Instructor Notes for the SSL Scenario (Angle Locks)
February 2011

Students should be provided with the "CyberCIEGE SSL" lab manual

This scenario assumes the student has already played PKI scenarios, e.g., Hard Rain – however this scenario could be the first PKI scenario.

Teaching points

- SSL is a means to authenticate a server to a client (e.g., a browser).
- Browsers come pre-loaded with a set of installed roots from public pay-per-cert certification authorities (CAs)
- Some users will not install other roots
- To offer SSL protection to the general public usually requires use of a CA whose root is pre-installed.
- Pay-per-cert CAs may not be as thorough as you'd like when they sign certificates, and in general they don't indemnify you for loss if the representation in their signed certificates are fraudulent.
- SSL alone does not authenticate the client or user to the server.
- TLS is like SSL, but it does require the client to provide the server with a certificate.
- The CA that signs the server certificate may be independent of the CA that signs the client certificate.

Phase One

Player must get a server certificate for the Web Server from VeriScream and enable SSL on the Web Server.

Phase Two

Player must configure Web Server to require TLS when accessing the schematics. The TLS setting should only permit access by members of the Protractus group. The Protractus root must be installed on the Web Server. Alternately the player can buy a CA and use that as the installed root and sign the Protractus CA's certificate using the new CA.

Phase Three

The player must buy a smart card minter and install its root in the web server. The pricing models must be protected with TLS, with access limited to member of Angle Locks. A "No XCert" certificate policy is needed. If the player had installed the Protractus CA as a root, this policy won't validate a Angle Locks cert signed by a Protractus CA. Similarly, if the player cross certified the Protractus CA, that would not validate for this purpose. Configure the "visitors" workstation to install the smartcard minter's certificate as a root, and require TLS when accessing the pricing model.