Event Timer for onboard Attack CTU RockSatx2019

Con opps events for on board system attacks. Event list 1.2:

1. Boot on all systems. *t = 0 min*.
2. Ping all systems on the LAN (C1, C2, C3, & S1).[1] *t = ~0.6 min* till *t = ~0.76 min*.
3. C1 & C2 Share previously defined Public Keys, the public keys are a constant throughout all of testing and the actual experiment, this is the beginning of the test connectivity session. This will loop three times to ensure connectivity. t = 0.8 min till *t = 1.2 min*.
4. Iridium and HAM radio turns on and starts broadcasting “I’m alive.” messages, this will happen while data is not being broadcasted. *t = 1.3 min*
5. This section will be split into Red Team systems (RT)[2] and Blue Team systems (BT)[3]--
    a. BT- If the connectivity session was successful C1 and C2 will exchange keys, which is the authentication session[4], *t = 1.7 min*. After the authentication session DATA1[5] begins sending *t = 2.0 min* till completion. Then DATA2[6] transfers the data from the Arduino to C2 from C1, begins at *t = ~2.9 min* till *t = ~3.5 min*.
    b. RT - beginning interception of all packets between C1 and C2 in an attempt to acquire the appropriate keys from messages *t = 1.7 min* till *t = ~3.5 min*. While still intercepting the data the system will attempt to pull the keys, if the keys are acquired the system will continue to intercept data until event 5.a is completed, this is because it is necessary to verify that the keys are actually the correct keys and that they are assigned to correct system. In this experiment we will be using randomly generated MD5 hashes as the private keys. This type of attack is called a man in the middle attack.
6. This section will be split into RT, BT and Iridium--
    a. Iridium - pause data transmission from *t = 3.5 min*, resumes “I’m alive” message, resumes data transmission at *t = 4.0 min*.

---

[1] C1 = Computer 1 (NanoPi M3).
C2 = Computer 2 (Raspberry Pi B+).
C3 = Computer 3 (Raspberry Pi B+).
S1 = Switch 1 (EspressoBin).

[2] Red Team consists of C3, which is the attacker.

[3] Blue Team consists of C1 & C2, these systems mainly C2 is the target.

[4] Authentication Session - checks public key then exchange private key(MD5) which will be used to sign and encrypt the data that is being transmitted, this occurs 4 times.

[5] DATA1 - first data collection period that loops the packets being sent three times to ensure delivery, this status message that the solar panels, which is if they retracted or not.

[6] DATA2 - first data collection period that loops the packets being sent three times to ensure delivery, this data is from the Arduino.

   b. BT - during the time that the data transmission is paused (6.a) the system will performs a test connectivity session, which is a short version of event 2, from *t = 3.5 min* till *t = 3.6 min.* After that session C1 & C2 will share previously defined Public Keys and there Private Keys this will simulate a temporary reset of a connection to the satellite. This occurs from *t = 3.6 min* till *t = 4.0 min*.
   c. RT - from *t = 3.5 min* till *t = 3.6 min* the interception will pause to calculate the keys and to ensure that the RAM from the previous interception. Then from *t = 3.6 min* till *t = 4.0 min*, while BT is sharing the key share for the simulation of the satellite reset it will attempt to intercept the keys again, if the keys are already intercepted C3 will mask it's public and private key as the C2 keys. Then will attempt to send a message masked as data to C1.
7. This section will be split between RT, BT, All Systems[7] and Iridium --
   a. RT - C3 will continue to attempt to mask and mask itself as C2 from *t = 4.0 min* till splashdown (*t = 15 min).*
   b. BT - after the solar panels have retracted the message DATA1 will be resent to let us know of the status of them*, t = 4.5 min.*
   c. BT - if the attack is successful the actual data being sent will be moved to another port on the LAN so that we still get DATA2. The timing on can not be determined on this part.
   d. All Systems - at *t = 5.0 min* and *t = 6.0 min* the data from everything will be backed up to an external USB drive.
   e. Iridium - will continue to send data from *t = 4.0 min* till splashdown.
8. Splashdown -- *t = 15 min.*

[7] All systems events are required events to ensure data integrity.