Computer Network의 暗號法

金 敬 植

A Cryptographic System for Computer Networks

Kim Kyung-sik

Summary

A cryptographic system is proposed for computer networks to protect from either disclosure or substitution. The system is implemented by the addition of key notarization facilities which give users the capability of key management. Key notarization facilities perform notarization which, upon encryption, seals a key or password with the identifiers of transmitter and intended receiver. The system features on-line and off-line application, local key generation, and a digital signature capability.

序 論

現 社會는 computer 利用을 급격히 增大시키고 있으며 이에 따라 computer network 構成도 host와 host를 連結하는 수많은 terminal들로 이루어지고 있다. 따라서 利用者 간의 通信內容을 保護해야할 필요성이 생기게 되었다.

이의 解決 方式으로 Diffie(1976)는 전달할 情報를 특정인 外에는 알 수 없는 形態로 바꾼 PK暗號法(public key encryption algorithm)을 提案하였으며 Rivest(1978)와 Willet(1979) 等의 PK暗號法이 여기에 해당된다.

이러한 暗號法을 computer network에 導入하는 경우 어떠한 暗號 方式을 使用하드라도 다음의 두가지 특징은 필히 갖고 있어야 한다. 첫째 特定한 送信者가 보낸 情報를 特定한 受信者 만이 받아 볼 수 있어야 한다. 둘째 送信者가 作成한 變形된 情報 즉, 暗號文을 送信者 이외의 사람이 削除 또는 添加等의 方法으로 變造할 수 없어야 한다. 이러한 暗號 system의 특징을 갖기 위해서는 어떤 情報의 暗號文을 전달하기 전에 약간의 protocol 交換이 있어야 한다.

本 論文에서는 computer network를 위한 새로운 形態의 暗號 方法을 提案하여 提案된 system의 動作 原理 및 利用方法에 대해 論議하고자 한다.

System構成 및 暗號 方法

1. System Design

먼저 受信者 만이 通信文을 理解할 수 있고 送信者 만이 通信文을 發生시킬 수 있도록 하기 위한 KNS(key notarization system)을 構成해야 하며, 이 KNS는 host computer, 利用者 terminal 및 KNF(key notarization facility)들로 構成되는 computer network에 적합하게 設計되도록 하였다. 이들 각 부분별 機能을 보면, host는 正常的인 動作과 terminal들 간의 通信을 control한다. 각 terminal은 host, host를 通해 다른 terminal 및 通信 channel을 거쳐 다른 host의 terminal들과 通信할 수 있다. 또한 각 terminal은 利用者 指令(command)으로 host KNF를 使用할 수 있다. 모든 指令은 KNF 내에서 履行되며 모든 KNF는 다른 host들이나 設備利用者에게 分配해 줄 key들을 生成할 수 있다.

KNF와 그 host사이의 line 및 각 terminal과 그 host 사이의 line들은 保護(protect)되어야 한다. 이는 물리적으로 安全하게 하거나 link들의 양쪽 끝단에 暗號 裝置를 덧붙임으로써 할 수 있다. 利用者가 host에 어떤 file을 編輯하고 있을 때, file은 보통 平凡한 text 形態이므로, host는 다른 利用者로부터 data를 保護해야 할 것이다. 일단 利用者의 編輯이 끝나면 data를 暗號化하기 위해 KNF를 指令하게 되며 그 結果로 나오는 暗號를 protect되지 않은 memory에 기억시키거나 멀리 있는 利用者에게 보내게 된다. 여기서, host computer에 두가지 형의 memory가 있다고 假定하면 즉, system memory라 부를 수 있는 利用者가 access할 수 없는 memory와 user memory라 부를 수 있는 利用者에 access될 수 있는 memory로 본다. 그러면, 利用者 i의 暗號 key는 user memory에 기억되고 利用者가 access할 필요가 없는 暗號 PW(password)는 system memory에 기억될 것이다. 그럼에도 불구하고 어떤 利用者가 system memory에 있는 모든 暗號 PW에 access할 수 있다고 假定해야 한다. 각 利用者는 자기에게 속하는 暗號 key를 manage하기 바라지만 어떤 clear key도 알지 못하게 된다.

KNF에는 暗號 data나 다른 key를 SK(secret key)로 나타내는 DES(Data Encryption Standard) 暗號法(美商務省 標準局, 1977)이 들어 있다. KNF는 指令과 data 移送을 履行할 control microprocessor와 memory를 가져야 한다. 또한 KNF는 暗號化되지 않은 IK(interchange key)와 active 利用者들의 狀態를 기억하고 있어야 한다. active狀態는 IV(initialization vector)와 함께 利用者 識別子(identifier) 및 送受信 data用 暗號化되지 않은 DK(data key)로 이루어진다. 利用者는 자기의 識別子가 KNF의 active user memory에 load할 수 있다.

KNF에는 예측할 수 없는 key를 生成할 수 있는 key 發生器가 들어 있다. 일단 적절한 parity가 生成되는 56-bit key가 決定되고 이것이 host에 되돌아가기 전에 완전한 64-bit key가 暗號化된다. 따라서 KNF 외부에는 clear key들이 알려지지 않는다. Key 發生器는 또한 DES暗號法을 initialize하는 64-bit IV를 生成하는데 사용된다. KNF에는 clear key, 暗號法, 指令 program 및 key 發生器가 들어 있으므로 외형적으로 protect되어야 한다.

2. 識別子와 key公證

이와 같은 KNS의 특이한 점은 key公證의 支持이다. 이 形式은 안전성을 증대시키고 system 設計를 간단화하며 또한 非PK system으로 digital署名을 履行할 수 있도록 하는 手段을 提供한다. 識別子는 network에서 각 利用者를

독특하게 識別토록 하는 28-bit로 된 비밀이 아닌 二進 vector이다. 利用者가 처음 KNF의 呼出을 試圖할 경우, KNF가 active 狀態로 되게 하기 위한 정확한 PW와 함께 자기의 識別子를 제출해야 한다. Host와 KNF는 모두 利用者를 認識하기 위해 識別子를 이용한다.

Key公證은 公證人의 역할과 비슷한 것으로 公證人이 文書에 公證印紙와 함께 고객의 署名을 捺印(또는 公證)하기 전에 주민등록증 等으로 고객의 身分證明을 요구하는 것과 같은 것이다. Message의 張本人을 認證하는 公證 기능 이외에도 KNS는 message 그 自体와 解讀을 요청하는 사람을 認證한다. 따라서 key 公證은 안전한 通信 channel의 兩端에 公證人을 가지고 있는 것과 마찬가지이다.

識別子를 i와 j로 K를 DES key로 생각하면, $(i/\!/j)$는 i와 j의 連鎖(concatenation)를 나타낸다. 64 bit key K는 각 byte가 7 情報 bit와 1 parity bit로 이루어진 전체 8 byte로 만들어진다. K XOR $(i/\!/j)$는 다음과 같이 定義되는 특수한 함수이다. K의 왼쪽 7 情報 bit는 i의 왼쪽 7 情報 bit와 XOR (exclusive OR)된 다음 parity bit에 해당하는 8 bit가 8 bit의 modulo 2의 합이 奇數(odd)가 되도록 추가된다. 그후 K의 그다음 7情報 bit가 i의 그다음 7 bit와 XOR되며 정확한 parity bit가 붙여진다. 이와같은 過程은 K의 마지막 7 bit가 j의 마지막 7 bit와 XOR될 때까지 계속되며 최종parity bit가 붙여짐으로써 完成되는 함수이다. 그러므로 K XOR $(i/\!/j)$는 56 情報 bit와 8 parity bit를 갖는 모순없는 DES key이다. 모든 PW와 DK는 어떠한 K와 (i,j)쌍 일지라도 K XOR $(i/\!/j)$ 形態로 暗號化된다.

이와같은 公證이 利用될 경우, key와 PW는 送信者의 識別子 또는 key 發生器 및 受信者와 함께 KNF에 의해 暗號化되어 秘密裡 處理된다. 公證된 key를 生成키 위해 送信者는 자신을 KNF가 識別토록 해야하며 자기의 정확한 PW를 제공함으로써 본인임을 證明할 수 있도록 해야 한다. 이것을 利用者 認證(autentication)이라 부른다. 또한 送信者는 예정된 key 受信者를 확인해야 한다. 일단 한번 暗號化된 key는 정확한 識別子 쌍을 다시 제공하지 않는 한 解讀될 수 없다. 이 key를 解讀하기 위해 受信者는 자기 자신이 本人임을 증명하는 PW를 제출해야 한다. 受信者는 또한 暗號化되지 않은채 보내지는 送信者의 身分을 제출해야 한다. 만약 身分證明 情報가 送信者에 의해 제출된 것과 똑같지 않으면 解讀될 key는 원래의 key와 다르게 되며 어떠한 情報도 정확히 解讀될 수 없다. 따라서 受信者는 정확한 送信者를 알아야 하고 예정된 受信者만이 受信이 可能하다.

3. Key 序列

Key 序列을 이루는 두가지 key 형태는 IK와 DK들이다. IK는 PW와 DK들을 暗號化하며

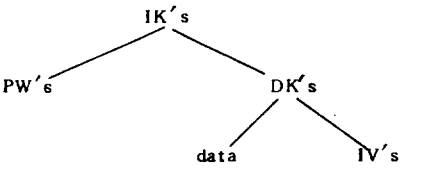

Fig 1. Key hierarchy.

DK는 data와 IV들을 暗號化한다. Fig 1에 key 序列을 나타내었다.

IK는 利用者들 사이의 key交換에 사용된다. 設備 IK라 부르는 한 종류의 IK는 利用者 PW로 設備內部 및 設備의 暗號와 通信하는데 쓰인다. 또다른 IK는 設備들 사이의 DK의 교환이

나 어떤 設備의 특수 subgroup 用으로 이용된다. 生成된 IK는 暗號化되지 않은채 바로 KNF로 들어가게 된다. 이것은 利用者가 다른 두 利用者에게 共用으로된 DK를 解讀할 수 없기 때문에 두 host의 모든 利用者들을 연결하는데 사용될 수 있도록 하여준다. 왜냐하면 두 當事者의 識別子들이 共用으로된 key의 暗號 속에 포함되어 있기 때문이다. 그러므로 KNF에 필히 기억될 key의 수는 감소한다.

DK는 한 특수한 利用者에 속하는 data나 두 利用者가 共有한 data를 暗號化하는데 쓰인다. DK는 key 發生器에 의해 生成되며 IK가 識別子 쌍과 XOR 됨으로써 즉시 暗號化된다. Key를 요청하는 利用者(送信者)의 識別子는 識別子 쌍에서 항상 왼쪽에 오게되며 예정된 受信者의 識別子는 오른쪽에 놓이게 된다. IV는 CBC (cipher block chaining), CFB(cipher feedback) 및 DAUT(data authentication) 方法에서 DES暗號法으로 나타내진다. 이들이 KNF를 떠나기 전에 DK가 해당되는 data를 暗號化하는데 사용됨으로써 모든 IV는 暗號化될 수 있다.

4. 利用者 認證

各 利用者는 利用者 認證 및 利用者 指令을 불러올 수 있게하는 PW를 가지게 된다. 平 PW는 利用者 識別子들이 들어있는 暗號 機能部를 통과하게 되며 이 결과로 利用者가 active되기 전에 기억되었던 값과 KNF에서 비교되어 진다. 그러므로 利用者는 자기의 신분증명이 認證될때까지 다른 어떤 指令도 이용할 수 없다. 各 利用者의 PW는 利用者의 識別子와 결합된 設備 IK로 暗號化된 system memory에 기억된다. Host가 利用者의 한번 認證되었던 정확한 身分證明을 維持할 수 있다면 利用者는 active인 동안 各 指令 때마다 자기의 PW를 다시 제출할 필요가 없다. Active 利用者 memory 속에 load된 자신의 認證 識別子가 自動的으로 자신의 · 識別子로 利用되기 때문이다.

5. Password와 Key의 記憶

Table 1은 host에서 key가 어떻게 KNF memory, system memory, 및 利用者 memory속에 나타나는가를 보여준다. KNF memory에는 現과 舊 IK 및 利用者들의 active狀態가 들어있다. IK가 변경될 경우, 舊 IK는 KNF

Table 1. Password and key storage

KNF memory at host 1

Current	Old
IK1	IK1′
IK2	IK2′
IK3	IK3′
.	.
.	.
.	.
Transmit	Receive
i. IVt DKt	IVr DKr

(for a limited number of active users)

(IK1 equals host 1's facility interchange key)
(IK2 is used to exchange keys with host 2)

System memory at host 1

i. E[IK1 XOR (i//i)](PWi)
j. E[IK1 XOR (j//j)](PWj)
k. E[IK1 XOR (k//k)](PWk)
.
.
.

User i's memory at host 1

Nonshared keys
E[IK1 XOR (i//i)](DK1)
E[IK1 XOR (i//i](DK2)
E[IK1 XOR (i//i](DK3)
.
.
.

Shared keys
E[IK2 XOR (i//j)](DKij)
(shared with user j at host 2)
(transmit key)

E[IK5 XOR (i//k)](DKik)
(shared with user k at host 5)
(transmit key)

E[IK7 XOR (m//i)](DKmi)
(shared with user m at host 7)
(receive key)
.
.
.

외부에 有效 data와 함께 은밀히 記憶된다. 現 IK는 舊 IK로 되며 新 IK가 現 IK로 된다. 이러한 변경 후 PW는 現(新) IK에 의해 再暗號化되며 利用者들은 자기의 DK로 再暗號와 交信하게 된다. System memory는 모든 利用者를 위해 暗號化된 PW를 가지고 있다. E[X](Y)가 X에 의한 Y의 暗號化를 나타낸다면 E[IK1 XOR (i//i)](PWi)는 IK1이 利用者 i의 識別子 쌍인 (i//i)와 XOR됨으로써 PWi가 暗號化됨을 나타낸다. IK 1은 host 1의 system memory에서 온 것이기 때문에 이용되며 또 IK 1은 host 1을 위한 設備交換 key이다.

PW는 代用에 대한 protect를 위해 IK 1이 識別子 쌍과 XOR됨으로써 暗號化된다. 만약 識別子가 사용되지 않고 利用者 j도 system memory에 access할 수 있다면, j는 利用者 i의 暗號化된 PW E[IK1](PWi) 대신 자신의 암호화된 PW인 E[IK 1](PWj)를 이용할 수 있게 된다. 결국 利用者 j가 자기 자신의 PW를 제출함으로써 利用者 i로 認證될 수 있게된다. 識別子가 Table 1에서와 같이 사용된다면, E[IK 1 XOR (i//i)](PWj)가 認證에 이용되고 利用者 i의 暗號化된 PW로 代用되었던 E[IK 1 XOR (j//j)](PWj)와 비교되지 않은 셈이다.

利用者 i memory에는 개인 및 共用 DK가 들어 있다. 개인 DK는 설비교환 key가 利用者의 識別子 쌍과 XOR 됨으로써 암호화되나 共用이 될 수는 없다. 또한 利用者 i memory는 이용자 i의 識別子 및 다른 利用者의 識別子가 連鎖(//)된 것에 IK가 XOR됨으로써 暗號化된 共用 DK를 가질 수 있다. (i//j)는 통신 當事者를 독특하게 識別한다. 만일 (i//j)가 사용되지 않으면, 다른 利用者가 IK로 暗號化된 자신의 DK로 代用한 다음 어떠한 계속되는 暗號文도 解讀할 수 있게된다. 마찬가지로 利用者 j가 E[IK, XOR (i//j)](DKij)를 받았을 때 j는 交換 p를 거쳐 i와 정확하게 暗號文 DKij를 交信하고 있음을 알아야 한다. 따라서 送信者는 누군가로 假裝되는 것을 防止할 수 있다.

6. Digital 署名

Digital 署名은 Rivest(1978) 等에 의해 PK system과 함께 開發되었다. 이러한 system에서 解讀 key는 暗號 key와 같지 않으며 또 推定해 낼 수도 없다. 解讀key가 비밀이 維持되는 반면에 暗號 key는 公共然하게 만들어 질 수 있다. 은밀한 解讀 key를 사용하여 解讀되는 digital 署名이 受信者에게 보내지면, 受信者는 PK를 사용하여 署名을 確證할 수 있으

나 送信者만이 은밀한 解讀 key를 알기 때문에 署名이 模造될 수는 없다. KNT는 代用 防止를 위해 識別子를 IK와 결합하며 다른 暗號와 解讀 key 記憶裝置를 쓰기 때문에 어떤 사람이 다른 利用者에 의해 生成되었던 key에 data를 暗號化할 수 없다. 따라서 署名이 可能하게 된다. 利用者 i가 한 key를 發生시켜 利用者 j에게 보낸다고 보면, 暗號化된 DK는 다음과 같이 된다.

$$ED = E[IK_p \text{ XOR } (i/\!/j)](DKij)$$

여기서 IK_p는 交換 p에 대한 IK이며 $DKij$는 j에게 전송하기 위해 i에 의해 發生된 DK를 나타낸다. i가 key를 發生할 때는 언제나 key의 暗號化에 사용되는 識別子 쌍 속의 왼쪽에 자신의 識別子가 있게 된다. 利用者 j가 DK ij를 load할 수 있는 단 한가지 方法은 受信 key로 load하는 것이다. 그러므로 相異한 送受信 key register가 필요하게 된다. 만일 j가 i에게 갈 data暗號用 전송 key로 $DKij$를 load하려 한다면, ED를 解讀할 때 暗號 module은 $(i/\!/j)$ 대신 $(j/\!/i)$를 사용하게 되며 만약 j가 개인 key로 key를 load하려 한다면 $(j/\!/j)$가 사용될 것이다. $DKij$가 受信 key로 load될 경우, 解讀 指令만이 access할 수 있다. 이밖의 다른 어떠한 key나 指令도 필요치 않다. j에겐 S를 특이한 S′로 변경할 방법이 없으며 $DKij$로 暗號化할 수도 없다.(Table 2 參照)

利用者가 자신의 ED key를 發生할 경우 ED key는 다음과 같이 된다. 즉, $E[IK_p$ XOR $(j/\!/i)](DKji)$. j는 $DKji$로 署名 S′를 暗號化할 수 있으나 i로 부터 왔다고 말할 수는 없다. 그렇게 하기 위해 j는 $E[IK_p$ XOR $(j/\!/i)](DKji)$를 KNF에 load시켜야 한다. 暗號 module은 識別子 쌍으로서 $(j/\!/i)$ 대신 $(i/\!/j)$를 사용하므로 올바른 $DKji$를 load할 수 없다. 따라서 署名이 歪曲된다.

모든 message는 署名으로 看做될 수 있다. 利用者 j가 할 것은 $E[IK_p$ XOR$(i/\!/j)]$ (DK ij), $E[DKij]$(IV), 및 i로 부터 자기에게 보내졌다는 사실을 證明할 수 있도록 하기 위해 暗號化된 message를 保存하는 일 뿐이다. 마찬가지로 j는 S도 保存하기 원할 것이다. 물론 j는 위에서 記述한 바와 같은 方法으로 $DKji$에 의해 暗號化된 署名 S′를 i에게 보낼 수 있다. (Table 2參照)

Table 2. Separate transmit and receive key storage

user i		user j
Transmit ; IV1 DKij S	→	Receive ; IV1 DKij
Receive ; IV2 DKji	←	S′ Transmit ; IV2 DKji

考　　察

어떠한 通信 狀況에서도 送受信者 간의 秘密通信이 이루어지기 위해 送信者가 受信者의 身分을 確認할 수 있어야 한다. 이를 위해서는 첫째 受信者 만이 그 文을 理解할 수 있어야 하고 둘째 送信者 만이 그 文을 發生시킬 수 있어야 한다. 提案된 KNF는 약간의 protocol만 있으면 暗號化 및 確證이 가능하다. Host OS(operating system) 들은 平文을 protect 하며 한번 認證된 利用者의 身分證明이 維持되지만 host를 露出 및 代用에 대해 protect할 필요는 없다. DK의 안전한 分配는 key 公證을 위한 暗號와 識別子를 使用함으로써 達成되었다.

摘　　要

個人이 file이나 terminal 利用者 간의 通

信을 保護하기 위해, key 代用 防止와 system 利用者 및 data의 認證을 위한 暗號 system을 提案하였다. 또한 署名者만이 署名文을 作成할 수 있고 다른 어느 누구도 그 署名文을 變造 또는 捏造할 수 없는 digital 署名 기능을 賦與하였다. 이 system은 data 暗號 기능과 아울러 key 運用 能力을 利用者에게 提供하여 實行할 수 있도록 構成하였다.

參 考 文 獻

Diffie, W., H.E. Hellman. 1976. New directions in cryptography. IEEE Trans. Information Theory. IT-22. 644-654.

Ehrsan. W.F., S.M. Matyas, C.H. Meyer and W.L. Tuchman. 1978. A cryptographic key management scheme for implementing the data encryption standard. IBM Systems Journal 17. 106-125.

Ingemarsson, I., C.K. Wong. 1981. Encryption and authentication in on-boad processing satellite communication systems. IEEE Trans. Commun. COM-29. 1684-1687.

National Bureau of Standards, U.S. Department of Commerce. 1977. Data encryption standard. FIPS Publication 46. Washington. DC.

Rivest, R.L., A. Shamir and L. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM. 21. 120-126.

Simmons, G.J. 1979. Symmetric and asymmetric encryption. Comput. Surv. 11. 305-330.

Willett, H. 1979. Recent result in public-key cryptography. Proceedings National Electronics Conference (NEC/79). Chicago. ILL.