제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

인증서 검증서버의 인증서 검증방법

노종혁*, 진승헌*, 이균하**
*ETRI 인증기반연구팀
**인하대학교 전자계산공학과
e-mail : jhroh@etri.re.kr

Validating Certificate of Certificate Validation Server

Jong Hyuk Roh*, Seunghun Jin* and Kyoon Ha Lee**
*Certification Infrastructure Research Team, ETRI
**Dept. of Computer Enginnering , Inha University

요 약

정보보호 핵심 기반 구조인 PKI는 인증서 검증에 따르는 클라이언트의 부담 및 CRL의 적시성 부재와 관리 문제, 또한 각각의 환경에 따라 구축된 PKI 도메인 간의 상호 연동 등 해결해야 할 문제점들이 있다. ETRI/VA는 클라이언트의 인증서 검증을 대신하여 클라이언트의 부담을 줄이고, 인증서의 상태 검증의 적시성 및 OCSP를 사용함으로써 CRL의 문제점을 해결하며, PKI 상호연동을 지원 및 도메인간의 인증서 정책을 중앙집중 관리함으로써 기존 PKI의 문제점들을 제거할 수 있다. 본 논문에서는 이러한 ETRI/VA의 각 모듈 및 프로토콜에 대하여 간략히 소개하고 ETRI/VA의 인증서 검증 방법을 설명하였다.

1. 서론

최근 몇 년 사이에 실생활의 많은 활동들이 오프라인에서 온라인으로 전환되고 있다. 개방형 네트워크인 인터넷을 통한 전자상거래는 정보의 위변조, 누출, 부인 등 각종 역기능에 의한 위협이 예상되고 있으며, 이에 따라 정보보호 기술은 전자상거래의 안정성과 신뢰성을 제공하는 중요한 요소로 인식되고 있다.

사용자의 공개키를 안전하고 신뢰성있게 공표하는 수단을 제공하는 공개키 기반 구조(Public Key Infrastructure)는 정보보호 핵심 기반구조로써 기밀성, 무결성, 인증, 부인봉쇄 기능을 제공한다. 선진국에서는 PKI를 기반으로 전자상거래의 안전성을 확보하려는 연구가 많이 진행되었으며 전자상거래의 정보보호 기반구조로 활용되고 있다. 국내에서도 1999년 7월 전자서명법이 발효되어 PKI를 이용한 정보보호를 위한 법적인 토대가 마련되었으며 2000년 국가공인 PKI 운용 기관인 공인인증기관이 지정되었고 현재 많은 정보보호 산업체들이 PKI에 대한 연구 개발을 진행하고 있다. 하지만, 기존 PKI는 인증서 검증에 따르는 클라이언트의 부담 및 CRL의 적시성 부재와 관리 문제, 또한 각각의 환경에 따라 구축된 PKI 도메인 간의 상호 연동 등 앞으로 해결해야 할 문제점들이 부각되고 있으며, 다양한 해결 방안들이 제시되고 있다.

ETRI/VA는 클라이언트의 인증서 검증을 대신하여 클라이언트의 부담을 줄이고, 인증서의 상태 검증의 적시성 및 OCSP를 사용함으로써 CRL의 문제점을 해결하며, PKI 상호연동을 지원하고 도메인간의 인증서 정책을 중앙집중 관리함으로써 기존 PKI의 문제점들을 제거할 수 있다. 본 논문에서는 이러한 ETRI/VA의 각 모듈 및 프로토콜에 대하여 간략히 소개하고 ETRI/VA의 인증서 검증 방법을 설명하였다.

본 논문의 구성은 다음과 같다. 2장에서는 인증 검증 기술 및 관련 프로토콜에 대하여 설명하고, 3장에서는 ETRI/VA의 각 모듈 및 인증서 검증 방법에 대하여 기술한 후, 4장에서 결론을 맺는다.

2. 인증서 검증 기술

인증서 검증 기술은 인증 경로 구축과 인증 경로 검증으로 이루어져 있다. 인증 경로란 검증자가 신뢰하는 지점(Trust Point)의 인증서로부터 검증 대상이 되는 인증서까지의 인증서 체인을 의미한다. 즉, 상위 인증서의 소유자(subject)가 하위 인증서의 발행자(issuer)가 되며, 인증서 체인의 마지막 인증서가 인증서 검증의 대상이 된다. 인증 경로 검증이란 인증 경로상의 모든 인증서의 유효성을 검증하는 절차를 말하며, 이를 통하여 상대방의 인증서를 신뢰할 수 있게 된다. 인터넷 기술의 표준화를 담당하는 IETF에서는 PKI 인증 경로 검증 절차는 X.509의 12.4.3절에 근거를 두고 있다[1].

일반적으로 인증 경로 생성은 복수개의 인증기관이 운영되는 배타적 환경에서 서로의 영역을 유지하며 확장성을 지원하여야 한다. 복수개의 인증 기관들은 서로간의 확장성을

지원하기 위해 계층 구조, 상호 인증 구조 등의 다양한 신뢰 모델(Trust model)을 따르고 있다[5]. 신뢰 모델은 PKI의 전체 구조를 결정하는 사안으로, 향후 국제 연동에 대한 준비가 필요하며, 각 모델에 관련된 인증 경로 검증 기술이 요구되고 있다. 신뢰 모델은 계층 구조, 상호 인증 구조, Bridge CA 구조, 신뢰 리스트 등으로 구분된다.

인증경로 생성은 신뢰하는 지점에서 시작하여 검증 대상 인증서까지의 인증경로를 생성하는 reverse 방법과 검증 대상 인증서로부터 시작하여 신뢰하는 지점까지 인증경로를 생성하는 forward 방법이 있고, 두 방법을 혼합해서 사용하는 방법이 있다. 또한 인증경로를 생성하며 인증경로 검증을 동시에 수행하는 방법도 있으며 동시에 수행하는 경우 forward 방법보다 reverse 방법이 보다 효율적이다[6].

인증경로 검증은 대상 인증서 안에 있는 소유자의 identity, 소유자의 공개키, 소유자의 특성들 간의 binding을 검증하는 것이다. 인증 경로는 검증자가 신뢰하는 지점의 인증서로부터 시작되어야만 하며, 인증 경로가 검증되기 위해서는 아래 사항들을 만족하여야 한다[1,5].

- 인증 경로의 첫번째 인증서는 신뢰 기관에서 발행해야 한다.
- 인증 경로의 마지막 인증서는 검증 대상의 인증서야 한다.
- 발행자와 소유자의 이름이 체인을 이루어야 한다. 즉, 첫번째 인증서와 마지막 인증서를 제외한 모든 인증서에서는 상위 인증서의 소유자가 다음 순서인 인증서의 발행자이어야 한다.
- 인증 경로의 모든 인증서는 요구되는 시간에 유효하여야 한다.

그러나 위의 조건은 필요 조건일 뿐 인증 경로가 완전히 검증되기 위해서는 기본 제한(basic constraints), 명칭 제한(name constraints), 정책 제한(policy constraints) 등이 고려되어야 한다.

다음은 인증 경로 검증의 절차를 나타낸다.

1. 초기화(Initialization)
2. 인증서 검증(Basic certificate checking)
3. 인증 경로에서의 다음 인증서 준비(Preparation for the next certificate in the sequence)
4. Wrap-up

위 네 단계 중 1, 4 단계는 각 한번씩 만 수행되고 단계 2는 인증 경로의 모든 인증서 마다 수행된다. 단계 3은 대상 인증서인 마지막 인증서를 제외한 모든 인증서에 대해 수행된다[5].

인증서 검증에 관련된 프로토콜로 OCSP와 SCVP가 있다. OCSP는 인증서 검증에 필요한 인증서의 상태정보를 제공하기 위한 프로토콜로써 기존에 사용되고 있는 CRL(Certificate Revocation Lists)의 크기 문제뿐만 아니라 검증 정보에 적시성을 제공할 수 있다[2,3]. 현재 IETF PKIX 워킹그룹에서 버전 2가 draft 상태이며, 실시간 인증서 검증 서비스인 ORS(Online Revocation Status) 뿐만 아니라 인증 경로 구축을 위한 DPD(Delegated Path Discovery), 인증 경로 검증을 위한 DPV(Delegated Path Validation)를 제공하고 있다[3]. OCSP는 CRL을 배포하지 않아도 되므로 CRL이 가지고 있는 한계적인 문제점들을 해결할 수 있다. 하지만 각 응답마다 서명을 해야 하는 부담과 요청이 많아 졌을 경우에 발생하는 OCSP Server의 부담, DOS(Denial of Service) 공격에 대한 취약성은 문제로 지적되고 있다.

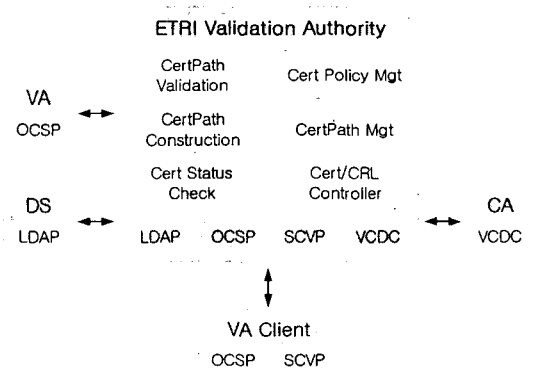
인증 경로 검증 서비스를 제공하기 위한 프로토콜로 IETF PKIX 워킹그룹에 현재 draft 상태인 SCVP가 있다. 검증 서비스를 제공하는 SCVP 서버는 클라이언트가 인증경로 검증을 수행하는데 필요한 정보를 제공하는 untrusted SCVP 서버와 인증 경로 구축에서 검증까지 모든 서비스를 제공하는 trusted SCVP 서버로 구분하고 있다. Trusted SCVP 서버는 클라이언트의 검증에 대한 부담을 줄이고 PKI 검증 정책을 중앙관리 할 수 있도록 되어 있다[4]. 서명에 대한 부담, 요청이 급증할 때 서버의 오버헤드 등의 단점을 가지고 있다.

3. ETRI/VA의 인증서 검증

본 장에서는 클라이언트의 인증서 검증에 대한 부담을 줄이고 통합적인 정책 관리를 위한 ETRI/VA에 대하여 설명하고, ETRI/VA의 인증서 검증 방법에 대하여 기술한다.

3.1 ETRI/VA

ETRI/VA는 클라이언트의 인증서 검증을 대행해 주는 시스템으로, 클라이언트는 인증서 검증에 대하여 VA를 신뢰한다. ETRI/VA는 효율적인 인증서 검증을 위하여 그림 1과 같은 모듈로 이루어져 있다. 모듈은 인증서 검증을 위한 모듈 3개와 인증서 정책 관리 및 인증서 검증의 효율을 높이기 위한 모듈3개로 총 6개로 이루어져 있다.



[그림 1] ETRI/VA

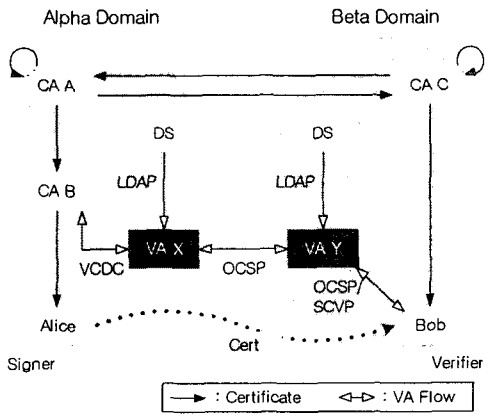
각 모듈은 다음과 같다.

- Certificate Status Check : 인증서의 상태를 검증하는 모듈. 인증서의 상태 정보는 ETRI/VA DB의 인증서 정보, Collaborative VA, CRL을 이용하여 검증한다. 방법의 선택은 ETRI/VA에 등록된 CA 구분에 따른다.
- Certification Path Construction : 인증 경로 생성 모듈. CA의 인증서로 이루어진 인증기관 인증경로(CACertPath)와 요청에 의한 응답으로 생성된 인증경로를 사용하여 인증경로를 생성한다. 클라이언트 요청 시 trust anchor가 선정하지 않는 경우, CA Trust

List(CA Table)를 이용하여 trust anchor를 선정한다.

- Certification Path Validation : 인증 경로 검증 모듈. 인증경로가 주어지면 인증서 정책 정보, 인증서 정책 사상 정보, Cert Status Check 모듈을 이용하여 검증한다.
- Certification Path Management : 인증경로 관리 모듈. 인증 경로 생성 또는 검증이 된 인증 경로를 저장하고 관리한다. 또한, 인증기관 인증경로를 생성 관리한다.
- Certificate Policy Management : 정책의 중앙 관리 모듈. 인증서 정책 정보와 인증서 정책 사상 정보를 관리하며 인증서 검증에 사용된다.
- Certificate/CRL Controller : CA의 인증서 상태 정보와 CRL 정보를 취득하는 모듈. 인증서 상태 검증에 사용된다.

ETRI/VA에서 사용되는 프로토콜은 클라이언트의 요청을 위한 OCSP, SCVP, LDAP, VCDC가 있다. OCSP는 클라이언트로부터 인증서 상태 정보 요청 또는 VA가 타 도메인의 인증서 상태정보를 얻기 위하여 Collaborative VA에게 요청할 때 사용되고, SCVP는 클라이언트가 인증서 검증, 인증경로 생성, 인증경로 검증 등을 요청할 때 사용된다. LDAP은 VA가 인증서의 상태 정보를 얻기 위하여 사용되고, VCDC(VA CA Data Connection)는 실시간의 인증서 상태 정보를 취득하기 위하여 CA의 DB 정보를 얻기 위한 프로토콜이다.



[그림 2] PKI 도메인

그림 2는 두 도메인간에 인증서 검증을 위한 VA의 동작을 표현하고 있다. Beta 도메인의 Bob이 Alpha 도메인의 Alice로부터 받은 인증서를 검증하기 위해서 VA Y에게 요청한다. VA Y는 Alpha 도메인에 속해 있는 Alice의 인증서 상태 정보를 얻기 위하여 VA X에게 OCSP로 상태 검증을 요청한다. VA X는 VCDC로 Alice의 실시간 인증서 상태 정보를 취득하거나 디렉토리 서버로부터 CRL을 취득하여 Alice 인증서의 상태 정보를 얻어서 VA Y에게 응답을 보낸다. VA Y는 인증서의 상태 정보가 유효한 경우, 인증경로를 생성하게 된다. 인증경로는 Bob이 신뢰하는 CA C로부터 Alice까지의 인증경로인 [CA C]→[CA A] →[CA B] →[Alice]를 생성하고 Bob이 요청한 정책에 맞추어 인증경로를 검증한다.

3.2 인증서 검증

3.2.1 Certificate Status Check

ETRI/VA가 인증서의 상태 정보를 얻기 위한 수단으로 CA의 DB 정보, CRL, Collaborative VA 세가지이다. CA의 DB 정보를 얻기 위하여 VA는 VCDC 프로토콜을 사용한다. VCDC는 CA측의 DB가 변경이 되면 VA측의 DB에게 해당 데이터를 전송한다. 전송되는 메시지의 무결성을 보장하기 위하여, CA와 VA는 인증서를 이용하여 세션키를 교환하고 데이터의 전송시 MAC(Message Authentication Codes)을 함께 전송한다. 또한 메시지의 유실을 대비하여 주기적으로 트랜잭션을 관리한다. CRL을 취득하는 방법은 두가지로 나뉜다. VA가 관리하는 DS의 CRL 주기에 맞추어 CRL을 획득하여 VA에 저장해두는 방법과 인증서 검증이 요구될 때 CRL을 획득하는 방법이 있다. Collaborative VA는 VA가 관리하는 도메인을 벗어나는 인증서의 상태정보를 얻기 위하여 해당 도메인의 VA에게 OCSP를 요청하여 정보를 얻는다. 해당 도메인에 VA가 없거나 VA간의 OCSP 전송이 용이하지 않은 경우에는 CRL을 획득한다.

인증서 검증을 위해서는 가장 최근의 정보를 이용하고, 인증서 상태 정보의 취득 방법을 클라이언트에게 제공하기 위하여 OCSP, SCVP의 확장 필드를 사용한다.

3.2.2 Certification Path Construction

ETRI/VA는 클라이언트의 요청에 대한 신속한 응답을 지원하고 효율을 높이기 위해 인증기관 인증서로 이루어진 인증경로를 미리 생성하여 저장한다. 검증서버가 지원하는 도메인이 확장됨에 따라 도메인에 속하는 모든 인증기관의 인증서를 수집하여 지원하는 도메인 내에서 생성될 수 있는 인증기관의 인증서로 생성될 수 있는 모든 인증경로를 생성하고 저장한다. 인증경로를 생성한 후 인증경로 검증 작업을 수행함으로써, 검증대상 인증서와 인증기관 인증경로를 결합하고 인증경로 검증을 수행할 때 성공확률을 높일 수 있다. 또한, 클라이언트의 요청으로 인증서 검증에 사용된 인증경로는 저장을 하여 다른 인증서 검증 요청에 재사용할 수 있도록 구성되어 있어, 인증경로 생성 시간에 소요되는 시간을 효과적으로 줄일 수 있다.

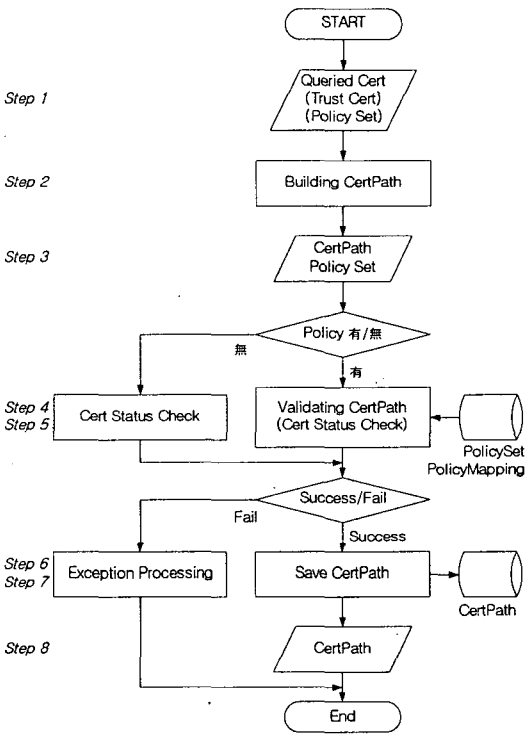
3.2.3 Certification Path Validation

인증경로 검증은 Certification Path Construction 모듈에서 생성된 인증경로를 이용하여 검증을 하게되며, Certificate Status Check 모듈을 이용하여 인증경로 상의 각 인증서 상태 정보를 획득하여 인증경로 검증을 수행한다.

ETRI/VA의 인증경로 검증은 그림 3과 같다.

검증서버가 클라이언트로부터 인증서 검증 요청을 받을 시, 검증서버는 클라이언트로부터 수신한 검증대상 인증서(Queried Cert)와 선택적으로 클라이언트가 신뢰하는 인증서, 인증서 검증에 사용될 인증서 정책을 수신하게 된다(*Step 1*). 검증서버는 Certification Path Construction 모듈을 이용하여 인증경로를 생성한다. 클라이언트의 신뢰 인증서가 제공되는 경우에는 반드시 신뢰 인증서부터 시작되는 인증경로를 생성한다(*Step 2*). 다음 단계의 입력값인 인증경로와 인증서 정책(Step 3). 클라이언트가 인증서 정책을 제공하지 않은 경우는 Certificate Status Check 모듈만으로 인증서 검증을 수행한다(Step 4). 이유는 CertPath Construction 모듈에서 인증경로를 생성 시 정책을 제외한 인증경로 검증 작업을 수행하였기 때문이다. 클라이언트가 인증서 정책을 제공한 경우에는 우선 클라이언트에 허용되는 정책임을 검사하고 타 도메인의

신뢰 인증서부터 시작되는 인증경로인 경우 ETRI/VA에서 관리하는 인증서 정책 사상 정보를 이용하여 타당한 인증서 정책을 선택한 후, IETF에서 제안하는 인증서 검증 방법에 따라 인증경로를 검증한다(step 5). 상기 절차에서 실패한 경우 ETRI/VA는 실패 처리를 수행하고 그 결과에 대한 로그 및 응답을 생성한다(step 6). 상기 절차에서 성공한 경우, 이후 동일한 인증서 검증 요청을 위하여 검증된 인증경로를 저장한다(step 7). 인증경로 검증에 성공한 인증경로(step 8).



[그림 3] 인증경로 검증

3.2.4 Certificate Policy Management

Certificate Policy Management 모듈은 인증기관의 인증서 정책, 클라이언트에게 허용 또는 제한하는 인증서 정책, 타 도메인과 자신의 도메인간의 정책 사상 등을 관리하여 인증경로 검증에 활용된다.

클라이언트는 인증서 검증 요청에 신뢰 인증서와 인증서 정책을 선택적으로 제공할 수 있다. 검증서버는 인증서 정책과 신뢰 인증서의 유무에 따라 아래 명시된 표1과 같이 구분되어 수행된다.

[표 1] 신뢰 인증서와 인증서 정책

	Policy 有	Policy 無
Trust Anchor 有	Case A	Case C
Trust Anchor 無	Case B	Case D

인증서 정책과 신뢰 인증서를 동시에 제공하는 경우(Case A), 우선 검증서버는 인증서 정책이 신뢰 인증서에 속한 도메인의 인증서 정책으로 판단하고 인증서 검증을 수행한다. 정책과 신뢰 인증서가 서로 다른 도메인인 경우에는 정책 사상 정보를 이용하여 신뢰 인증서부터 시작되는 인증경로에 해당하는 인증서 정책으로 변경한 후 인증서 검증을 수행한다. 인증서 정책은 제공되고 신뢰 인증서는 제공되지 않는 경우(Case B), 우선 검증서버는 인증서 정책이 클라이언트의 도메인에 포함되는 정책인지를 찾는다. 클라이언트의 도메인에 포함되는 정책인 경우에는 검증서버의 신뢰 인증서 리스트(Trust Certificate List)로부터 클라이언트의 도메인에 해당하는 신뢰 인증서를 선택한 후 인증경로를 생성하여 인증경로 검증을 수행한다. 클라이언트의 도메인에 포함되지 않는 정책인 경우에는 정책에 해당 도메인을 찾은 후 신뢰 인증서 리스트로부터 해당 도메인의 신뢰 인증서를 선택한 후 인증경로를 생성하여 인증경로 검증을 수행한다. 인증서 정책이 제공되지 않는 경우(Case C, D)는 제공 받은 신뢰 인증서 또는 검증서버가 관리하는 신뢰 인증서 리스트로부터 인증경로를 생성하여 인증서 검증을 수행한다.

4. 결론

본 논문은 인증서 검증서버인 ETRI/VA의 각 모듈의 기능을 설명하였고 ETRI/VA의 인증서 검증 방법을 기술하였다. 클라이언트의 요청을 효율적으로 처리하기 위한 인증서 상태 검증, 인증경로 생성, 인증경로 검증 및 인증서 정책 관리 방법을 설명하였다.

ETRI/VA는 인증서의 상태 검증의 적시성을 제공하고 인증 경로 생성 및 검증에 대한 클라이언트의 부담을 줄이며, PKI 상호연동을 지원하고 도메인간의 인증서 정책을 중앙집중 관리함으로써, 다양한 신뢰 모델에 대해서 독립적으로 인증 경로 검증을 제공하므로 향후 국제 PKI 연동에도 활용될 수 있다.

참고문헌

[1] R. Housley, W. Ford, W. Polk and D. Solo, " Internet X.509 Public Key Infrastructure, Certificate and CRL Profile," RFC 2459, January 1999.

[2] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, " X.509 Internet Public Key Infrastructure Online Certificate Status Protocol □ OCSP," RFC 2560, June 1999.

[3] M. Myers, R. Ankney, C. Adams, S. Farrell and C. Covey, " Online Certificate Status Protocol, version 2," draft-ietf-pkix-ocspv2-02, March 2001.

[4] A. Malpani, P. Hoffman and R. Housley, " Simple Certificate Validation Protocol (SCVP)," draft-ietf,-pkix-scvp-09, June 2000.

[5] R. Housley and T. Polk, *Planning for PKI*, John Wiley & Sons, 2001.

[6] Y. Elley, A. Anderson, S. Hanna, S. Mullan, R. Perlman, and S. Proctor, "Building Certification Paths: Forward vs. Reverse," *Network and Distributed System Security Symposium Conference Proceedings*, 2001.

[7] R. Perlman, " An overview of PKI trust models," *IEEE Network* , Vol 13, No 6 , Nov 1999.

[8] M. Naor and K. Nissim, " Certificate Revocation and Certificate Update," *IEEE Journal on Selected Areas in Communications*, Vol 18, No 4, April, 2000..