Assignment Report
Introduction to Information Security Infrastructure

PhD student: Phan Xuan Thien
Student ID: 20141712

- Problems:

1. Describe differences between checksum and cryptographic hash.
2. Describe the basic mechanism of CHAP.
3. Describe differences between WEP, WPA and WPA2.

- Answers:

1. The differences between checksum and cryptographic hash:

Although both of Checksum and Cryptographic hash are methods for checking data integrity which uses integrity codes to detect changes to data, they have some differences:

- In checksum method, the sender computes the parity bits (use even parity, or polynomial math,…) and transmit them with the data. The receiver applies the same formula to the data and compares the result with the integrity code that was transmitted to ensure with high probability that the message he received is intact. Checksum can detect simple transmission and other accidental errors, but cannot detect malicious errors in which the data is modified intentionally. This is because checksums are easily predicted and forged. If a bit is changed, it is easy to determine how the checksum are change. Similarly, for every bit change it is easy to determine an additional bit in the stream to change to counteract the effect of the first change, thus leaving the unchanged checksum still valid.
- Unlike checksum, cryptographic hash is a one-way hash function in which a small change in the input results in a very large change in the hash. Thus it is computationally infeasible to invert, for example, the source cannot be easily computed from a given hash. Typically, a single-bit change is the source lead to the changes of approximately half bits in the hash. Therefore, cryptographic hash is much securer than checksum and it can be used especially to protect the integrity of data from malicious changes from a compromised middleman.

2. The basic mechanism of CHAP:

CHAP (Challenge handshake authentication protocol) is a popular protocol for authenticating users of the Point-to-Point Protocol based dial-up systems. CHAP is used for one system to identify itself to another system if they have shared secret. In CHAP, the authenticator issues a Challenge number and send to the peer. This challenge consists of an identifier and a value. The peer then replies by a 'response' back to the authenticator. This response is created by computing the MD5 hash of the identifier concatenated to the shared secrete concatenated to the value. When receiving the response from the peer, the authenticator computes this value too, then compare it with the peer's response. The authenticator issues a "success" notification message and sends it to the peer if the peer successfully identified itself, otherwise it sends a "failure" message. Fig. 1 illustrates the basic mechanism of CHAP.

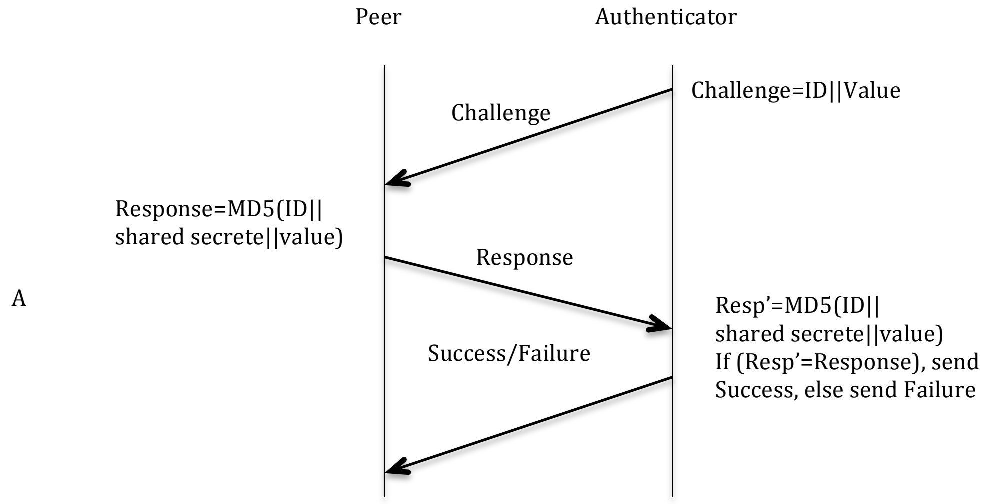

Fig. 1: Basic mechanism of CHAP

3. The differences between WEP, WPA and WPA2

The WEP, WPA and WPA2 were designed for the security of 8.02.11b wireless networks. Although sharing the same goal, they are basically different in their mechanisms and security level that each one can support.

- The WEP consists of a secrete key of 40 or 104 bits and an initialization vector (IV) of 24 bits, thus the total protection is 64 or 128 bits.
  - In WEP encryption, the key plus the IV is used to seed an RC4-based pseudorandom-number generator (PRNG). This sends a stream of pseudorandom number that is XORed with the data stream to produce the ciphertext. In addition, an integrity check value (ICV), which is a simple CRC-32 checksum, indicates if the data stream was corrupted.
  - The WEP decryption algorithm takes the secrete key and the message consisting of the cyphertext and ICV as input and produres the plaintext message and an error flag as output by performing these steps: (1) generate the key sequence k using the IV of the message; (2) decrypt the ciphertext message by doing a bitwise XOR with k to generate the original plaintext and ICV; (3) verify the integrity of message by computing the ICV on plaintext, ICV', and comparing it with the recovered ICV from step 2; (4) trap errors, if ICV=/=ICV', by sending an error to the MAC management layer and back to the sending station.
  - WEP also includes authentication. APs perform an optional challenge/response style of authentication to the wireless stations similar to the CHAP mechanism present in the answer of question 2 above.
  - WEP contains a variety of flaws. It provides no automated key management and no distribution mechanism. All keys must be entered manually, and all wireless stations in one network typically use the same password. When the number of devices sharing the password increases, the risk that a device inadvertently shares this password increases. In addition, rekeying an entire network is very difficult. All user must be informed that the passwords are changing as of a certain date, after which they will be locked out of the network until they get the new code. Another weakness is the limit of the number of keys that can be used. And finally, using a single key for the whole network increase the chance of keystream reuse.

- WPA is different from WEP in some points. WPA uses 128-bit keys for encryption and hashing to generate new ‘random’ keys for each use (not just 40-bit keys as used in WEP). This protocol is called the Temporal Key Integrity Protocol (TKIP). WPA also uses the Extensible Authentication Protocol (EAP) that allows network administrators to select the method to use for authentication, such as biometric. More over, the authentication in WAP is perform in both ways, by the client and by the server. This is securer than WEP since WEP provides only client authentication via a static password, which must be shared by all users of a network. In addition, WAP also provides automatic key management to generate, configure, and distribute keys. In conclusion, WAP provide a higher layer of security than WEP and is designed as a replacement of WEP.

- *WPA2* is a security technology commonly used on Wi-Fi wireless networks. WPA2 (Wireless Protected Access 2) replaced the original WPA technology on all certified Wi-Fi hardware since 2006 and is based on the IEEE 802.11i technology standard for data encryption. WPA2 improves the security of Wi-Fi connections by requiring use of stronger wireless encryption than what WPA requires. Specifically, WPA2 does not allow use of the TKIP algorithm that has known security holes (limitations) in the original WPA implementation. Several different forms of WPA2 security keys exist. *WPA2 Pre-Shared Key (PSK)* utilizes keys that are 64 hexadecimal digits long and is the method most commonly used on home networks. Many home routers call WPA2 PSK as "WPA2 Personal" mode, these refer to the same underlying technology.