Andrew Chin
A8chin
20378330
A2 CS458

1a.

1i. Bob removes the name tag from the function and passes r1 and r2 to Alice.

Mallory can impersonate Bob with this modified protocol by doing the following.

- Mallory has intercepted communications between Bob and Alice
- Mallory waits till Alice initiates the protocol
- Alice initiates the p rotocol by sending r1 which Mallory intercepts
- Mallory needs to calculate y1 = MyF(K, r1, r2).
    - In a separate connection, Mallory initiates the protocol with Alice by sending r1
    - Alice calculates y1 = MyF(K, r1, r2) with an r2 she chooses.
    - Alice responds to Mallory with {r2, y1}
    - Mallory ends the protocol prematurely
- Mallory sends {r2, y1} that Alice computed to Alice
- Alice computes x1 = MyF(K, r1, r2) which will match y1 that Mallory sent
- Alice sends Mallory x2 = MyF(K, 0, r2)
- Mallory accepts and begins conversation with Alice

1ii. R1 and r2 are both stored in a 64 bit uint, with r1 taking up 14 bits and r2 being 50 bits.

Since r1 is 14 bits in length, there are a maximum of 16,384 (2^14) possible r1 values.

Mallory can either:

- Eavesdrop on Alice and Bob when the protocol is in the first 2 steps to record {r1, r2, and y1} sets.
- Mallory can spam Bob with incremental r1 challenges and record his response until all 16,384 values have been tried.

Mallory builds a dictionary of responses, {r2, y1}, using {r1} as an entry key.
With r1 being only 14 bits, Alice will eventually reuse an r1 challenge, which is when Mallory can intercept and impersonate the Bob.

Mallory can impersonate Bob with this modified protocol by doing the following.

- Mallory has intercepted communications between Bob and Alice
- Mallory waits till Alice initiates the protocol
- Alice initiates the protocol by sending r1 which Mallory intercepts
- Mallory looks up {r1} in her dictionary to find {r2, y1} with y1 =MyF (K, “Bob”, 2^{50}(r1) + r2).

- Mallory sends {r2, y1} that bob computed to Alice
- Alice computes x1 = MyF(K, “Bob”, 2^{50}(r1) + r2) which will match y1 that Mallory sent
- Alice sends Mallory x2 = MyF(K, “Alice”, r2)
- Mallory accepts and begins conversation with Alice

1b. There are two authentication factors Alice has to provide to the bank, the ownership of her credit card, and her knowledge of her credit card PIN. Alice identifies the bank by exclusively using her bank’s designated ATMs, and the bank identifies Alice by her credit card.

2a. Alice can read D105. Alice can write to D103.

2b.

	Object	Alice
i	D101: (Classified, {Delta})	(Secret, {Beta, Delta, Epsilon})
ii	D102: (Secret, {Alpha, Beta, Delta})	(Secret, {Beta, Delta})
iii	D103: (Top Secret, {Beta, Epsilon})	(Secret, {Beta})
iv	D104: (Secret, {Beta})	(Secret, {Beta})
v	D105: (Classified, {Delta, Epsilon})	(Classified, {})

3A FAR Stranger A: 5% R: 95%

AAA AAA 0.05^6 =

AAA AAR $(0.05^5 \times 0.95^1)\binom{6}{1}$ =

AAA ARR $(0.05^4 \times 0.95^2)\binom{6}{2}$ =

+ ______

= 0.000086406

FAR = 0.0086406%

FRR Alice A 90% R 10%

AAA RR$\boxed{R}$ $(0.9^3 \times 0.1^3)\binom{5}{2}$

AAR R$\boxed{R}$ $(0.9^2 \times 0.1^3)\binom{4}{2}$

ARR $\boxed{R}$ $(0.9 \times 0.1^3)\binom{3}{2}$

RR$\boxed{R}$ (0.1^3)

+ ______

= 0.01585

FRR = 1.585%

3b What is the chance a stranger is using Alice's phone AND it is locked within 6 swipes.?

$$\left.\begin{array}{ll} AAA\ RR\boxed{R} & (0.95^3 \times 0.05^3)\binom{5}{2} \\ AAR\ R\boxed{R} & (0.95^2 \times 0.05^3)\binom{4}{2} \\ ARR\ \boxed{R} & (0.95^1 \times 0.05^3)\binom{3}{2} \end{array}\right\}$$

chance a stranger locks the phone within first 6 swipes

$RRR \quad 0.05^3$

$$+ \overline{}$$

$= 0.002229$

0.002229×0.08

$= 0.000178$

0.0178% chance it locked correctly