**Question 1: When it comes to Smash the Stack, what are the stack canaries? Give a definition and an example.**

Answer: Like canaries in a coal mine, stack canaries help to detect trouble - in this case, buffer overflow. An example of a canary is a “random canary” that consists of a NULL byte followed by three random bytes.

**Question 2: The following code contains errors that could be exploited. How would you fix it?**

***hashOut.data = hashes + SSL\_MD5\_DIGEST\_LEN;***

***hashOut.length = SSL\_SHA1\_DIGEST\_LEN;***

***if ((err = SSLFreeBuffer(&hashCtx)) != 0)***

***goto fail;***

***if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)***

***goto fail;***

***if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)***

***goto fail;***

***if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)***

***goto fail;***

***if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)***

***goto fail;***

***goto fail;***

***if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)***

***goto fail;***

***err = sslRawVerify(...);***

Answer:

hashOut.data = hashes + SSL\_MD5\_DIGEST\_LEN;

hashOut.length = SSL\_SHA1\_DIGEST\_LEN;

if ((err = SSLFreeBuffer(&hashCtx)) != 0){

goto fail;

}

if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0){

goto fail;

}

if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0){

goto fail;

}

if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0){

goto fail;

}

if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0){

goto fail;

}

if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0){

goto fail;

}

err = sslRawVerify(...);

**Question 3: How could you catch this error in the future?**

Answer: Through static and dynamic analysis. https://dwheeler.com/essays/apple-goto-fail.html has a good review of the possible countermeasures.

**Question 4: Heartbleed bug could be traced to a single line of code. What was that line of code?**

Answer:

memcpy(bp, pl, payload);