Transport Security Basics

- Http: – Insecure
- SSL/TLS(SSL3.1) – Encryption Transport
- Telnet – Default Insecure, can initiate TLS to become secure
- FTP – Insecure
- IMAP/SMTP/POP3 – Default Insecure, can initiate TLS to become secure
- SSH – Secure telnet like using SSL/TLS to secure
- Https: – Http secured using SSL/TLS

SSL/TLS

- SSL – Secure Socket Layer, protocol defining a mechanism for negotiating an encryption/decryption path that is protected against being decrypted by 3rd parties. One of the most popular libraries implementing this protocol is called OpenSSL. This definition has stopped being improved upon, and has been renamed to TLS as of SSL spec 3.1

SSL/TLS 2

- TLS – Transport Level Security next generation of SSL protocol. It starts with SSL 3.1. There were various factors behind the renaming, one of which was the purpose of becoming a IETF RFC standard.

SSL/TLS Critical Information

- Uses RSA, Diffie-Hellman (DHE) or the modified Elliptic Curve Diffie-Hellman (ECDHE) for negotiating the session keys used to protect the content
- In order to be secure, it utilizes Trusted Certificate authorities, in order to verify that the servers being interacted with are who they say they are.

SSL/TLS Implementation

- Uses a key exchange mechanism in order to generate a unique transient session key that
- Relies on well know certificate authorities
- Will encrypt and decrypt the conversation using the transient session key, not the server certificates. Those are only used when generating the transient session key.

SSL/TLS Resources

- How SSL Works
  https://publib.boulder.ibm.com/tividd/td/TRM/GC32-1323-00/en_US/HTML/admin231.htm
- MS How SSL/TLS works.
  https://technet.microsoft.com/en-us/library/cc785811%28v=ws.10%29.aspx
- SSL Forward Security
  https://community.qualys.com/blogs/securitylabs/2013/06/25/ssl-labs-deploying-forward-secrecy
- SSL FAQ
  https://www.rapidssl.com/learn-ssl/ssl-faq/

Trust Relationships

- SSL/TLS – Trusted Certificate Authorities. A keystore built into all modern web browsers that list the primary trusted CA's on the web. Often web browser updates are to modify this keystore as CA's become untrusted, because their master private keys get decrypted
- OAUTH – Trusted sites that are used to validate user authorizations, at a cost. The cost is the user privacy. The trusted sites will often keep track of what sites you are logging in to for their own purposes. Possibly to sell to unknown 3rd parties.

Trust Relationships

- WSIT – Web Service Interoperability Technology. A version of JAX-WS that is compatible with both Java and .NET 3.0. Designed to be able to securely define tokens to authenticate various portions of the communication and authentication domains for an application.
- WS-Trust – WSIT Sub that defines the protocol to pass around trusted tokens.

Trust Information Resources

- WSIT
  https://wsit.java.net/docs/trust-whitepaper.pdf
- OAUTH
  https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2
- OAUTH Tutorial
  http://blog.oauth.io/oauth-tutorial
- Spring OAUTH
  http://projects.spring.io/spring-security-oauth/docs/tutorial.html