Journal of Digital Contents Society Vol. 5. No. 2. June. 2004(pp.157~162)

CC 기반의 보안환경 컨텐츠 리파지토리 모델

최상수*, 방영환*, 이강수*

요 약

CC 환경에서는 PP와 ST의 개발이 필수적이며, CCRA 가입을 앞둔 국내에서는 향후 PP/ST의 수요가 폭발적으로 증가할 것으로 예상된다. 특히, PP/ST 개발 경험이 부족한 국내 실정상 보안환경(가정, 위협, 정책) 및 보안목적 컨텐츠를 공개된 작성가이드 문서만을 참조하여 개발한다는 것은 매우 어렵다. 따라서, 본 논문에서는 공통 보안환경 및 보안목적 컨텐츠를 웹서비스 기반의 리파지토리로 구축하여 개발자들이 PP/ST 작성을 간편하게 수행할 수 있도록 하는 모델을 제시한다. 제시한 모델을 통해 개발 경험이 부족한 개발자들도 간편하게 PP/ST 개발을 수행할 수 있을 것으로 기대된다.

A Repository Model of Security Environment Contents based on CC

Sang-Soo Choi*, Young-Hwan Bang*, Gang-Soo Lee**

ABSTRACT

A development of PP/ST is essential in CC environment. And, the KOREA is expected that PP/ST's demand increases explosively by joining to CCRA hereafter. Specially, PP/ST development experience of the KOREA is lacking. So, development of security environment(assume, threat, policy) and security objective contents refer only PP/ST Guide(ISO/IEC PDTR 15446) are very difficult. In this paper, we propose a web service based common security environment and security objective repository model that make developers can run PP/ST creation to be simple. Through proposed model, developers who development experience is lacking are expected to achieve PP/ST development to be simple.

Key words : Common Criteria, Security Environment Contents, Repository Model

1. 서 론

정보화사회에서 보안 및 프라이버시 문제와 같은 정보화의 역기능문제는 필연적이며, 정보보호기술은 정보화의 역기능을 예방, 방지, 발견 및 복구하기 위한 종합기술이다. 특히, 정보보호시스템 평가·인증 체계는 정보화의 역기능문제를 다소 해결하며 정보보호시스템의 품질(특히, 보안성)을 평가하고 공인하는 것이다. 미국의 TCSEC과 FC, 유럽연합의 ITSEC, 캐나다의 CTCPEC은 자국내 정보보호시스템을 위한 평가기준이며 이들이 통합된 국제기준은 CC(common criteria, ISO/IEC 15408)이다[1~4].

CC 환경에서는 제품유형별 공통 보안요구사항명세서에 해당하는 PP(protection profile)들이 요구되며, 개발자(또는 평가신청자)는 대응되는 PP들을 참조하여 TOE(target of evaluation, 평가대상물) 및 ST(security target)를 준비한다. 특히, ST는 특정한 보안제품(즉, TOE)에 대한 보안요구사항명세서라 할 수 있다. 외국의 경우 이미 43종의 PP(2004년 7월 기준)들이 개발되어 평가 및 인증된 상황이며, 이를 토대로 다수의 보안제품들에 대한 개발 및 평가가 진행중에 있다[5].

국내의 경우, CC Version 2.1을 번역하여 정보통신부고시 2002-40호(2002년 8월)로 공표하여 KISA(평가기관)와 국가정보원(인증기관)을 중심으로 운영하고 있다. 특히, CCRA(CC 상호인증협정) 가입을 앞둔 상황에서 PP/ST의 수요가 폭발적으로 증가할 것으로 예상되며, 2004년 7월 현재 국가용 PP 7종이 개발되어 공개된 상황이다[6].

PP/ST 작성을 위해서는 보안환경(가정, 위협, 정책), 보안목적 및 보안기능/보안보증요구사항 등의 컨텐츠가 요구된다. 보안기능/보안보증요구사항 컨텐츠는 CC 내에 명시되어 있지만, 보안환경 및 보안목적 컨텐츠에

※ 제일저자(First Author) : 최상수, 주소 : 대전광역 시 대덕구 오정동 133 한남대학교 대학원 컴퓨터공학과,
접수일 : 2004년 4월 28일, 완료일 : 2004년 6월 23일

대해서는 작성 가이드만을 제시하고 있는 실정이어서 실무 경험이 부족한 국내 실정상 외국의 공개된 PP들을 번역하여 사용하고 있는 실정이다. 또한, PP/ST 개발자들이 특정 개발도구나 가이드 문서만을 참조하여 PP/ST의 보안환경 및 보안목적 컨텐츠를 작성하는 것은 매우 복잡하고 어려운 일이며, 이들 사이의 관계를 맺어주는 것 또한 힘들다.

따라서, 본 논문에서는 PP/ST 개발자들이 손쉽게 검색해서 사용할 수 있도록 공통 보안환경 컨텐츠를 구축하고, 다양한 개발도구와의 연결이 용이하도록 하는 "CC 기반의 보안환경 컨텐츠 리파지토리 모델"을 제시한다. 체계적으로 구축 및 관리되는 리파지토리를 통하여 개발자들에게 서비스되고 이를 이용해 PP/ST 개발도구 및 PP/ST 작성에 서비스됨으로써 가용성과 효과성을 극대화시킬 수 있을 것이다.

본 논문의 2장에서는 CC의 기본개념, PP/ST의 구성요소(즉, 컨텐츠) 및 웹서비스 개념 등의 관련연구를 다룬다. 3장에서는 제안하는 웹서비스 기반의 CC 기반 보안환경 컨텐츠 리파지토리를 설계하고 활용방안을 제시하며, 4장에서 결론을 맺는다.

2. 관련연구

2.1 CC의 기본 개념

CC는 그림 1과 같이 모든 정보보호시스템에서 필요로 하는 보안기능요구사항의 전체집합을 클래스-패밀리-컴포넌트-엘리먼트를 통해 계층적으로 분류되어있다. 또한, 보안기능에 대하여 구현의 정확성에 대한 보증요구사항의 전체집합을 계층적으로 분류하였고 7단계의 보증수준별로 요구하는 보증요구사항(컴포넌트)을 정의하고 있다. 상위의 보증수준은 하위의 보안수준보다 완전하고 엄격하며 정형적이므로, 보증수준간에는 완전성, 엄격성 및 정형성 관계를 갖는다[2,3].

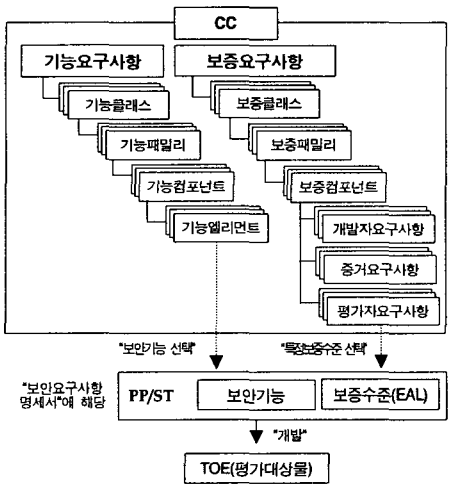


그림 1. CC의 구성과 사용의 개념

정보보호시스템(TOE)의 제품유형에 따라 CC 보안기능요구사항의 일부를 선택하고 7수준의 보안수준 중 하나를 택하여 PP 또는 ST를 구성한다.

PP는 제품유형별 공통보안요구사항명세서이며 특정한 제품유형의 운영에 대한 보안환경(가정, 보안정책, 위협문장을 포함), 보안목적, 보안요구사항(보안기능/보안보증 요구사항)으로 구성된다. 보안요구사항에서의 보안기능은 CC의 보안기능 요구사항집합의 부분집합이며, 보안보증은 보안보증 요구사항집합의 부분집합이다. 일반적으로 PP는 사용자(PP 개발자)가 원하는 요구사항을 포함하여 개발하며 별도의 PP평가와 인증이 요구된다.

ST는 특정한 정보보호제품(즉, 평가대상물, TOE)의 보안요구사항명세서이다. 해당 제품유형의 PP가 존재할 경우, 기존의 PP에 개발환경을 부가하여 사용할 수 있으며 이 경우 "PP준수선언"이 필요하다. ST는 TOE의 보안요구사항명세서에 해당하므로, ST도 TOE와 함께 평가 및 인증한다.

2.2 PP/ST 구성요소

PP/ST는 각각 CC의 부록 B와 부록 C에 서술된 구성 요구사항을 따라야 하며, 사용자가 쉽게 이용할 수 없는 기타 자료의 참조를 최소화하도록 사용자 중심의 문서로 표현되어야 한다. CC에서 제시하는 PP의 구성요소는 그림 2와 같다.

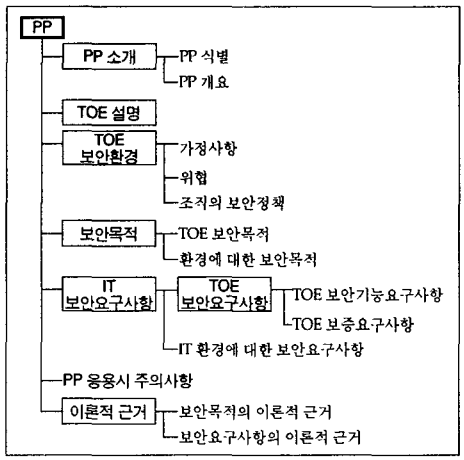


그림 2. PP의 구성요소(컨텐츠)

ST의 경우 PP의 구성요소에 "TOE 요약명세"와 "PP 수용" 및 이론적 근거에 서술이 추가된 형태이다.

2.3 웹서비스

웹서비스는 발행이 가능하고 웹이나 로컬 네트워크 상의 어떤 곳에도 위치할 수 있으며, 호출될 수 있는 자기 기술적이며 모듈화된 분산 컴퓨팅 기술이다[7]. XML 웹 서비스의 공급자와 사용자는 XML 웹 서비스를 작성하는 데 사용된 운영체제나 언어 환경 또는 컴

포넌트 모델에 관해서는 신경쓰지 않아도 되는 플랫폼 독립적인 기술이다. 이는 웹서비스가 XML, HTTP, SMTP와 같은 개방 인터넷 표준을 기반으로 하기 때문이다. 웹 서비스의 일반적인 구조는 그림 3과 같다.을 보여주고 있으며 웹 서비스의 핵심 기술에 대한 설명은 아래와 같다[6].

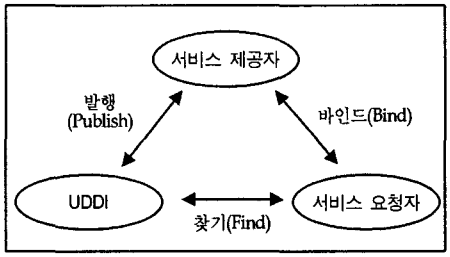


그림 3. 웹서비스의 구조

웹 서비스의 핵심 기술은 SOAP(simple object access protocol), WSDL(web service description language), UDDI(universal description, discovery and integration)으로 구성된다[8~10].

3. CC 기반의 보안환경 컨텐츠 리파지토리 모델

본 장에서는 본 연구팀의 기존 연구결과인 CC의 PP/ST 작성을 위한 공통 보안환경 및 보안목적 컨텐츠를 웹서비스 환경에서 쉽게 검색하고 이용할 수 있도록 하는 "CC 기반의 보안환경 컨텐츠 리파지토리 모델"을 제시하고, 그 활용방안을 모색한다.

3.1 CC 기반의 공통 보안환경 및 보안목적 컨텐츠

CC 환경에서 PP/ST 작성을 위해서는 그림 2와 같이 다양한 컨텐츠들을 작성해야만 한다. 특히, PP/ST의 구성요소 중에서 보안요구사항(보안기능/보안보증) 컨텐츠는 CC에서 제시하는 컨텐츠들을 그대로 이용할 수 있지만, 이들을 도출해내기 위한 보안환경(가정, 위협, 정책) 및 보안목적 컨텐츠의 경우에는 PP/ST 작성자가 직접 작성해야만 한다. 그러나, 아직 CC 환경에 익숙하지 않은 국내 실정상 PP/ST 작성가이드만을 참조하여 필요한 컨텐츠를 작성한다는 것은 상당히 어려운 문제이다. 이러한 문제점을 해결하기 위하여 본 연구팀은 이미 CC 환경의 보안환경 및 보안목적 컨텐츠를 위한 공통 컨텐츠 목록 도출방법을 제안한 바 있다[11~13].

즉, 공개된 PP들과 CC-ToolBox/PKB[14,15] 내의 보안환경 및 보안목적문장 컨텐츠들을 분석하여, 항목 사이의 일관성을 제고하고 모순없는 일정수준의 보안환경 및 보안목적 문장인 공통 보안환경 및 보안목적 컨텐츠 목록을 도출하였다. 특히, 71종의 공통 가정, 115종의 공통 위협, 30종의 공통 정책 및 163종의 공통 목적 컨텐츠 목록을 생성하였다. 여기서, "공통"이라는 의미는 일반화된 문장을 의미한다.

그러나, 기 연구결과에서는 도출된 보안환경 및 보안목적 컨텐츠 목록만을 제공할 뿐이며, 실제 PP/ST 작성을 위한 웹서비스 기반의 리파지토리와 PP/ST 개발 지원도구가 필요하다.

3.2 리파지토리 모델의 구조

CC 기반의 보안환경 컨텐츠 리파지토리 모델의 구성요소는 보안환경 컨텐츠 목록 서비스를 제공하는 컨텐츠 리파지토리 부분과 서비스를 검색하여 찾을 수 있는 UDDI, 마지막으로 서비스 수요자라 할 수 있는 PP/ST 개발 지원도구로 구성되어 있다. 특히, UDDI는 서비스 검색을 위한 일반적이고 공통된 기능을 수행하므로, 본 논문에서는 서비스 공급자인 보안환경 컨텐츠 리파지토리와 서비스 수요자인 PP/ST 개발 지원도구의 모델에

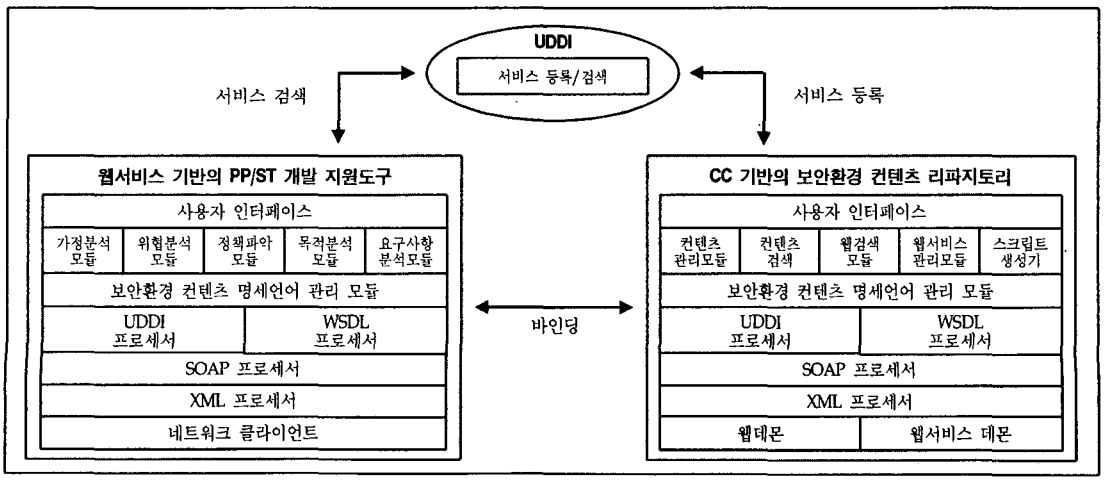


그림 4. CC 기반의 보안환경 컨텐츠 리파지토리 모델

```
<!DOCTYPE CommonAssumeList [
  <!ELEMENT CommonAssumeList (AssumeContents*)>
  <!ELEMENT AssumeContents (assumeInfo, relatedThreat, comment)>
      <!ATTLIST assumeId CDATA #REQUIRED>
  <!ELEMENT assumeInfo (assumeId, assumeClass, assumeFamily, assumeComponent)>
  <!ELEMENT assumeId (#PCDATA)>
  <!ELEMENT assumeClass (#PCDATA)>
  <!ELEMENT assumeFamily (#PCDATA)>
  <!ELEMENT assumeComponent (#PCDATA)>
  <!ELEMENT relatedThreat (#PCDATA)>
      <!ATTLIST threatId CDATA #REQUIRED>
  <!ELEMENT comment (#PCDATA)>
]>
```

그림 5. 가정 컨텐츠 명세 언어

대해서만 다룬다. 그림 4는 이들 구성요소들의 전체 구조를 보인다.

3.3 CC 기반의 보안환경 컨텐츠 리파지토리

보안환경 리파지토리는 3.1절에서 설명한 것처럼 본 연구팀의 기 연구결과인 공통 보안환경 및 보안목적 컨텐츠 목록에 웹서비스 모듈을 매핑하여 쉽게 구축할 수 있다. 그 구성은 크게 웹 검색부분, 보안환경 컨텐츠 DB 관리 부분, 웹서비스 모듈의 3부분으로 구성된다. 각 모듈별 주요 기능은 다음과 같다.

- 웹 검색 기능 : PP/ST 작성을 위한 참고자료로써 보안환경 컨텐츠 리파지토리 내의 컨텐츠들을 웹을 통해 검색할 수 있는 기능
- 서비스 등록 기능 : UDDI에 접속하여 자신의 서비스 정보를 등록
- 데이터베이스 관리 기능 : 지식-기반 형태로 신규 공통 컨텐츠가 추가로 요구될 시에 DB를 갱신하고 관리하는 기능

3.4 보안환경 컨텐츠 명세 언어

CC 기반의 보안환경 컨텐츠 리파지토리를 웹서비스 기반으로 구축하기 위해서는 PP/ST 작성을 위한 보안환경 및 보안목적 컨텐츠를 표현하는 표준화된 명세 방법이 필요하다. 따라서, 본 논문에서를 XML의 DTD를 이용하여 CC의 보안환경 및 보안목적 컨텐츠를 명세하였다. 그림 5는 공통 가정 컨텐츠에 대한 DTD를 보인다.

3.5 서비스 시나리오

본 논문에서 제시한 리파지토리 모델을 웹서비스 기반의 PP/ST 개발 지원도구와 연동하여 사용한다고 가정하면 시나리오는 그림 6과 같으며, 상세한 설명은 다음과 같다.

① 보안환경 컨텐츠 리파지토리는 UDDI에 서비스를 등록한다.
② PP/ST 개발 지원도구(또는, CC 환경에서 컨텐츠를 이용하는 모든 작업 및 도구)는 UDDI에 접속하여 서비스를 검색한다.
③ 등록된 서비스 명세에 따라 보안환경 컨텐츠 리파지토리와 바인딩한다.
④ PP/ST 개발 지원도구는 리파지토리에 보안환경 및 보안목적 컨텐츠에 대한 질의를 수행한다.
⑤, ⑥ 질의결과를 이용하여 PP/ST를 작성한다.

한번 바인딩된 서비스는 다음부터 자동으로 연결하여 보안환경 및 보안목적 컨텐츠를 갱신하고 데이터베이스를 관리할 수 있다.

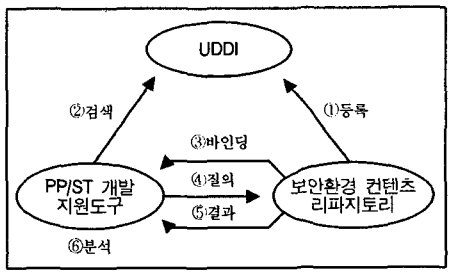


그림 6. 서비스 시나리오

3.6 웹서비스 기반의 PP/ST 개발 지원도구

본 논문에서 제시한 CC 기반의 보안환경 컨텐츠 리파지토리 모델은 CC 환경의 다양한 분야에서 응용이 가능하다. 특히, 본 논문에서는 웹서비스 기반의 PP/ST 개발 지원도구와의 연동을 가정으로 한다. 본 연구팀은 국내 실정에 적합하도록 PP/ST 개발 지원도구를 개발한 바 있으며, 본 절에서 제시하는 사례는 기존에 개발된 도구에 웹서비스 모듈을 추가한 것이다.

웹서비스 기반의 PP/ST 개발 지원도구의 구조는 크게 보안환경 분석 부분, 보안요구사항 분석 부분, 웹서비스 모듈 등의 3부분으로 구성되며, 도구에서 제공하는 주요 기능은 표 1에서 보인다. 또한, 도구의 주요 화면은 그림 7과 같다.

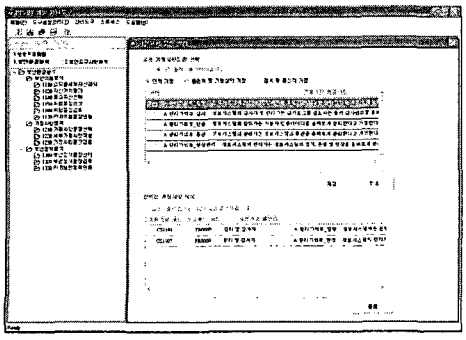
표 1. PP/ST 개발 지원도구의 주요 기능

기능클래스	세부기능명	기능설명
보안환경 분석	자산파악	위협 분석을 위한 자산파악 기능
	위협문장 생성	자산별 위협문장 생성 기능
	PKB 위협문장 연동	생성된 위협문장에 대한 유사 PKB 위협문장 연동 기능
	가정문장 선택	공통가정목록 중에서 조직을 위한 가정문장 선택 기능
	보안정책 선택	공통정책목록 중에서 조직을 위한 정책문장 선택 기능
	PKB 정책문장 연동	선택된 정책문장에 대한 유사 PKB 정책문장 연동 기능
보안요구사항 분석	PKB 보안목적 도출	선택된 위협 및 정책을 통해 관련 보안목적문장 도출 기능
	보안기능 선정	도출된 보안목적별 구현가능한 보안기능 선택 기능
	보안강도/보증수준 분석	보안강도(SOF) 및 보증수준(EAL) 분석 기능
PP/ST 작성	PP/ST 생성	보안요구사항명세서 생성 기능
관리도구	프로젝트 관리	개발 프로젝트 생성 및 열기 기능
	역할기반 접근통제	도구에 대한 역할기반접근통제 기능

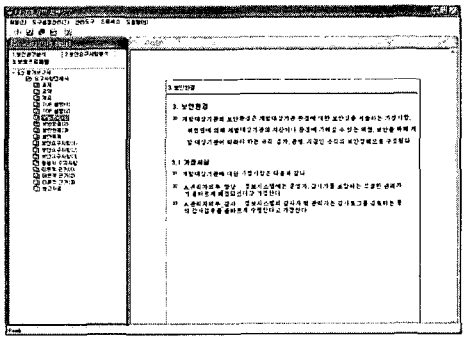
4. 결 론

본 논문에서는 PP/ST 개발 지원도구와의 연동을 위한 웹서비스 기반의 보안환경 컨텐츠 리파지토리 모델을 제시하였다. 특히, CC 환경의 공통 보안환경 및 보안목적 컨텐츠를 웹서비스 환경에서 쉽고 간편하게 검색 및 사용함으로써 CC 평가·인증 체계에서 개발자들이 간편하게 PP/ST를 작성하거나 검토할 수 있도록 하였다. 또한, 웹서비스를 이용함으로써 서비스 수요자(PP/ST 개발 지원도구 등)는 자동화된 관리를 통해 오버헤드를 줄일 수 있도록 하였다. 제시한 리파지토리 모델을 통해 CC 환경의 PP/ST 개발의 폭발적인 증가에 따른 개발경험의 부족과 필요한 컨텐츠의 개발 및 작성 문제에 유연하게 대처할 수 있을 것으로 기대된다.

그러나, 실제 PP/ST 개발시에 개발자가 직접 작성 가이드를 참조하여 생성한 문장을 리파지토리에서 제공하는 컨텐츠와 매핑시키고자 할 경우 가장 적절한 컨텐츠 항목을 찾아서 연동해주는 기능이 요구되며, 이에 대한 연구 및 개발을 향후 연구과제로 남긴다.



(a) 가정문장 선택 화면



(b) PP 작성 화면

그림 7. 도구의 주요 화면

참 고 문 헌

[1] "정보보호시스템 평가·인증 가이드", 한국정보보호진흥원, 2002. 12.

[2] CC, Common Criteria for Information Technology Security Evaluation, Version 2.1, CCIMB-99-031, August 1999. http://www.commincriteria.org/site_index.html.

[3] CC, Commin Evaluation Methodology, Version 1.0, CEM-99/045, August 1999, http://www.commoncriteria.org/site_index.html.

[4] http://www.commincriteria.org/docs/pdf/ccpart1V21 .PDF

[5] List of PPs, http://www.commoncriteriaportal.org/public/developer/index.php?menu=7.

[6] 보호프로파일 등재현황, 국가사이버안전센터, http://www.ncsc.go.kr/.

[7] 웹서비스 아키텍처, http://www.w3c.org/TR/ws-arch/.

[8] SOAP 1.2, http://www.w3c.org/TR/soap12-part1/.

[9] WSDL 1.2l, http://www.w3c.org/TR/wsdl12/.

[10] UDDI, http://oasis-open.org/commitees/uddi-spec.

[11] 고정호, 이강수, "PP의 보안환경을 위한 가정문장 생성 방법," 한국인터넷정보학회 논문지, 5권 2호, pp.17-31, 2004년 4월.

[12] 고정호, 이강수, "PP의 보안환경을 위한 위협문장 생성 방법," 한국전자거래학회지, 8권 3호, pp.69-86, 2003년 8월.
[13] 고정호, 이강수, "PP의 개발을 위한 보안정책문장 생성 방법," 한국정보보호학회 논문지, 13권 4호, 2003년 8월.
[14] NIAP, CC ToolBox Reference Manual, Version 6.0f, http://niap.nist.gov/tools/cctool.html, 2000.
[15] NIAP, List of Threat, Attack, Policy, Assumption, and Environment Statement Attribute, CC Profiling Knowledge base Report, 2002, http://niap.nist.gov/tools/CCTB60f-Documentation /CC_pkb/Reports/Index.htm.

최 상 수

2001년 한남대학교 컴퓨터공학과 졸업(학사)
2003년 한남대학교 대학원 컴퓨터 공학과 졸업(석사)
2003년~현재 한남대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 소프트웨어공학, 웹공학, 보안공학, 실시간 시스템 모델링 및 분석

방 영 환

1997년 한남대학교 컴퓨터공학과 졸업(학사)
2002년 대전대학교 대학원 컴퓨터공학과 졸업(석사)
2002년~현재 : 대전보건대학 컴퓨터정보처리과 프로그래밍 전문강사
2002년~현재 : 한남대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 소프트웨어 품질 평가 및 보증, 소프트웨어 표준화, 보안공학, 위험분석 및 정보시스템 위험관리

방 영 환

1981년 홍익대학교 컴퓨터공학과 졸업(학사)
1983년 서울대학교 대학원 전산학과 졸업(이학석사)
1989년 서울대학교 대학원 전산학과 졸업(이학박사)
1985~1987년 국립대전산업대학교 전자계산학과 전임강사
1992~1993년 미국일리노이대학교 객원교수
1995년 한국전자통신연구원 초빙연구원
1998~1999년 한남대학교 멀티미디어학부장
1987~현재 한남대학교 컴퓨터공학과 정교수
관심분야 : 소프트웨어공학, 병행시스템 모델링 및 분석, 정보보호시스템 평가, 멀티미디어교육 커리큘럼