CG1112 Engineering Principles and Practies II for CEG

Tutorial 7 (Week 11)

Part I

1. When Vincent's Raspberry Pi communicates with his Arduino, we populate a variable of type TPacket, then serialize the TPacket data structure simply by copying over the entire structure into an array of char (i.e. an array of bytes):

   ```
   TPacket packet;

   … Code to populate packet's fields …

   char buffer[MAX_PACKET_LEN];
   memcpy(buffer, &packet, sizeof(TPacket));
   ```

   However when Vincent communicates with another host over the Internet through vincent-server.cpp and vincent-client.cpp, he populates an array instead of a structure, using a format similar to the following, where each element is of type int32_t.

0	1	2	3	4	5	6	7	8	9
3	Command	Param 0 (4 bytes)				Param 1 (4 bytes)			

   Why do you think this was done in place of serializing a data structure? What are the relative advantages and disadvantages of each approach?

   Given your answer above, suggest how we could have implemented data structure serialization on vincent-client.cpp and vincent-server.cpp.

2. What is a digital signature, and how are they created? Explain the idea of a Certificate Authority, how they work, and why they are important.

3. In Week 11 Studio 1 it was mentioned that in order for your certificates to be accepted on web browsers, they must be signed by a recognized Certificate Authority, and not by yourself. Explain how web browsers enforce this requirement.

4. In early March 2018 certificates issued by Trustico on behalf of Digicert for 23,000 websites were revoked when the CEO of Trustico emailed the private keys matching these certificates to Digicert. Why was such action taken?