전자서명법 , 전자금융거래법 개정안

- 인증제도 및 보안기술 규제의 선진화 , 글로벌화 전략 -

김 기 창

고려대학교 법학전문대학원

2013. 5. 23

‘정부 주도’ 보안 1 - 공인인증서

- 유저 권한 구분 부재 OS(윈98 이전)를 전제로 한 미개한 보안설계
  - Non-admin ActiveX (윈 비스타 이후) 몰이해
- Keystore, keychain, keyring 개념 몰이해
- 인증서 복사시 “암호입력 코스프레”
- 플러그인에 의존하는 해법 - “예”하는 습관
  - 추가적 ‘보안플러그인’ 설치, 설치, 설치
  - No ‘real’ mitigation; ‘심리 보안’, 보안 쇼 (security ‘theatre’)
- ‘서버’인증 개념 부존재 (http + plugins): ‘유저’인증만
- 루트인증기관에 대한 독립적, 전문적, 정기적 검증(실사) 부재
- ‘권위’에 의존한 보안 : 정부가 믿으라면 믿어 !

‘정부 주도’ 보안 2

- 이른바 ‘규정 보안’ -

- 전자금융감독규정 (금융위 고시), 제 3 장
  - “손전등 비치” 등
- 공인인증기관의 시설 및 장비등에 관한 규정 (미래부 고시)
  - “RSA 또는 KCDSA 1024 비트 이상의 전자서명키 생성 기능”
- 공인인증기관의 보호조치에 관한 규정 (미래부 고시)
  - “ 시스템에 대한 논리적인 접근통제를 설정할 것”
- 이런 규정들이 과연 ‘행정규칙’으로 존재해야 하나 ?

‘정부 주도’ 보안 3

- 점검 부실 / 부재 -

- ‘규정’ 준수 여부를 누가 검사 / 검증 / 실사 하나 ?
- 전자금융감독규정 - 금감원 ?
  - “ 보안성 심의” ?
  - 언제 , 얼마나 자주 ?
- 공인인증기관에 대한 검증은 KISA 가 수행 , 그러나
- KISA 에 대한 검증은 누가 하나 ?
- 정부 , 공무원이 과연 검증 역량이 있나 ?
- 검증수행기관을 공무원이 ‘지정’할 역량이 있나 ?

관치 보안의 결과

- “북한이 그랬어요 ㅠㅠ …”
- 악성코드 배포 웹서버 ‘비율’ 세계 최고
- 개인 PC 감염 비율 세계 정상급, 스팸메일 발송국 세계 정상급
- 면피용 보안, 규정 보안 : “규정이 하라는 것은 다했다”
- 보안 투자 인센티브 부재 - 억지 보안투자 강요
- 소비자 피해로 귀결
- “인터넷뱅킹 사고금액은 미국이 한국보다 약 290 배 (2009 년)”?
  이게 사실이면 어째서 미국 업계나 학계에 가서 발표 안하는지 ?

보안 기술 발전 , 보안감사 서비스 산업 토대 마련

- **기준 제정 , 관리** : 금융보안 / 인증업무수행 기준은 업계 / 전문기술 단체가
  - PCI DSS (Payment Card Industry Data Security Standards)
  - WebTrust Program for Certification Authorities
  - Electronic Signatures and Infrastructures (ESI) Policy requirements for certification authorities (ETSI)
  - Public key infrastructure for financial services — Practices and policy framework (ISO)
- **검증 수행** : 보안감사 전문 업체 (security auditor) 가
  - Licensed WebTrust Practitioners
  - SysTrust Seal
  - WebTrust Seal
  - PCI Qualified Security Assessors (QSAs)

질문

- 전자금융감독규정(손전등…), 공인인증기관 시설장비규정(1024bit…)을 정해두고 강행력을 부여하면, 한국 업계/전문가 단체는 언제 PCI DSS기준이나 WebTrust 기준 같은 것 만들 역량이 길러질까?
- 정부 공무원이 보안감사 '시늉' 하고 OK한다면, PCI 또는 WebTrust가 인정하는 전문적 보안감사 서비스 업체에게 돈을 내고 매년 점검(실사)를 받을 이유가 있나?
- KISA는 어째서 전문성을 구비한 제3자에 의한 보안검증을 받지 않는가?
- 개도국에 한국의 인증기술을 "수출"했다? 그 중 한국의 재정 원조없이 자기 돈으로 도입한 나라 있는가? 선진국에는 어째서 수출 못하는가?
  - 한국 국민의 세금 → 개도국 정부 → 삼성SDS, 한국정보인증 등이 현지에서 수주
- 현행 공인인증서의 경우, "전자서명생성정보가 가입자에게 유일하게 속할 것"이라는 요건이 과연 충족되는가?
  - 개인키(private key) 파일 복제 무제한 가능
  - 언제 어떻게 복제되었는지도 인식 불가능
  - '부인방지', '무결성' 운운하는 것은 잘못된 환상 (개인키 유출안된다고 무조건 전제할 때만 가능한 개념)

Any comments?

"I am well aware of the South Korea screw up. We use it as an example of how not to do it."

-- Mr Andy Smith (BCS The Chartered Institute for IT)

Mr Andy Smith 는 영국 정부 국무회의 (Cabinet Office) 가 채택한 아래 백서의 집필자 :

- PKI Implementation Strategy, v. 1.0 (2013.2.28)
- Public Key Infrastructure, v. 1.0 (2011.7.28)

전자금융거래법 개정안

- 제21조 제3항 개정

  ② (현행규정 유지) 금융회사 등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자금융거래의 종류별로 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치 등의 정보기술부문 및 전자금융업무에 관하여 금융위원회가 정하는 기준을 준수하여야 한다.

  ③ (개정) 금융위원회는 전 항의 기준을 정함에 있어서 보안기술과 인증기술의 공정한 경쟁을 저해하거나, 특정기술 또는 서비스의 사용을 강제하여서는 아니된다.

- 전자금융감독규정 전면 재검토 필요
  - 감독규정은 원칙만을 제정 (BCBS 전자금융위험관리 원칙 참조)
  - 상세한 보안감사기준 (Korea FSI DSS) 은 업계/전문기술 단체가 제정, 관리
  - 보안점검 (audit) 은 보안감사 전문 업체가 매년 실시
  - 보안감사 전문 업체는 자신의 전문성을 소명하고 금융위에 등록하고 영업
  - 금융회사는 누구로부터 보안감사를 받는지 공개하고, 보안감사 보고서 공시
  - 금융위/금감원은 사고 현황을 정확하게 파악하여 투명하게 공개, 공격 기법 신속히 공유

전자서명법 전면개정

- “공인”이라는 명칭은 폐지하되, 점검 기준은 강화
- ‘일방적’ 전자서명 강요 중단: 합의에 기한 전자서명 사용 (계약 자유, 한미 FTA 참조)
- 전자서명의 ‘추정력’ 규정 삭제
  - 육필서명과 동일 대우 = 서명, 날인은 ‘증거자료’에 불과 = 법관의 자유심증 존중
  - 어차피, 개인키의 유일귀속성 요건 충족 어려움
- **루트인증기관에 대한 제3자 검증 제도 도입** (Governance, safety assurance)
- 미래부는 인증업무수행기준의 ‘근본 원칙만’ 제정, 공지
  - 구체적인 인증업무수행기준은 업계/기술전문 단체가 작성, 제정, 상시 관리 (업데이트)
  - 국제적으로 널리 인정받는 인증업무수행기준 존중 (WebTrust, ETSI, ISO)
- 인증업무수행기준 준수 여부는 보안감사 전문 업체가 정기적으로 점검 (실사)
  - 보안감사 전문 업체는 자신의 전문성을 소명하고 미래부에 등록하고 영업
  - 국내 업계/전문기술 단체도 자율적인 Licence, 보안감사 서비스 품질 관리 제도 운영
  - 국제적으로 널리 인정받는 보안감사 업체의 전문성 존중

사전 규제 v 사후 통제

- 정부의 지정, 인가, 면허가 능사인가?
  - 보안감사 전문 업체를 정부가 '지정', '면허'?
  - ex. 정보보호 사전점검에 관한 고시 (방통위 고시)
  - 진입장벽, 특혜로 되어서는 곤란
  - 정부 '지정' 업체와 민간/업계가 인정 (accredition) 하는 업체 간 경쟁
- 진입 장벽 제거, 자유 경쟁
  - 정부 '지정' 업체가 더 나은지, 민간 '인정' 업체가 더 나은지는 시장이 판단.
  - 업계/전문가/수요자의 평판에 기초한 품질 관리
  - 유료 검증: 금융회사/수검인증기관의 "self interest"
  - **'배상 책임'을 줄이는데 필요한 합리적 선택은?**
  - "충분한", "적절한", "합리적인" 등에 대한 판단은 (사후적) 재판 절차를 통하여 판정

전자금융 사고거래에 대한 책임 (개인고객)

- 한국 : **금융회사가 배상**
  - (개인고객의 고의 , 중과실을 금융회사가 입증하면 고객 부담)
- 미국 : **금융회사가 배상** (EFTA)
  - 접근매체 유출 / 분실을 고객이 " 알고나서 이틀 내에 신고하면 " 그 사이에 아무리 많이 사고거래가 이루어졌더라도 50 달러만 책임
  - '카드번호'를 공격자가 알아내서 거래한 경우 , 고객이 해당 거래사실을 통보 받은 날로부터 60 일 내에 항의하면 , 고객 부담은 0
  - 문제의 거래내역을 통지받고 60 일이 지나도록 고객이 문제 제기를 안하면 , 고객 부담 .
- 영국 : **금융회사가 배상**
  - Your bank may only refuse a refund for an unauthorised transaction if it can prove you are at fault because you acted fraudulently, or because you deliberately, or with gross negligence, failed to protect the details of your card, PIN or password in a way that allowed the transaction.