대한민국, 대도약을 위한 창조경제 추진계획
3년의 혁신, 30년의 성장

미래창조과학부 **보 도 자 료** http://www.msip.go.kr

2014. 10. 17(금) 조간(온라인 10. 16. 12:00)부터 보도하여 주시기 바랍니다.

문의 : 국립전파연구원 이동정 과장(061-338-4400), 이경희 연구관(061-338-4440)

대한민국, 정보보호 분야 국제표준화 주도

- 웹 기반 공격 대응 기술 등 국제 표준 다수 채택 -

□ 미래창조과학부 국립전파연구원(원장 최영진)은 2014년 9월 26일에 끝난 국제전기통신연합의 전기통신표준화 부문(ITU-T) 연구반 17(정보보호) 회의에서 한국 주도로 개발된 「웹기반 공격 예방기술」 등 2건이 국제표준으로 최종 승인(approval) 되었다고 밝혔다.

표준제목	표준 번호	에디터
웹 기반 공격 예방 기술	X.1211	염흥열(순천향대)
스마트폰 앱 배포 프레임워크(X.1121-X.1149)	부속서 24	김미주(KISA), 염흥열(순천향대)

※ ITU-T : 전기통신관련 기술·운용·요금 문제를 연구하고 그 결과를 국제표준화 하는 국제전기통신연합(ITU)의 전기통신표준화 부문

o 「웹 기반 공격 예방 기술」은 사용자가 단순히 웹 사이트에 방문만 해도 악성코드에 감염되는 웹 기반 공격에 대응하기 위한 표준으로,

- 웹 기반 공격 대응 시스템이 가져야 할 세부 기술과 구조를 제시하고 있으며, 웹 공격 대응 시스템 설계와 운영 시 널리 활용될 수 있다.

o 「스마트폰 앱 배포 프레임워크 부속서」는 스마트폰을 위한 안전한 앱 배포 프레임워크에 대한 국제표준으로, 앱 배포 사이트의 보안성을 향상시키고자 할 때 가이드라인으로 활용 가능하다.

□ 아울러 이번 회의에서 우리나라가 주도한 「모바일 기기를 이용한 다중요소 인증 메커니즘」등, 4건의 표준안이 승인준비과정(consent)으로 채택되어, 차기 회의(2015. 4.)에서 표준으로 승인될 예정이다.

※ 승인준비과정(consent) : 4주 동안 회원국의 의견을 수렴하여, 응답한 회원국의 70% 이상이 동의하면 차기 회의에서 표준으로 승인

표준제목	표준 번호	에디터
고수준 보안을 요구하는 서비스를 위한 이상행위 탐지시스템 기능	X.1157	임형진(금융보안연구원), 김태경(서울신학대)
모바일 기기를 이용한 다중요소 인증 메커니즘	X.1158	염흥열(순천향대), 김근옥,송성현 (금융보안연구원)
ITU-T X.813 기반의 위임부인방지 구조	X.1159	김근옥,심희원,송성현(금융보안연구원)
X.1311(유비쿼터스 보안 프레임워크) 정정서	정정서 1 (X.1311)	염흥열(순천향대)

□ 이번 성과로서 국제전기통신연합(ITU) 내 정보보호 표준화 활동에서 우리나라의 입지를 다시 한 번 확인하였으며, 앞으로도 정보보호 표준화 분야에서 우리나라가 주도적인 역할을 해나갈 수 있을 것으로 기대된다.

첨부. 승인 권고 설명 자료

〈첨부. 승인 권고 설명 자료〉

1. X.1211(Techniques for preventing web-based attacks)

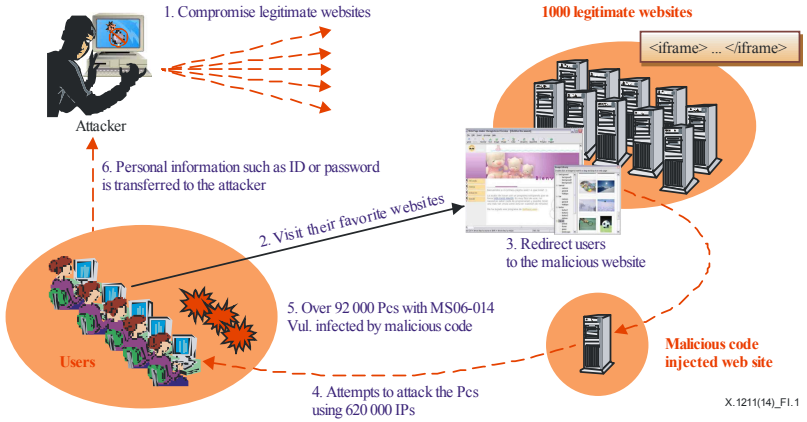
□ 기술 개요

o 웹 기반 공격은 웹 사이트의 취약성이 악용되어 악성코드가 삽입되고 다시 사용자 컴퓨터를 감염시키는 공격 방법이다. 이 국제표준은 사용자가 단순히 웹 사이트에 방문만 하더라도 악성코드에 감염되게 하는 웹 기반 공격의 공격 시나리오와 이에 대응할 수 있는 다양한 기술을 제시한다.

□ 권고(안)의 주요 내용 및 의미

o 웹 기반 공격 시나리오 및 대응 기술

- 웹 기반 공격의 대표적인 시나리오 : 공격자 정상 웹 사이트 해킹 → 공격자 웹 사이트 악성코드 삽입 → 사용자 방문 → 사용자 악성코드 감염 →사용자 정보 유출 및 파괴



o 웹 기반 공격을 막기 위한 웹 기반 공격 예방 시스템에 대한 다음과 같은 기술 특성과 요구사항을 제시

- 일반 요구사항 : 다중 보안 도메인에서 동작 가능해야 하고, 도메인간에 웹 취약성 정보가 서로 공유되어야 하며, 중앙 집중 방식과 분산 방식으로 동작해야 하고, 계층적 구조로 동작해야 하는 등

- 기능적 기술 : 알려진 악성코드를 검출해야 하고, 웹 기반 공격에 이용될 수 있는 취약성을 검출해야 하며, 행위 기반 분석 기법을 이용해 알려지지 않은 악성코드를 검출해야 하는 등
- 관리적 기술 : 서로 다른 보안 도메인 간의 보안 관리를 지원하고, 하나의 관리 인터페이스를 제공해야 하는 등
- 관리 인터페이스 기술 : 도메인 간의 교환되는 정보의 기밀성, 무결성, 가용성 보장, 개인정보의 유출을 방지해야 하는 등
- 핵심 보안 기술 : 악성 코드 유포 사이트 탐지 기능, 악성코드 경유지 사이트 검출 기능 등

2. 부속서 24(Supplement on a secure application distribution framework for communication devices)

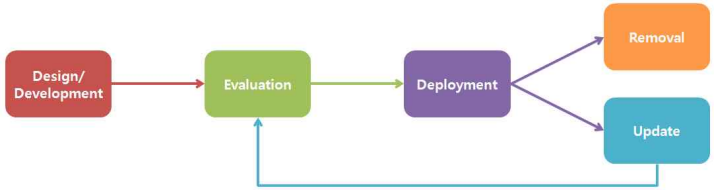
□ 안전한 앱 배포 프레임워크에 대한 부속서

o 이 부속서에서는 스마트폰을 위한 안전한 앱 배포 프레임워크를 제시한다. 개발자로부터 개발한 스마트폰 앱은 앱 배포 사이트에서 앱을 다운로드하여 사용자가 앱을 실행한다. 앱 배포에 대한 절차와 더불어, 이 부속서에서는 앱 배포 사이트의 보안 요구사항을 제시하고 있다.

□ 권고(안)의 주요 내용 및 의미

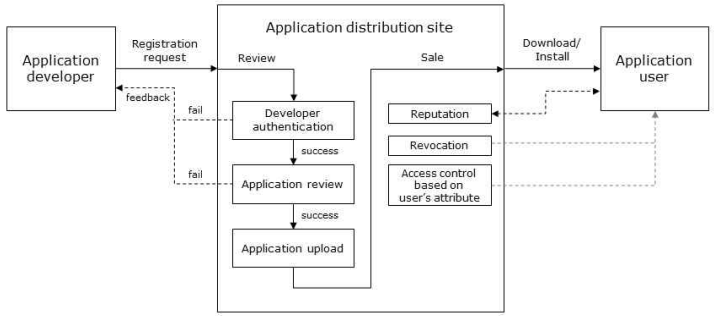
o 앱 배포 단계

- 이 국제표준은 앱 설계/개발 단계, 평가 단계, 배포 단계, 제거 및 업데이트 단계에서 요구되는 보안 요구사항을 기술하고 있다.



o 안전한 앱 배포 프레임워크

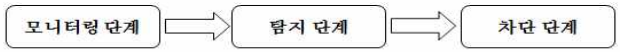
- 스마트폰을 위한 앱 배포 프레임워크는 다음 그림과 같으며, 각 프로세스에서 요구되는 보안 요구사항을 기술한다.



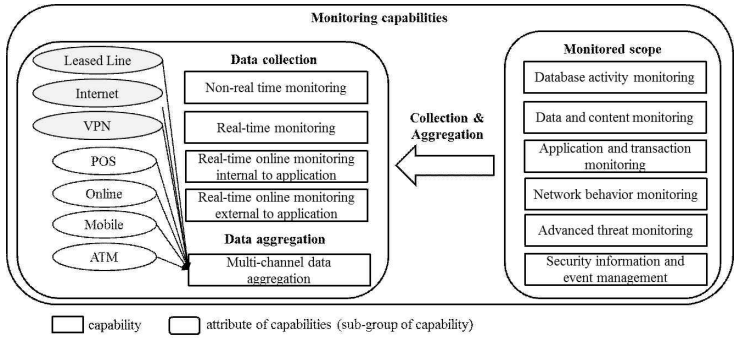
3. X.1157(Technical capabilities of fraud detection and response for services with high assurance level requirements)

□ 이상행위 탐지시스템의 주요 기능

o 이상행위 탐지시스템은 모니터링, 탐지, 차단 3가지 단계로 그림과 같이 구분되며, 부정행위 제어를 위하여 단계별 세부 기능을 요구한다.



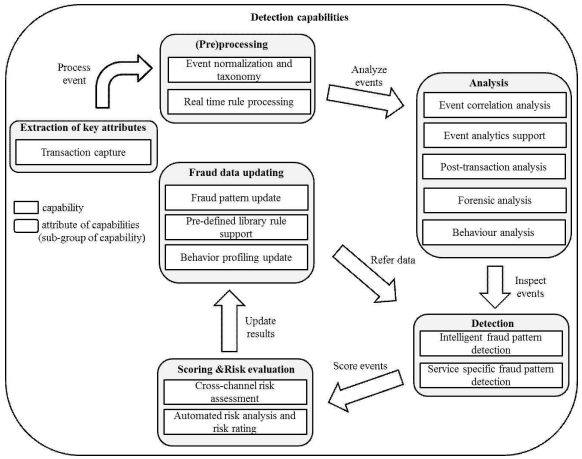
- 모니터링 단계 세부 기능



모니터링 단계의 경우 모드에 따라 배치타임 모니터링 기능, 리얼타임 모니터링 기능 등 5가지 기능을 정의하고 있으며, 또한 모니터링 대상에 따라 데이터베이스, 서비스, 네트워크, 보안이벤트 등의 5가지 기능을 정의한다.

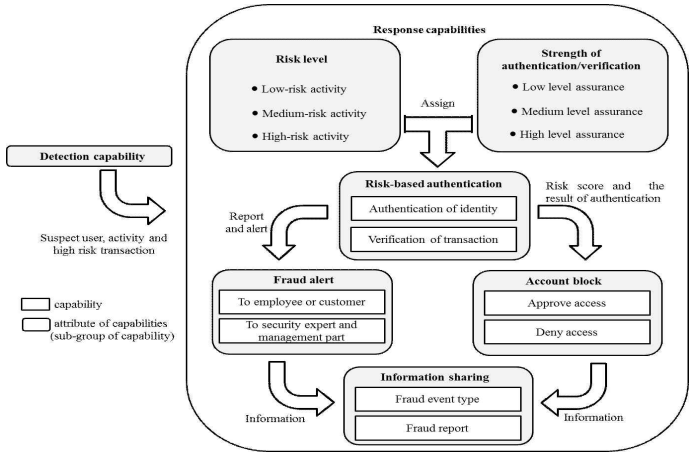
- 탐지 단계 세부 기능

탐지 단계에서는 이상행위를 탐지하기 위하여 트랜잭션 캡쳐, 이상행위 패턴갱신, 사전정의 규칙 지원, 실시간 툴 처리 기능, 관리도구 지원, 사후 트랜잭션 분석, 사용자 행위 프로파일 및 학습 기능, 지능적인 이상행위 패턴 탐지, 특정 서비스의 이상행위 패턴 탐지 패턴, 다중 채널 위협 평가, 자동 위협 분석 및 수준 평가의 12가지 기능을 정의하고 있다.



- 차단 단계 세부 기능

마지막으로 차단 단계에서는 추자적인 사용자 인증 및 검증, 부정행위 통지 및 경고, 사용자 계정 차단, 부정정보 공유 4가지 기능을 정의한다.



4. X.1158 (Multi-factor authentication mechanisms using a mobile device)

□ 모바일 기기를 이용한 다중 요소 인증 메커니즘

o 이 국제표준은 모바일 기기를 이용한 다중 요소 인증 메커니즘을 제시한다. 이를 위해 단일 요소 인증 방식의 취약점과 다중 요소 인증 방식의 필요성을 제시한다. 더불어 다중 요소 인증 메커니즘이 고려해야 할 중간자 공격 등의 여러 인증 위협 요소와 다중 요소 인증 메커니즘을 선택하기 위한 기준을 정의한다. 또한, 다중 요소 인증 메커니즘을 적용하기 위한 다중 요소 인증 모델과 관련 프로토콜을 제시한다.

□ 권고(안)의 주요 내용 및 의미

o 보안 요구사항

- 본 권고(안)에서는 사용자, 모바일 기기, 보안요소, 서비스제공자를 메커니즘의 구성 객체로 정의하고 있으며, 해당 표준에서는 일반적인 보안요구사항과 각 객체별 보안요구사항을 구체적으로 제시하고 있다.

o 다중 요소 인증 서비스 모델

- 본 권고(안)에서는 기본 서비스모델로 다중채널을 이용하는 경우와 안전한 모바일 기기를 이용하는 모델을 정의하고 있으며, 서비스 특성에 따라 다양한 방식으로 결합하여 서비스가 가능하다.

기본 모델		설명	예시
Using multiple channels	One-directional multiple channels model	사용자가 모바일 기기를 이용하여 인증정보를 생성한 후, 서비스 제공자에게 전달하는 일반적인 모델	Multi-device login, Multi-channel login
	Bi-directional multiple channels model	서비스 제공자로부터 인증정보생성에 필요한 정보를 전달받아 인증정보를 생성한 후, 다시 서비스 제공자에게 전달하는 서비스 모델	SMS OPT, OOB
Using secure mobile devices	Mobile device with secure elements model	보안요소(secure elements)를 이용하여 안전하게 인증정보를 생성하여 서비스 제공자에게 전달하는 서비스 모델	PKI tokens, Mobile OPT
	Stand-alone mobile device model	전용기기를 이용하여 안전하게 인증정보를 생성하여 서비스 제공자에게 전달하는 서비스 모델	OPT tokens

※ OOB : Out Of Band / OTP: One-Time Password
PKI: Public Key Infrastructure / SMS: Short Message Service

5. X.1159 (Delegated non-repudiation architecture based on ITU-T X.813)

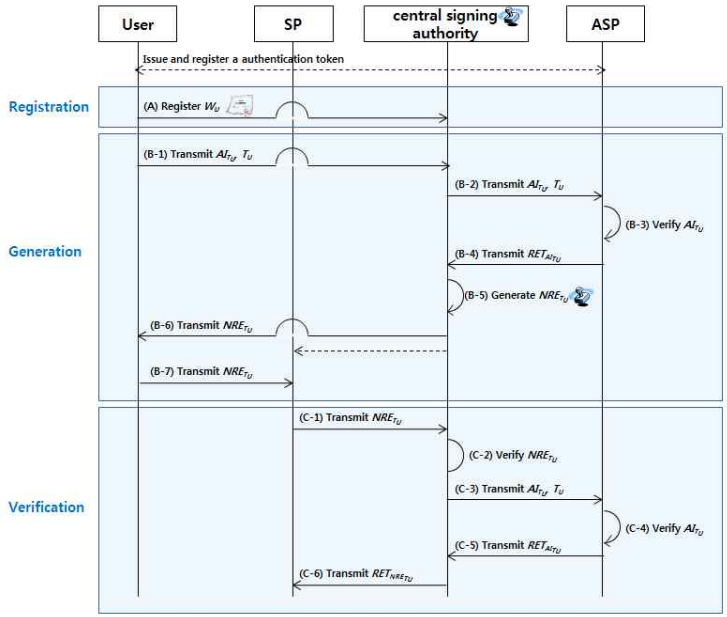
□ 위임부인방지 구조

o 이 국제표준은 ITU-T X.813 부인방지 표준안을 확장하여 사용자가 제3의 신뢰기관에 부인방지증거(evidence) 생성을 위한 권한이나, 권한과 서명키를 위임하면, 신뢰기관은 사용자를 대신하여 전자거래에 대한 부인방지 증빙을 생성 및 관리하는 위임부인방지 구조를 제시하고 있다.

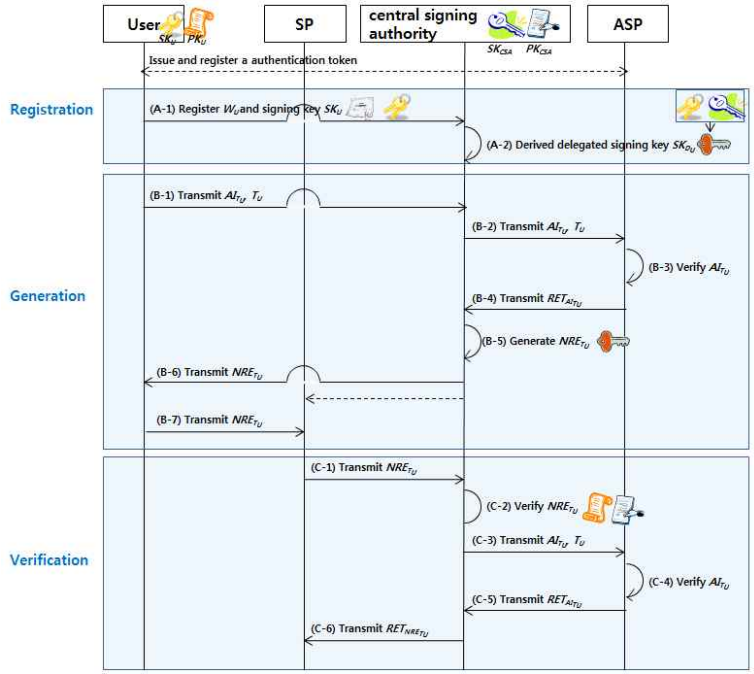
□ 권고(안)의 주요 내용 및 의미

o 위임부인방지 서비스 모델은 부인방지증거 생성에 관한 권한만을 위임한 경우와 권한과 부인방지증거 생성을 위한 키를 동시에 위임하는 2가지 모델을 정의한다.

- (권한만 위임한 경우) 사용자로부터 부인방지증거 생성을 위한 권한을 위임받은 신뢰기관은 사용자로부터 전달받은 거래 서명값을 검증 한 후 유효한 경우 자신의 키로 위임부인방지 증빙을 생성하는 모델이다.



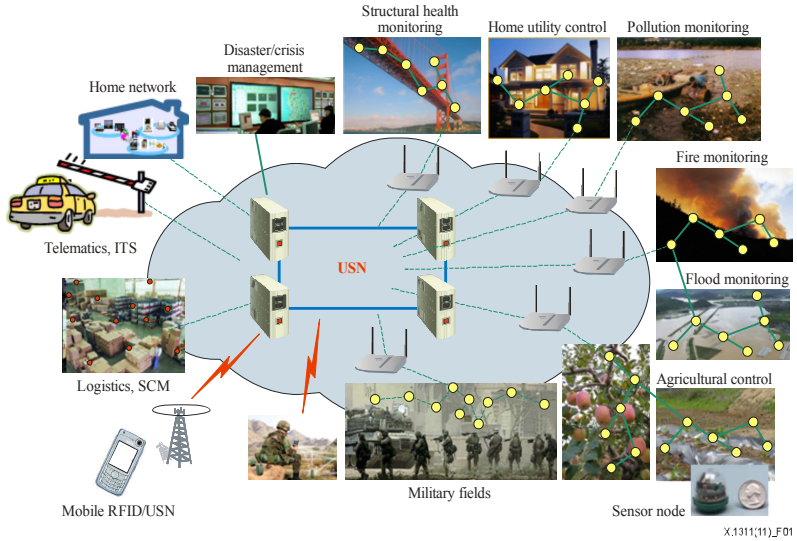
- (권한과 서명키를 위임한 경우) 사용자로부터 부인방지증거 생성을 위한 권한과 서명키를 위임받은 신뢰기관은 사용자로부터 전달받은 거래 서명값을 검증 한 후, 유효한 경우 위임받은 서명키로 위임부인방지 증빙을 생성하는 모델이다.



6. Draft Technical Corrigendum 1 of Rec. ITU-T X.1311, Information technology - Security framework for ubiquitous sensor networks

□ 유비쿼터스 센서 네트워크 보안 프레임워크 X.1311

o 본 표준은 USN(Ubiquitous Sensor Network) 보안 프레임워크를 제시하였으며, 국제전기통신연합(ITU-T)과 국제표준화기구(ISO)에서 2011년 2월, 동시에 국제표준으로 채택되었다.



- USN 보안 모델, 다양한 보안 위협을 비롯해, 위협에 대응할 수 있는 보안 기술(키관리, 인증된 브로드캐스트, 안전한 데이터 통합 등) 및 각 보안 기술의 요구사항 등을 제시하고 있다.

□ 유비쿼터스 센서 네트워크 보안 프레임워크 X.1311의 기술적 정정서1

o X.1311에서 인용하고 있던 ISO/IEC 문서(ISO/IEC 18028-2)가 폐지됨에 따라 이에 따른 후속조치가 필요하게 됨으로써,

- 이 국제표준 정정서는 ITU-T X.1311에서 인용한 ISO/IEC 18028-2 문서를 모두 삭제하고 그 대체 표준인 ITU-T X.805로 변경하여 구성하였다.