Michael Guidry
March 10, 2017

Some SSL implementations may continue introducing far ranging attack vectors beyond compromising electronic communications

Secure Socket Layer (SSL) is a protocol that sits layered on top of the world wide web's Hypertext Transfer Protocol (HTTP) protocol. HTTP is the communication layer of the majority of web browsing actions such as loading a web page from websites. SSL is also layered into other protocols that do not relate to web browsers. Corporations, and software engineers like to use SSL due to its extensive history. Lots of effort in the form of money, and time has been used researching, modifying, and securing the protocols, and their various implementations. It is generally the first choice as an acceptable form of secure communications for any software that communicates across networks. It gives the ability to use various load balancers which may work on top of SSL related services. Operating systems, web browsers, and software often use the global SSL certificate hierarchy. Custom software may create their own brand new private hierarchy as an alternative option to lower the vulnerability of trust landscape.

Certificate Authorities (CA) are companies which sell certificates as a product to websites. CA themselves are given trust by corporations such as Microsoft to distribute certificates which are to be trusted by Microsoft Windows. Each link in this chain will get verified from the bottom to the apex for each verification, or use. Microsoft is at the top of the pyramid for their certificates. It may have three or more links connecting other certificates before reaching Microsoft's initial certificate. The beginning of the chain for three, or four layers are usually installed on every computer through the operating system.

Rules and regulations surround becoming a CA because trust is required for secure communications throughout all of the links being verified with the certificate's chain of trust. It is only necessary to use a CA if your application doesn't use a custom chain of certificates. The certificate chain verification is required to secure their connections to the clients browsing their web sites. The trust comes from that verification process which follows the entire chain to approve its secure. The process initiates every time a connection is made which uses this security mechanism to secure communications. This is the basis of how SSL verification, and its security works. Encryption keys are distributed using the certificates which is how the cryptographic functions ensure protection. Further details are beyond the scope of this document.

Online Certificate Status Protocol Daemon (OCSPD), and other Certificate Revocation Lists (CRL) distribution mechanisms are a method for web browsers, operating systems, and other security related services to ensure SSL certificates are continuously verified against a list of certificates that were deemed invalid before expiration. Historically it would require the operating system, browser, or other types of software updates to remove invalid certificates. The importance of a certificate being valid is directly related to securing credit card transactions, communications, or other information deemed private between computers across a network. It allows a user browsing the internet to expect that their government, a hacker, or their internet provider cannot monitor the connections they create to secured web sites such as PayPal. It is becoming very popular for all major web sites to automatically redirect a user to their HTTP over SSL (HTTPS) version of the web pages.

Certificate Authorities began to abuse their trust by giving out certificates which shouldn't ever have been valid. An example would be to give a government, or corporation a valid certificate for a site such as "google.com," which obviously isn't owned by Google, Inc. Web browser clients began to upload information regarding SSL certificates to worldwide statistical servers designated for public consumption. Many other certificates were discovered that should have never been created for clientele which had no ownership of the particular site in question, or corporation they claimed relation to. OCSPD, and CRL were born to defeat the mistrusts of CA interests. Countries themselves partner, or outright own certificate authorities. One case was for a security product which intended to inspect web related internet communication regardless of whether SSL was used or not. For example, this particular scenario or others may have been directly state sponsored. Countries would sponsor these security bypass products to spy on their citizens for various political, and security reasons.

After several more highly publicized problems, the revocation protocols for removing 'bad' certificates began being installed within various operating systems, and software packages. In all modern operating systems, and browsers most connections through methods of SSL are verified to ensure they are still valid, and accepted globally as secure. It doesn't come without its own set of issues though.

The first possible vulnerability is pretty straightforward. SSL connections sometimes could cover a range of domains under the same IP addresses. OCSPD, and various other of these verification protocols will communicate within plaintext. It ensures that any Internet Provider (ISP) could implement a simple system to monitor which websites are being used from any particular computer. It is a huge leak of information on a protocol which is supposed to ensure secure cryptographically communications of SSL connections. It gives the ability for an ISP to block a revocation from even happening if that ISP is using a certificate against a particular site for intelligence gathering of their clientele.

Certificate Revocation methods may also be abused to introduce false revocations which could hinder software, and security products useless. It would be fairly easy to ensure any security product, operating system or browser would stop trusting particular sites that they require for continuing to secure their clients. If an anti virus didn't use its own protocols, and possibly even if it does use SSL revocation then it may be simple to block it from updating its virus lists, or submitting activities such as samples of attack software being used on the target to the security industries cloud networks. Firefox is a web browser which for a short time had versions which completely blocked access without ability to ignore invalid certificates, although changed this policy due to so many self signed sites.

Certificates built directly into the operating system may also be used to disable drivers signed by stolen certificates. It allows the ability for finding some certificate that is within a chain, and then blocking any types of drivers you wish. It could be used to completely destroy operating systems from booting if the attack is performed correctly. The revocation could be done on embedded systems that have nothing to do with any of these prior fields which could allow destroying some devices from ever communicating with any other devices permanently.