Intro to Computer Security

Assignment 3 - Part 1

Name: Rahul Verma
email: rverma4@binghamton.edu
B-number: B00892091

Ans 1) (i) Given: Block size = 4 bits

Message (M) = 0110 1001 1101 0101 $\left\{\begin{matrix}0110\\1001\\1101\\0101\end{matrix}\right\}$

By XORing 1st bit of all the blocks we will get 1st bit of the hash code,

$h_1 = 0 \oplus 1 \oplus 1 \oplus 0$

$\therefore h_1 = 0$

Similarly, XORing 2nd bit of all the blocks we will get 2nd bit of the hash code,

$h_2 = 1 \oplus 0 \oplus 1 \oplus 1$

$\therefore h_2 = 1$

Similarly, XORing 3rd bit of all the blocks we will get 3rd bit of the hash code,

$h_3 = 1 \oplus 0 \oplus 0 \oplus 0$

$\therefore h_3 = 1$

and similarly, XORing 4th bit of all blocks we will get 4th bit of the hash code,

$h_4 = 0 \oplus 1 \oplus 1 \oplus 1$

$\therefore h_4 = 1$

$\longrightarrow$ Hash Code H(M) = 0111

Page No.
Date

Ans 1) (2) To prove: Hash function is not secure by creating another message M' so that $H(M') = H(M)$

In order to prove the Hash function is not secure, we will prepare the desired alternate message and then append an n-bit block that forces the new message plus block to yield the desired hash code.

We have, $H(M) = 0111$
and, Block size = 4 bits

Considering, $M' = 0000\ 0000\ 0000\ 0000\ 0111$

$\rightarrow 0000 \oplus 0000 \oplus 0000 \oplus 0000 \oplus 0111$

$0000 \oplus 0000 \rightarrow 0000 \oplus 0000 \rightarrow 0000 \oplus 0000 \rightarrow 0000$

$0000 \oplus 0111 \rightarrow 0111 = H(M')$.

$\therefore H(M') = H(M)$

$\rightarrow$ Hence Proved, Hash function is not secure as $H(M') = H(M)$

Page No.
Date

Ans 2)(1) Difference between Virus and Worm:

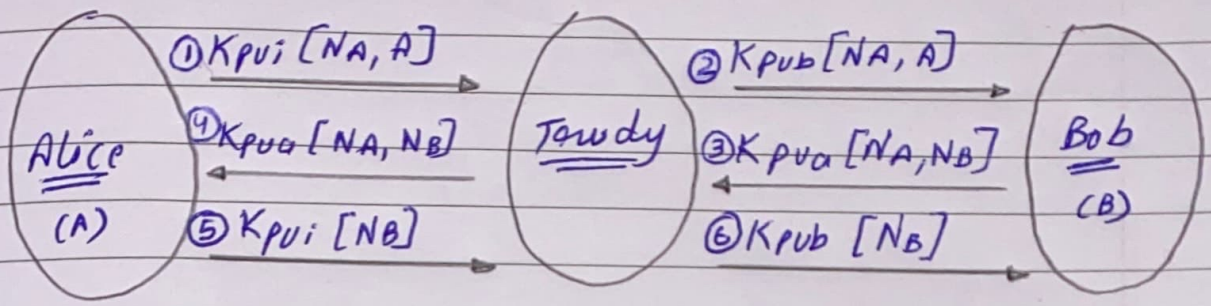
Virus	Worm
1) A piece of software that can infect other programs by modifying them, the modification includes a copy of the virus program which can then go to infect other programs	1) A program that can replicate itself and copies from computer to computer across network connections.
2) Virus need a host program: fragments of programs that cannot exist independently of some actual application program, system program	2) Worms are independent: self-contained programs that can be scheduled and run by the operating systems.

Ans 2)(2) Difference between User-mode & kernel rootkits

User-mode rootkits	Kernel rootkits.
1) User-mode Rootkits focus on replacing specific system programs commonly used.	1) Kernel Rootkits alter the kernel, provides all user-mode Rootkit features, also enables the redirection of any program execution.
2) List of typical files substituted by user-mode rootkits: Hide files, Hide processes, Hide connections, Hide logs, Hide log ins, Backdoor. (dated in 1989).	2) Some of typical actions kernel rootkit can perform: Execution redirection, File/process hiding: Hide processes (appeared in 1997)

Page No.
Date

Ans 3) Attack representation:



Here, We assume that the attacker Tawdy is a friend of Alice and we also assume that Alice wants to communicate with Tawdy. These are steps:

① Alice generates nonce NA, encrypts nonce NA and identity of Alice using Tawdy's Public Key and sends the encrypted message to Tawdy.

② After receiving the message Tawdy decrypts the message and gets nonce NA, Tawdy encrypts nonce NA and identity of Alice using Bobs public key and sends the encrypted message to Bob.

③ After receiving the message, Bob thinks that its from Alice, so Bob generates another nonce NB, encrypts both NA and NB using Alice's public key and sends it to her.

④ Tawdy intercepts the message but he's not able to decrypt the message, because he doesn't have Alice's Private Key, so Tawdy simply forwards this to Alice.

⑤ After receiving the message, Alice thinks that its from Tawdy so Alice encrypts nonce NB using the public key of Tawdy and sends the encrypted message to Tawdy.

⑥ After receiving the message, Tawdy decrypts the msg using the private key of Tawdy and gets nonce NB, Tawdy then encrypts nonce NB using public key of Bob and sends the encrypted message to Bob. After Bob receives the message, Bob thinks hes talking to Alice, but actually hes talking to Tawdy.

- To counter this attack we should add Bob's identity in the message sent by Bob, in this case when Trudy replays the message sent from Bob to Alice, Alice will be able to tell that, it is a replay attack because the identity is Bob's identity instead of Trudy's identity