A Key Recovery Scheme

Suhas Aggarwal
Dept. of Computer Science & Engineering
Indian Institute of Technology,Guwahati
Assam 781039

suhasagg@gmail.com

Abstract
With the increased use of encryption in business, key recovery has emerged as a critical issue to users. As encryption is deployed to protect files and network communications, users must include safeguards that prevent the inadvertent loss of data and use of the network for malicious intent. This paper explains what key recovery is, presents a refined practical model of a key recovery scheme and describes a new key recovery scheme compliant with this model. A novel feature of this key recovery scheme is that it is resistant to online guessing attack. Most of key recovery schemes used today are able to detect online guessing attack but not able to prevent it. Consequently, users face the problem of denial of service which occurs when key recovery server shuts down the service to legitimate users though temporarily as a security measure. Key recovery server also, often ask users to change password which was attacked causing further inconvenience. So, a security solution Captcha is employed in this new key recovery scheme to make it secure against online guessing attack.

1.Introduction
What is Key Recovery? A key recovery scheme allows the owner of encrypted data or an authorized third party to recover a lost or otherwise unavailable key. The most popular schemes are trusted third parties (TTPs), key escrow, and key recovery. In the trusted third party schemes, the TTP generates and owns the key. The TTP makes a copy of the key available to the user, who uses it to encrypt data. If the user loses the key, the TTP still has the original key. The key escrow scheme achieved notoriety during the U.S. Government's Clipper initiative. In this scheme only government-controlled law enforcement agencies could recover keys. Both trusted third party and key escrow schemes have received a lukewarm (and occasionally even hostile) reception from standards bodies and the business community. The key recovery scheme is the most recent technique for recovering encryption keys. Key recovery involves the use of a key recovery field and a key recovery agent as described in Cykey [1], the only entity with the authority and capability to recover the key. The agent keeps information needed to recover the key, but is never actually in possession of the key until recovering it. Key recovery schemes are administered according to strict policies that ensure key recovery is triggered only legitimately. These policies governing who and under what conditions the key can be recovered are published by the agent and agreed to by the community that the agent services. There exists few other key recovery solutions such as by Bell Labs [2] and an improvement of Bell Labs key recovery scheme, practical key recovery by Sung Ming Yen [3]. But Sung Ming Yen's scheme is prone to online guessing attack which is detectable by key recovery server but result in consequent Denial of Service which causes inconvenience to users.

1.1 Examples of Key Recovery Use
This section describes the three typical business situations in which key recovery support is needed.

Case 1: To Recover Important File Data

Business people carry sensitive information on laptops or other unprotected computers. For example, an executive might have customer lists, contracts in negotiation, and business plans on a single laptop. A business can be destroyed in the event that this kind of information falls into the "wrong hands". It is prudent to encrypt sensitive files. But what happens if the key is lost? Without a backup of the key or a method of recovering the key, the data is lost forever. Copying the key or otherwise backing it up weakens the security. Therefore, a key recovery scheme is an attractive alternative. In the event the user losses the key, the user can take the key recovery field (typically appended right to the file) to the responsible key recovery agent. After the agent determines that the user owns the encrypted data, the agent will recover the key and give it to the user. The user privately decrypts the data. Similarly a co-worker can recover the key by presenting affidavits to the key recovery agent that prove that the co-worker has legitimate access to the data. The agent can recover the key and make it available to the co-worker.

Case 2: To Monitor Communications

More and more, organizations are using strong encryption to protect communication among computers on its own network or with its trading partners. Now consider, an employee who is using the company computers for industrial espionage, running his/her own business, or distributing pornography. The company has a fiduciary, legal, and moral obligation to prevent such uses of its assets and facilities; but without a way to convert the ciphertext to clear text, the company cannot detect when a misuse has occurred. Key recovery provides corporate security with the means to monitor encrypted network traffic. When circumstances warrant it, the network traffic (first the key exchange handshake and then the subsequent communications) is captured, the key recovery field is extracted and copied to the key recovery agent, the session key is then extracted by the agent, and finally, the message content is decrypted.

Case 3: To Export Encryption

U.S corporations run into U.S. Government policy governing the export of encryption when they want export products that perform strong encryption. U.S Government policy, while perhaps controversial, currently includes the right to monitor citizens targeted by criminal or national security investigations. Many other governments around the world are adopting a similar stance. Key recovery, to be accepted by governments and still be effective, must protect the communicating parties against the abuse of power while providing legitimate authorities access to file and message contents. Key recovery schemes satisfy both requirements because the government does not have direct access to the encryption key. Although a government agency may capture the encrypted data, it cannot decrypt it without the key. Only the key recovery agent, an independent agency whose actions are governed by its agreements with its users and the laws of the land, can produce the key. Privacy is protected because the government must present sufficient evidence to warrant key recovery to the key recovery agent before anything is decrypted.

2. The Model of a Practical Key Recovery

Since, the problem of how to recover a forgotten password or key is a practical issue, key recovery scheme should be practical in nature as well.

Following are the requirements of practical key recovery scheme as described in [3] and on which Sung Ming Yen's key recovery solution is based.

(1)The key recovery protocol should be performed at the user's location through an on-line process interacted with the recovery server. For this purpose, the on-line process must also provide both secrecy and authenticity.

(2) The key recovery server should not know the exact passwords or keys to be recovered by the user. This implies that a simple key backup approach does not match the requirement of a good key recovery.

(3) An attacker cannot try to impersonate to be a specific valid user without being detected and recovers that user's passwords or keys via the assistance from the key recovery server which acting as an oracle. In another word, any on-line impersonating and guessing attack should be detectable by the recovery server.

(4) In the real world of using digital systems, any user may have many passwords or keys to remember, however the user does not have to keep a cleartext backup of them in order to prevent forgetfulness.

(5) Even if the user loses his local copy of the most important personal secret information, the key recovery scheme should also enable the server to assist the user to recover his password or key. Although, in this situation, it may be requires the user to return back to the recovery server physically and performs the recovery process.

This key recovery model lags one important step which should be incorporated in point (3) of the model. Apart from detecting online impersonating and guessing attack, key recovery server should be able to prevent it as well. On detecting online guessing attack, generally key recovery server shuts down the service to the user whose account is being attacked, may be on a temporary basis, Consequently, it causes denial of service to legitimate user, causing inconvenience who might be in urgent need of service at that time. Key recovery service may further demand change of long term personal password of user which has been attacked, which may cause further inconvenience to the user, as he has to change his password each time the attack occurs. This is important drawback in the existing model which renders it impractical. So, it is essential that the key recovery service should be able to prevent online guessing attack, a measure should be taken which makes online password guessing infeasible. One such security solution which exists today is a CAPTCHA [4], a challenge, which makes sure that a human being is entering a password or sending login information.

Another drawback in the existing model is that, a legitimate authority should also be present which is always able to decrypt the file or monitor communication to avoid illegal activities. This is also one of the most prominent application of key recovery 'to monitor communication' as described earlier. These additional measures make key recovery truly 'practical', convenient and law abiding.

Following is the new key recovery scheme described which apart from adopting model described in [3], also incorporates additional measures describes above.

3.A NEW KEY RECOVERY SCHEME

3.1 Registration process

When user creates his account Id, a simple personal password(P_a) is created and a strong key (K_2) is generated for him which he will use to encrypt key used to encrypt the file. Each user is assigned his unique K_2. All this information is stored in key recovery server. Also we can have a AUTHORITY SERVER which has the capability to decrypt any file incase of order by court. Public key of key recovery server and of authority server can be downloaded anytime.

3.2 Description of encryption process

K_1 is random strong key generated by user for encrypting a file. After encrypting a file, K_2 is to be obtained for encrypting K_1. K_1 is encrypted with key K_2 using any strong symmetric cryptographic algorithm.

1) K2 obtaining protocol

User will have to authenticate himself to the key recovery server in order to obtain his unique K_2. K_2 corresponding to his Id supplied will be provided.

2)Authentication process

1)User sends login request to key recovery server server.

2)A CAPTCHA is presented by key recovery server to the user. This is done to secure the interface from an online guessing attack.

3)After solving CAPTCHA, user sends login information (Id,P_a) to the key recovery server.

If and only if login is successful, a modified encrypted key exchange protocol is carried with key recovery server to get K_2. (Above login phase is essential as encrypted key exchange is not secure against online attack). Encrypted key exchange protocol is described in [5].

3)Modified Encrypted Key Exchange protocol

1)User sends P_a(a randomly generated public key) to key recovery server. Instead of using P_a as an exchange password shared between key recovery server and user, we can also use a different, unique and simple exchange password shared between key recovery server and user to add to security and it won't be difficult to remember as well.

2)Key recovery server decrypts public key and sends P_a(public key(K_2)) to the user.

3)User decrypts K_2.

K_1 is encrypted with K_2 and this encrypted information can be stored in user's personal PC or can be added to key recovery field in file.K_1 is also encrypted with public key of master server (or AUTHORITY SERVER) and is added to key recovery field in file which is used to decrypt file in case of order by court or legal issues.

3.3 Recovery process

1)User obtains K_2 from key recovery server by same protocol described above.

2)K_2 is used to decrypt K_1 stored in encrypted form in key recovery field.

After obtaining K_1, user can decrypt the file.

Convention - A(B) shows B is encrypted with key A. h(a,b..) denotes a one way hash function where a,b etc are inputs to hash function.

4.Security Analysis of New Key Recovery Scheme

Key recovery scheme described above is compliant with practical key recovery model described in [3]. Apart from this, it also employs additional measures described in this paper, which are a must for key recovery to be practical and convenient. First of all, key K_1 used to encrypt the file is also encrypted with the public key of AUTHORITY SERVER and is appended to the key recovery field. In case of order by court, K_1 encrypted with the public key of AUTHORITY SERVER is extracted and decrypted, hence K_1 obtained can be used to decrypt file. This feature can also help in monitoring communication in a company. Secondly, a strong key K_2 is used to encrypt file encryption key K_1, and K_1 is encrypted with K_2 using strong symmetric algorithm and is appended to key recovery field in file. As a strong key and strong cipher is used for encryption, this makes offline password guessing attack infeasible. Also, K_2 is obtained each time from key recovery server during encryption and while recovery. Encrypted key exchange protocol is used to exchange K_2 between user and key recovery server. This makes exchange safe from eavesdropping. Most importantly, before encrypted key exchange protocol is carried between user and key recovery to exchange K_2, user has to login to the key recovery server. Each time, before entering user Id and password, user is expected to solve a CAPTCHA. This step makes sure that a human is entering the login information not a program. If and only if, login is successful, encrypted key exchange protocol is carried between key recovery server and user. If login is unsuccessful, user has to solve CAPTCHA and enter login information again. Thus, this step makes key recovery scheme resistant to online guessing attack, thereby making it more practical and convenient. Also, user won't have to remember any complex password for a successful key recovery or for performing file encryption.

5.Conclusion

In this paper, we have presented a key recovery scheme secure against online guessing attack. There exists few key recovery scheme's such as Cykey key recovery solution by Cylink, Bell labs key recovery scheme by bell labs, practical key recovery by Sung Ming Yen which is improvement of Bell Labs key recovery protocol but is prone to online guessing attack. This scheme takes into account the vulnerabilities of existing key recovery solutions and is secure to online guessing attack. As described earlier in this paper, implementation of this feature is a must as an online guessing attack makes key recovery impractical and inconvenient.

6.Acknowledgments

I would like to thank Dr. Sung Ming Yen and Murphy Hsu for their immense guidance and support.

7.References

[1] CyKey : *Cylinks* Key Recovery Solution

[2] D.P. Maher,"Crypto backup and key escrow," *Commun. ACM*, vol.39, no. 3, pp. 48–53,1996.

[3] Practical Key Recovery Scheme
(S.M. Yen) In Proc. of *the 6th Australasian Conference on Information Security and Privacy--ACISP 2001*, Lecture Notes in Computer Science, Vol.2119, Springer-Verlag, pp. 104-114, 2001.

[4] CAPTCHA project – CMU, *www.captcha.net/*

[5] S. M. Bellovin; M. Merritt (May 1992). "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks". Proceedings of the *I.E.E.E. Symposium on Research in Security and Privacy*, Oakland.

[6] The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. Neumann, R. Rivest, J. Schiller, B. Schneier

[7] Introduction to cryptography and coding theory(First Edition)Wade trappe and Lawrence C. Washington