**Discussion 2: Man-in-the-Middle Attack**

**Describe a man-in-the-middle attack. Provide two examples of these attacks and countermeasures used by organizations within the last 12 months.**

Man-in-the-Middle attack. Refers to the attacker that puts up a fake organization like bank website and entices user to that website. User types in his password, and the attacker in turn uses it to access the bank's real website. Done right, the user will never realize that he isn't at the bank's website. Then the attacker either disconnects the user or makes any fraudulent transactions he wants, or passes along the user's banking transactions while making his own transactions at the same time. The thing that would be damaging for them would be if somebody released a targeted null prefix certificate for Bank of America," he said. "That would affect all Microsoft products that are still unpatched (Goodin, October 1, 2009).

In this technique the attacker take advantage of a weakness in the TCP/IP protocol stack, and the way headers are constructed in the network. Hijacking occurs when the individual between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data (CWE, 2013).

Another example of the Man-in-middle attacks is like someone assuming your identity in order to read and monitor your messages. The person on the other end might believe it is you, because the attacker might be actively replying as you, to keep the exchange going and gain more information.

A critical issue was the that of Belkin router according to John Leyden “In response criticism, a Belkin product manager came forward this week to confirm the behavior was designed into the products as a way to make it easier for consumers to sign up to a free trial of its parental control software. Belkin's Eric Deming is keen to allay concerns about the technique which have produced sharp criticism of the company on the news.admin.net-abuse. Email newsgroup” this a case of man in the middle attack (Leyden, 2003).

Reference

CWE (2013). Channel Accessible by Non-Endpoint ('Man-in-the-Middle'). <http://cwe.mitre.org/data/definitions/300.html>

Goodin, Dan (October 1, 2009). "SSL spoof bug still haunts IE, Safari, Chrome; Thanks to Microsoft". The Register.co.uk. Retrieved July 17, 2010.

Leyden, John (2003-11-07). "Help! My Belkin router is spamming me". Nagware promotes censorware. http://www.theregister.co.uk/2003/11/07/help\_my\_belkin\_router/