CS 336 Fall 2015

Assignment 10: Security and Encryption

Due the week of November 19/20, 2015

The two topics for this week, security and encryption, are certainly related, but not as clearly related as one might assume. Encryption can be used as a tool to improve security and privacy on the network, but it is far from sufficient to guarantee security and privacy. In an assignment like this (or in a textbook!) it is tempting to focus on encryption algorithms and applications of encryption to design more secure protocols. There is plenty of interesting material to discuss and plenty of problems to assign. The problem is that there is a lot more to security than encryption. Most significant violations of system security involve exploitation of bugs in software or of human weaknesses rather than the cracking of complex encryption algorithms. Alas, there are not many good homework problems one can ask about software bugs and human weaknesses.

As a result, this week will consist of readings that cover both topics together with a number of exercises that are far more about encryption than about security.

To start, read the book. In particular, please read all of chapter 8.

Then, so that you appreciate what I mean when I say that security requires much more than encryption, I would like you to read two papers describing techniques that can be used to defeat the original security mechanism designed for 802.11 wireless networks, WEP. The first paper, "Intercepting Mobile Communications: The Insecurity of 802.11," discusses the basic design of WEP and explains its weaknesses. The second paper, "The Final Nail in WEP's Coffin," explains how the security of an 802.11 network can be compromised even more quickly by taking advantage of interactions between WEP and 802.11 fragmentation mechanisms. While reading both papers, recall that RC4, the encryption scheme used by WEP is fundamentally secure!

Exercises

1. You intercept a binary message consisting of 16 digits whose value as a binary number is 40679 when expressed in decimal. You know that the public key of the intended recipient was (77059, 47). You suspect that the message is a two letter word encoded in ASCII. What is the recipient's private key? What is the decrypted message? Explain how you determined these values. Hint: A spreadsheet may help you solve this problem.

2. Complete problem 8.9 from Peterson and Davie.

3. Complete problem 8.14 from the text.

4. Complete problem 8.10 from the text.

   The way the problem is stated makes it a bit unclear what they really want. The first sentence mentions poker, but the rest of the problem talks about picking random numbers. While picking random numbers might be necessary to play poker, it isn't clear that it is enough. To deal cards, you need some way to make sure both players never think they both have a particular card in their hand. If you "deal" by just picking random numbers between 1 and 52, this will not be guaranteed. Two player might end up picking the same number.

   Accordingly, I would suggest you view this as a two part problem:

   (a) Simply make it possible for players A and B to choose a single card for B in such a way that

- Neither A nor B alone can control which card is chosen.
- While the hand is being played, only B can tell which card has been selected.
- When the hand is complete, B must provide information to A that will enable A to learn which card was chosen.

(b) Now, for the hard part. Propose a scheme by which players A and B can choose a hand of 5 cards for A and 5 cards for B from a deck of 52 cards. That is, propose a scheme that will enable A and B to select two sets of 5 random numbers between 1 and 52 in such a way that

- Neither A nor B alone can independently control which numbers are chosen.
- The 10 numbers chosen are distinct.
- While the hand is being played, only A knows the first 5 numbers chosen and only B knows the second 5 numbers chosen.
- When the hand is complete, A and B must provide each other with additional information that will enable each of them to determine all 10 of the cards/numbers selected.

Hint(?): This is close to an open-ended problem. Based on the answer key, the book only expected an answer to part a. I think I have concocted a scheme to solve (b) based on a generalization of a scheme known as "blind signatures". The following description of blind signatures is adapted from the RSA inc. web site:

> Suppose Alice has a message m that she wishes to have signed by Bob, and she does not want Bob to learn anything about m. Let (n, e) be Bob's public key and (n, d) be his private key. Alice generates a random value r such that $gcd(r, n) = 1$ and sends $x = (r^e m) \bmod n$ to Bob. The value x is "blinded" by the random value r; hence Bob can derive no useful information from it. Bob returns the signed value $t = x^d \bmod n$ to Alice. Since
>
> $$x^d = (r^e m)^d = rm^d \bmod n$$
>
> Alice can now obtain a copy m that has been encrypted using Bob's private key (and therefore "signed" by Bob) by computing $s = r^{-1} t \bmod n$.

5. A key weakness of the WEP protocol is the fact that all computers interacting with a base station use the same key to generate RC4 keystreams. The techniques described by both of the papers included in this week's readings exploit this weakness.

Sharing a password has obvious advantages (it simplifies configuration since the access point does not have to be reconfigured for each new station that arrives), but it makes it much easier for an attacker to send message and decrypt messages sent by or to others.

One alternative that preserves the advantages of a common key but might increase the security of the system would be to only use the common key to exchange messages between computers and the base station when a station first joins the network to establish separate keys that can be used for communication between the base station and each computer. That is, when a computer first communicates with the base station it will send a message encrypted using the common key to the base station requesting that the base station assign it a randomly chosen key and send that key to it encrypted using the common key. From then on, all messages sent between the base station and this computer will be encrypted using this randomly chosen key. Both the base station and the computer must save copies of the randomly chosen key. In fact, the base station will need to maintain a table associating the correct key with the MAC address of each computer to which it had assigned a key and use this table together with each message's source address to determine which key to use.

Obviously, every computer using the network legitimately will be able to decrypt all of the messages used to deliver randomly chosen keys. So any computer that knows the common key can build a table of all the private keys and decrypt any traffic it intercepts. So this technique does not prevent a legitimate user's computer from intercepting messages sent to other legitimate computers. That is not the goal. The goal is to make it more difficult to attack the network without somehow obtaining a copy of the common key. In particular, since far fewer packets would be sent encrypted using the common key, it would be more difficult to collect keystream sequences for one or more IVs as suggested in both papers.

I would like you to do two things with this scheme. First, fill in its details. In particular, assuming that this scheme were to be deployed as an improvement of the existing WEP system, marketing concerns would demand that the improved protocol be backward compatible. Explain what would be required to ensure backward compatibility (computers using the old scheme should continue to work).

Second, can you find a way to attack a network using this new system. That is, can you either identify an attack in one of the papers that will work even in the presence of this new mechanism or devise a new attack (probably derived from an attack in the papers) that works even when every legitimate computer uses a different key to encrypt/decrypt messages.

At a minimum, explain why/how this key distribution mechanism defeats any of the techniques described in the paper.