eclypses®

MicroToken Exchange Data Security Solutions

Protecting Commands, Control And Data Transfers with UAV'S

eclypses

Drone Technology and Today's Needs

As UAV usage increases, the more cybersecurity protocols become necessary. Cyberattacks of UAV's or drones, not only include hijacking, but also attempts to collect data, including GPS coordinates and live video feed.

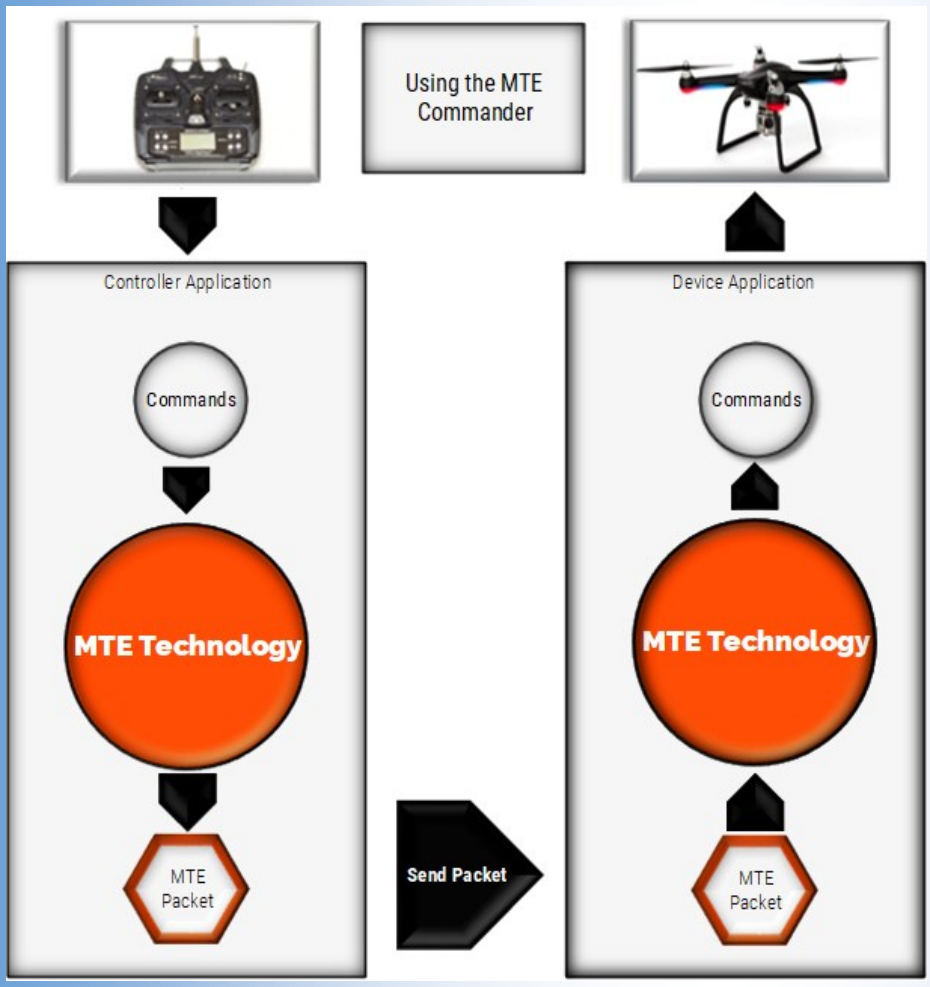
The lack of securing these instances is an issue for most all UAV users. These breaches also cause issues for police forces and military operations, when news outlets and/or adversaries attempt to gain access to the live video feed of drones in highly sensitive high risk operations

Eclypses has capabilities to:
Enable any drone manufacturer to secure electronic transmission of commands, control and data, from being breached and attacked through the implementation of MicroToken Exchange.

The implementation of MTE will improve the reliability of the drone by making commands and data inaccessible to cybercriminals.

eclypses

The USE CASE Process Flow and Eclypses MTE



Eclypses has developed an innovative data protection solution that protects data and commands from man-in-the-middle attacks.

Eclypses' proprietary MicroToken Exchange® (MTE) data security solutions protect commands and data from a breach. The solution replaces streaming commands or data with MicroTokens™ and provides drones with a unique pairing to their controller.

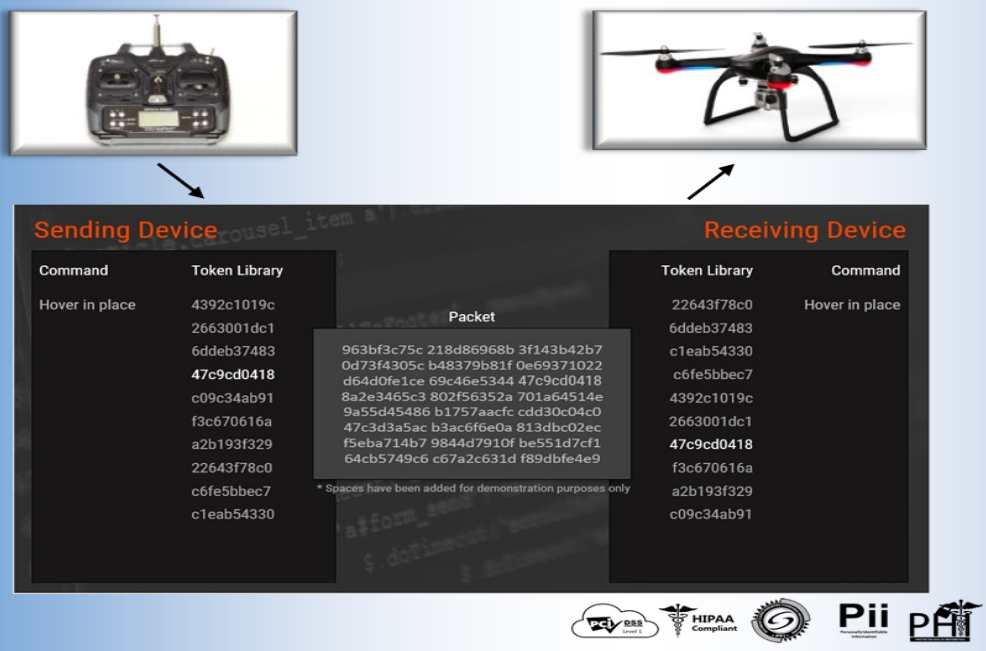
Ensuring that sensitive data remains unavailable to exploitation in the event of an internal or external network breach

The cyber resilience of this architecture plays a critical role in keeping data and commands secured. The implementation of MTE within the architecture would provide the cyber resilience necessary to keep intellectual data and commands safe from hacking.

MTE security protocol for data-in-transit and command and control would provide invulnerable cybersecurity coverage for this effort.

eclypses

The Threats



- **Command take over of UAV's, (i.e. hijacking).**
- **Accessibility of data collections, including live video feeds**

Fig. 1 MTE Tokens being substituted for commands between the controller and the drone.

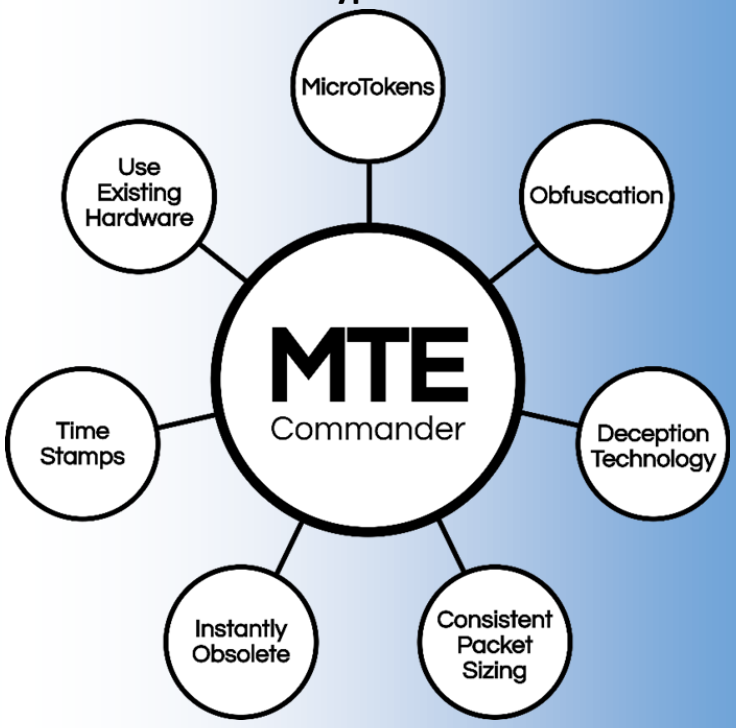
Drones are driven by many commands communicating from a remote control. These include commands to move up, down, side to side, to increase speed, decrease speed, hover, and many others. With additional sensor capabilities come additional commands and data communicating from the drone back to the controller.

For each command or sensor value, our MicroToken Exchange (MTE) technology provides a substitute MicroToken hidden in an MTE packet which is sent from one device to the other. This creates a communication stream where no real commands or data are ever sent between devices for hackers to manipulate. The receiving side identifies the valid MicroToken within the MTE packet and executes the desired action. Once this action is executed, that valid MicroToken is instantly obsolete and can never be used again. The ultimate result of this is a unique one to one relation-ship between the drone and its controller allowing only the paired remote to control the drone. In this instance, our MTE technology prevents drone hijacking, protects the video feed, and any data collected.

eclypses

MTE for Data in Transit

Eclypses MTE Commander is a compiled software library that can integrate into existing networks and infrastructures with minimal effort. The Eclypses MTE Commander is a small footprint library that requires a minimum of 165KB of RAM (10KB for each additional endpoint). MTE also needs 600KB of non-volatile storage for integration and operation. MTE is currently available in C++ with wrappers available for C#, Java, Java Script and Swift.



System Capability

MTE is unique in its design as it can be integrated into various existing platforms and systems. MTE to secure command and control and/or data-in-transit requires minimal processing power, so no changes to hardware or architecture are needed. The MicroToken is created on-the-fly and is instantly obsolete. In instances where there is one controller and multiple devices, each device would receive its own unique pairing of MTE to the controller. When the application calls the MTE Library, MTE transforms the external input into a packet, containing MicroTokens as substitute values for the real data. MTE is agnostic to the communication protocol -- it only requires that the route be established. When a device receives an MTE packet, it transforms the appropriate MicroTokens back into the desired data.

eclypses

Logic

- How we are going to prevent cybersecurity breaches?
- How does MTE change the way command and control is secured?

Priority

- To provide a cybersecurity method (MTE) that prevents breaches of drone commands.
- To provide a cybersecurity method (MTE) to protect data collections of a UAV. drone, including live video transmission.

Customer Pain Points

- Cyber breaches occur when least expected.
- Keeping up with the latest hacking intel.

MTE Prevents

- Hijacking of the drone
- Man-in-the-middle attacks on video feed
- Deciphering of GPS coordinates
- Data collections

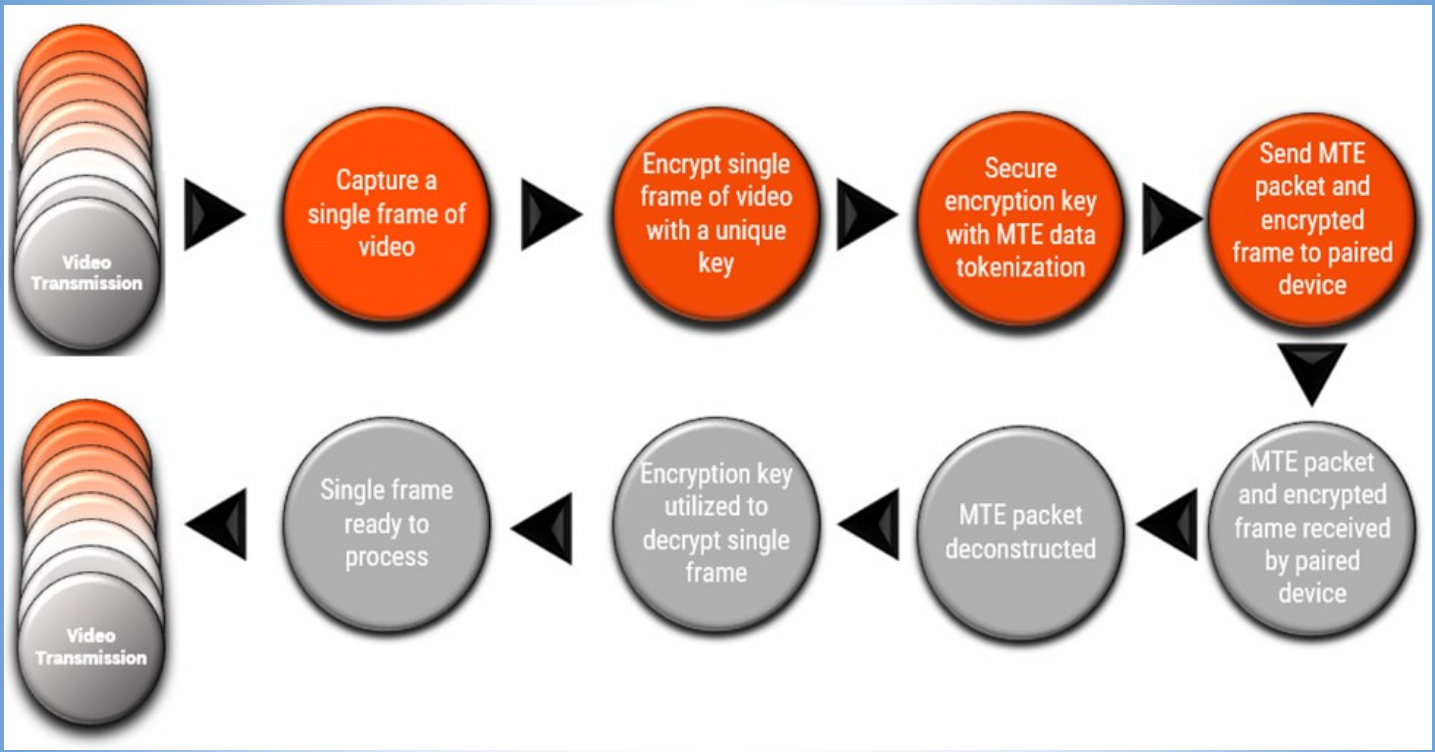
MTE
MicroToken Exchange

eclypses

Proposed Approach : Cyber Resiliency for Data in Transit

MicroToken Exchange, (MTE) is a process for information security that consists of replacing your command and/or data with a MicroToken just before transmission and is compatible with any communication protocol. Once the transmission packet has reached the receiver it is then translated back into the original command and/or data.

By processing data through the MTE, a new paradigm is created by removing the vulnerability that exists today with command and control and data-in-transit, including live video feed. This process secures the commands and/or data, providing the user with an unequivocal layer of protection against cybersecurity breaches, including unauthorized users. Below shows a more extensive overview of how MTE works to secure live video feed one JPEG at a time.



eclypses

About Eclypses

Eclypses' industry leading disruptive cybersecurity software replaces commands and/or data with MicroTokens™ to provide the highest level of data privacy available with the company's patent proven MicroToken Exchange™ (MTE) technology.

Applications range from secure command and control needs, including Internet of Things (IoT), to secure storage and retrieval of sensitive data, such as credit card information and healthcare records. Eclypses' MicroToken Exchange technology is helping enterprises and government agencies protect their most sensitive and private information from cybercriminals and cyberterrorists today.

Eclypses' MicroToken Exchange (MTE) software complies with the European Union's General Data Protection Regulation (GDPR). In addition, Eclypses' technology is certified as Payment Card Industry Data Security Standard Level 1 (PCI-DSS) and Health Insurance Portability and Accountability Act (HIPAA) compliant.

In addition to MTE's certified status, MTE has recently been penetration tested by H2L Solutions. H2L is one of the trusted penetration companies to work closely with the DoD. H2L has multiple government contracts and partners, adding to their reputation in this sector. Through H2L's almost 6 weeks of penetration testing, our technology was unassailable through all attempts. Below is a commentary from their final report.

"As the MTE Technology stands, the likeliness that the MTE Authentication Token technology will be victimized by a replay/reuse attack is highly improbable (H2L)."

eclypses

Securing Data via MicroToken Exchange

Ensuring that sensitive data remains unavailable to exploitation in the event of an internal or external network breach.

Contact Us

Info@Eclypses.com

www.Eclypses.com

+1.719.323.6680