**Johns Hopkins University**

**EN.601.444/644 Network Security**

Fall 2018

Seth James Nielson

Lab #2 PRFC

***Revision 1.0 (2018/11/5:1830)***

**ASSIGNED:** 2018/11/5

**LAB #2 PRFC DUE:** 23:59:59 on 2018/11/12

For this assignment, you need to create a PRFC (Playground RFC) to specify a protocol that provides confidentiality, message integrity, and mutual authentication.

Requirements:

1. Within your github, the file MUST be named doc/prfc/drafts/secure\_transport.xml
2. The XML file must be compatible with the xml2prfc.tcl script in the class GitHub
3. Your “Secure Transport” PRFC document must:
   1. Specify a ***name*** for the protocol. In past years, we’ve had:
   2. Enable to Playground hosts to *mutually authenticate*. That is, before exchanging information, each side must be assured of the other’s identity. In typical TLS, however, only the server is authenticated.
   3. Provide for confidential communication between the authenticated peers. That is, only the two peers should be able to read each other’s communications.
   4. Provide for message integrity. No unauthorized party should be able to undetectably change the contents of the communications

**RFC 5246 and 8446: TLS 1.2 and 1.3**

Take a look at RFC’s 5246 and 8446 for TLS versions 1.2 and 1.3. Use these RFC’s as guides for your own protocol and the specification thereof.

Note that TLS is a very complicated protocol. It has a lot of functionality that is designed for systems that need to be more flexible than yours. For example, you probably need not specify a record layer, although you’re welcome to if you wish.

There is also no functional requirement for anything like TLS 1.2’s extension headers. However, if you and your team would like to have customized communications, you may want to leave open the possibility for additional data exchange in the handshake.

Your protocol need not be anything like TLS, of course. You could do something similar to Kerberos or even IP-SEC when some kind of share secret or trusted authority is required, but then be prepared to live with the consequences!!! No matter how you chose to do the algorithm, “trust” will always be the hardest problem. You will either have to trust a central authority, or have some kind of out-of-band way of establishing trust.

Assuming you do something like TLS, you will need certificates. You should learn how to generate an X509 certificate. The teaching staff can provide a trusted root authority for signing. Typically we have done this in the past by giving each team a “block” of addresses, usually something like x.\*.\*.\*. We sign an intermediate CA for “x” for the team, and then each team can generate x.a.b.c certificates for as many addresses as they want.

Note that we don’t work much with domain names in class, so certificates will be tied to addresses instead of names.

Unlike TLS, you need to fully define how certificate chains are validated in your PRFC if, in fact, you chose to use certificates.

Your protocol needs to enable two nodes to connect, identify each other, and then exchange confidential messages with integrity. You can assume that the transport layer provides reliable delivery. However, as we discussed, you cannot simply “break” the lower layer to shutdown a connection, so your protocol needs to define some kind of “close” message to send to the other side so that both sides will shut down cleanly.

**Grading**

Your Lab #2 PRFC will be graded out of 100 points according to the following schedule:

* 50 Points for addressing all necessary issues. You MUST address the following:
  + Purpose/technical background
  + Mutual authentication, setup
  + Trust model (e.g., TLS uses chains of trust to a “root”)
  + Confidential communications
  + Integrous communications
  + Algorithm specifications
  + Shutdown
* 25 Points for thoroughness. We (the grading staff) will make a judgement as to how well someone could use your PRFC to implement a compliant protocol.
* 25 Points for grammar, correct punctuation, etc.

Please note that a full ***25% of your grade*** for the writing assignment is based on correct use of the English language. If you are not a native English speaker, ***I HIGHLY RECOMMEND GETTING EDITING HELP FROM AN ENGLISH SPEAKER OR JHU’S WRITING LAB.***

There will also be 25 points of extra credit awarded to the team with the best PRFC. Said PRFC will be selected as the official PRFC for the class.

***LATE POLICY: You will be marked off 5 pts for day late. After 10 days late, you will receive NO CREDIT for this lab. That’s a significant portion of your final grade. DON’T BE LATE.***

**Collaboration Policy**

For this assignment, you will create the PRFC as a team. Do not collaborate with anyone outside of your team.