TTA 정보보호 표준화 활동

2013.10.08

□ 배경

○ 정보보호는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 보장하기 위한 보안기술과 사용자(User, Service Provider, Developer 등) 관점에서 요구사항 만족, 서비스 품질 보장, 상호운용성 확보 및 보안 적용을 위한 응용보안 기술로 정의됨

○ 현재, TTA는 ICT 기반 정보보호 표준화 활동으로 총 5개의 그룹으로 단체표준을 개발하고 있음

- 정보보호기반: 암호알고리즘, 공인인증서 등 기반 기술
- 개인정보보호 및 ID관리: 프라이버시 보호, Identity 관리 기술
- 사이버보안: DDoS 방지 기술, 사이버보안 정보교환 기술
- 응용보안 및 평가인증: 신규 서비스(ITS, 클라우드, 스마트그리드 등)에 보안기술 탑재하기 위한 응용기술, 보안성 평가(CC, CMVP, ISMS, PIMS 등)
- 바이오인식: 사용자 인증 강화를 위한 바이오정보 탑재 기술

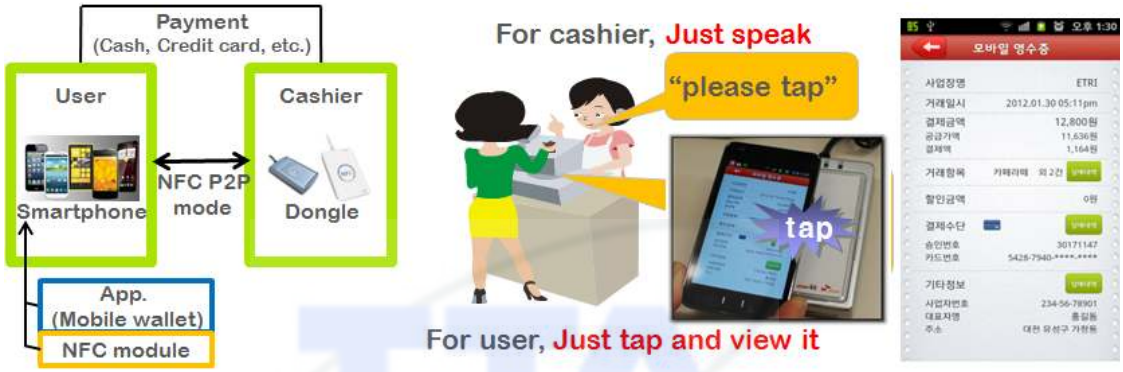
□ 주요내용

○ 모바일 전자 영수증 관리 규격

- 2011년, 한국은 영수증 발급을 위해 약 250만km 분량의 종이가 활용되어 자연환경 파괴나 환경호르몬 유발, 그린ICT 활동에 역행하고 있음
- 한편, 스마트폰이 대중화되면서 종이 영수증을 전자 영수증으로 대체할 수 있는 기술 구현 및 적용이 가능한 인프라가 충족되어 있음
- 따라서, TTA는 2012년도 국내 카드사 및 가맹점에서 요구되는 종이 영수증 내에 데이터 항목들을 수요 조사하여, 공통(Mandatory) 항목 및 선택(Optional) 항목을 선정하였으며, “모바일 전자 영수증 규격(TTAK.KO-12. 0197)”을 개발함
- 실제 동작 방식은 근거리통신기술(NFC) 중에 P2P 모드를 이용하여, 사업자(가맹점) 동글과 사용자 모바일 단말 간에 NFC 프로토콜을 이용함
- 2013년도 주요 표준화 활동은 상기 규격을 실제 산업체에 적용하기 위해

타사 모바일 전자 지갑(Mobile Wallet) 간에 연동이 가능하고, 전자 영수증을 쉽게 관리할 수 있는 “모바일 전자 영수증 관리 규격” 표준초안을 추가적으로 개발하고 있음

- 추가 규격의 주요 기능은 모바일 전자 영수증을 모바일 앱을 통해 관리하기 위한 기능, 전자 영수증 내에 전자 서명을 확인하기 위한 기능, 단말에 저장된 전자 영수증을 취소 거래할 수 있는 기능, 가맹점에 제공되는 부가서비스를 사용자 인터페이스를 통해 접근 가능한 기능, 전자 영수증을 다른 단말 및 애플리케이션 간 공유 가능한 기능을 추가하였음
- 향후 모바일 전자 영수증 관련 단체표준이 모두 완료되면 국내 산업체 활성화와 친환경 보호, 사용자 편리성 제공이 가능할 것으로 기대됨



[그림 1] 모바일 전자 영수증 개요

○ 온라인 청소년 보호 연령 검증 기술

- 한국은 초고속 인터넷 구축과 최첨단 디바이스 보급으로 온라인 환경에서 아동 및 청소년들이 시간과 지역(geography)에 구애받지 않고, 자유롭게 교육, 문화, 엔터테인먼트 등의 부가서비스를 이용하고 있음
- 한편, 온라인 환경에서의 검색 엔진 고도화와 악성사이트들의 증가로 아동 및 청소년들에게 부적절한 대중매체나 위험요소들이 여과 없이 그대로 노출되고 있음
- 현재 이러한 문제들을 해결하기 위한 방법으로는 기술적인 방법, 관리적인 방법, 정책/법적인 방법으로 구분될 수 있음

· 기술적 방법 : 유해물 차단 기술, 콘텐츠 필터링 기술, 성인사이트 등의 사용자 고유 실별/본인확인 기술 등

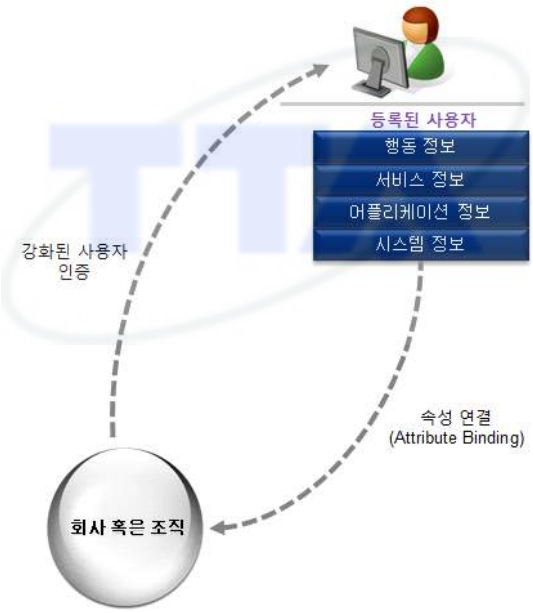
· 관리적 방법 : 콘텐츠 생성→분배→활용→폐기 전체 라이프 사이클에서 각 사용자(콘텐츠 개발자, 사이트 운영자, 부모 및 교육자, 아동 및 청소년) 간 일정한 역할 분담

· 정책/법적 방법 : 아동 및 청소년 대상으로 부적절한 콘텐츠 및 서비스를 제공하는 사업자들에게 법적 대응하거나 심야시간 PC 방 출입을 통제하는

셧다운 제도 등 강제적 조치

- 현재 TTA는 기술적 접근 방법에 하나로 사용자 속성 정보를 근거로 온라인 환경에서 실사용자의 연령을 검증하는 방법에 대한 표준화를 추진하고 있음. 즉, 온라인 사용자가 성인이 아닌 청소년들이 부모님들의 아이디를 도용하거나 불법적으로 유통되는 아이디 생성기에 만들어진 가짜 아이디들의 진실성을 판단하기 위함
- 속성바인더 수집 정보 예시

구분	정보
시스템 계층	위치정보, 이전 위치정보, 장비 타입, 장비 ID, IP 주소, OS 패치 레벨 정보, 디바이스 드라이버 정보, 대역폭 정보 등
어플리케이션 계층	사용하는 프로그램 정보, 활용 DB 정보, 행동 패턴, 트랜잭션의 양, 브라우저의 특성 등
서비스 계층	하루 중 주로 이용하는 시간대 정보, 사용시간 정보, 이용자의 조직 및 그룹에 대한 정보, SNS 연결 및 태그 정보 등



[그림 2] 사용자 속성 정보 기반 연령 검증

○ 스미싱 사고에 대한 대응 지침

- 스미싱(Smishing)이라는 키워드는 SMS(단문 메시지 서비스)와 Phishing (피싱)의 결합어로 문자메시지를 가장하여 다른 연결 수단에 접속되는 피싱 사고를 말한다. 즉, 공격자는 핸드폰이나 스마트폰에 사회공학적 문자 메시지를 송부하여 소액결제, 자동결제, 금액이체 등 금융사기와 개인 정보 탈취와 같은 해킹 침해사고를 발생시킴
- 스미싱과 같은 사고는 사회공학적 공격 방법(돌잔치, 결혼식 등 초대장)을

취하고 있어, 누구에게나 발생할 수 있고, 실수로 잘못 누르는 경우라도 결제가 이루어질 수 있는 위험을 내포하고 있음

- 특히, 문자메시지에 내포된 URL을 클릭할 경우, 소액 결제(최대 30만원)와 같은 1차 피해 이외에 악성코드와 같은 불법 소프트웨어가 설치되어 휴대폰 내에 저장된 개인정보 유출이나 2차 피해로 확대될 수 있음
- 따라서, TTA는 스미싱 사고에 대한 보안 대응 지침으로 사용자 측면에서 취할 수 있는 기술적인 사항과 주의사항에 대해 정의하고 있으며, 서비스 제공자 측면에서도 고려되어야 할, 법/제도, 규제, 공동 대응 체계와 준수사항에 대해 정의하고 있음
- 또한, 사용자가 실제 스미싱 사고 피해가 발생할 경우, 취할 수 있는 유관 기관들의 정보 및 처리 절차 등의 정보를 제공하고 있음
- 본 표준은 일반 사용자 및 서비스 제공자 관점을 모두 고려하고 있어, 향후 스미싱 사고 피해 감소에 많이 기여할 것으로 예상됨

[그림 3] 스미싱 문자 사례

□ 향후전망

○ TTA 정보보호 표준화 활동은 앞서 설명한 3가지 이슈 이외에도 개인정보 영향평가 기준 개발, 스마트그리드 보안, 차량통신 보안, 클라우드 컴퓨팅 보안, 스마트폰에 바이오인식 기술을 접목하기 위한 기술 등 다양한 정보보호 표준들을 개발하고 있음

○ 또한, 국내 정보보호 산업체 육성과 ICT 인프라 보호, 실생활에 적용 가능한 표준 발굴을 위해 산학연 전문가들 간에 지속적으로 협력할 예정임