eclypses®

WHITE PAPER

Protecting Command and Control for Real Time Devices

Document ID:ECLYPSES-1532395320-502
Version No.:2.0

www.eclypses.com

Introduction

When the need arises to securely use remote devices such as Mobile Robots or Drones, certain vulnerabilities that are essential to secure operation must be addressed. The ability to ensure that the proper commands have absolute integrity is important. Also, any information that may be collected must be securely protected from prying eyes.
To accomplish this, any “pre-loaded” instructions or data must be guarded in such a way that if the device was to be misplaced or captured; the information is secure.

Additionally, if real-time commands are communicated to the device, one must ensure that if intercepted they are not discernable and that any “replay” attacks are rendered useless.

These challenges are difficult to overcome with today’s current technology – a new paradigm is needed that will render absolute security.

Data Gathering

A remote device’s purpose may be to gather information to be reviewed and analyzed once the device returns to its original demarcation point. An example could be a reconnaissance robot that is sent into an unfriendly environment to take sensory readings such as temperature, humidity, atmospheric analysis, or terrain mapping. This information, once collected, may be very sensitive and if the robot is lost or captured the sensitive information must be securely stored. Once the robot has returned to its point of origin, the information must be downloaded for analysis and processing by only a trusted system.

Pre-loaded Information

Many times, pre-loaded information is uploaded to a device prior to it accomplishing its purpose. This may be true if real-time communication is not feasible for any number of reasons. An example is to pre-load GPS waypoints into a drone so that once a waypoint is reached, the current waypoint is discarded, and the next waypoint becomes the current destination. If the drone is captured or runs out of power and crashes, the waypoints may be available within its data storage exposing sensitive information to anyone that may recover the drone.

Real Time Control

Another situation that must be secure is real time control. This may be as simple as a “pilot” using a joystick device to control the movement of a drone, or a real time transmission of data to a device to inform it of its next waypoint. If these communications are captured in-flight, they would contain sensitive and proprietary information. If they are delayed, or captured and replayed, the device may not accurately complete its task. Furthermore, if a communication is captured and substituted the results would be unacceptable.

Protecting the Data

Each of these scenarios requires the protection of data. That data may be created and stored, retrieved from storage, or received in real time. In each case, the protection of that data is the real issue that must be addressed.

Cryptography

Obviously, the data should be encrypted when created and decrypted when retrieved. In the case of data gathering, as soon as the information is collected, it must be encrypted prior to its storage. In the case of reading pre-loaded information, once the protected data is retrieved from storage, it must be decrypted so that the proper information is provided to the device. In the case of real time control, the information must be encrypted in real time with each input and decrypted in real time to provide the device with its proper command.

Standard cryptography such as AES-256 is quite secure, however the Achilles Heal is “key management”. Obviously, the same encryption key that is used to encrypt information must be available when the information needs to be decrypted and used. This is a vulnerability that must be managed. Typically, these keys may be “rotated”, or otherwise derived or loaded when the data is created. That is not totally acceptable since if the device is compromised, the key to unlock the data is also present.

Another issue with standard cryptography is that the “context” (size, shape, contents) of the encrypted payload may be used to determine the outcome of the device. AES-256 encryption produces the same exact information for the same input as long as the encryption key is the same (which it must be!).

Clearly, there must be a better way to ensure the integrity of the information.

Replay

If a real-time communication is captured and replayed, the receiving device will attempt to execute the same command which is quite often not desired. For example, if the command was “Set heading to 270 degrees and proceed for 2 kilometers” and that was replayed, the device would end up travelling too far.

Delay

If a real-time communication was captured, and delayed, the device would seriously go off course and not end up where it is intended.

Substitution

If a real-time communication was captured, and substituted, the device would once-again not end up at its intended destination.

Eclypses MTE

Eclypses has a patented technology that ensures the integrity of information in all the above cases.
For short pieces of information, each individual byte in the communication is replaced by an instantly obsolete token.
These tokens can only be reversed back into the original bytes by a paired endpoint.

For larger pieces of information, the data is encrypted with AES-256, however, the encryption key is generated uniquely for each occurrence of information. There is NO need to manage encryption / decryption keys, as they are guaranteed to be unique and are generated in real time (never stored) each time that they are needed.

For storage of information (and its subsequent retrieval), the information is concealed in a way that cannot be revealed except using the same licensed MTE technology for both sides. In other words, when information is created (such as a waypoint) it is concealed in such a way that only the intended destination can reveal it. Furthermore, if the same exact information is concealed, its shape and values are unique so that pattern recognition cannot be used to determine that the underlying information is the same.

Data Gathering

In a data gathering situation, once the data is collected, it should be “concealed” using the Eclypses technology and then stored. There is no need to create an encryption key, the technology handles all the processing to securely and uniquely conceal the information.

Once the data must be retrieved, the same technology is used to “reveal” the protected data making it available to be acted upon. If the device is captured, the data itself is useless since it can only be revealed using Eclypses technology.

Pre-loaded Information

When information needs to be created at a point of origin and then loaded onto a device, the system that creates the data “conceals” it with the Eclypses technology. Then, as needed, once the device is deployed, the Eclypses technology loaded onto the device “reveals” the information for processing.

Real Time Control

When commands or instructions are being transmitted to a deployed device, that transmission is extremely vulnerable to being compromised. The “controller” should encode the information with the Eclypses technology and transmit it using whatever communication method the device is capable of.

Then, when the device receives the transmission, the Eclypses technology decodes the information and presents it to the device for execution.

Replay

Each transmission is unique (even if the actual information is identical) and once a particular piece of information is decoded, it cannot be decoded again, so a replay attack will ignore the duplicated information.

Delay

If the information is time-sensitive, the Eclypses technology can be configured to allow an acceptable window of time for processing. For example, if you require commands to be consumed within one tenth of a second, you can set your acceptable time window to one tenth of a second and if a transmission is received more than one tenth of a second after it was created, it will be discarded. This is an optional feature that you can choose to utilize if your implementation is time sensitive.

Substitution

If a transmission is captured and a similar looking transmission is substituted in-flight, the arriving transmission is discarded as an error. This ensures the integrity of the sender / receiver pair and further serves to authenticate the source of the information.

Conclusion

The patented technology from Eclypses ensures that your real time device is secure, and that the most important aspect of your system (the actual information) is protected in a way that prevents any capture or analysis of that information. For further information, or to arrange a demonstration, please visit the Eclypses website at https://eclypses.com