Use Cases for the Maxwell Pro TLS Test Suite

1 Maxwell Pro discovered SSL Security Flaw in iOS

Executive Summary: The Maxwell Pro TLS Test Suite includes nine tests related to ServerKeyExchange; three of these tests yield failing grades for iOS TLS or SSL code had been tested with the Test Suite.

The problem found in the open source SSL code used in iOS may be reviewed here:

http://opensource.apple.com/source/Security/Security-55471/libsecurity_ssl/lib/sslKeyExchange.c?txt

In the function SSLVerifySignedServerKeyExchange() there are two goto statements where there should only be one:

```
...
        if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
                goto fail;
                goto fail; /* <<----- ****** Problem! ******/
        if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
                goto fail;
        err = sslRawVerify(ctx,
                           ctx->peerPubKey,
                           dataToSign,              /* plaintext */
                           dataToSignLen,           /* plaintext length */
                           signature,
                           signatureLen);
        if(err) {
                sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify "
                        "returned %d\n", (int)err);
                goto fail;
        }
fail:
        SSLFreeBuffer(&signedHashes);
        SSLFreeBuffer(&hashCtx);
        return err;
...
```

The second indented "goto" causes a section of code to get skipped (it is unreachable, and the compiler allegedly fails to warn about that.) The code that gets skipped is verifying the ServerKeyExchange message for SSL. That code validates that the host is who it claims to be.

2 Gnu TLS cryptographic bug

The Red Hat Bugzilla report explained:

> "A malicious server could use this flaw to send an excessively long session ID value, which would trigger a buffer overflow in a connecting TLS/SSL client application using GnuTLS, causing the client application to crash or possibly execute arbitrary code."[1]

IWL used our Maxwell Pro TLS Test Suite to test one version of the GnuTLS library. It failed 39 out of 116 of our tests! Fortunately most of those failures are benign, typically caused by responding with the wrong response to a malformed or out of sequence message. Others, such as improper handling of buffer overruns, can be open to exploits. Because this bug attacks clients rather than servers, it requires extra steps at subterfuge to be taken by attackers to exploit it.

Use the Maxwell Pro TLS Test Suite to test for session ID overflow.