CNT4406 – Network Security **Spring 2024**

Homework 1: Deadline Thursday 2/8

Instructor: Viet Tung Hoang

Recall that your solution must be produced via Latex.

1. (**Timing attacks**) (60 points) Let $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher. For a string X, let $X[i]$ be the i-th bit of X. In our convention, string index starts from 1, meaning that an n-bit string X is $X[1]X[2]\cdots X[n]$.

Consider the following implementation of the challenge-response protocol. For each n-bit challenge N, you are allowed to make as many responses as you like. For each response X, the sever will first compute $T \leftarrow F_K(N)$, where K is the secret key. It then runs the following code:

```
For $i \leftarrow 1$ to $n$ do
    If $T[i] \neq X[i]$ then output **reject** and exit
Output **accept**
```

Assume that you can measure the running time of the server with reasonable accuracy to know *exactly* how many iterations the for-loop takes. Given a challenge N, recover the secret answer $T \leftarrow F_K(N)$ after $O(n)$ responses.

2. (**Reconnaissance attack**) (80 points) The IP packet header contains a 16-bit ID field. The protocol standard states that the ID field should differ between different packets sent by a source to a given destination.[1] A common method that hosts use to implement the ID field is to maintain a single counter that the host increments by one for every packet it sends, regardless of to which destination it sends it. The host sets the ID field in each packet it sends to the current value of the counter. Since with this implementation the host uses a single counter for all of its connections, we say that the host implements a global ID field.

(a) (30 points) Suppose a host P implements a global ID field. Suppose further that P responds to ICMP ping requests. You control some other host A. How can you test if P sent a packet to anyone (other than A) within a certain one minute window? You are allowed to send your own packets to P.

(b) (30 points) Your goal now is to test whether a victim host V is running a server that accepts connection to port X (that is, test if V is listening on port X). You wish to hide the identity of your machine A. Hence, A cannot directly send a packet to V, unless that packet contains a spoofed source IP address. Explain how to use P to do this.

Hint: The trick here is to send TCP packets to V with the spoofed source IP address. Recall the following facts about TCP.

- A host that receives a SYN packet to an open port X sends back a SYN/ACK response to the source address.
- A host that receives a SYN packet to a closed port X sends back a RST packet to the source address.
- A host that receives a SYN/ACK packet that it is not expecting sends back a RST packet to the source address.
- A host that receives a RST packet sends back no response.

[1] If a host sends more than 2^{16} packets, the field will necessarily repeat. That consideration doesn't matter for this problem.

c) (20 points) How would you change P to avoid this problem? You are not allowed to modify the TCP/IP protocol or the services running on P. You may only modify the implementation of TCP/IP on P.

3. (**DoS attacks**) (30 points) You want to perform a DoS attack against some host with a known IP address. You have become aware that a mis-configured sub-network, corresponding to the range `w.x.y.z/24`, allows for external access to its *broadcast address*, i.e., traffic sent to `w.x.y.255` reaches *all* hosts simultaneously on that sub-network. Note that neither you nor your target are on this sub-network.

Describe as clearly as possible how you can take advantage of the sub-network to perform a denial-of-service attack on the target.

4. (30 points) You are given a 16-byte string X. Describe briefly how one could find a **message** M such that the last three bytes of $\mathrm{AES}_X(M)$ are `0x000102`. You are allowed only a **single call** to AES or its inverse.