정보학연구 제5권 제2호 2002년 6월(pp.35-45)
The Journal of Information Technology, Vol.5, No.2

OSI-분산 시스템에서의 Biba Security 모델의 구현

박종화*

요 약

분산 시스템에서는 정보가 공중망을 통해 교환되므로 쉽게 도청되거나 또는 변경될 수 있다. 따라서 분산 시스템에서의 보안정책은 전송 중이거나 또는 단말기 내에서 정보를 보장할 수 있어야한다. 이 논문에서는 두 단말기 내에 각각 존재하는 두 AP(Application Process)들 사이의 통신은 Open System Interconnection(OSI-RM)을 위한 ISO Reference Model[2]에 따라 일어난다고 가정하였다. OSI 보안 services와 Biba 보안모델 사이에 관계를 만들어 내는데 Public Key Systems(PKSs)가 사용되었고, 대칭과 비대칭 cryptographic systems에서 어떻게 하면 key 분배가 최소화할 수 있는지에 대하여 연구되었다.

Ⅰ. 서론

정보화 사회에서 개인이나 조직에서의 정보의 교환은 필수적인 것이 되었다. 또한 정보는 개인이나 조직에 중요한 자산이므로 이를 적절히 관리하는 것이 무엇보다 중요하다. 따라서 정보의 기밀을 보호할 수 있는 적절한 보안대책이 요구된다. 이와 같은 보안대책은 자연어의 모호성을 배제하기 위해 일반적으로 FSPM(formal security policy model)와 같은 정형화된 언어를 사용하는데 Biba 보안모델[1]이 그 하나의 예라 할 수 있다.

보안정책은 정보를 전송하는 컴퓨터의 체계에서 독립적으로 만족되어져야 한다. 좀더 상세하게, 그 컴퓨터의 체계는 같은 컴퓨터 내에 두 개의 AP(Application Process)들 사이에서 통신이 일어나게 하는 단일 시스템이 될 수도 있고, 또 다른 단말기들에 존재하는 AP들이 공중망을 통해 연결된 분산 시스템이 될 수도 있다. 단일 시스템에서는 정보가 항상 시스템 내에 존재하므로 비교적 안전하다 하겠다. 그러나 분산 시스템에서는 정보가 공중망을 통해 교환되므로 쉽게 도청되거나 또는 변경될 수 있다. 따라서 분산 시스템에서의 보안정책은 전송 중이거나 또는 단말기 내에서 정보를 보장할 수 있어야한다. 이 논문에서는 두 단말기내에 각각 존재하는 두 AP들 사이의 통신은 Open System Interconnection(OSI-RM)을 위한 ISO Reference Model[2]에 따라 일어난다고 가정하였고, OSI 보안 services와 Biba 보안모델 사이에 관계를 만들어 내는데 역점을 두었다. 이는 OSI 보안 service와 B-LP 보안 모델[3] 사이에 관계를 형성한 Verschuren과 Govaerts의 논문[4]에서 많은 부분 참조되었다.

* 세명대학교 컴퓨터정보학부 소프트웨어학과 교수

II. 분산시스템에서의 Biba 모델

2.1. Biba의 보안 모델

Biba 모델은 정보의 비밀성을 강조한 BLP 모델이 간과한 정보의 무결성을 보장하기 위한 모델을 제안하였다. Biba 모델은 BLP 모델과 유사하게 주체 또는 객체의 무결성이나 신뢰도에 따라 등급을 부여하여 자료의 무결성을 유지하기 위한 모델이다. Biba 모델에 있어서 기본 개념은 낮은 무결성 정보가 높은 무결성 정보에 흘러가지 못하도록 하는 모델로 하나의 무결성 등급이 다른 무결성 등급을 지배하는 경우에만 정보 흐름이 발생할 수 있도록 하고 있다.

Biba 모델은 무결성을 보장하기 위한 안전한 접근 경로를 정의하기 위하여 쓰기 성질과 읽기 성질을 각각 단순 무결성 성질(simple integrity property)과 무결성 *-성질 (integrity *-property)의 두 가지 무결성 성질로 정의한다. Biba 모델의 구성은 주체의 집합 S와 객체의 집합 O, 그리고 주체와 객체의 등급 I로 구성되며, 각 주체와 객체는 고정 된 무결성 등급을 부여받는다. 다음은 두 무결성 성질을 정의한다.

2.1.1. 단순 무결성 성질(simple integrity property)

주체 S는 객체 O에 대하여

$I(s) \geq I(o)$인 경우 객체에 쓰기 허가

2.1.2. 무결성 *-성질(integrity *-property)

객체 O에 대하여 읽기 접근이 있는 주체 S는

$I(o) \geq I(p)$인 객체 p 에 쓰기 허가

2.2. 분산 시스템에서의 Biba 모델

Biba 모델을 분산 시스템에 적용하기 위해서는 객체 즉 정보의 보안등급(sensitivity)과 수신자 AP의 해제등급(clearance)이 결정되어야 한다. 그래야 Biba 모델의 분산 시스템에서 서로 다른 등급을 갖는 AP들 사이의 정보 교환을 막을 수 있다.

하나의 단말기(end-system)에 존재하는 하나의 AP가 다른 AP로부터 정보를 수신하고자 할 때, 다음의 두 단계가 필요하게 된다.

- **접근 제어(Access Control)**
  - 수신자 AP는 자신의 신분을 밝히고, 수신하고자 하는 정보를 지정한다.
  - 그 요구된 정보가 수신자 AP에 보내질 수 있는지 결정되어 진다.

- **정보 전송(Data Transfer)**
  - 정보 전송이 허용되어지면, 그 정보는 암호화되어 진다.
  - 이 때 정보의 보안등급에 무결성이 보장되어야 한다.

두 번째 단계에서 정보 전송시 보안정책의 적용 즉 암호화는 공중망을 통해 정보를 전송하는 동안 자료누출을 막기 위함이다. 이 때 수신자는 정보의 보안 등급을 결정할 수 있다.

만약에 위의 요구 중 어떤 것이라도 만족되지 않는다면 다음과 같은 일이 이 Biba 모델에서 발생하게 될 것이다. 즉, 다음과 같다.

- 정보가 암호화되지 않는다면 허가되지 않은 주체가 그 정보를 읽을 수 있다.
- 만약에 정보의 보안 등급이 수정될 수 있다면 그 정보 수신이 허용되지 않은 주체에

전 달될 수 있다.

이때 두 종류의 보안 서비스가 필요하게 되는데, 이는 정보의 누출을 막기 위한 비밀성(confidentiality)과 불법적인 정보의 변경을 금지하는 무결성(integrity)이다.

이 보안 서비스를 구현하는데 이 논문은 International Standard 7498-2[5]의 지침서를 따를 것이며, 해독(deciphering)에 필요한 비밀 key의 분배에 초점을 맞출 것이다. 즉 어떤 주체(entity)가 어떤 비밀key를 갖게 될 것인지가 결정된 후 비밀성과 무결성을 구현하기 위해 cryptographic technique을 적용할 것이다. 이 cryptographic technique가 적용될 때 다음의 약어가 사용된다.

EK : 암호 key(enciphering key)
SK : 비밀 해독 key(secret deciphering key)

PSK에서 EK는 public이고 SK와 동일하지 않다. 또 Symmetric Cryptographic System 에서 EK는 public이 아니고, SK와 동일하다. 즉 EK = SK.

2.3. 정보의 암호화

중요한 정보는 암호화되는 것이 필요하다. Biba 모델은 모든 주체(entity)들이 이 정보를 해독하는 것을 허용하지 않는다. 따라서 어떤 특정한 등급의 정보를 해독이 허용되는 주체의 해제 등급이 결정되어야 한다.

따라서

- 정보는 특정한 key들을 사용하여 암호화되어야 한다.
- 주체의 해제 등급은 그 주체가 어떤 key들을 가지고 있는가에 따라 결정된다.

이들을 형식화하면

c = AP의 해제 등급, c 는 AP가 취급하는 정보의 해제 등급을 나타낸다. 즉 등급 1의 정보는 가장 낮은 등급을 나타낸다.

s = 정보의 비밀 등급.

Biba 모델은 AP의 해제 등급 c 와 정보의 비밀 등급 s 사이에 관계를 설정하는데, 만약,

$s \leq c$ 일 때 (1)

해제 등급 c를 갖는 AP는 비밀등급 s의 정보를 취급할 수 있다. 유사하게 [6]으로부터 해제 등급 c를 갖는 AP는 다음의 해독 key(deciphering key) SK(i)를 취급할 수 있다. 즉,

$SK(i),\ i \leq c$ (2)

또한 Biba 모델은 비밀등급 s의 정보의 해독은 다음의 해독 key들의 하나에 의해 행해질 수 있다는 것을 보인다. 즉,

$SK(i),\ i \geq s$ (3)

2.4. 등급의 무결성

등급은 정보의 중요도를 나타낸다. 그 중요도는 암호화되기 전의 정보에 따라 정해진다. 비밀성의 측면에서 암호화 후의 정보는 모든 사람에 읽혀지는 것이 허용된다.

무결성 서비스의 구현을 위해서 어떤 특별한 비밀 정보를 요구하게 되는데, 그렇지 않으면

모든 사람에게 정보를 허용하게 될 것이다. 무결성을 보호하기 위한 비밀 정보는 cryptographic technique을 수행하기 위해 사용되는 하나의 key가 될 수 있다.

우리는 여기서 어떻게 등급의 무결성이 유지될 수 있는지에 대해 논의 한 후에 등급이 어떤 정보를 포함해야 하는지를 언급할 것이다. 서로 다른 등급의 정보가 전송되는 상황을 고려해보자

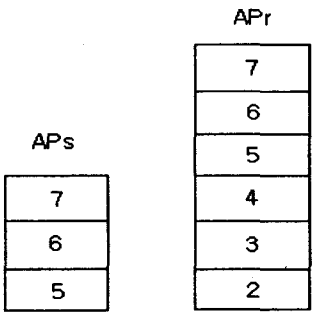

Fig. 1. APs which may exchange data of three class.

식 (3)으로부터 등급 5,6, 그리고 7의 정보가 같은 key를 사용하여 암호화 될 수 있다. 즉 EK(7)이 등급 5,6, 그리고 7의 정보를 암호화하기 위해 사용된다. 이 때 정보의 중요도를 나타내는 등급화가 필요하다. 만약 등급 4와 5의 정보가 EK(5) key를 이용하여 암호화된다면 등급은 그 key가 등급 4의 정보 또는 등급 5의 정보에 관한 것인지를 나타내야 한다. 다시 말해서 하나의 key가 여러 등급의 정보를 암호화하기 위해 사용된다면 그땐 등급화가 필요하게된다. 또한 하나의 key가 오직 한 등급의 정보를 보호하기 위해 사용된다면 그땐 등급화가 필요 없게 될 것이다.

즉, il이 가장 낮은 등급을 나타낼 때 암호화를 위한 key가 다음과 같다면,

$$EK(i), \quad i \neq il \tag{4}$$

등급화가 필요하게 된다. 이때 등급은 정보의 중요도를 나타내는데, 그 값은 i와 il의 사이값이 될것이다. 따라서 EK(il)이 사용된 경우에는 등급은 필요치 않을 것이다.

정리하면, 두 개가 AP가 서로 정보를 교환하고자 할 때, APs를 송신자, 그것의 해제 등급을 cs라 하고, 또 APr을 수신자, 그것의 해제 등급을 cr 이라 하자. 이때 s 는 APs가 보내고자 하는 정보의 비밀등급이라고 할 때, 하나의 public key EK가 data를 암호화하기 위해 사용되었다면, 해독 key SK는 다음과 같다.

$$SK = SK(i), \quad s \leq i \leq cr \tag{5}$$

또 해제 등급 c를 갖는 하나의 AP는 다음의 비밀 해독 key SK(i)를 갖게 된다.

$$SK(i), \quad i \leq c \tag{6}$$

암호화 key EK(i) ≠ EK(il)이 사용되면 등급화가 필요하고, 등급의 무결성을 제공하기 위한 다른 key는 필요 없게 된다.

Ⅲ. OSI-RM에서의 비밀성 확보

앞에서 해독(deciphering)을 위한 key 분배 관한 것들이 언급되었다. 그리고 서로 다른 단말기에 있는 두 AP들 사이의 정보 교환에 대해 고려했고, 하나의 단말기에는 오직 하나의 AP가

존재하는 것으로 생각했다. 지금 다시 하나의 단말기에 하나 이상의 AP들이 존재하는 상황을 고려해보자. 앞에서의 요구는 각각의 AP에 대해서 고려되어 졌다. 여기서 우리는 하나의 단말기에 여러 개의 AP들이 존재하는 상황에서 비밀성과 무결성이 보장되는지에 대해 논의 할 것이다. 더 상세히 다음의 두 항목 사이의 관계를 발견하려고 노력할 것이다. 즉,

- OSI - communication subsystem의 여러 protocol entities 통한 단말기에 어떻게 해독 key를 분배할 것인가.
- 단말기에 존재하는 AP의 해제등급.

3.1. 분산 시스템에서의 Biba Security 모델을 위한 key 분배

앞에서 비밀 key의 분배는 오직 정보를 수신하는 AP의 해제등급에 의존함을 알았다.

단말기

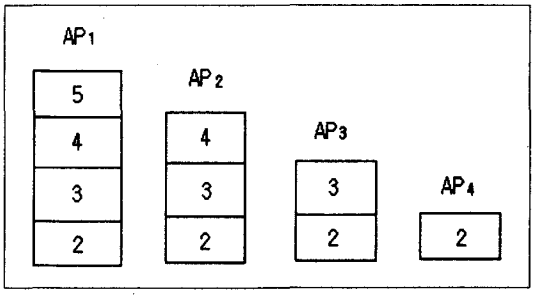

Fig. 2. APs which different clearances resident on end system.

Fig. 2는 하나의 단말기에 4개의 AP들이 각각 다른 해제등급을 갖는 것을 보인다. AP_1의 해제 등급은 5이고, AP_2는 4, AP_3는 3, 그리고 AP_4의 해제등급은 2 인 것을 알 수 있다. 하나의 정보가 위의 단말기에 보내질 때, 그 정보는 AP_1, AP_2, AP_3, 또는 AP_4에 주소지정 되어야한다. 식 (5)로 부터 AP_4로 주소 지정된 정보는 다음과 같이 암호화되어야한다.

즉,

$$EK(i), \quad 2 \le i \le 2$$

결과적으로 AP_4는 SK(2)를 갖는 것이 필요하게 된다. AP_3은 등급 2와 3의 정보를 해독할 수 있는 하나이상의 SK key들이 필요하게되고, AP_2는 등급 2, 3, 그리고 4의 정보를 해독할 수 있는 SK key들이 필요하게되며, AP_1를 위해서는 등급 2, 3, 4, 그리고 5의 정보를 해독할 수 있는 SK key들이 필요하게된다. 따라서 AP들은 각각 해독(deciphering)이 허용된 정보를 해독할 수 있는 여러 개의 key들을 갖게되는데 Table 1은 이들을 보이고 있다.

Table 1. Keys which may be used by APs of fig.2 for deciphering data.

AP1	AP2	AP3	AP4
(5) (2,3,5)	(4)	(3)	(2)
(2,5) (2,4,5)	(3,4)	(2,3)	
(3,5) (3,4,5)	(2,4)		
(4,5) (2,3,4,5)	(2,3,4)		

Table 1에 대한 설명은 다음과 같다.

(1) (s1,s2,...,sN)은 하나의 비밀 key로 비밀등급 s1,s2,...sN의 정보를 해독하기 위해 사용될 수 있다.

예를 들면 (2,3,4)는 비밀등급 2, 3, 또는 4의 정보를 해독하기 위해 사용된다. 결과적으로, 비

밀등급 2, 3, 그리고 4의 정보를 암호화하기 위해 일치하는 public key를 사용하는 것이 적절하다.

(2) AP들은 감소하는 해제등급과 함께 group될 수 있다. 따라서 AP들은 표에서 그들의 오른쪽 열에 있는 key들을 가질 수 있다. 예를 들면, AP_2는 (2), (3), (2,3), (4), (3,4), (2,4), (2,3,4)를 key로 가질 수 있다. 또한 각 AP는 자기열로부터 최소한 하나의 key를 갖고 있어야한다.

요약하면, 모두가 다른 해제등급을 갖는 n개의 AP들이 하나의 단말기에 존재한다면, Biba 모델을 적용하기 위해서 최소한 n 개의 비밀 key들이 필요하다. 하나 이상의 비밀등급을 취급하기 위해 하나의 key가 사용된 경우 등급화가 필요하다.

3.2. Symmetric Cryptographic Systems를 이용한 비밀성의 실현

우리는 [7]로부터 PKS(public key systems)에 관한한 비밀 key 분배는 해독 작용(decipher operation)을 수행하는 단말기 내의 AP의 해제등급에 의해서 오직 결정됨을 알았다. 그러나 Symmetric Cryptographic System이 사용되어졌을 때 암호화를 위한 key는 해독화를 위한 key와 같아야한다. 따라서 송신자와 수신자는 최소한 하나의 key를 공유해야한다. 다른 말로 하나의 Symmetric system이 사용될 때 해독화를 위한 key 분배는 오직 수신 단말기 내의 AP들의 해제등급에만 의존하지 않는다.

다음은 위 사실을 예로서 보여주고 있다. 여기서 두 단말기에 각각 4개의 AP들이 존재하며 그 주소와 해제등급은 다음과 같이 주어진다 (Fig. 3).

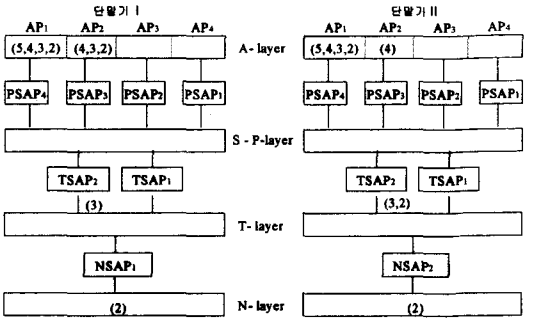

Fig. 3: 2 key distributions going with APs having the same clearance

$$AP_{1,I}\,address = PSAP_4 + TSAP_2 + NSAP_1 \quad (7)$$

$$AP_{2,I}\,address = PSAP_3 + TSAP_2 + NSAP_1 \quad (8)$$

$$AP_{3,I}\,address = PSAP_2 + TSAP_2 + NSAP_1 \quad (9)$$

$$AP_{4,I}\,address = PSAP_1 + TSAP_1 + NSAP_1 \quad (10)$$

$$AP_{1,II}\,address = PSAP_4 + TSAP_2 + NSAP_1 \quad (11)$$

$$AP_{2,II}\,address = PSAP_3 + TSAP_2 + NSAP_1 \quad (12)$$

$$AP_{3,II}\,address = PSAP_2 + TSAP_2 + NSAP_1 \quad (13)$$

$$AP_{4,II}\,address = PSAP_1 + TSAP_1 + NSAP_1 \quad (14)$$

$AP_{1,I}$: $c_{1,I} = 5$ $AP_{1,II}$: $c_{1,II} = 5$
$AP_{2,I}$: $c_{2,I} = 4$ $AP_{2,II}$: $c_{2,II} = 4$
$AP_{3,I}$: $c_{3,I} = 3$ $AP_{3,II}$: $c_{3,II} = 3$
$AP_{4,I}$: $c_{4,I} = 2$ $AP_{4,II}$: $c_{4,II} = 2$

여기서 $AP_{1,II}$는 단말기Ⅱ의 AP_1을 나타내고, $AP_{3,I}$는 단말기Ⅰ의 AP_3을 나타낸다. 따라서 $AP_{2,I}$은 $AP_{2,II}$와 마찬가지로 해제등급 4를 포함해서 자신보다 낮은 등급의 data를 취급할 수 있다.

위의 그림(Fig. 3)에서 key 분배는 서로 다른 AP들이 각각 다른 해제등급들을 가지고 있는 것을 볼 수 있다. 만약 위의 key 분배에 대하여 PKS(Public Key System)이 사용되어졌다면 어떠한 문제도 발생하지 않을 것이다. 그러나 Symmetric Crypto-System에서 위의 key 분배가 사용되어진다면, data 교환이 어려워 질 것이다. 즉 $AP_{2,I}$이 key (4,3,2)를 사용하고, $AP_{2,II}$가 key (4)을 사용하여 등급4의 data를 교환하고자 한다면, 이 때 data 교환은 이루어 질 수가 없다. 이와 같은 문제는 두 AP들 사이에 같은 key 즉 key (4) 또는 key (4,3,2)를 사용하므로써 해결될 수 있다.

다음의 예는 쉽게 해결되는 위의 예와는 달리 다른 어려움을 나타낸다. 하나의 단말기에 4개의 AP가 존재하는 상황으로서 각 AP들의 해제등급은 다음과 같다. (각 AP들의 주소는 식(7)-식(14)로 주어진다.)

$AP_{1,I}$: $c_{1,I} = 6$ $AP_{1,II}$: $c_{1,II} = 4$
$AP_{2,I}$: $c_{2,I} = 5$ $AP_{2,II}$: $c_{2,II} = 3$
$AP_{3,I}$: $c_{3,I} = 4$ $AP_{3,II}$: $c_{3,II} = 2$
$AP_{4,I}$: $c_{4,I} = 3$ $AP_{4,II}$: $c_{4,II} = 1$

Fig. 4에서 key 분배는 각각의 AP들이 서로 다른 해제등급을 갖는 것을 보이고 있다. $AP_{2,I}$와 $AP_{2,II}$사이에 교환되는 등급 5의 data는 key (5,4,3)이나 key (6,5,4,3) 또는 (5,4,3,2,1)을 사용하여 암호화 될 수 있다. 이때 key (6,5,4,3)과 (5,4,3,2,1)은 단말기Ⅰ이 갖고 있지 않기 때문에

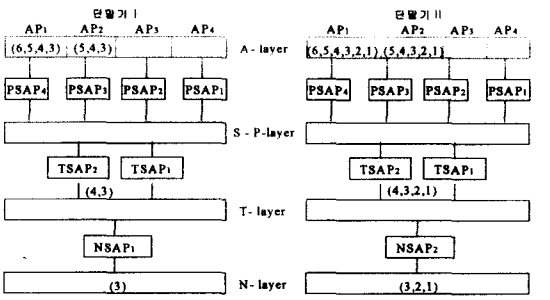

Fig. 4: Key distributions which enable no communication of data of classes 6, 5 and 4

고려의 대상에서 제외되고, key (5,4,3) 만이 사용될 수 있다. key (5,4,3)의 사용은 단말기Ⅰ이 A-layer의 수준에서 암호화하고 단말기Ⅱ는 N-layer의 수준에서 해독화를 수행할 것을 요구하게된다. 이 문제는 단말기Ⅱ에서 key (5,4,3)을 해독화를 위해 A-layer의 수준으로 전달되게 하므로써 해결되어 질 수 있다. 이는 모든 cryptographic operation들을 A-layer의 수준에서 수행하게 하는 것이 최선이라고 할 수 있다. 그러나 A-layer의 수준에서 key (5,4,3)의 사용이 모든 문제를 해결하지는 않는다. Fig. 4에서 등급4 또는 등급3의 data를 암호화하는 것이 가능하지 않기 때문이다. 문제는 key (3), (4), (5,4,3)에 같은 값을 할당하기 때문이다. 따라서 이를 해결하기 위해서는 단말기Ⅱ가 N-layer의 수준에서 key(3)과 key(4) 또는 key (3)과 key (4,3)를 가지게 하는 것이 필요하다.

위로부터 다음과 같은 사실을 이끌어 낼 수 있다. APh를 단말기에 존재하는 가장 높은 해제등급을 갖는 AP라 가정하고, 이 AP의 해제등급을 Ch라 하자. 이때 단말기의 AP들은 다음의 비밀등급 S의 data를 취급 할 수 있다(Sl이 가장 낮은 비밀등급이라 할 때).

$$Ch \geq S \geq Sl$$

이 data는 서로 완전히 다른 해제등급을 갖는 AP들에 의해서 보내질 수 있다. 이때 단말기는 각 data 의 비밀 등급 당 하나의 key를 갖고 있어야한다. 즉 Table1의 각 열로부터 하나의 key를 갖고 있어야한다. 그리고 각 열이 많은 key로 구성되어 있다면 그 비밀등급의 data를 위하여 어떤 key를 사용 할 것인지를 결정하여야한다. 그렇지 않으면 같은 비밀등급의 data를 암호화와 해제화에 대해 서로 다른 key를 사용하는 경우가 발생할 수 있다.

3.3. Asymmetric Cryptographic Systems를 이용한 비밀성과 무결성의 실현

table 1로부터 여러 가능한 key의 분배가 존재한다는 것을 알 수 있다. 그 여러 key 분배 가운데서 가장 적은 수의 key를 갖는 분배를 찾는 것이 중요하고, 그 찾은 key 분배를 Application-layer 아래의 layer에서 비밀성과 무결성을 구현 할 수 있어야한다. 암호화와 해독화는 낮은 layer에서 실현될 때 더 효과적이다. 그것은 인증(authentication)이 낮은 layer에서 행해질 때 적은 포로토콜들을 거치기 때문이다.

인증을 행함에는 접근제어 단계(access control phase)를 수행하는 것이 필요한데, 접근제어단계는 정보가 전송되기 전에 수행되는 것이 효과적이다. 그때 암호화된 정보가 그에 맞는 해독 key를 갖지 않은 AP에 보내지는 것을 막을 수 있다. 결론적으로, 해독 key가 인증을 목적으로 사용되어 졌다면 암호/해독 절차는 낮은 단계에서 수행되는 것이 최선이다.

가장 적은 수의 key를 갖는 분배의 관점에서 하나의 단말기에서 모두 다른 해제등급을 갖는 n 개의 AP들은 최소한 n 개의 다른 key를 갖고 있어야한다. 따라서 Table 2는 가장 적은 수의 key를 갖는 분배라 할 수 있다.

Table 2. Keys distribution where 4 APs (which different clearances) all have different keys.

AP1	AP2	AP3	AP4
(2,3,4,5)	(2,3,4)	(2,3)	(2)

그러나 각 AP가 각각 다른 비밀 key를 갖게 될 때, 하나의 key에 의해 다른 AP들에 지정된 정보를 해독할 가능성이 일어나지 않는다.

따라서 이 분배는 Application-layer 아래의 layer에서 암호/해독 과정이 실현되지 않을 것이다.

어쨌든, 낮은 layer들에서 암호화과정을 실현하면서, 더 많은 key를 요구하지 않는 key 분배가 존재하는데 다음이 그 예이다.

AP1 : (2)(3)(2,3,4,5)
AP2 : (2)(3)(3,4)
AP3 : (2)(3)
AP4 : (2)

이때 AP1, AP2, AP3, 그리고 AP4는 다음의 주소를 갖게 된다.

AP1address = PSAP4 + TSAP2 + NSAP1
AP2address = PSAP3 + TSAP2 + NSAP1

AP3address = PSAP2 + TSAP2 + NSAP1
AP4address = PSAP1 + TSAP1 + NSAP1

여기서, PSAP는 AP가 연결된 Application layer 포로토콜과 Presentation layer 사이의 SAP(Service Access Point)의 주소를 나타내고, TSAP는 Session-layer와 Transport-layer 사이의 SAP주소를 나타내며, NSAP는 AP가 존재하는 컴퓨터 시스템의 물리적 network-wide 주소를 나타내다.

Fig. 5은 위의 key 분배를 이용한 해독과정을 나타낸다.

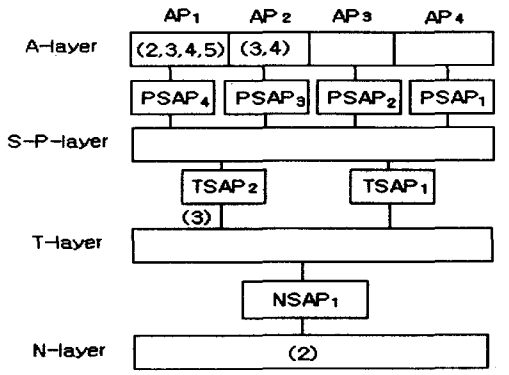

Fig. 5. Key distribution which offers the possibility to use common keys at lower layers.

정리하면, 하나의 단말기에 있는 AP들은 다음의 key들을 갖게된다.

즉, AP들(AP1,AP2,...,APn) 이 다음의 해제등급들(c1,c2,...,cn)을 갖는 다고 가정하고, 낮은 index를 갖는 AP가 높은 해제등급을 갖는다고 가정하면,

$$ci > cj \ , \ i < j$$

이때,

- APn(가장 낮은 해제등급을 갖는 AP)는 표 1과 같은 표에서 자기 열에서 하나의 key를 선택한다.
- APi($1 \le i \le n-1$)는 다음의 key들을 갖는다.
- 하나의 key는 다음의 등급의 정보를 취급할 수 있다.

$$ci \ge s \ge ci+1$$

- APi+1이 갖는 key들.

Ⅳ. 결론

우리는 분산 시스템에서 Biba 보안 정책 모델을 보장하기 위한 Symmetric cryptographic algorithm의 key 분배에 관해 다음과 같은 원칙에 도달할 수 있다. 이것은 단말기 당 최소한의 서로 다른 key들을 갖게 하는 것을 의미한다.

AP들(AP_1, AP_2,...,AP_n)이 각각의 해제등급들 c_1, c_2,...,c_n을 각각 갖는다고 할 때, 높은 색인을 갖는 AP들이 낮은 해제등급을 갖는다면 다음과 같은 관계가 형성됨을 알 수 있다.

$$c_i > c_j \quad \text{for } i<j$$

이때 Table1과 같은 table이 형성되는데, 이 table은 전체 network 안에 존재하는 data의 비밀등급 만큼 많은 열을 갖고 있어야하며 각 열에서 어떤 key가 선택되어 질 것인지는 사전에 결정되어야 한다. 또한 모든 AP들은 자기열과 자기열의 오른쪽에 있는 모든 열로부터 key를 선택할 수 있다.

결론적으로 이 논문은 어떻게 최소한의 key를 갖는 key 분배를 찾아내는지에 초점이 맞추어 졌으며, key 분배는 어떤 종류의 crypto-

graphic system을 사용했는지에 의존되며, Symmetric system을 사용하는 key 분배가 PKS (Public Key Systems)을 사용하는 key 분배보다 많은 key를 요구함을 알 수 있었다.

그리고 Asymmetric system에서

- key 분배는 하나의 단말기에 존재하는 AP들의 집합에 의존한다. 즉, key 분배가 다른 단말기에 존재하는 AP들의 집합에 의존하지 않는다는 사실로 우리는 다른 단말기에 존재하는 AP들과 통신할 수 있다는 것을 알 수 있다.

- 하나의 단말기 안에 AP들이 가장 높은 해제등급을 갖는 AP의 해제등급 아래의 모든 해제등급을 다 감당하지 못한다면, 각 등급의 정보를 위한 각각의 SK를 사용할 필요가 없다. 따라서, 다음 특성의 key를 갖는 PSAP에 속하는 해독이 최선이라는 결론에 이르게된다. 즉, 그 key는 AP가 취급하는 모든 정보를 해독할 수 있어야하며, 낮은 등급의 key에 의해서는 해독되어서는 안 된다. 마지막으로, Fig. 4는 위의 요구에 일치하는 key 분배를 보여준다.

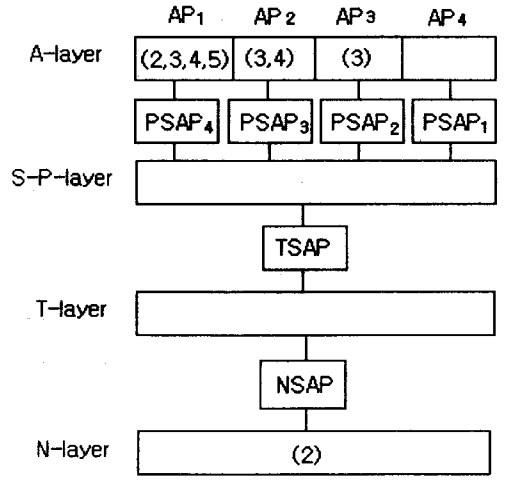

Fig. 6. Key distribution which is efficient with repect to the total amount of keys.

참고문헌

[1] Biba, K. J., "Integrity Considerations for Secure computer System", US Air Force Electronic System Division, 1977.

[2] Open Systems Interconnection Reference Model, Part 1: Basic Reference Model, ISO 7498-1 (CCITT X.200). Melbourne 1988.

[3] Bell, D. Elliot and LaPadula, Leonard J.," Secure Computer Systems: Unified Exposition and Multics Interpretation", MTR 2997 rev.1, The MITRE Corporation, March 1976.

[4] Verschuren Jan, Govaerts Rene and Vandewalle Joos, "Realisation of Bell-Lapadula Security Policy in an OSI-distributed System Using Asymmetric and Symmetric Cryptographic Algorithms", Workshop on Computer Security Foundations, Franconia, New Hampshire(USA), June 16-18, 1992, pp. 168-178.

[5] Open Systems Interconnection Reference Model, Part 2: Security Architecture ISO DIS 7498-2, July 19, 1988.

[6] Verschuren Jan, Govaerts Rene and Vandewalle Joos, "Efficient Realisation of Security Services in the OSI-RM", International Workshop on Advanced Communications and Applications for High Speed Networks, March 16-19, 1992, Munich, Germany, pp. 155-161.

Realization of the Biba Security Model in an OSI-distributed System

Chong-Hwa Park*

Abstract

This paper discusses a distributed implementation of the Biba security policy model. Implementation of an integrity service in the OSI-RM is not sufficient for enforcing the Biba model. Also confidentiality services are necessary. Public Key Systems(PKSs) are considered for the realization of these security services. In this paper symmetric & asymmetric cryptographic systems are considered for the realization of these security service. It is investigated how key-distributions can be found resulting in a minimum number of key.

* Dept. of software, semyung university