공인인증서와 금융마피아

오픈넷 아카데미 공개 강연

김 기 창

2014.2.27

기술원리 v 실제 구현 과정

- 인증서 기술
  - 거래 내역 전자서명 (위조 , 변조 여부 확인 ?)
  - 서버 인증 (웹브라우저사들이 자발적으로 형성한 글로벌 신뢰 체계)
- Concept only
  - 당사자 인증 ?
  - 부인방지 ?
  - 교신 암호화 (키교환 과정 ?)

구현 과정의 치명적 오류

- 보안경고를 무시하라 .
- 웹사이트에 적힌 내용을 믿으라 .
- 반드시 “예”하라 .
- 웹사이트의 지시에 절대 복종하라 .

- 정부의 “공식”입장 : ‘ 공인’인증서는 안전하다 !

참담한 현실

수집 정보 목록

접속일시	로그인 ID	거래구분	OS언어	Web IP	VPN Nat IP	Nat IP	Client IP	MAC	우회 형태	위험등급	액션
(P)2011-11-19 12:12:10	KYG9812031	로그인	ko	115.141.144.182	112.224.2.109		192.168.100.4	00-53-45-00-00-00	vpn	심각	-
(P)2011-11-19 11:36:59	KYG9812031	로그인	ko	115.141.144.182	112.224.2.109		192.168.100.4	00-53-45-00-00-00	vpn	심각	-
(P)2011-11-19 11:14:34	KYG9812031	로그인	Korean	115.141.144.182	112.224.2.109	115.141.144.182	192.168.100.4	00-53-45-00-00-00	vpn	심각	-
(P)2011-11-14 09:38:54	KYG9812031	로그인	Korean	59.10.56.113		59.10.56.113	192.168.0.5	00-11-5B-BC-D0-37	미사용	정상	-
(P)2011-11-08 10:08:46	KYG9812031	로그인	Korean	59.10.56.113		59.10.56.113	192.168.0.5	00-11-5B-BC-D0-37	미사용	정상	-
(P)2011-11-08 09:58:25	KYG9812031	로그인	Korean	59.10.56.113		59.10.56.113	192.168.0.5	00-11-5B-BC-D0-37	미사용	정상	-
(P)2011-11-04 10:03:09	KYG9812031	로그인	Korean	59.10.56.113		59.10.56.113	192.168.0.5	00-11-5B-BC-D0-37	미사용	정상	-
(P)2011-11-03 10:54:51	KYG9812031	로그인	Korean	59.10.56.113		59.10.56.113	192.168.0.5	00-11-5B-BC-D0-37	미사용	정상	-
(P)2011-11-02 15:04:19	KYG9812031	로그인	Korean	59.10.56.113		59.10.56.113	192.168.0.5	00-11-5B-BC-D0-37	미사용	정상	-
(P)2011-11-02 14:42:37	KYG9812031	로그인	Korean	59.10.56.113		59.10.56.113	192.168.0.5	00-11-5B-BC-D0-37	미사용	정상	-
총 10 건											

- 보이스피싱 천국 : Why?
- 사고 건수 : 매년 수천 - 수만
- 피해 액수 : 매년 수백억 - 수천억
- 아무도 공신력있는 조사 / 집계 / 공표 안함 : Why?
- 부인방지 ?

금융 카르텔

- 경쟁 부재 , 눈치 작전 , 책임 회피
- 엄청난 공인인증서의 “장점”
  - 접근매체의 위조 , 변조 (전자금융거래법 제 9 조)
  - 보이스피싱은 접근매체 위조가 아니다 ?
  - 설사 위조라 하더라도 , 누출 , 누설한 고객에게 잘못이 있다 ?

정부의 책임

- 관치 보안
- 공인인증서 쓰기만 하면 만사 OK
- 서버 보안 ? Waz dat?
- PCI DSS, WebTrust ? 이건 뭥미 ?
- 자율에 맡길 역량이 “아직” 없다 ?
  - 지난 15 년간의 관치보안 치하에서 민간 역량이 안생겼다면 , 그럼 언제 생길까 ?

독소 조항

- “ 공인인증서 또는 이와 동등한 수준의 안전성이 인정되는 인증방법”
- 인증방법평가위원회
- 보안성 심의
- 감독규정 제 3 장 (전자금융거래의 안전성 확보 및 이용자 보호) 전체

개선 방향

- 관치 보안 중단 : How?
- 전자금융감독규정 제 3 장 전면 개정
- 바젤위원회의 전자금융위험관리 원칙 수용 / 반영
- 민간의 보안점검 전문 서비스 시장 활성화
- 정부 또는 금감원 '산하 위원회'가 보안기술에 대하여 심의 , 평가 , 점검 , 확인하겠다는 발상은 이제 그만
- 인증 / 전자서명에 대한 집착을 버리면 새로운 세상이 열릴 것 ==> 거래 패턴 및 내용을 종합적으로 분석하여 위험 거래 차단)

배상 책임 철저히 부과

- 정부의 편파적 개입 중단
- 기술중립성의 의미
- 공인인증서 위주로 규정된 전자금융거래법 개정 필요
  - “ 접근매체”관련 조항 삭제
  - “ 무단 이체 (unauthorized fund transfer)” 에 대한 배상책임 규정 필요
  - 미국법 , 영국법 참조
- 배상책임 안져도 된다면 , 보안 투자는 요원

이공계 천시의 제도적 구조

- 왜 ?
- 관 의존의 습성
- 자신에 대한 불신 → 관 의존 → 민간 역량 함양 및 검증 기회가 원천 봉쇄 → 민간 불신 → 관 의존
- 미래부 과장께서 공개석상에서 HTML5 “ 설교” 를 하시는 불행한 상황
- 금융위 사무관이 기술을 이해할 때까지 모두 정지