HW2

Problem C-2.11

1. Cryptographic hash is not secure. Even though it's not plain text, an 8-digit hash is not extremely hard to figure out. Especially when the user might use a wiretapping device to get tons of hashed account numbers, it becomes easier for the attackers to figure the hash out.
2. Public-key cryptography is not secure because public keys are visible to everyone, including the attacker, which might be helpful with decrypting the encrypted account number. It could be very dangerous if all the accounts are using the same public key to encrypt.
3. Private-key cryptography is safer because the private key is not visible to the attacker. The private key can be as long as the bank wants, and it's harder for hackers to figure out the number without knowing the length of the key.

Problem C-4.6

We can look at the source code for the C compiler and login system and find out where the inserted code is. Then we add commands to skip the malicious code. Recompiling the source code should be able to fix the issue.

Problem C-4.8

Because the keylogger only reads the keyboard input, we can enter the password without typing it out. We first paste all the needed characters to the text editing window. Instead of typing it with the keyboard, we can copy and paste the characters one by one to form our password.

Problem EMV

Magnetic stripe cards use a magnetic stripe on a card to store all customer's information, including account number, PIN, card verification number. When the customer uses a card, magnetic stripe cards transmit static information, which is easier to copy the information by an attacker.

EMV is much more secure because the transaction data is continuously changing for EMV chips. Unlike the magnetic stripe card, EMV uses a one-time digital code for every transaction or purchase. This one-time data will be more difficult for the attackers to steal the information from an EMV card.

EMV also prompts the user to enter the PIN code instead of storing it in the card. This builds an extra layer of security. If the card is physically lost or stolen, other people will not be able to use the EMV card because it requires the PIN. However, they can use the magnetic stripe cards and make transactions until the cardholder reports to the bank and replaces the card.

When users are using the EMV chip cards, they will need to confirm the amount of transaction before it happens. In this case, the cardholder will know exactly how much they are spending or transmitting. However, for cardholders of the magnetic stripe card, they won't know if they are spending extra money until they check the completed transaction.

Problem Acoustic Direct Attack

When a computer is running, the electronic components vibrate and generate high-pitched noise. Those noises are the same to human ears, but actually distinguishable from each other if users perform different operations. Additionally, since the normal room noise is usually at a lower frequency than what the computer generates. They are really easy to detect and filter out. Any physical protection, like having a fan or shielding, doesn't fix this leakage because it doesn't interfere with the acoustic signal generated by a computer operation.
The acoustic direct attack uses this information to get some knowledge about this computer There are many ways for the attacker to collect the noise. It could be something physically near the target computer, like a suspicious phone near the computer or a sensitive microphone within 4 meters of the target computer. It can be something invisible, like an attack app, a web browser requiring microphone access or eavesdropping bugs existing in your devices.
Once the attacker collects those noises, they can analyze the data, and get some information about the target computer. In many machines, the attacker can learn patterns of CPU operations and programs running on the computer. On some machines, the attacker can even convert the noise to get the RSA secret keys for encryption or decryption.

Problem Cold Boot Attack

Encrypting hard drives is commonly believed to be a good data protection method. It protects the sensitive data against data theft even if the attacker can access the machine physically. However, the cold boot attack indicates disk encryption itself is not a sufficient protection.
Cold Boot Attack is mainly based on two facts about the memory. One is that memory data decay gradually as time passes after power off. The other is that the decay rate of data is significantly reduced as temperature decreases. It allows the attackers to recover the residual data and access sensitive data.
Additionally, there is limited protection against those attacks. BIOS may overwrite the memory and wipe out the data before powering off. However, even though many machines use a destructive memory check, this feature can be bypassed or disabled. The others either have the BIOS which only overwrites a small portion of memory or they use ECC memory which could potentially help the attacker.
A simple attack is to reboot the target machine in cold temperature which significantly reduces decay rate and avoids data whipping by OS and applications. If the target machine cannot be rebooted, cold temperature allows the attacker to minimize the data decay while transferring the memory data to another machine. After getting the residual data, the attacker could use algorithms to identify and reconstruct the cryptographic keys, such as DES, AES, tweak keys, and RSA private keys. Once the key information is extracted, the attacker can steal this machine and access any data they want.