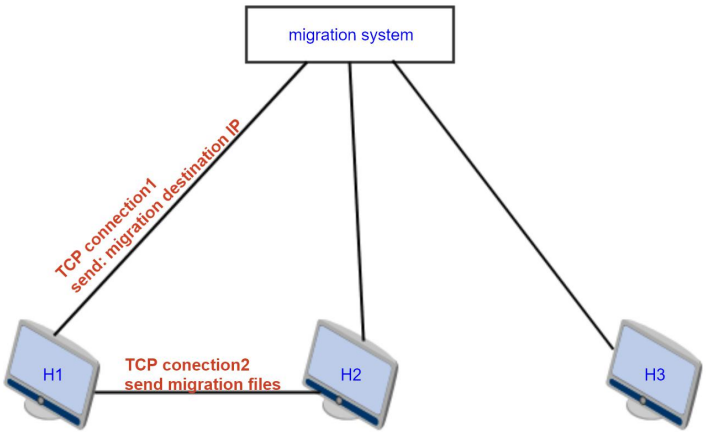
Initial inspiration of security

In the original system, for attack defence we have random policy. The system every time generates two random number using random generate function, these two numbers are easy to predict if someone study the random generation function. Hence, we start to think about updating the system with a more secure way to protect the server against attacking.

In the original system, the migration decision is made by system, then it send the migration destination host IP to migration source host though TCP connection. Here, we propose that the task of making decision is delegated to both migration system and each host. Migration system will not send the clear migration destination IP anymore.

First i analysis the possible potential attacks in the system, then I propose some solutions for each potential attack.

Initial system:



Possible attacks:

1. TCP connect1, attacker could see the migration destination IP address since it is in a clear way
2. TCP connection2

->For small traffic generation network, attacker could do network traffic analysis. It can determine the destination host if the migration container images files set is huge, the throughput from source to destination will increase dramatically.

->For attacker inside the host, it can know which host it opens TCP connection with. Hence, the destination migration destination is compromised.

Concerning different potential attack point, I propose the security solution as following:

<u>The concept of MTD(Moving Target Defence)</u>

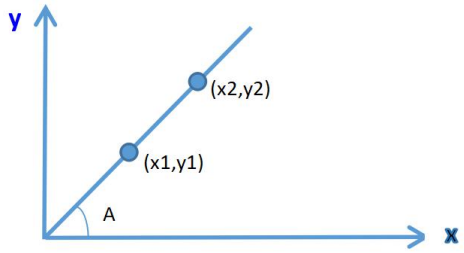
Instead of defending unchanging infrastructure by detecting, preventing,monitoring,tracking,

or remediating threats, moving target defence makes the attack surface dynamic.It try to make the system dynamic and therefore harder to explore and predict.The ultimate goal of MTD is to increase the attacker's workload so as to level the cybersecurity playing field for both defenders and attackers.

How to share a secret?

I adopted the concept of threshold schema a(k,n), which is to construct the key from majority members. The key stored in each host is only a part information to construct the Master Key. Here, I use a liner function y=Ax+b, A is the mater key which is known by the migration system. Each host will have a key pair (x,y), this is not enough to computer the mater key A, Only if there are at least two hosts contributing the key Pair (x1,y1) and (x2,y2). The master key A can be computed.

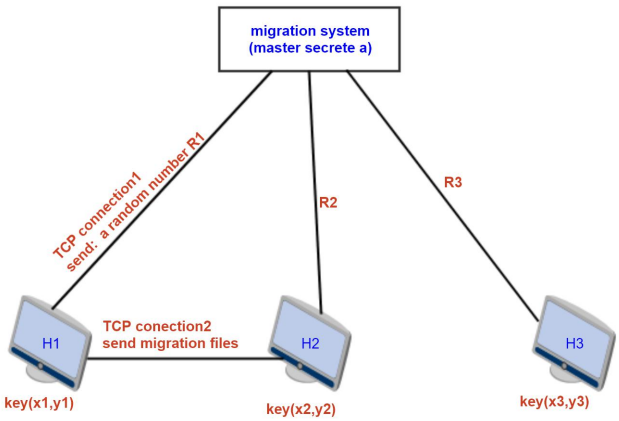
This master key A is to encrypt the loop up table.



Here, we create an security algorithm to protect the migration server by combining the concept of MTD and threshold schema to share the key.

Security solutions:

1)*change the migration decision algorithm(potential attack 1)*



New Items:

Mater secrete A: a number only known by he migration system. Y=Ax

Random number R: a number generated by migration system and send to host to make the migration decision.

Key pair (x,y): a point generated and distributed by the migration system which is in the linear function, a part of information to construct the master key.

Look up table : it contains two columns, first column is the index, second column is the corresponding IP Address. It is encrypted using the master key(A)

index	IP
1	10.0.0.1
2	10.0.0.2
3	10.0.0.3

Initialization:
Configuration migration system:
1. linear function Y=Ax
2. Hash function hash(x)=MOD5(R1+X1*Y1)%(N+1) (N is the total hosts number)
3. Encrypt look up table using master key A

Process:
1.Migration system generate a set of key pairs (x,y) and distribute to each host. Hence each host has a part of information to decrypt the look up table.
2.Migration system choose an arbitrary host, open TCP connection(TCP connection1 in the figure), send a random number to the host(H1).
3.H1 apply hash(x), the results is the migration destination host index i.
4.H1 open TCP connection to another arbitrary host(H2) to get another key pair.
->H1 send first message " get key"
->H2 need to authenticate H1, send a random number N
->H1 send response to H2
->H2 send key pair (x,y) if the response is correct
5.H1 use key pair (x1,y1) (x2,y2) to compute the master key A
6.H1 decrypt the look up table, find corresponding destination host of index i.

Diversity:
Migration system distribute new key pair for each host after some time.

2)multiple TCP connections and fake traffic in the network(potential attack 2)

If the attacker is inside the migration source host, it can see the TCP connection opening. Here, we propose a multiple TCP connection to different hosts including the migration source host. In this way, we can make attacker be confused to which is the real migration destination host.
Concerning the small traffic generation network, if migration happens, the traffic between migration source host and migration destination host will increase dramatically.If the attacker do traffic monitoring among the network, probably the migration destination host will be compromised. In this case, the migration source host can send fake data to the network to confuse attacker even when network monitoring is applied.