해외 ICT 표준화 동향

2016. 4

2nd Week

목 차

■ 본문

1. NIST, 정보보안 관련 형태보존 암호화(FPE) 표준 제정

■ 기타소식 ..... 4 쪽

한국정보통신기술협회
Telecommunications Technology Association

게시물 보기 : TTA 홈페이지 ▷ 자료마당 ▷ TTA간행물 ▷ 표준화 이슈 및 해외 동향

1. NIST, 정보보안 관련 형태보존 암호화(FPE) 표준 제정

(New NIST Security Standard Can Protect Credit Cards, Health Information)

보도날짜 2016.03.29

출 처 NIST

사 이 트 http://www.nist.gov/itl/csd/new-nist-security-standard-can-protect-credit-cards-health-information.cfm

■ 2016년 3월 29일, 미국 NIST(국립표준기술연구소, National Institute of Standards and Technology)는 컴퓨터 보안표준(NIST Special Publication (SP) 800-38G)을 제정함

- 신용카드를 카드 리더기에 인식할 때, 카드번호가 리더기에 저장되고 이는 정보 암호화를 더욱 어렵게 만듦

- 새로이 제정된 표준은 사업자가 소비자 카드번호 보호를 위한 음성적 방법과 개인의 의료기록을 보호하는 방법을 제시함

■ 'NIST SP 800-38G(블록 암호 운용방식에 관한 권고: 형태보존 암호화 방법)'*은 '형태보존 암호화(FPE)'와 그에 관한 2가지 기술(FF1, FF3)을 명시함

* NIST Special Publication (SP) 800-38G, Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38G.pdf)

- 이번 표준은 신용카드 번호를 소프트웨어의 기존 숫자 형태(길이, 형식)로 유지하면서 해커들이 판독할 수 없는 숫자 또는 문자열로 변경하는 방법을 제시함으로써, 금융 데이터 및 기타 민감한 정보 등을 처리하는 많은 소프트웨어 패키지 문제들을 해결함

■ 형태보존 암호화 기법 개발자인 모리스 드워킨(Morris Dworkin)은 암호화 기술인 FF1, FF3이 기존 1과 0으로 구성된 이진법 데이터 암호화 방식보다 더 안전함을 언급함

- 카드 리더기나 결제에 사용되는 금융 소프트웨어는 보통 16자리의 카드번호를 인식하기 때문에, 길이가 더 긴 암호화 숫자는 소프트웨어 상의 문제를 야기함

- 새로운 FPE 방법은 알파벳 순서의 이진법과 십진법의 숫자 및 문자를 모두 사용하며 기존과 동일한 길이의 암호를 생성하므로, 일반적인 카드번호처럼 보여 기존 설치된 기기의 개선을 가능토록 함

■ 이처럼, 암호화 기술에 대한 상업적 요구가 신용카드 번호 암호화로 이어졌으며, 향후 민감한 의료 정보를 포함하는 데이터베이스의 개인적 식별이 가능한 정보의 "익명성" 부분이 잠재적 응용기술이 될 수 있음

- 이러한 의료 정보 데이터베이스는 다양한 질병 치료법의 영향을 연구하는 중요 정보지만, 개인 환자 식별을 위해 사회적 보안 번호를 이용하거나 다른 개인 정보를 포함할 수 있음

- 드워킨은 FPE 암호화가 개인정보를 어느 정도는 보호할 수 있지만, 완벽한 보안은 힘들 것이라며, 만약 환자 샘플이 적은 곳에서의 암호화는 그들의 다른 특징을 보면 바로 누구인지 알아낼 수 있기 때문에 애초에 데이터를 맡기는 사람을 조심스럽게 선별해야 한다고 강조함

기타 소식

중국, 2016 스마트시티 혁신 컨퍼런스 개최

▶ 출처 : http://www.sac.gov.cn/sgybzeb/xwxc/201603/t20160329_206194.htm (2016.03.25.)

○ 2016년 3월 25일, '2016년 중국 스마트시티 혁신 컨퍼런스'가 국가 스마트시티 표준화 총괄팀 및 스마트시티 발전 연맹 주관, 산동성 표준화 연구원 및 산동성 사물인터넷 협회 주최로 개최됨

- 중국 정부는 중국의 스마트시티 건설 및 발전을 위해 표준화 중요성을 강조하고, 스마트시티 평가지표(9등급, 36개 보조지표) 마련 및 개선을 발표함

ITU 아시아 CTOs, 5G, IoT 관련 ITU 표준 강조

▶ 출처 : http://newslog.itu.int/archives/1231 (2016.03.29.)

○ 2016년 3월 21일, 한국, 중국, 일본의 ICT 선도기업 CTO(기술 담당 최고책임자)는 자문회의를 통해 5G 시스템, 사물인터넷(IoT), 차세대 비디오를 위한 ITU의 표준화 작업의 중요성을 강조함