Design Document version 2 for Team KC

Our team has generally left the functional aspect of the MISC as it was in the reference design. There were a few necessary changes that are listed below followed by changes for the security requirements.

The changes are as follows:

1. **PIN and token validation.**
    a. We added a timer and a counter for the validation. After each failed attempt, you must wait 5 seconds to retry.
2. **Attest Components.**
    a. So that a threat actor cannot replace the AP with the corrupt AP and get the attestation data, once we validate the PIN, we will establish an encrypted connection with the component before requesting the attestation data. The components will no longer respond to the unencrypted attestation request.
3. **Boot system.**
    a. Just as for attest components, before we send the boot command to a component, we establish an encrypted connection if not already established. The component will not boot unless it receives a valid encrypted boot message.
4. **Security Requirement 1 -**The Application Processor (AP) should only boot if all expected Components are present and valid.
    a. We did not accomplish this as we initially planned. In the reference design the code already accomplishes this but does not verify the component is a valid component. The addition that we made was to establish an encrypted connection with each component before requesting either component to boot. If either expected device does not reply with the proper encrypted response the AP will not boot.
5. **Security Requirement 2 -** Components should only boot after being commanded to by a valid AP that has confirmed the integrity of the device.
    a. See security requirement 1.
6. **Security Requirement 3 -** The Attestation PIN and Replacement Token should be kept confidential.
    a. See item 1, PIN and token validation.
7. **Security Requirement 4 -** Component Attestation Data should be kept confidential.
    a. See item 2, attest components.
8. **Security Requirement 5 -** The integrity and authenticity of messages sent and received using the post-boot MISC secure communications functionality should be ensured.
    a. When the AP is powered up, a random 16-byte encryption key is created. Before the system is booted, this encryption key is encrypted and exchanged with each component.
9. **Protocol changes** – For encrypted data, we encapsulate the protocol from the reference design in the following message. This is added in secure_send and removed in secure_receive.

0x00	0x01	0x02	0x03	0x03 to (length-3)	Length-2	Length-1
0xFF	Length	Seq Num	cmd	Data if any	CRC low byte	CRC high byte