1998 International Computer Symposium
Workshop on Cryptology and Information Security
December 17-19, 1998, N.C.K.U., Tainan, Taiwan, R.O.C.

# Apply Tier Form Security Architecture to Intranet

Chuan-Fu Wu, Hui-Wen Wu, Wen-Shyong Hsieh
Institute of Computer and Information Engineering
National Sun Yat-Sen University
Kaohsiung, Taiwan 804, ROC
E-mail: cfwu@cie.nsysu.edu.tw

***Abstract:***

In this paper, we propose the Inter-Torsion Mechanism in Tier-Form Architecture (ITMTFA) and apply this architecture to the Intranet to provide a security environment for message transmission in the Intranet or between Intranets. As we know that the firewall is used in the Intranet to be as the traffic filter of the incoming message and as the proxy server of the members in the Intranet. But the firewall suffers from the attackers who may be the members in the Intranet, or the outer attackers who are logging on the nodes in the Intranet. In ITMTFA, the firewall is used to be as the agent of the members in the Intranet also, it supports the one time key security environment to the members who are communicating with other nodes which may be in or out the Intranet. This is the reason why the scheme is called as Tier-Form. The one-time key will be changed by a transformation scheme called as Function Torsion (FT) which is performed in the agent (firewall) after the key is used. FT is processed by a randomly logic operation on the old session key and randomly permuting on the result to form the new session key. Based on the advantage of one time key and random function FT, the ITMTFA can provide a very high security environment in the Intranet or between Intranets.

## *1. Introduction:*

Today the internet environment is much less collegial and trustworthy. It contains all the dangerous situation, nasty people, and risk that one can find in society as a whole [1]. In a workshop held by the IAB back in 1994 [3], scaling and security were considered to be the two most important problems for the internet. Internet security can only be achieved by providing the following two classes of security services [3,4]:1.*Access control services* that protect computing and networking resources from unauthorized use. 2.*Communication security services* provide authenticaiton, data confidentiality and integrity, as well as nonrepudiation services to communication peer.

To provide a safety internet environment, the firewall is used to filter the message and acts as the proxy server of the members (nodes) in the Intranet. But as we know that the firewall suffers from the attacks which may be initiated in the Intranet, or be the outer attackers who are logging on the nodes in the Intranet. The original idea of ITMTFA is to use the firewall to be as the communication agent, when a node A in the Intranet wants to communicate with node B which may be in or out the Intranet. The negotitation between node A and agent, and node B and agent will be made to get two session keys: SkA and SKB. The message from node A will be encrypted by SkA and be sent to agent, the encrypted message will be decrypted by SkA and reencrypted by SkB in agent, and then the reencrypted message will be sent to node B. Using SkB, node B can get the original message sent from node A. The Function Torsion (FT) will be applied to SkA and SkB to get the new session keys for next communication between node A and B. FT is processed by a randomly logic operation on the old session key and randomly permuting on the result to form the new session key, we call the action in FT as Inter-Torsion. The form between node and agent is the reason why we call the scheme as Tier Form.

In the second section, we introduce the Intranet and firewall technology, we focus on the screening router and proxy server of firewall technology. In the third section, we will scrutinizingly elucidate the inter-torsion mechanism in tier form architecture we proposed. Next, the strategy of the ITMTFA will be shown in fourth section. We also analyze the security and performance of the ITMTFA. Consequently, some simulations are done to obtain the results and analyze them in this section. Finally, conclusions are drawn in the fifth section.

## *2 .Intranet and firewall:*

In the whole internet environment, we have more interest in the Intranet [2]. Because more and more businesses and enterprises have their own Intranet. Most of these Intranets use a intermediate systems that can be plugged between their network and the internet to establish a controlled link, and to erect

an outer security wall or perimeter. The aim of this perimeter is to protect the network from network-based threats and attacks, and to provide a single choke point where security and audit can be imposed. These intermediate systems are called *firewalls*, or *firewall system* [3,7,8].

The firewall system usually consists of screening routers and proxy servers.A screening router is a multiport IP router that applies a set of rules to each imcoming IP packet, and decides whether it is to be forwarded or not. The screening router filters IP packets, based on information that is available in packet headers, such as protocol numbers,source and destination IP address and port numbers, connection flags, and eventually some other IP options.

A proxy server is a server process running on a firewall system to perform a specific TCP/IP function as a proxy on behalf of the network users. A proxy is, in essence, an application-layer gateway; which links one network to another for a specific network application. The user contacts a proxy server using a TCP/IP application, such as telnet ,ftp or STMP, and the porxy server asks the users for the name of the remote host to be accessed. When the user responds and provides a valid user identification and authentication information, the proxy contacts the remote host, and replay IP packets between the two communication points. The whole porcess can be made transparent to the users. The identification and authentication information that a user provides may be used for user-level authentication. In the simplest case, this information consists of the user identification and password. However, if a firewall is accessible from the Internet, it is recommended to use strong authentication mechanisms, such as one-time password or challenge-response systems.

The advantages of screening routers are simplicity and low (hardware) costs. The disadvantages are related to the difficulties in setting up packet filter rules correctly, the costs of managing screening routers, and the lack of user-level authentication. The advantages of proxy servers are user-level authentication, logging, and accounting. The disadvantages are related to the fact that for full benefit, an application-layer gateway must be built specifically for each application. This fact may severely limit the deployment of new applications. More recently, an all-in-one proxy package called SOCKS [7] has become available. SOCKS basically consists of a proxy to be run on a firewall system, as well as a package of library routines to be linked into network application programs.

Screening routers and proxy servers are usually combined in hybrid systems, where screening routers mainly protect against IP spoofing attacks. The most widely deployed configurations are dual-homed firewalls [7], screened host firewalls, and screened subnet firewalls. The firewall technology is interesting because it doesn't use cryptography. However, most of the firewall systems currently offered support some sort of IP layer encryption. Another interesting feature of the firewall technology is related to the fact that its use is not restricted to TCP/IP protocols or the Internet. Indeed, a similar technology can, in principle, be used in any packet-switched network, such as an X.25 or ATM network.

Firewall systems can help us control damage,regulate traffic flow and protect the network in case of an internet intrusion. But the firewall systems still have some limitations. Firewall systems have no data confidentality functions and can't protect against internal threats. In order to enhance the security of the Intranet. We propose a technique using the existent firewall to supplement the Intranet with the scant security functions. This technique we proposed is called inter-torsion mechanism in tier form architecture(ITMTFA).

### *3. Inter-torsion mechanism in tier form architecture:*

The skeleton of Inter-Torsion Mechanism in Tier Form Architecture is shown in figure 1.

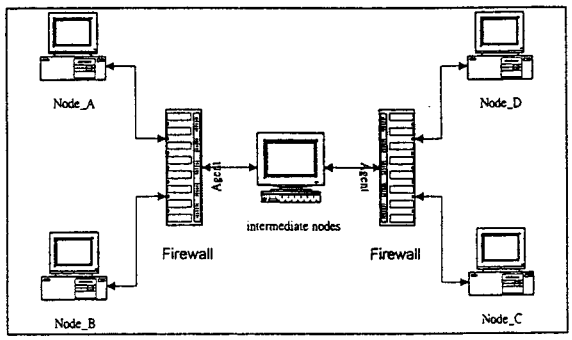


Figure 1: The skeleton of ITMTFA.

Seeing the form of this architecture is very like tier, so this's the reason why we call it tier form architecture. The tier form system adopts symmetric cryptosystem. By using *torsion* action in connection, we can use at least two different keys to encrypt or decrypt the information tranferred between peers. By increasing the complexity of the session keys, we improve the security of the system. In the inter-torsion mechanism we employ one transformation function called Function Tosrion (FT). The FT is

similar to one-time key technique [4]. But FT needlessly worry exposing the seed-key, since FT performs random transformating and random permuting on session key without any seed key. An intruder can't get the initial key even he has cumulated enough session keys. Inter-torsion mechanism is the core of this architecture. We need a trusted third party to perform the FT function. The existent firewall system is the best choice in an Intranet. So we use the existent firewall as the major component called agent doing the main computation in this architecture.

### *3.1 Inter-torsion mechanism:*

Why we name the transformation acted on session key as *inter-torsion*. The reason is that the operation of transformation is very similar to torsion. Every time we use different session key for connection between two peers. Figure 2.1 and 2.2 illustrate how inter-torsion mechanism works. In this case, we assume node A in Intranet_1 wants to connect to node C in Intranet_2. Let's show below:

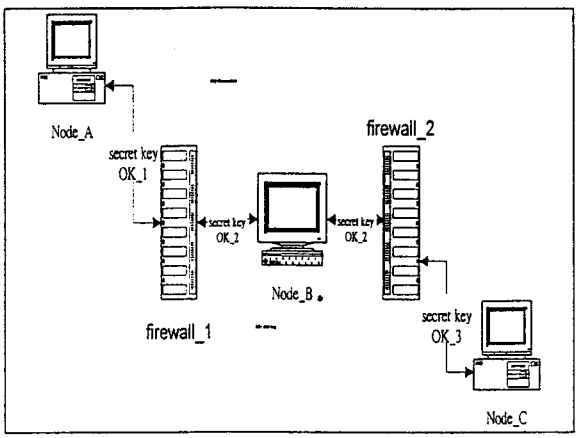


Figure 2.1: The old connection state.

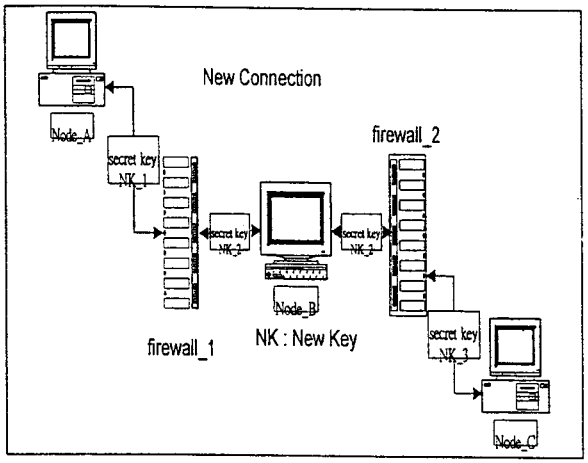


Figure 2.2: The new connection state.

### *3.2 Authentication and Session Key Exchange Protocol* [5] :

Before we show our strategy of inter-torsion mechanism in tier form architecture, we should show the authentication and session key exchange protocol first. By using this protocol, the connection peers can authenticate the identity of each other. At the same time, they can share a common session key created by Diffie-Hellman algorithm[6]. We have interest in three protocols which are similar, but they have their own merit and drawback. Client owns the *X*client,Certclient, and Agent owns the *X*agent,Certagent. The X is the randomly assigning value in client and agent for generating of initial session key. The Cert is the certificate of client and agent, it contains the IP address, Y, valid data, and the digest of these information signed by the Certificate Authority (CA). Now let's show how the protocols work below:

Certclient = {IPclient, Yclient, DateClient, [h(IPclient, Yclient, DateClient)]SCA} ,
Certagent = {IPagent, Yagent, Dateagent, [h(IPagent, Yagent, Dateagent)]SCA }

***(Protocol_I)***

$Y_{Client} = \alpha^{X_{client}}$, $Y_{Agent} = \alpha^{X_{Agent}}$

(1)*Client*→*Agent* : $CERT_{Client}$

Agent computes $KC1 = (Y_{client})^{X_{Agent}} \bmod N = \alpha^{X_{client} * X_{Agent}} \bmod N$

(2)*Client* ← *Agent* : $CERT_{Agent}$

Client computes $KC1 = (Y_{Agent})^{X_{Client}} \bmod N = \alpha^{X_{client} * X_{Agent}} \bmod N$

(3)*Client* ↔ *Agent* : EKC1[IPagent, IPclient]

At the last step, client and agent will verify the [IPagent, IPclient]. If it is correct, the session key is taken.

***(Protocol_II)***

$Y_{Client} = \alpha^{-x_{client}}$, $Y_{Agent} = \alpha^{-x_{Agent}}$

(1)$Client \rightarrow Agent$ : $\alpha^{r_{Client}+x_{Client}}$, $CERT_{Client}$

Agent computes $KC1 = (Y_{client} * \alpha^{r_{Client}+x_{Client}})^{r_{Agent}} \bmod N = \alpha^{r_{client} * r_{Agent}} \bmod N$

(2)$Client \leftarrow Agent$ : $\alpha^{r_{Agent}+x_{Agent}}$, $CERT_{Agent}$

Client computes $KC1 = (Y_{Agent} * \alpha^{r_{Agent}+x_{Agent}})^{r_{Client}} \bmod N = \alpha^{r_{client} * r_{Agent}} \bmod N$

(3)$Client \leftrightarrow Agent$ : EKC1[IPagent, IPclient]

Protocol II gets a random value *r* to help generating different *KC1* on every new connection.

***(Protocol_III)***

$Y_{Client} = \alpha^{-x_{client}}$, $Y_{Agent} = \alpha^{-x_{Agent}}$

(1)$Client \rightarrow Agent$ : $Sig_{client}(\alpha^{r_{Client}+x_{Client}})$, $CERT_{Client}$

Agent verifies the signature of client, then

Agent computes $KC1 = (Y_{client} * \alpha^{r_{Client}+x_{Client}})^{r_{Agent}} \bmod N = \alpha^{r_{client} * r_{Agent}} \bmod N$

(2)$Client \leftarrow Agent$ : $Sig_{agnet}(\alpha^{r_{Agent}+x_{Agent}})$, $CERT_{Agent}$

Client verifies the signature of agent, then

Client computes $KC1 = (Y_{Agent} * \alpha^{r_{Agent}+x_{Agent}})^{r_{Client}} \bmod N = \alpha^{r_{client} * r_{Agent}} \bmod N$

(3)$Client \leftrightarrow Agent$ : EKC1[IPagent, IPclient]

Protocol III is similar to Protocol II, except for signature on $\alpha^{r_i+x_i}$.

### *3.3 Transformation Function FT:*

Now we show the proceeding of transformation function FT. First, we divide the old session key SK into eight pieces that we name SKi. SK is recomputed by some simple functions like XOR to get the new session key NSK. For example: **NSKi+1=SK(i+2mod 8)+1 ⊕ SK(i+4 mod 8)+1** or **NSKi+1=SK(i+1mod 8)+1 ⊕ SK(i-1 mod 8)+1** . Then we randomly combine the **NSKi** to get the new key. We make a general form of FT that is performed by a full random function that contains three random steps.

General Form of FT:

(1) Divide step:

We divide the old session key into N pieces of sub keys SKi. N is one integer in the interger group{8,16,32,64} and it's always randomly chosen. $SK=[SK_1,SK_2,SK_2,\cdots,SK_N]$ is the general form of SK. Every $SK_i$ has 64/N bits.

(2) Combination step:

Let NSKi = (Ri1*Sk1) ⊕(Ri2*Sk2) ⊕(Ri3*Sk3) ⊕...(Rin*Skn).

$R_i = [R_{i1}, R_{i2}, R_{i3}, ..., R_{in}], 1 \le i \le n$, Rij = 0 or 1. Ri is a binary array. $R = [R_1, R_2, R_3, ..., R_n]^T$,R is a $N \times N$ binary matrix, the limitations of Ri is that at least two element of the array are nonzero. And no two same Ri will apper in one R.

(3) Permutation step:

After we get the NSKi from step(2). We randomly permuting these NSKi to form the NSK. The

$NSK=[NSK_a, NSK_b, NSK_c, \cdots, NSK_n]$ is the general form of NSK. The permutation of these NSKi that compose the NSK is processed randomly.
With the full randomly generation steps of NSK we mentioned above, the intruders almost cannot break this process. So we can get a very high security one time key system.

### *4. Strategy of Inter-Torsion Mechanism in Tier Form Architecture:*

What we show here is the proceeding of just only two peers implement the *inter-torsion mechanism in tier form architecture* on their connection. Every two peers can apply this architecture to the connection between them. Figure 3 illustrates how the ITMTFA works.

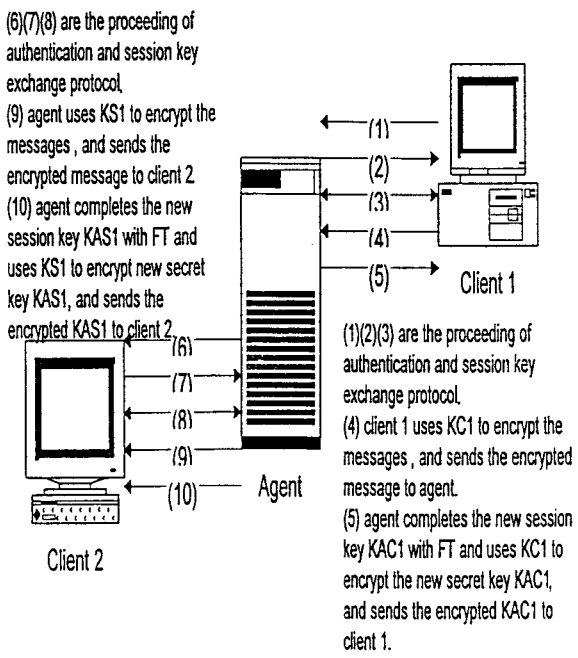


Figure 3: Inter Torsion Mechanism Strategy

The strategy of *inter-torsion mechanism in tier form architecture* can be divided into 3 steps:
Step (1), first, client 1 and agent use authentication and session key exchange protocol to authenticate the identity of each other, and share a common session key KC1. When client 1 gets the KC1, he uses KC1 to encrypt the information M. The encryption method can be DES, IDEA, or just only XOR. And sends the encrypted information Ekc1(M) to agent.
Step (2), when agent receives the encrypted information Ekc1[M] from client 1, he uses the KC1 got from step(1) to decrypt the Ekc1(M). Agent gets the information now. Subsequently, agent should use transformation function FT to transform KC1 to the new session key KAC1. Agent uses KC1 to encrypt KAC1 then sends Ekc1[KAC1] back to client 1. We finish first torsion action now.
Step (3), similarly, agent and client 2 use authentication and session key exchange protocol to authenticate the identity of each other, and share a common session key KS1. Subsequently, agent uses KS1 to encrypt the information M received from client 1. And uses FT to get new session key KAS1. Then agent sends the encrypted information and KAS1 to client 2. We finish secondary torsion action and complete the whole operation.

### *4.1 Security Analysis:*

After we propose the ITMTFA, what we should do is analyzing the security of this architecture. Contemplating the existent attacks, we can analyze the influence of these attacks seriatim as follow:

*Ciphertext-Only attack.* The attacker can only get some ciphertexts, and he wants to directly acquire the plaintext from the ciphertext. This attack can not do any mischief to our architecture, since the session key will be changed every new connection.

*Known-Plaintext attack.* The attacker has some pairs of plaintext and ciphertext: {m1, C1}, {m2, C2}, {m3, C3}...{mi, Ci}. He wants to acquire the session key or next ciphertext from the pairs of plaintext and ciphertext. Identically, this attack can't do any mischief. Although the attacker may get the session key, but the session key can not do any help for breaking our architecture. The reason is the same as the foregoing.

*Chosen-Text Attack.* The *Chosen-Text Attack* is a more powerful attack that can be divided into two sub-attacks: (a) Chosen-Plaintext attack, (b) Chosen-Ciphertext attack. We assume the attacker has the ability to select or control plaintext or ciphertext. The attacker can choose some pairs of plaintext and ciphertext that are easily attacked for him. Even the attacker can get the session key using chosen-text attack, our architecture still can protect the attack. Since the session keys will be changed randomly when every new connection is established. Although the attacker has one session key, he still can not guess what next key will be.

*Replay attack.* The attacker intercepts the message and replays the message after a while. The attacker can impersonate other people on the network in this way. But in our architecture, the replay attack can not do any help for the attacker.

*Intruder-in-the- middle attack.* The attack is used to break the Diffie-Hellman key exchange protocol. Figure_4 illustrates how it works: U and V are the communication peers, and W is the intruder.

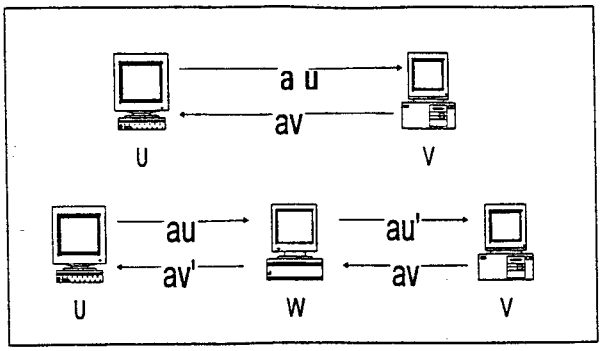


Figure 4:Intruder-in-the-middle attack.

The intruder-in-the-middle attack can not do any damage to our architecture. Since the Diffie-Hellman key exchange protocol we used in our architecture is protected by the trusted third party: Certificate Authority (CA). We use the CA to authenticate and sign the public value of client or agent. Take advantage of the CA, we can prevent the public value in Diffie-Hellman key exchange protocol from falsifying. Consequently make sweeping generalizations, we think our architecture is strong enough to defense the most attacks on the network that we mentioned above.

ITMTFA is similar to the one-time key technique, but we don't have the problem of worrying the exposing of seed. The one–time key technique uses the seed to help generating the one-time session key. An attacker can cumulate enough session keys to conjecture the seed. Once the seed is exposed, the generation of session keys will be not safe any more, although the probability of exposing seed is very low. The seed is the merit but also the drawback of the one-time key technique. Learning the one-time key's lesson, we loosen the relation between the seed and every session key. In ITMTFA, every session key almost independent of the seed key besides the first generated session key. The generation of session keys is one way and random. The attacker can't conjecture the next session key by analyzing the existent session key unless he knows the generation function of session keys. But the agent randomly chooses the generation function of session key, wherefore it's not easy to conjecture the session keys. And further, we use at lease two different session keys for the connection between two communication peers. We divide the connection between two peers into several sub-connections. Every sub-connection uses a independent session key. And the session keys will be randomly changed when every new connection is established. Although we do the transform of session keys on the connection between two peers for the security reason, but we should also consider the efficiency of the whole connection. Consequently, we discuss the efficiency of the ITMTFA at next session.

### *4.2 Performance analysis:*

Besides the security of the inter-torsion mechanism in tier form architecture, we also consult the performance of the architecture. We can do some simulations of possible situations to achieve our purpose. In the simulations, we configured a SUN ULTRASPARC II running the Solaris 2.6 OS as the agent. By analyzing the result of simulation, we can decide if the architect is operable or not. And we can choose a better way to operate the inter-torsion mechanism in tier form architecture, to reduce the overhead of FT.

In the first simulation, we consider the overhead of ITMTFA. When a message is transmitted between two nodes. The location of the two nodes may be one of three cases. Case1, two nodes are located in the same Intranet. Case2, two nodes are located in the neighbor Intranet. In case3, there are more than one third network located between the Intranets where the two nodes are in. when two nodes are located in the same Intranet, the message can be transmitted directly from one node to another node. In the case the operation of encrypting, decrypting, reencrypting, and decrypting performed by two nodes and firewall (agent) is the overhead of ITMTFA. From the result shown on figure 5, we can find that the overhead is acceptable.

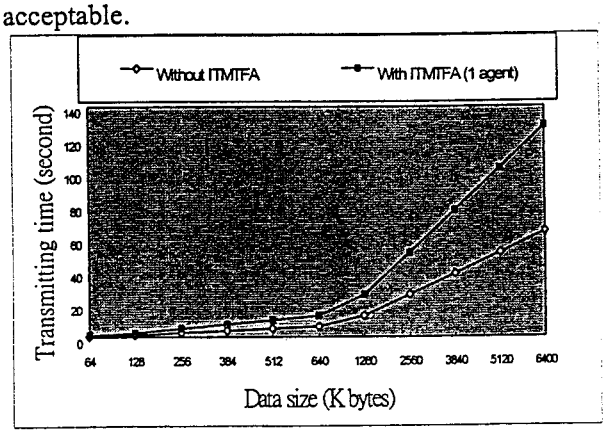


Figure 5: The simulation result of Case 1.

In case2 or case3, the message must be transmitted through one or more firewalls. Due to the scheme of store and forward, whole message must be received, checked and forwarded to next node by the firewall (agent). The operation performed in ITMTFA can be considered as the message translating and can be piped in the scheme of store and forward. From the results of figure 6 and figure 7, we can find that the overhead is very light in case2 on case3.]

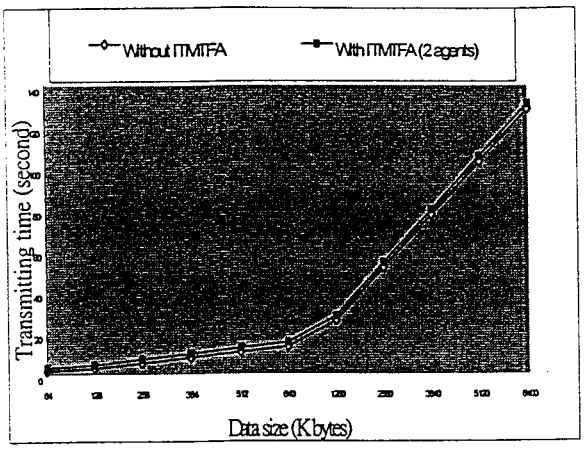


Figure 6: The simulation result of Case 2.

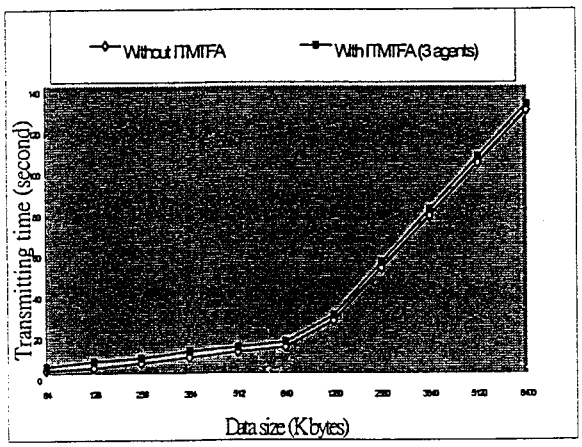


Figure 7: The simulation result of Case 3.

The length of session key used in ITMTFA is 64 bits. The encrypting method can be DES, IDEA, or just only XOR. Because any session key is used only one time, and the FT is fully random. So we don't need to use the complex encrypting method to protect the one time key. In ITMTFA, the message block will XOR with the session key.

*Encryption*: Esk [M]=M⊕SK, SK is 64 bits session key.

*Decryption*: Dsk [Esk [M]]=SK⊕M⊕SK=M, Dsk is the decrypting.

The session key will be changed by FT into new session key. As the described in session3, the session key is divided into N parts and the FT is applied on the N parts. In combination step of FT, a random $N \times N$ binary matrix R and a random permutation will be made to form the new session key. If we divided the session key into 4 parts, or 16 parts, the degree of random matrix R and random permutation are (4x16,1x4) and (16x4,1x16) . the complexity of random binary matrix R are 4x16, 8x8, and 16x4 respected, it means that the complexity of random binary matrix R are similar when the session keys are divided into 4,8,16 parts. But the degree of random permutation is the largest when N is 16. It means that more divided oarts in the session key has more complexity in tranformation. Figure 8 and figure 9 show the different system load when N is 8 and 16. As the shown result, we can find that there is not significant difference in system load whereas n is 8 or 16. In fact we can get that the assignment of N=8,16,32,64 is a random process also. So that we have three random steps in FT, they are random dividing, random combinating, and random permuting.

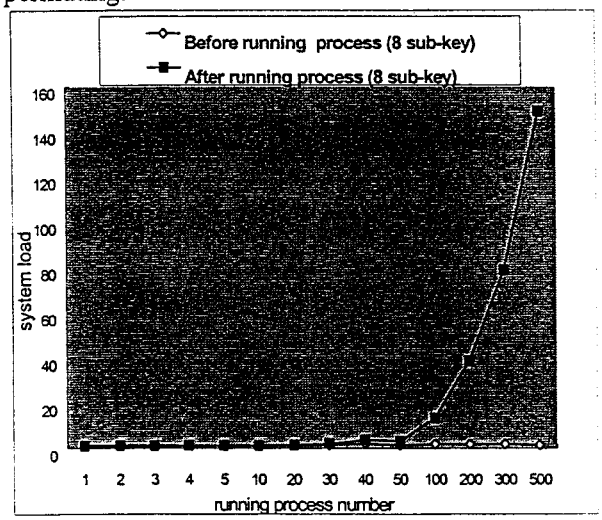


Figure 8: system load of running FT(I).

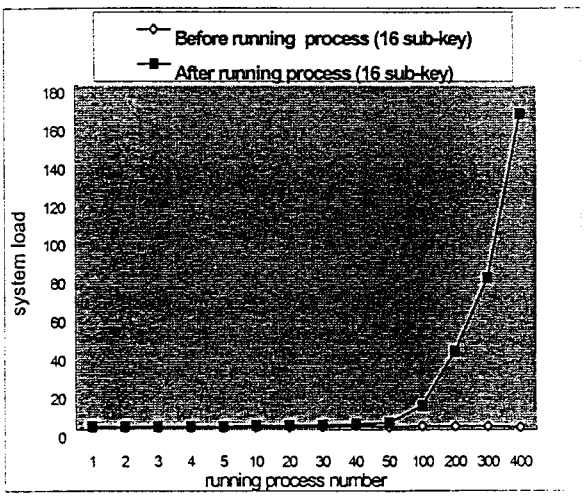


Figure 9: system load of running FT(II).

Figure 10 shows the different system load when n is 8,16 and 32. As the shown result, we can find that there is not significant difference in system load whereas n is 8, 16 or 32. In fact we can get that the assignment of n=8,16,32,64 is a random process also. So that we have three random steps in FT, they are random dividing, random combinating, and

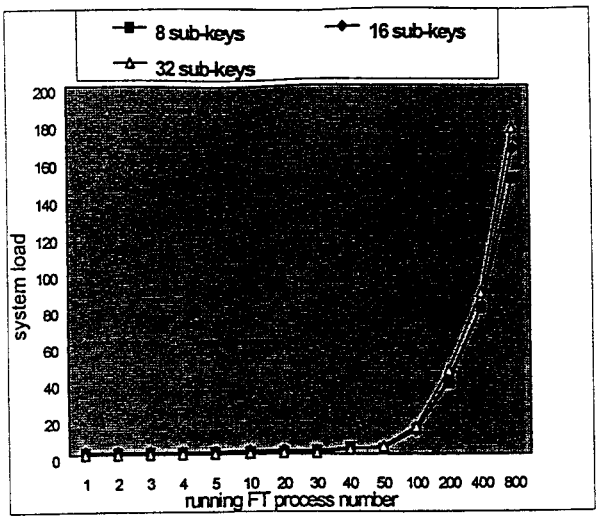


Figure 10: system load of running FT.

## 5. Conclusion:

In this paper, we provide a technique to enhance the security of the Intranet. Our technique is similar to one time key technique, but doesn't have the problem of seed key. The main prerogative of our technique is that we divide a connection into several sub-connections. Every sub-connection uses it's own session key and the session key will be changed when a new connection is established. Consequently, we can use at least two different keys to encrypt or decrypt the information tranferred between two nodes. According to this, we can provide more security than the stiuation that always only one session key used to protect a connection.

Any two nodes in different Intranet can communicate more securely. Generally speaking, the number of session keys used to protect the connection for two nodes in different Intranet is three. Besides, two nodes in an Intranet can communicate more securely. Since any information transferred between them is protected by the session key. Additionally, the manager of the Intranet can monitor and control some connections inside the Intranet by getting the takeover of agent if the condition is necessary. We have to consult the performance and security. So we employ existent firewall system as the agent.

The Inter-Torsion Mechanism in Tier Form Architecture we proposed uses the existent firewall system to provide data confidentiality and protect against internal threats fit the Intranet. In order to estimate the performance of ITMTFA, two simulations are made. The result of first simulation shows that the overheads of the encrypting in tier form are tolerable or very light whenever the two nodes are located. There are three random processes in FT to form the new session key, and the result of simulation shows that the more divided parts in session key can get more security, but can not due the significant overhead in system load. Show as the simulation and the discussion on attack protecting, ITMTFA can make a very high security environment for Intranet.

## 6. References:

[1] D.W. Davies and W.L. Price "*Security of Computer Networks*", John Wiley & Sons, 1989.

[2] Randy J. Hinrichs, "*Intranets: What's The Bottom Line*?", published by SunSoft/Prentice Hall, 1997 ; http://www.intranetjournal.com/expert.html.

[3] Rolf Oppliger "*Internet Security: FIREWALLS and BEYOND*", Communication of the ACM, May 1997/Vol.40, NO.5.

[4] C.S. Laih, Lein Harn and C.C. Chang "*Contemporary Cryptography and Its Applications*" published by Unalis Corporation, Sep. 1995.

[5] Chang-Seop Park *"On Certificate-Based Security Protocols for Wireless Mobile Communication Systems"* IEEE Network. Sep. / Oct. 1997.

[6] Larry J. Hughes, Jr. "The security technology of Internet " p69, published by New Rider.

[7] Chapman, D. and Zwicky, E. "*Internet Security Firewalls.*" O'Reilly, Sebastopol, Calif., 1995.

[8] Cheswick, W., and bellovin, S. *"Firewalls and Internet Security: Repelling the Wiley hacker."* Addison-Wesley, Reading, Mass., 1994.