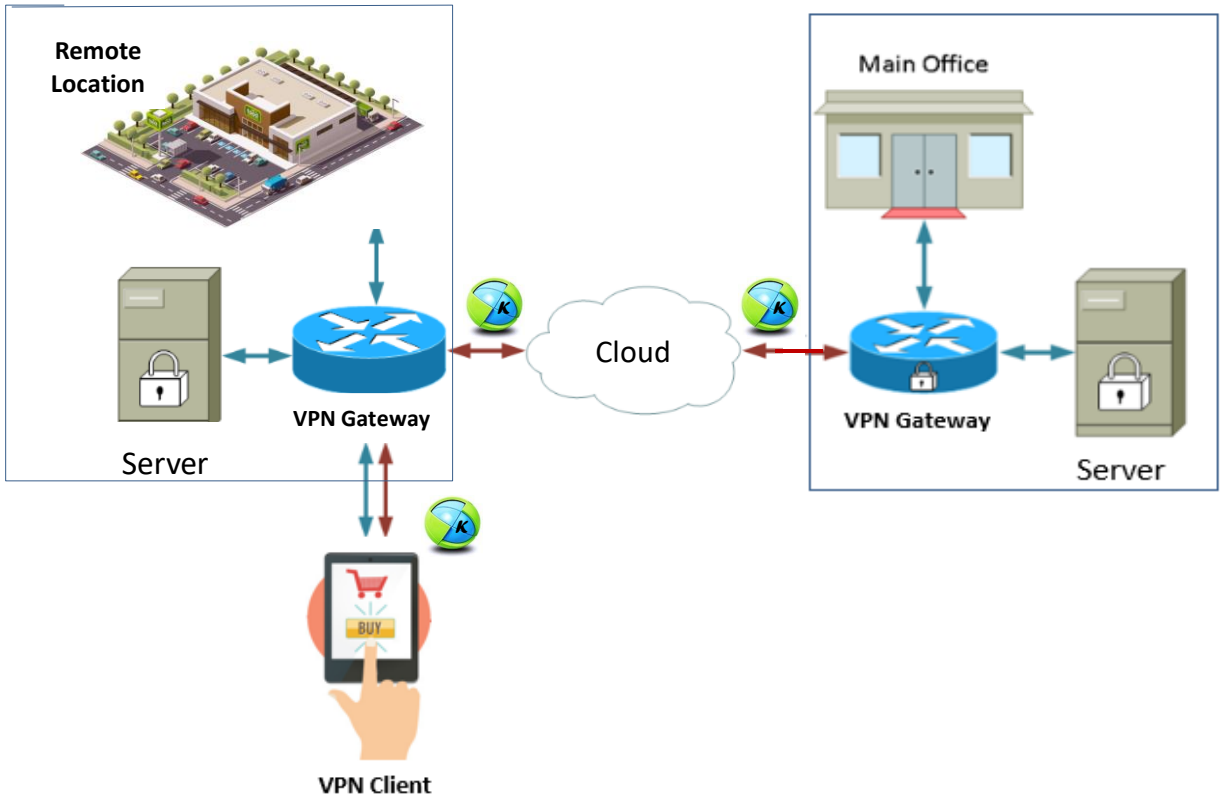
Embedding the Kaleidoscope algorithm in VPN software or appliances adds security to communications including improved secrecy, integrity, and continuous authentication

Enhanced Retailer/Customer Communications

(Illustrative)

An enterprise uses Virtual Private Network VPN's to connect its remote locations with its main office.

It secures VPN gateways and clients with embedded Kaleidoscope Secure Channel capabilities. Each endpoint is authenticated continuously, and the data is encrypted, and tamper protected.



Kaleidoscope: Enhancing VPN Security

APPLICATION: Kaleidoscope enhances and extends protection of Virtual Private Networks (VPN)

Embedding the Kaleidoscope algorithm in VPN software or appliances adds security to communications including improved secrecy, integrity, and continuous authentication

Business Challenge

- **VPN network technology is increasingly vulnerable to attack**
- **Anticipated attack methods require businesses to consider expensive and unproven security upgrades**

VS² Contribution

- **Adds improved privacy, integrity, and continuous authentication to VPNs**
- **KSC potentially adds quantum-resistant properties to existing VPNs**

Usage

- **Kaleidoscope flexibility allows a variety of VPN implementations including new drivers or embedded within the VPN software**

Benefits Include…

- **Future-proofs existing VPN solutions as it is potentially quantum resistant**
- **Provides adjustable security, operating, and resource usage parameters**
- **Enhanced secrecy, integrity and endpoint authentication**

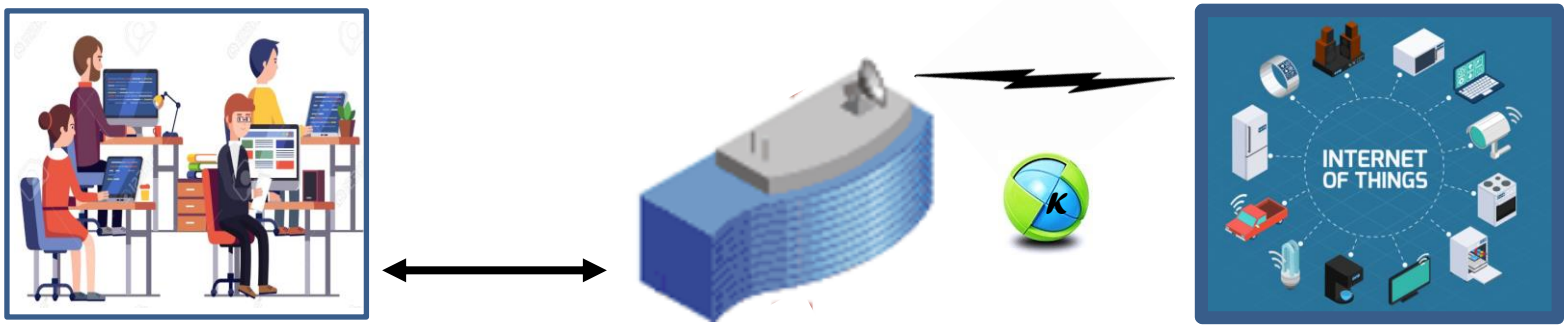
Kaleidoscope: Securing the Software Supply Chain

APPLICATION: Provide an authenticated, secure communications channel for software updates and revisions to any remote device, or appliance

Kaleidoscope Secure Channel provides secrecy, continuous authentication, and data integrity to secure software and firmware transmissions to a specific target

Secure Software Upgrade System

(Illustrative)



Developers send tested upgrade to distribution center

Distribution point identifies target and sends upgrades over any network

Only the specific target receives the upgrade

Kaleidoscope's unique synchronized encryption ensures that the upgrade is delivered securely, and only to the target for which it was intended

Kaleidoscope: Securing the Software Supply Chain

APPLICATION: Provide an authenticated, secure communications channel for software updates and revisions to any remote device, or appliance

Kaleidoscope Secure Channel provides secrecy, continuous authentication, and data integrity to secure software and firmware transmissions to a specific target

Business Challenge

- **Securely sending the right software upgrade to the appropriate, authorized device**
- **Ensuring that upgrades are not tampered while being delivered**

VS² Contribution

- **Kaleidoscope enhances existing security technologies, increases secrecy, integrity, and continually authenticates communicating end-points**
- **Kaleidoscope's synchronized encryption feature guarantees that the correct upgrade is delivered to the platform, device, vehicle, or appliance for which it was intended**

Usage

- **The software to be delivered is secured and sent via a Kaleidoscope Secure Channel so that only the intended target can receive and decode the update**
- **The KSC can also be used to send back any diagnostic and operational data**

Benefits Include…

- **Secure updates reduce risk, improve time-to-update, increase product quality, and provide operational efficiency**

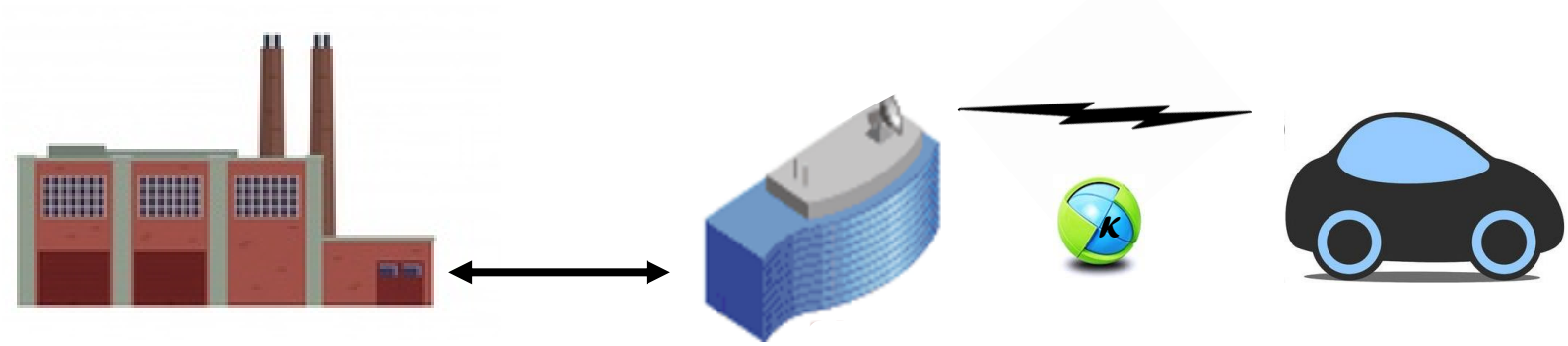
Kaleidoscope: Securing Autonomous Vehicle Updates

APPLICATION: Automotive: Provide an authenticated, secure OTA (Over The Air) communications channel for autonomous vehicle software updates and revisions

Kaleidoscope Secure Channel provides secrecy, continuous authentication, and data integrity to secure OTA vehicle data transmissions

Over-the-Air Software Upgrade System

(Illustrative)



Manufacturer sends software upgrade to autonomous vehicle technology center

Center transmits the upgrade over the air

The specific targeted autonomous vehicle receives the upgrade

Kaleidoscope's unique synchronized encryption ensures that the upgrade is delivered securely, and only to the vehicle for which it was intended

Kaleidoscope: Securing Autonomous Vehicle Updates

APPLICATION: Provide an authenticated, secure OTA (Over The Air) communications channel for autonomous vehicle software updates and revisions

Kaleidoscope Secure Channel provides secrecy, continuous authentication, and data integrity to secure OTA vehicle data transmissions

Business Challenge

- **The amount of in-vehicle software is growing steadily. Drivers need to bring their cars to a dealership to have new software installed, which is inconvenient and has its own difficulties**
- **Over-the-Air (OTA) software updates could resolve this problem but concerns about existing security solutions are hampering acceptance and deployment**

VS² Contribution

- **K enhances existing security technologies, increases secrecy, integrity, and continually authenticates communicating end-points**
- **K's synchronized encryption feature guaranties that upgrades are only delivered to the vehicle for which they were intended**

Usage

- **Connected vehicles receive "Kaleidoscope-secure" remote, OTA updates and can also transmit secure diagnostic and operational data from on-board systems and components back to a dealer and/or the manufacturer**

Benefits Include…

- **Secure OTA updates reduce recall expense, improve time-to-update, increase product quality and operational efficiency, deliver post-sale vehicle performance and feature enhancements**

Kaleidoscope: Securing and Authenticating Remote Communication

APPLICATION : Securing all communications between endpoints (e.g. application and its server) even if the network has been compromised

A Kaleidoscope Secure Channel (KSC) uniquely protects data communicated between any two endpoints

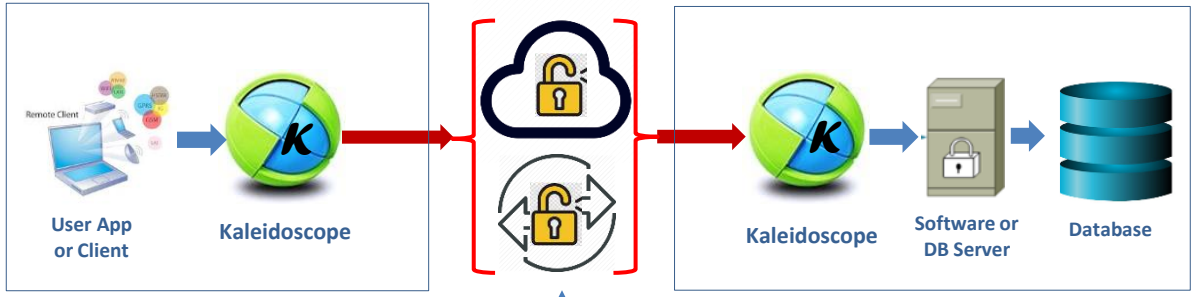
Tamper-Resistant, Secure Transmissions

(Illustrative)

KSC can be implemented using ~~as~~ a library or embedded in either software or hardware.

With a KSC connecting two endpoints, all transmissions, whether device to device, application to application, client to server, etc. is "locked down" to only those endpoints, even if the transport mechanism is compromised

The KSC secures the content of the data (secrecy), ensures that the data comes from only its partner endpoint (authentication), and detects any tampering or alteration of the data in transmission (integrity).



Sending Endpoint

Receiving Endpoint

KSC

Secures Public (ex: cloud) or Private Local Connections

Kaleidoscope: Securing and Authenticating Remote Communication

APPLICATION : Securing all communications between endpoints (e.g. application and its server) even if the network has been compromised

A Kaleidoscope Secure Channel (KSC) uniquely protects data communicated between any two endpoints

Business Challenge

- **Existing communications protocols (SSL, TLS) are vulnerable to zero day and other attacks**
- **Current encryption schemes are also vulnerable to more sophisticated including expected quantum computer attacks predicted by the NSA**

VS² Contribution

- **Continuously changing KSC characteristics make an attacker's task significantly harder**
- **The KSC can extend and enhance existing encryption schemes without altering them**
- **The KSC API enables easy integration. The software can be embedded in an application or in hardware**

Usage

- **An on-line voting developer is using the KSC to protect against zero-day exploits affecting TLS and address concerns about possible "backdoors" in currently certified cipher algorithms**
- **Any application's security and integrity can be enhanced with a KSC**

Benefits Include…

- **Easy to integrate with existing applications**
- **Significantly increases the cost of attacks**
- **KSC-enhanced secrecy, integrity, and continuous authentication capabilities future-proof existing encryption technologies against new threats including potential quantum computer attacks**

For More Information Please Contact:

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