정 보 보 호 학 회 지
제25권 제1호, 2015. 2

시큐어 소프트웨어 개발을 위한 위협 모델링 기법의 기술 동향

이 진 호*, 이 혁*, 강 인 혜**

요 약

소프트웨어의 보안속성이 중요해짐에 따라 소프트웨어의 개발 단계에서 설계상의 보안약점이나 구현 단계에서의 보안 약점을 제거하는 작업이 강조되고 있다. 시큐어 소프트웨어를 개발하기 위해 제안된 마이크로소프트사의 위협 모델링 기법은 마이크로소프트사가 자체적으로 개발한 시큐리티 소프트웨어 개발 생명 주기(MS SDL, Security Software Development Lifecycle) 전반에 걸쳐 하나의 방법론으로 적용되고 있으며, 다른 유사한 위협 모델 기법들도 연구되고 있다.

본 논문에서는 위협 모델링 기법들에 대해 살펴보고, MS 위협 모델링 기법을 기반으로 인터넷 웹사이트 개발에 적용하여 MS 위협 모델링 기법의 분석 결과를 살펴본다.

Ⅰ. 서 론

기존의 응용소프트웨어로부터 클라우드 환경이나 사물인터넷 환경의 온라인 소프트웨어에 이르기까지 소프트웨어의 종류와 동작 환경이 다양해짐에 따라, 소프트웨어의 보안 속성이 강조되고 있다. 소프트웨어 보증(assurance)을 위한 여러 가지 소프트웨어 개발 원칙들이 제시되었고, 소프트웨어 개발 생명주기 단계 전반에 걸쳐 적용되는 보안 활동들이 연구되었다. 특히 소프트웨어의 개발생명주기 중에서 설계단계에서 보안약점을 제거할 수 있는 위협 모델링 기법을 적용하고, 구현단계에서 시큐어 코딩 규칙을 사용하는 정적 분석을 수행하여 코드의 보안약점을 제거하는 작업 등이 효과적인 시큐어 소프트웨어 개발 방법론으로 소개되고 있다[1].

공격 분석을 위해 6가지 공격 유형(STRIDE)를 사용하는 위협 모델링 기법과 도구가 마이크로소프트사에 의해 2004년에 제안되었다[2]. 마이크로소프트사에서는 시큐어 소프트웨어 개발 생명주기(SDL)에 사용되는 하나의 개발 방법론으로 통합되어 사용하고 있으며, 위협 모델링 기법의 결과로 얻은 보안 요구사항이 보안 테스팅 단계에서 활용된다[3].

위협 모델링 기법은 시큐어 소프트웨어 시스템을 개발하기 위한 방법론으로서 개발생명주기 상 주로 설계 단계에서 수행되는 일련의 프로세스 방법론이다: 개발 대상 소프트웨어 시스템의 개념적 모델인 데이터 흐름 모델에 대해 발생 가능한 공격들을 파악하고 공격의 발생 경로를 분석하여 공격이 발생하지 않도록 공격에 대한 방어책을 보안 요구사항으로 만들어 설계에 반영하도록 하고 이를 다시 검증하는 작업을 반복한다[4].

위협 모델링의 목적은 소프트웨어 개발 생명주기 상에서 앞부분에 해당하는 설계단계에서부터 공격에 악용될 수 있는 논리적인 약점을 미리 제거함으로써 보안적 측면을 강화하는 것이다. 위협 모델링 기법의 특징은 단순히 소프트웨어 관점만이 아니라 공격자와 보안 관점에서의 목적과 요구사항을 설계에 반영한다는 점이다. 공격의 유형과 적용 분야에 따라 여러 가지 위협 모델링 기법들이 제시되었다[5].

본 논문에서는 위협 모델링 기법을 설명하고, 인터넷 웹 서비스에 대한 적용사례를 통해 분석 결과를 살펴본다.

이 논문은 2014년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것입니다(2012R1A1A2009354)

* 고려대학교 컴퓨터학과 ({jhlee,hlee}@formal.korea.ac.kr)
** 서울시립대학교 기계정보공학과 (inhye@uos.ac.kr)

Ⅱ. 관련 연구

본 논문에서는 마이크로소프트사의 위협 모델링 기법을 중심으로 위협 모델링을 설명한다.

2.1. MS 위협 모델링

마이크로소프트사의 위협 모델링 기법은 여러 가지 도구와 방법을 사용한다[4]: 데이터 흐름도(DFD, dataflow diagram)을 사용하여 개발 대상 소프트웨어 시스템을 기술하고, 대상 시스템에 대한 공격을 파악하기 위해 6가지 공격 유형인 STRIDE 분류를 사용하고, 공격 위협의 리스크를 결정하기 위해 DREAD 방식을 사용한다. MS 위협 모델링 기법은 개발 대상 시스템에 대한 배경 정보를 수집하고, 보안 적용 범위를 결정하고, 시스템의 구성요소에 대해 세부적으로 기술하고, 각 구성요소에 대한 공격 위협들을 분석하고, 공격 위협을 방지하는 5가지 작업으로 이루어진다. 세부적으로 대략 9단계의 절차로 구분할 수 있다. 세부적인 절차를 살펴보면 [표 1]과 같다:

1단계에서 개발 대상 소프트웨어 시스템의 사용 시나리오를 작성하고, 주요 기능들을 결정한다.

2단계에서 개발 대상 소프트웨어가 의존하게 되는 외부 요소-예를 들어 동작하기 위한 운영체제 혹은 데이터베이스 서버-들을 기술하게 된다.

3단계에서는 보안 사항 중에서 개발 소프트웨어 시스템 내부와 관련된 가정 사항들을 모두 나열한다(ex. 인터넷 연결 시 파이어 월 설치 유무).

4단계에서 개발 소프트웨어 시스템 외부와 관련된 보안 가정 사항들을 모두 기술한다. (ex.인터넷에 연결되는 경우 혹은 DB서버가 외부에서 접근되는 경우에 필요한 포트 할당 등).

5단계에서 개발 대상 소프트웨어 시스템의 DFD를 작성하기 위해, 시스템의 구성 요소들을 분할하고 구조를 작성한다. DFD는 5가지 요소를 사용하여 시스템을 기술하며, 시스템의 프로세스를 계층적으로 표현할 수 있다: 직사각형은 고객사용자와 같은 시스템의 외부 개체를 나타내고, 타원은 시스템 내부에 있는 프로세스(프로그램이나 기능 단위)를 표시하고, 데이터 저장소는 데이터나 파일등을 나타내고, 데이터 흐름은 프로세스, 외부개체, 데이터 저장소 사이의 데이터 교환을 표시하며, 점선은 신뢰 경계선을 나타낸다.

6단계에서 STRIDE 분류를 사용하여 각각의 공격 위협들을 나열한다.

STRIDE는 6가지 공격 유형의 첫머리글자이다: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege. spoofing은 공격자가 타인인 척 위장하는 공격이고, tampering은 공격자가 전송중이거나 저장된 데이터를 변조하는 공격이고, repudiation은 공격자가 수행 주체가 누구인지 추적이 불가능한 악의적 행위들을 수행하는 공격이고, information disclosure는 공격자가 전송중이거나 저장된 데이터를 획득하는 공격이고, denial of service는 공격자가 정상적인 시스템 기능이 수행되지 않도록 방해하는 공격이고, elevation of privilege는 공격자가 부정한 수단을 사용하여 상위 신뢰 수준의 사용자 권한을 획득하여 상위 신뢰 수준의 행위들을 수행하는 공격을 나타낸다.

7단계에서 DFD의 각 요소와 공격 위협들을 대응시켜서, 시스템에 대해 가해질 수 있는 공격 위협들을 파악한다.

8단계에서 DREAD방식을 사용하여 각 공격 위협마다 리스크 수준 값을 할당하여 공격위협들 중에서 우선순위를 결정한다.

DREAD방식은 소프트웨어의 5가지 취약성에 대해 3 혹은 4 단계의 만족도 점수를 할당한다: Damage potential, Reproducibility, Exploitability, Affected users, Discoverability. damage potential은 만약 보안 약점이 악용되어 피해가 발생했을 경우 피해의 정도를 점수화하는 것이고, reproducibility는 보안약점이 악용되는 공격을 재현할 수 있는 난이도의 수준을 점수화하는 것이고, exploitability는 보안약점을 실제 공격으로

〔표 1〕 MS 위협 모델링 절차

1단계	사용자 시나리오의 정의
2단계	외부 의존성 수집
3단계	보안 가정사항 수집
4단계	외부 보안 요소 고려
5단계	대상 응용 프로그램의 DFD 생성
6단계	위협 유형의 결정
7단계	시스템에 대한 위협의 파악
8단계	리스크 계산
9단계	공격 보안대책 수립과 반영

활용하기까지 요구되는 시간과 노력의 정도 수준을 점수화하는 것이고, affected users는 만약 보안약점이 공격당했을 경우 예상되는 피해 사용자 수의 비율을 수치화한 것이고, discoverability는 보안약점이 발견될 수 있는 난이도의 수준을 점수화한 것이다.

9단계에서 우선순위의 공격위협에 대한 보안 경감책을 위협 트리를 사용하여 수립하고, 앞선 이전 개발 단계에 다시 반영한다. 위협 트리(threat tree)는 루트 노드가 최종 공격 목표가 되고 하위 노드들은 상위 노드의 공격을 달성하기 위해 필요한 전제 조건이 된다. 형제 노드 사이의 관계는 AND와 OR 2가지로 표현될 수 있다. 위협 트리의 맨 아래 리프 노드는 더 이상 분해할 수 없는 기본 조건이나 기술을 표현한다. 위협 트리의 리프 노드에서 루트 노드에 이르는 하나의 경로는 공격 가능한 경로를 나타내는 것으로, 보안 방지책은 리프 노드로부터의 경로를 차단하는 방법에 초점을 맞춘다.

2.2. 위협 모델링 연구 동향

OWASP에서는 주로 웹 응용프로그램 설계를 목적으로 위협 리스크 모델링 기법을 제안하였다[6]. 미국 소프트웨어 공학연구소 CERT에서는 조직 차원의 정보보호를 위한 위험 관리 목적의 OCTAVE 기법을 제안하였다[7]. 미국 국토보안부에서는 소프트웨어 시스템 개발을 위한 공통 취약점 점수 체계(CVSS, common vulnerability scoring system)을 개발하여 소프트웨어의 취약점들에 대한 이해와 위협에 대한 평가를 가능하게 하였다[8]. Trike는 오픈 소스 위협 모델링 방법론과 도구이며 마이크로 소프트사와는 달리 리스크 중심의 위협 모델을 사용한다[9]. 소프트웨어 개발보다는 조직 차원의 위험 관리를 위한 표준으로 호주/뉴질랜드 표준 가이드라인 AS/NZS ISO 31000:2009가 제시되었는데 특정 기법이나 대책을 제시하는 대신 파악된 위험요소에 대한 중요도를 평가는 것이 주된 목적이다[10]. 비즈니스 로직에 대한 위협을 분석하는 PASTA기법이 소개되었고[11], 임베디드 소프트웨어 환경에 맞는 시큐어 임베디드 소프트웨어 개발을 위한 위협 모델이 Klockwork사 의해 연구가 시도되었다[12]. 소셜 미디어 네트워크 환경의 응용 소프트웨어를 대상으로 privacy 위협 모델링기법으로 LINDDUN이 제안되었다[13].

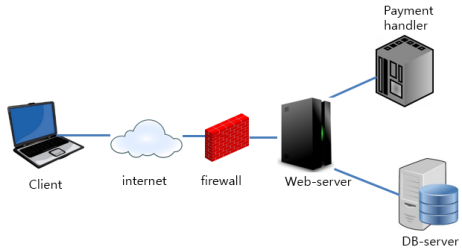
Ⅲ. 적용 사례

MS위협 모델링 기법을 단순한 온라인 쇼핑몰 웹 사이트의 웹서비스에 대해 적용해본다.

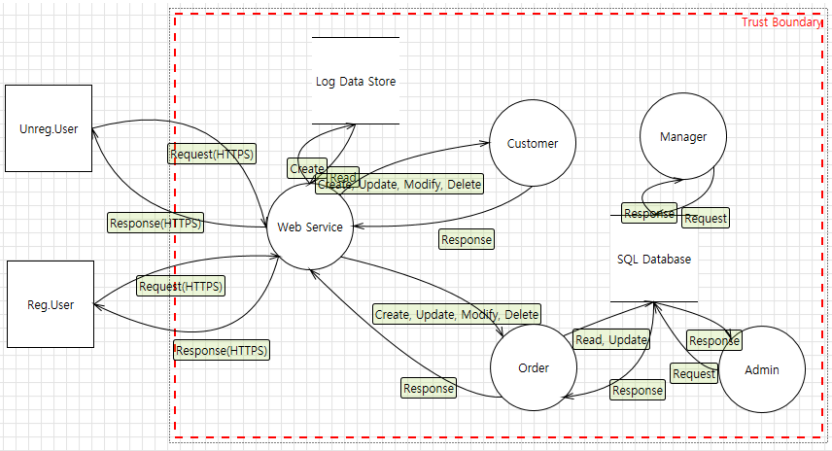
3.1. 적용 대상 시스템

고객이 온라인 쇼핑몰에 접속해 물건을 구매하고, 온라인상점 매니저는 온라인 쇼핑몰 상점에서 판매되는 상품의 설명과 홍보, 재고와 가격 정책을 관리하며, 웹 사이트 관리자는 웹 사이트의 모든 부분을 담당하는 쇼핑몰 웹 사이트를 개발 대상으로 가정한다.

- 개발할 웹 서비스는 3가지이다: 고객(client)과 웹서버(web server)와의 연결을 담당하는 웹서비스, 웹서버와 지불처리기(payment handler) 사이의 데이터 교환을 제공하는 DB서버스, 신용카드 유효 검사를 위해 은행관련 처리 작업을 제공하는 지불처리 서비스.
- [그림 1]의 웹 사이트의 구조는 웹서버와 DB서버, 지불 서버로 내부 인트라망으로 연결하고, 외부 인터넷망과 시스템 사이에는 파이어월 서버를 설치한다.
- 웹 사이트에서 다루는 데이터는 다음과 같다: 고객 계좌(고객 아이디, 고객 이름, 이메일, 로그온 정보), 고객 프로필(고객 이름, 신용카드 종류, 신용카드 번호, 신용카드 유효기간), 상품정보(상품 번호, 상품 이름, 상품 설명, 상품 가격, 상품재고수량, 상품 사진), 주문정보(상품번호, 상품수량, 주문총합계, 배송지 주소, 청구지 주소, 지불정보), 로그정보(고객 아이디, 액션)
- 웹 사이트의 구성요소의 행위는 [표 2]와 같다:
- 웹 사이트를 구성하는 구성요소의 기술적인 가정사항은 [표 3]과 같다:
- 웹 사이트의 최상위 DFD는 [그림 2]에 묘사된 것처럼 외부 사용자와 웹 서버를 기점으로 내부 인트라넷에



〔그림 1〕 웹 사이트의 시스템 구성



〔그림 2〕 웹 사이트의 최상위 수준의 DFD

서 동작하는 고객관리, 주문관리, 지불관리, 매니저, 관리자 프로세스로 구성된다:

- DFD요소마다 적용되는 STRIDE 유형은 [그림 3]의 매핑을 사용하여 결정하고, 대표적인 공격 유형을 선택한다:
- threat tree는 하나의 DFD요소에 대해 열거된 공격의 전제 조건들을 노드들로 구성하여 하나의 공격 경로를 파악할 수 있게 해준다. 비인가 고객이 정상 로그인하게 되는 경우의 공격에 대한 위협 트리는 [그림 4]와 같다:
- 파악된 공격 위협에 대한 보안 방지책은 현재 사용가능한 기술과 대책을 사용한다. [표 4]에서 부정 사용자 인증 방지를 위한 보안 요구사항과 대책을 기술하

〔표 2〕 웹사이트 구성요소의 행위

구성 요소	행위
웹사이트 관리자	- 고객 계좌 정보 읽기 - 고객 프로필 생성, 읽기, 갱신 - 상품 정보 생성, 읽기, 갱신, 삭제 - 주문 정보 생성, 읽기, 갱신
등록된 고객	- 고객 계좌 정보 생성 - 고객 계좌정보 읽기, 갱신(생성후) - 고객 프로필 생성 - 고객 프로필 읽기, 갱신(생성후) - 상품 정보 읽기 - 주문 정보 생성 - 주문 정보 읽기(생성후)
미등록 고객	- 고객계좌 생성 - 상품 정보 읽기 - 주문 정보 생성 - 주문 정보 읽기(생성후)
매니저	- 고객 계좌 생성, 읽기, 갱신, 삭제 - 고객 프로필 생성, 읽기, 갱신 - 상품 정보 생성, 읽기, 갱신, 삭제 - 주문정보 생성, 읽기, 갱신, 삭제 로그 생성
웹 서비스	고객 프로필 생성, 읽기, 갱신 상품정보 생성, 읽기, 갱신, 삭제 주문정보 생성, 읽기, 갱신, 삭제 로그 생성

〔표 3〕 웹사이트 구성요소의 기술적인 가정 사항

구성 요소	기술	세부 구성요소
웹 서버	.NET framework 4.5	- FORM 인증 - C/C++ 코드 사용 - 암호기법 사용 - 네트워크 프로토콜 사용 - HTTP 사용 - 웹 브라우저 인터페이스 사용 - 수치 계산 사용 - SQL검색
DB 서버	SQL server 2000	- 네트워크 연결 사용 - SQL검색
로그 저장	파일 서비스	없음
웹 서비스	.NET framework 4.5	없음.
웹서버 관리자	.NET framework 4.5	- 암호기법 사용 - 네트워크 연결 사용 - HTTP 사용 - SQL검색
DB 서버 관리자	.NET framework 4.5	- 네트워크 연결 사용 - HTTP 사용

	S	T	R	I	D	E
외부 개체	O		O			
프로세스	O	O	O	O	O	O
데이터 저장소		O	O	O	O	
데이터 흐름		O		O	O	

〔그림 3〕 DFD 요소와 STRIDE 유형의 대응관계

고 있다:

Ⅳ. 적용사례의 분석

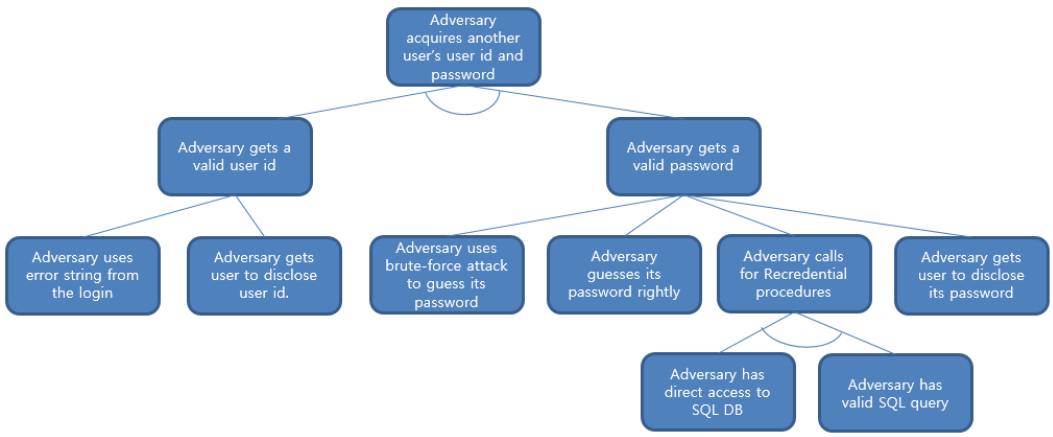
온라인 쇼핑몰 웹 사이트에 대해 위협 모델링 적용 결과, '부정 사용자 인증' 공격을 묘사한 위협트리로부터 '사용자 id'와 '사용자 password' 2가지 데이터가 모두 공격자에게 노출되는 경우에 발생함을 확인할 수 있다. 이 2가지 조건을 세분화하면, 사용자 인증에 대한 보안 요구사항과 DB SQL검색에서 나타날 수 있는 보안약점과 사용자의 권한에 대한 보안 요구사항을 도출해낼 수 있다.

'사용자 권한 제한 정책 사용'은 '인증'과 '사용자 관리'의 서로 다른 2가지 요구 사항에서 공통으로 필요한 보안 대책으로 사용되지만, 문맥상 구별된다는 점에 주목할 필요가 있다: '인증'의 경우, 인터넷 외부 접속 환경에서 '등록된 고객'과 '미등록 고객' 사이의 구분, 인트라넷 내부 접속 환경에서 '관리자'와 '매니저' 사이의 구분이 보안 정책에 일관되게 반영되어야 한다.

시스템에 공격 위협에 대한 보안 요구사항의 보안 속성이 비슷하거나 겹치는 부분이 발생할 수 있는 경우, 보안 솔루션으로 이용 가능한 보안 기술이나 기법들의 세분화된 정도에 따라 제약을 받을 수 있다. 이것을 해결하기 위해서는 가능한 최신의 보안 공격 기술과 보안 기술과 기법에 대한 지식과 정보를 유지하고 사용해야 하는 것이 요구된다[14,15].

'사용자 id'보호와 '사용자 password' 와 같은 데이터나 정보 보호 보안 요구 사항을 도출해낼 필요가 있는데, 내부 인트라넷을 사용하는 경우에도 정보 흐름의 요소가 공격 위협 대상이 될 수 있기 때문이다.

'사용자 id와 비밀번호'이외에 '사용자의 구매정보 내역'과 같은 '개인 정보 유출과 악용'에 대한 공격 위협에 대한 보안 대책도 추가적으로 이루어져야 할 필요가 있다. '개인 정보 유출과 악용' 공격을 방지하기 위해서 요구되는 '고객의 활동 내역에 관한 정보가 그 고객의 신원 정보 사이의 연계나 추적이 어려워야 한다'는 보안 요구사항[16]을 MS 위협 모델링 기법으로 도출하기에는 적합하지 않다. 이미 유출된 개인 정보에 대한 보호 수단을 인증과 사용자 관리와 같은 STRIDE유형으로 분석하는데 충분하지 않기 때문이다. 공격 위협을 파악하기 위해 사용된 6가지 공격 유형에는 기본적인 정보 흐름의 보안 속성에 해당하는 기밀성(confidentiality), 무결성(integrity), 가용성(availability)의 3가지 속성 요소를 기준으로 하고 있기 때문에 적용범위를 넓히기 위해 개인정보(privacy) 보호와 같은 추가적인 보안 속성 요소를 확장할 필요가 있다.



〔그림 4〕 비인가 고객의 정상 로그인 공격 위협 트리

V. 결 론

본 논문에서는 MS 위협 모델링 기법과 유사한 위협 모델링 기법들에 대해 살펴보고, MS사의 위협 모델링 기법에 기반하여 온라인 쇼핑몰 웹 사이트에 대해 위협 모델을 적용하고 분석하였다.

위협 모델링은 소프트웨어 개발 단계의 초기 단계에서 설계 단계의 보안약점을 파악하여 제거하고 보안 대책을 설계 사항에 반영시키는 작업을 반복적으로 수행하는 개발 방법론이다.

기본적인 6가지 공격 유형 STRIDE 분류는 3가지 보안 속성(기밀성, 무결성, 가용성)에 기초하고 있는데, 개인 정보 보호(privacy)와 같이 추가적인 보안 속성에 대한 고려와 확장이 필요하다.

위협 모델링 기법의 적용 분야가 다양해지기 위해서는 예를 들어 임베디드 소프트웨어와 같이 특정 분야에 특화된 보안 속성의 새로운 정의가 추가로 이루어져야 할 것이다.

참 고 문 헌

[1] SAFECode, *Fundamental Practices for Secure Software Development*, 2nd Ed., Software Assurance Forum for Excellence in Code, 2011.

[2] F.Swiderski, W.Snyder, *Threat Modeling*, Microsoft Press, 2004.

[3] M.Howard, S.Lipner, *The Security Development Lifecycle*. Microsoft Press, 2006.

[4] M.Howard, J.A.Whittacker, “Demistifying the Threat-Modeling Process”, *IEEE Security & Privacy*, 2005.

[5] A.Shostack, *Threat Modeling: Designing for Security*, John Wiley & Sons, 2014.

[6] OWASP https://www.owasp.org/index.php/Threat_Risk_Modeling

[7] Octave http://www.cert.org/resilience/products-services/octave/index.cfm

[8] National Infrastructure Advisory Council, *Common Vulnerability Scoring System*, US.Dept.Homeland Security, 2004.

[9] Trike http://www.octotrike.org/

[10] AS/NZS ISO 31000:2009 http://shop.standards.co.nz/catalog/31000%3A2009%28AS%7CNZS+ISO%29/view

[11] PASTA http://www.myappsecurity.org

[12] Klockwork, Threat Modeling for Secure Embedded Software, *Security Innovation & Klockwork White Paper*, 2011.

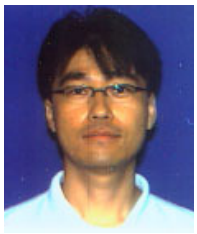
[13] M.Deng, K.Wuyts, et.al, “A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements”, Journal of Requirements Engineering, Springer-Verlag 2011.

[14] CWE(Common Weakness Enumeration) http://cwe.mitre.org/

[15] CVE(Common Vulnerabilities Exposures) https://cve.mitre.org/

[16] Y.Cherdantseva, J.Hilton, “A Reference Model of Information Assurance & Security”, *Int. Conf. on Availability, Reliability, & Security*, IEEE 2013.

〈저 자 소 개〉



이 진 호 (Jeanho Lee)
학생회원

1996년 2월 : 연세대학교 전산학과 졸업
2001년 8월 : 고려대학교 컴퓨터학과 석사
2004년 3월～현재 : 고려대학교 컴퓨터학과 박사과정

관심분야 : 정형기법, 소프트웨어 공학, 임베디드 소프트웨어, 정보보호, 안전필수 시스템

이 혁 (Hyuk Lee)
학생회원

2006년 2월 : 호주 시드니 공과대학 IT학부 졸업
2009년 2월 : 고려대학교 컴퓨터학과 석사
2009년 3월~현재 : 고려대학교 컴퓨터학과 박사과정
관심분야 : 정형기법, 소프트웨어 공학, 정보보호

강 인 혜 (Inhye Kang)
정회원

1987년 2월 : 서울대학교 전자계산기공학과 졸업
1989년 2월 : 서울대학교 전자계산기공학과 석사
1997년 5월 : Univ. of Pennsylvania 컴퓨터정보과학 박사
2002 ~현재 : 서울시립대학교 기계정보공학과 교수
관심분야 : 정형기법, 소프트웨어 공학, 인터넷 보안, 무선통신