Assignment #4

Cryptanalysis

Due: November 1, 2016

1. Recall the meet in the middle attack against Double DES with two keys: $C = E(K_1, E(K_2, M))$, where M is the plaintext, C is the ciphertext, and K_1, K_2 are the keys, each 56-bit long. Using its time and space complexity figures in the lecture slides, determine an optimal cost to compute one Double DES key K_1, K_2. Use the following rough OpenSSL performance numbers for DES (from one of my Linux VMs running on a Haswell class CPU): 6 million DES operations (encrypt or decrypt) per second, per 64-bit block. *Hint: You can use the price of any cloud provider with a general purpose VM and storage offering.*
2. We mentioned that the Bellcore RSA attack computes GCD using a faulty signature, a real signature, and the modulus to factor the prime divisors of the modulus. This attack requires a real signature S known. But, it is possible to deploy the same attack without a known real signature S due to $p = gcd(\tilde{S}^e - M, N)$. Using the slides on Bellcore RSA attack, show how the attack without a real signature S works.
3. One of the side channel attacks against RSA exploits the time difference between squaring and multiplication as follows. Note that the code is simplified by removing input error checks for clarity; they are not pertinent for this question. As discussed, assume that squaring is faster than multiplication.

```
function ModularExp(base, exponent, modulus)
    t := 1
    while (exponent > 0)
        if (exponent mod 2 == 1) then
           t := (t * base) mod modulus
        exponent := exponent >> 1
        base := (base * base) mod modulus
    return t
```

   An attacker can observe the execution trace of a program running the code above and determine the timing of each step from beginning to the end of the code. We alluded to a timing attack to determine the private key if the exponent input is the RSA private key.
   a. Describe how that attack would work.
   b. Come up with a countermeasure (not necessarily efficient).
4. Car fobs and garage door openers use a one-way protocol from a key fob or opener button to a door lock or garage opener. This used to be done with a fixed code wherein the transmitter sends a code and the receiver opens the door or lock whenever it receives the code. Because of the massive weaknesses, newer devices *roll* the code with each press of the transmitter, and the receiver listens for and activates with any of the next several (where several may be up to a thousand) codes. The transmitter gets no feedback, so it always just transmits the next code in its sequence. When the receiver accepts a valid code, it synchronizes by invalidating that code and will then only respond to the next code(s).

Assume that good cryptography is used to produce the code sequence and that an attacker has no ability to predict future codes but that an attacker can build a transmitter/receiver powerful enough to receive a signal while jamming the transmission so that the receiver doesn't hear it. Describe how this device can be used by an attacker to gain access to a home or car.

5. Suppose we have constructed an excellent fare payment system in which cards and readers authenticate each other properly as follows.
    a. Card transmits, "I'm here and want to pay."
    b. Upon hearing this, reader transmits its authenticated credentials which includes an authenticated encryption public key.
    c. Upon validating credentials, card encrypts its identity and a payment instruction.
    d. Upon receiving and validating payment instruction, reader flashes green to accept rider.

   Every day, I go to a crowded bus stop, queue up to board, and tap my satchel against the reader to get it to flash green. Describe how I can do this without ever paying a fare.

   Bonus [0 points]: In local transit lingo, ORCA is an acronym for "One Regional Card for All" – which (beyond sounding ridiculous) makes the term "ORCA Card" redundant. Provide a better acronym.