### Assignment 5: Certificate pitfalls

John Smith generates a public/private key pair, and buys from a trusted CA (e.g. Symantec) a personal certificate for John Smith on his public key. He then generates a second public/private key pair, and uses his John Smith private key to sign a certificate on the second public key where the common name is set to *www.amazon.com*. John now has two certificates: one signed by Symantec for subject *John Smith* and another signed by John Smith for subject *www.amazon.com*.

Now, John, being the malicious sort mounts a man-in-the-middle attack on an SSL connection to Amazon.com from some unsuspecting user. John presents his forged certificate chain for *www.amazon.com* to the intercepted user. The intercepted user’s browser incorrectly accepts the fake Amazon certificate as legitimate because there is a valid certification path to Symantec's trusted CA.

1. Why does this scenario present an attack? How can it be exploited?
2. How would you fix this problem? That is, what would the intercepted user's browser need to do to prevent the problem? What would Symantec need to do? Hint: The certificate format is called X509v3. Read about the "CA bit" in the Basic Constraints field of an X509v3 certificate.