□특집□

New Networking Environment Security 구현

홍 정 기†

목 차

1. 서론

요사이 인터넷과 분산 C/S 환경의 보안에 대해서 각 매거진에서 자주 기고되는 바 본 기고에서는 자주 언급되는 각종 기술의 유의할 점, 즉 각 기술의 전면이 아닌 뒷면을 살펴보도록 하겠다. 이에 독자들은 각 기술의 장점뿐 아니라 단점과 파악하므로서 균형있는 감각을 보유할 수 있게 될 것이다.

2. 암호화 알고리즘

먼저 보안 S/W의 수출 문제에 대해서 알아본다. 주지하다시피 미정부에서 1977년 채택한 DES 알고리즘은 원래 56비트 키이를 가지고서 작동된다. 그런데 요사이 워낙 워크스테이션 성능이 좋다보니 DES 키이를 풀어내는 것이 그다지 어렵지 않게 되었다. 이에 미정부는 극히 중요한 문서에는 오히려 DES 알고리즘을 이용치 말고 덜 민감한 문서만 DES를 이용할 것을 규정하고 있다.

현실이 이럴진데 미국 이외 지역 수출용 S/W는 56비트는커녕 40비트로 키이가 구성되어야 수출통관이 되니 보안 측면에서는 불행한 일이라고 하겠다.

다음으로는 Encryption의 수준에 대해서 알아본다. 흔히들 Encryption은 유저 데이타를 대상으로 OSI 7 Layer중 최상위 Layer인 Application Layer에서 발생한다고 생각할 수 있지만 요사이는 이보다 더 근원적으로 Encryption을 가하고 있다. 즉 OSI Layer 중 3번째인 Network Layer에서 Encryption을 수행하는 것이다. 이럴 경우의 장점으로서는 유저 데이터는 물론 송수신자의 IP 어드레스까지도 암호화를 시킴으로써 해커가 제아무리 네트워크 계측기로서도 아무런 정보를 획득 못하게 만드는 효과가 있다.

† 정회원 : 한국휴렛팩커드 차장

국제 표준기구인 IETF에서 RFC 1827 규격으로서 표준을 규정하였으며 ESP(Encapsulating Security Payload)라고 불리운다. 이는 원래의 Layer3 데이터에다가 새로운 송수신 IP 어드레스를 추가로 덧붙이는 것을 의미한다. 참고로 OSI의 규격은 다음과 같다.(그림1)

그러나 이러한 Layer3 레벨의 Encryption이 반드시 좋은 점만 가지고있는 것은 아니다. 즉, 두가지 단점이 있는바 성능상의 오버헤드 문제와 호환성의 문제가 있다.

성능상의 오버헤드라함은 Layer3에서 Encryption 시 소요되는 CPU 성능상의 오버헤드가 있을 수 있다. 이에 일부 벤더는 아예 별도의 Encryption 전용 chip을 CPU 보드에 함께 장착해서 판매하고 있기도 하다. 또 다른 성능상의 오버헤드는 Layer3에서 원래의 패킷 앞부분에 새로운 송수신 IP 어드레스를 덧붙이는 과정에서 생기는 오버헤드이다. 즉, 패킷이 가뜩이나 큰 경우 새로이 송수신 IP 어드레스가 추가됨으로써 Fragmentation이 발생하는 경우의 오버헤드이다. 만일 Fragmentation이 발생된다면 수신측은 이를 다시 Re-assemble 해야되는 부담을 떠 맡게되며 더 문제가 되는 것은 수신되는 패킷이 일렬순서로 입수된다는 보장이 없기에 일일이 일련번호를 재확인해야되는 문제이다.

물론 각 벤더간 호환성의 문제도 있기는 하다. 그렇지만 이상과 같은 여러 단점에도 불구하고 Layer3 레벨의 Encryption이 워낙 보안이 강하므로 시스코를 비롯한 라우터 벤더와 체크포인트를 비롯한 파이어 월 벤더에서 거의 모두 채택하고 있다.

다름으로는 Layer7에서 Encryption이 일어나는 경우에 대하여 알아본다. 이때는 시스템 관리자가 어떤 부분을 Encrypt 할 것이고 어느 부분을 Encrypt하지 않을 것인지를 사전에 결정해야 된다.

그런데 이 작업은 사실 그리 쉽지 않은 작업으로서 각각의 어플리케이션마다 사전에 충분히 성격을 파악하고 있어야 된다는 것이 어려운 숙제로 남게 된다.

3. 키이 배포 알고리즘

다음은 DES 계열 알고리즘의 키이 분배 주의사항에 대해 살펴본다. 간단하게 사용자 키이의 배포를 원할때는 상대방에게 전화로서 통보하거나 우편물 또는 전자우편을 통해서 보내게 된다. 그러나 좀 더 상황이 심각한 경우라면 별도의 키이 배포용 써버를 설치 운영할 필요성이 생긴다. 이에 커버로스 써버를 이용하여 각 개인의 Private Key를 배포하는 방법이 있다.

그러나 이 경우 단점이 있다면 모든 사람의 Private Key가 한곳에 집중 보관되므로 해커들의 좋은 표적이 될 수 있다는 점과 커버로스 설치 과정이 매우 쉽지 않다는 점이다.

다음으로는 공개 키이 알고리즘, 즉 Public Key 알고리즘의 주의사항에 대해서 알아본다. 원래 공개키이의 발명자는 스탠포드 대학의 Diffie와 Hellman 교수로서 현재 가장 상용화되어 있는 버젼은 대부분 미국 RSA 회사가 공급하고 있다.

이러한 공개키의 알고리즘의 가장 큰 단점은 핸드쉐이킹 절차이다. 즉 메시지가 교환되기 이전에 상대방의 신원을 파악하기 위하여 핸드쉐이킹이 필요하게 되는데 이것이 CPU 오버헤드와 네트워크 성능에 오버헤드를 초래하게 된는 것이다. 물론 암호화 작업 그 자체도 오버헤드를 초래하게 된다. 그래서 보통 공개키이 알고리즘은 20%의 오버헤드가 발생한다고들 흔히들 얘기한다.

그런데 핸드쉐이킹에 따른 오버헤드를 줄일 수 있는 방법이 있다. 즉, SKIP(Simple Key Exchange Internet Protocol)을 이용한다면 이를 줄일 수 있는

바 이는 매번 두 사용자가 세션을 맺을 때 매번 상대방 신원을 점검하는 것이 아니라 오로지 한번만 점검하는 것이다.

즉, SKIP은 세션 키이라는 개념을 도입하여 일정 기간 유효하게 운영하는 방식을 채택하고 있다. 예를 들어 기존의 방식에서는 갑과 을이 오전에 상호 화된 데이터 교환시 별도의 사전 핸드쉐이킹이 필요하게 되고 또한 오후 근무시간 끝날때쯤 데이터 교환 필요성이 생기면 또 다시 사전 핸드쉐이킹을 수행해야만 되었었다. 그러던

것이 일단 오전에 세션 키이가 생성되었다면 이를 오후에도 계속 활용할 수 있기에 별도로 핸드쉐이킹에 소요되는 오버헤드를 줄일 수가 있게 되는 것이다. 세션키이의 유효기간은 관리자가 임의로 지정할 수 있게 된다. 따라서 어떤 경우에는 몇일이고 동일한 세션키이를 이용할 수도 있다.

그렇지만 SKIP에도 약점은 있다. 즉 해커가 만일 세션키이를 해독했을 때 모든 내용이 공개된다는 약점이다. 이에 국제 표준기구인 IETF에서는 PSKMP(Photuris Session Key Managerment Protocol)을 제정하였다. 이는 난수와 상대방의 IP 어드레스를 근거로 세션 키이를 발행한다. 그리고 매번 RSA 알고리즘을 이용하여 데이타 교환시마다 새로운 세션 키이를 발행하게 되므로 보다 안전하게 운영이 가능해진다. PSKMP는 비록 SKIP 보다는 느리지만 대부분의 공개키이 알고리즘 보다는 속도가 빠르다. 참고로 OSI규격은 그림과 같다.(그림2)

4. 사용자 신원확인 알고리즘

다음은 Authentication에 대해서 주의할 점을 알아본다.

Authentication이라함은 자신의 신원을 상대방에게 증명해 보이는 작업을 의미하며 두가지 분류 방법이 있는데 H/W, S/W로 분류하는 방법이 있으며 사용 알고리즘에에 따라 분류하는 방법이 있다.

먼저 H/W Authentication에 대해서 알아보면 일면 H/W 토큰이라고도 불리우는 방법으로써 사용자가 자기 주머니 속에 항시 소형의 장치를 휴대해야 되는 방식을 의미한다. 대표적인 제품으로는 SecureID가 이에 속한다. 이때 유의할 사항은 배터리가 소모시 교환 가능한지 여부를 점검해보아야 된다. 만일 일회용이라면 H/W 토큰이 수명을 다했을 때 중앙에서 어떻게 새로운 H/W 토큰을 공급할 것인가에 대해서도 정책을 세워두어야 한다.

S/W 토큰은 PC상에 TSR 모드로 동작되는 S/W를 의미하며 장점으로는 로그인 과정이 H/W 토큰에 비해서 용이하다는 점이다. 반면에 단점으로서는 PC상의 다른 S/W들과 메모리 충돌이 일어날 확률이 높으며 해커 프로그램이 메모리 상주해 있다가 유저가 입력한 사용자 인식번호(PIN 번호)를 낚아 챌 수도 있다는 점이 주의할 사항이 되겠다. 두번째 분류법인 Authenticate 사용 알고리즘에 따라 분류해 보면 Time-Sync방식과 Challenge-Response 방식이 있는바 Time-Sync알고리즘이라함은 Security Dynamic사가 개발한 알고리즘으로써 매 60초마다 새로운 난수를 발생시키는 알고리즘이다. 각 토큰과 중앙의 서버에는 각 유저마다의 고유한 64bit Key가 저장되어 있다. 동작 순서는 매 60초마다 새로이 나타나는 6digit의 숫자(시각, 64bit 키이값, 알고리즘에 의해 결정됨)를 보고서 사용자는 어플리케이션 운영시 4 digit의 개인 식별 번호(PIN)와 6 digit의 숫자를 입력한다. 이에 중앙에서는 미리 기록되었던 해당 유저의 PIN 번호를 참조하여 서버 스스로 6 digit의 숫자를 생성시킨후 상호 비교하여 일치할 경우 로그인을 허락하게 되는 것이다.

여기서 주의할 점으로서는 시간대는 동일한 Time Zone을 이용해야 된다는 것과 60초내에 모든 로그

온 절차가 수행되어야 한다는 사실이다. 장점으로서는 Dumb Device 및 Fax, 전화기에서도 손쉽게 이용 가능하다는 것이 장점이다. 그 이유는 별도의 CPU 및 메모리가 불필요하기 때문이다.

Challenge-Response 방식은 난수로 구성되는 Challenger 와 Challenge값 및 유저 Key로 구성되는 Response 로써 운영되는 방식을 의미한다. 내부적으로는 DES, RSA 또는 유사 알고리즘이 사용된다. 동작 순서는 먼저 중앙의 Authentication 써버에 연결을 시도한 후 유저는 화면상에서 PIN 번호를 입력한다. 이에 써버는 난수(Challenge)를 유저에게 주게 된다. 이에 유저는 Challenge값을 토큰에 입력시키면 토큰은 DES와 유저 Key에 근거하여 Response값을 나타내게 한다. 이에 유저는 터미널상에서 Response값을 입력한다. 중앙의 써버는 스스로 유저의 PIN에 의거해서 Response를 계산 해낸후 이를 비교해서 접근을 허락하게 되는 방식이다. 해당 제품으로써는 SCC Lockout과 Cryptocard등이 있다.

이때의 단점으로서는 유저가 반드시 Computer를 보유해야 된다는 사실이다. 이는 앞서의 Time Sync 방식에서는 굳이 Computer 없이도 FAX, 전화등에 이용할 수 있었었던 것과 비교한다면 차이가 있다고 하겠다. 참고로 ISO에서 정의한 표준은 그림3과 같다.

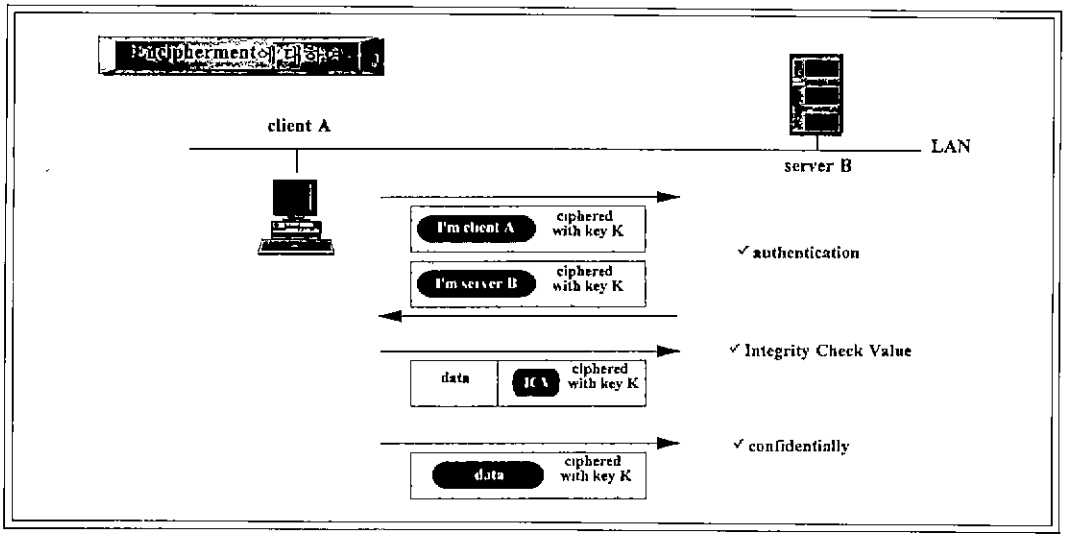
5. 결론

이상에서 살펴본 바와 같이 분산 C/S 환경에서 보안을 고려한 네트워크 및 시스템 구축에는 고려해야 될 요소가 무척 많다고 하겠다. 어느 한 부분만 고려한 솔류션을 구축한다면 본의 아니게 다른 쪽에서 취약한 모습을 보이게 된다.

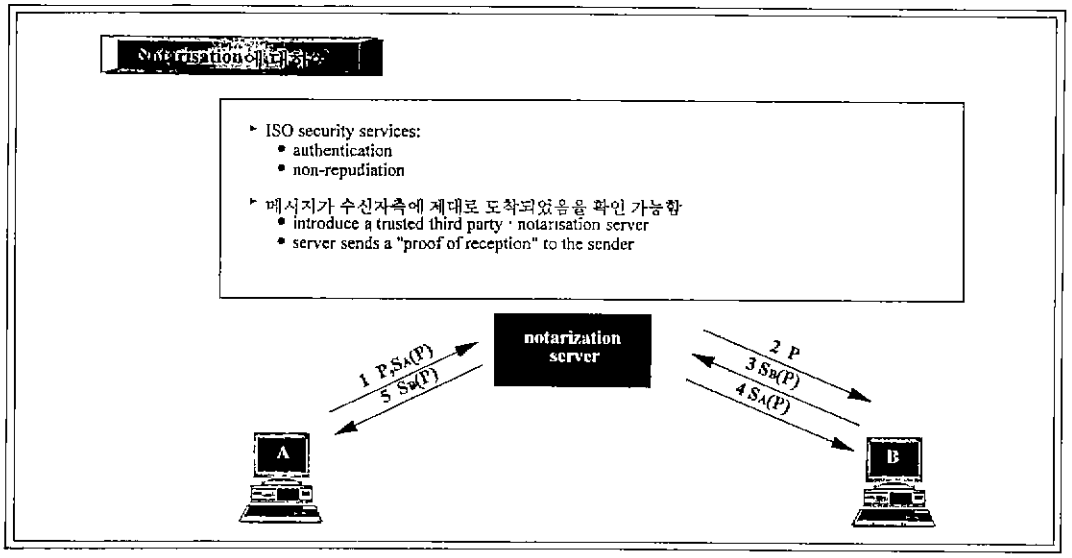
이에 앞에서 언급한 여러 요소를 모두 고려해서 종합적인 솔루션을 구축해야 되겠다.

홍 정 기
IT-Managonunl 부문 컨설팅
인터넷의 보안 부분 컨설팅
삼성 그룹 자문위원
한국 정보문화센터 초정강사
현재 한국휴렛팩커드 차장

<그림1> ISO 7498-2 규격



<그림2> ISO 7498-2 규격



<그림3> ISO의 보안 기준

- 7498/2 OSI Reference Model
  - Part 2 : Security Architecture 언급
- *7816/1-6 Smart Card* 표준
  - Smart Card Forum
    - 600여개 회사 (Visa, Master, Citybank)
  - VME (Visa, Master, Europay)
    - Smart Card와 Credit Card의 결합
  - ICF (Intntl Cryptographic Framework)
    - 미국 이외 수출 가능한 규격, HP 제정
    - HP, Infomix, GemPlus 공동 제정

- ✓ 9796 Digital Signature Scheme
- ✓ 9797 Data Integrity Mechanism
- ✓ 9564 PIN management & Security
- ✓ 10202 Financial Transaction Card