CH-06

1. Public-key announcement
2. Public-key authority (understand the pic and every step).
3. Public-key certificates (understand the pic and every step).
4. Simple secret key distribution (understand the step, and why it is not secure, and how to attack).
5. Diffie-hellman key exchange:
   1. what is primitive root, how to prove.
   2. Understand Diffie-hellman key exchange algorithm , how to prove that.
6. Man in the middle Attack

CH-07

1. Diff between Massage encryption, message authentication code(MAC)

Encryption needs reversible, MAC doesn’t need.

Encryption is one-to-one coding, MAC is many-to-one.

1. Diff between MAC and Hash

Hash doesn’t use key, MAC uses a symmetric key.

1. Understand the MAC (every part)
2. Understand Hash function (every part) (such as: “Why this requirement is important”)
3. Understand Simple Hash Functions
4. Know SHA-512 work

CH-08

1. Understand sample of HTTP
2. Base idea of SSL
3. How HTTP website work.

CH-09

1. What is Malicius Programs and its subclass definition
2. Difference between Worms and Virus
3. What is Compression Virus
4. Type of Virus and how to classify them and 特点 of each one
5. What is Trojan Horse
6. Difference between Email Virus and Worms
7. What is Rootkit, how to use rootkit to hack, and how rootkit works.

CH-10

1. What is Replay Attack, how it works and how to prevent, understand Protocol
2. What is Suppress-Replay Attack and how to prevent, understand protocol

CH-11

1. What is Phishing Email, how to prevent and tell.
2. Understand every step of PGP
3. What if a user has Multiple public pair, how to solve.
4. Understand PGP Message Format.

CH-12

1. What is Buffer Overflow Attack, why output is weird, what type of error it is( 2 type or more)
2. Understand every example.
3. How to counter buffer overflow attack ( at least two methods)

CH – 13

1. Login pages
2. Basic idea of SET and why we need Dual signature

CH-14

1. Understand every thing.

06 chapter

1.Public-key authority 会给一个图问time stamp是干啥用的

2.public key certificate

3.simple secrete key distribution我们要知道这是不安全的

4.primitive root是什么要知道，要证明比如2是不是5的primitive root

5.不需要记住diffie hellman key exchange是什么，题目会给，但是要回证明ya的xb次方 mod q = yb的xa次方 mod q

6.man-in-the-middle attack要知道

07 chapter

1.authentication function中要明白：

1>message encryption和message authentication code的区别

encryption：（1） reversible（2）1 to 1 mapping

mac：（1） doesnot need to be reversible（2）many to 1 mapping

2>mac vs hash

mac: uses a symmetric key

hash: doesnot use key

2.requirements for hash function:

page 30中following properties中的given x is infeasible to find y s.t. H（y） = H（x）还要明白这些properti为什么是necessary

1. simple hash functions要证明是不安全的因为可以找到一个sequence have same hash function ，要找到一个例子

08 chapter

1.明白http request例子中那些是什么意思

2. certificate

certificate authority -------------- https

|

|

|

|

encrypt using

the private key

of certificate authority

browser：public key of certificate authority

09 chapter

1.malicious programs:明白什么是backdoor，flooder rootkit

2.明白virus 和worm前者need host program后者不需要，因为她是程序的一部分

3.compression virus

4.各种types of viruses：（1）parasitic virus（2）memory-resident virus（3）polymorphic virus

5.要明白trojan horse是什么

6。要明白email virus and worm

6.明白如何用rootkit去hide user' activities

7.typical actions of kernel rootkit

第二个方法是modify system call table

10 chapter

1.replay attack

2.suppress-replay attack

3.要明白 needham-schroeder public key protocal

pui是public-key of trudy

Alice is talking to trudy

bob thinks that he is talking to alice，but actually he is talking to trudy。

11 chapter

1.simple mail transferr protocol

2.如何判断email is a phishing email

3.记住figure of PGP 和PGP public and private keys 的KEY IDS

4. PGP message format

12 chapter

1.buffer overflow attack eg：page10例子

2.page17 解释为什么output是0而不是1

3.counter buffer