Apple GoTo Fail Self Study

1. What is this vulnerability?
   This vulnerability essentially bypassed SSL certificate validation checks in Apple's SSL/TLS implementation in MacOS and IOS. This allowed for "secure" connections to be vulnerable to man in the middle eavesdropping by attackers forging SSL certificates and being unconditionally trusted.

2. What is its root cause?
   The root cause was a duplicated line of code that would essentially bypass SSL certificate validation. It essentially looked like the following:

   ```
   if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
           goto fail;
           goto fail;
   ```

   There were a series of failures that allowed for this to have been pushed to Apple's SSL/TLS implementation, such as improper code review techniques, poor code structure, lack of using curly brackets around multi-line if statements, lack of compiler warnings, etc.

3. What is the extent of its impact?
   All devices running IOS 6, IOS 7, and MacOS X 10.9 Mavericks, as well as all software that used Apple's SSL/TLS implementation, such as safari, mail, calendar, etc. were vulnerable to man in the middle (mitm) attacks. This means that every single device could have been compromised and revealed sensitive information, such as personal information, bank login information, or other sensitive information.

4. How to patch it? (Or how it was patched by the vendor)
   To patch this issue, Apple essentially just removed the second, unnecessary goto fail; line of code. This allowed for the SSL certificate verification to not be avoided and made it such that attackers could not forge SSL certificates with impunity.

5. How could it have been prevented?
   There were many ways that this could have been prevented. For example, Apple could have simply not overlooked the duplication of the goto fail; line, they could have caught it at some point during the code review process, they could have hired penetration testers that could look for severe bugs like this, they could have enforced proper code formatting (brackets for multi-line if statements), or they could have taken many other steps that could have potentially prevented this failure.