“ 한국적인 보안”의 취약성과 문제점
- 공인인증서를 중심으로 -

2013.5.23 / 이주혁

보안 ? 보안 !

- 보안은 결국 “집을 지키는 일” 전산보안도 일상적인 보안 범주에서 벗어나지 않음
  - 집을 지키는 일은 단순한 몇 가지 지침으로 해결될 수 없다 .
  - 집을 지키는 주체는 “우리 모두” 이다 .

- “ 한국적 보안”은 이 범주에서 크게 벗어나 있다 .
  - 보안 시스템은 솔루션 구매와 동치로 생각하고 있다 .
  - 시스템 설계자나 시스템 관리자가 철저한 보안적 개념을 갖고 있지 않고 , 전산보안은 외부 용역 업체가 담당하는 특수한 분야라고 생각하고 있다 .
  - 이런 까닭으로 매우 위험한 방식의 보안 시스템을 유지하고 있으면서도 , 일반적으로 보안 시스템은 “외부 전문가들이 알아서 하는 영역” 이라는 선을 긋는 경우가 많다 - 그리고 그들은 일반적으로 문제가 생겼을 때 책임을 떠넘길 “을” 이다 .

- “ 공인인증서와 동등한 수준이 인정되는 방식은 존재하지 않음”
  - KISA 의 공식적인 의견임 . 한국적 보안의 출발은 이러한 시각에서 비틀어진다 .

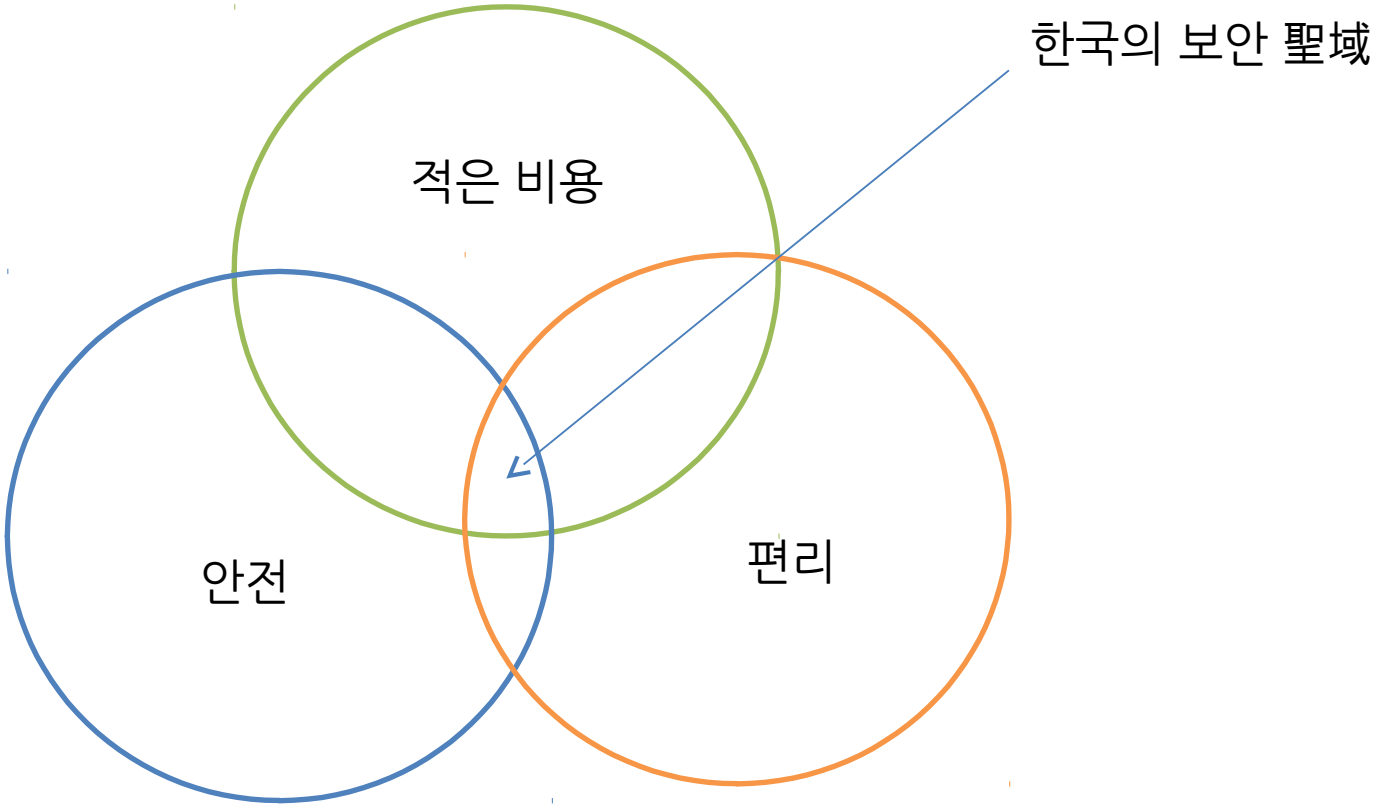
보안 문제의 아킬레스건

- 어떠한 방식의 보안을 적용해도 안전을 담보하기 어렵다 .
  - 어떠한 방식의 방범시스템을 적용해도 도둑을 막기 어려운 것과 마찬가지 .
  - 이 말은 “그러니까 보안 시스템 적용하지 말자”는 것이 아니다 .
  - 안전을 담보하기 어려우니 , 계속적인 안전을 지키고자 하는 노력이 필요하다는 것이다
  - 그래서 키보드보안이니 개인방화벽… 그런데 이것이 “노력” 이 맞음 ?

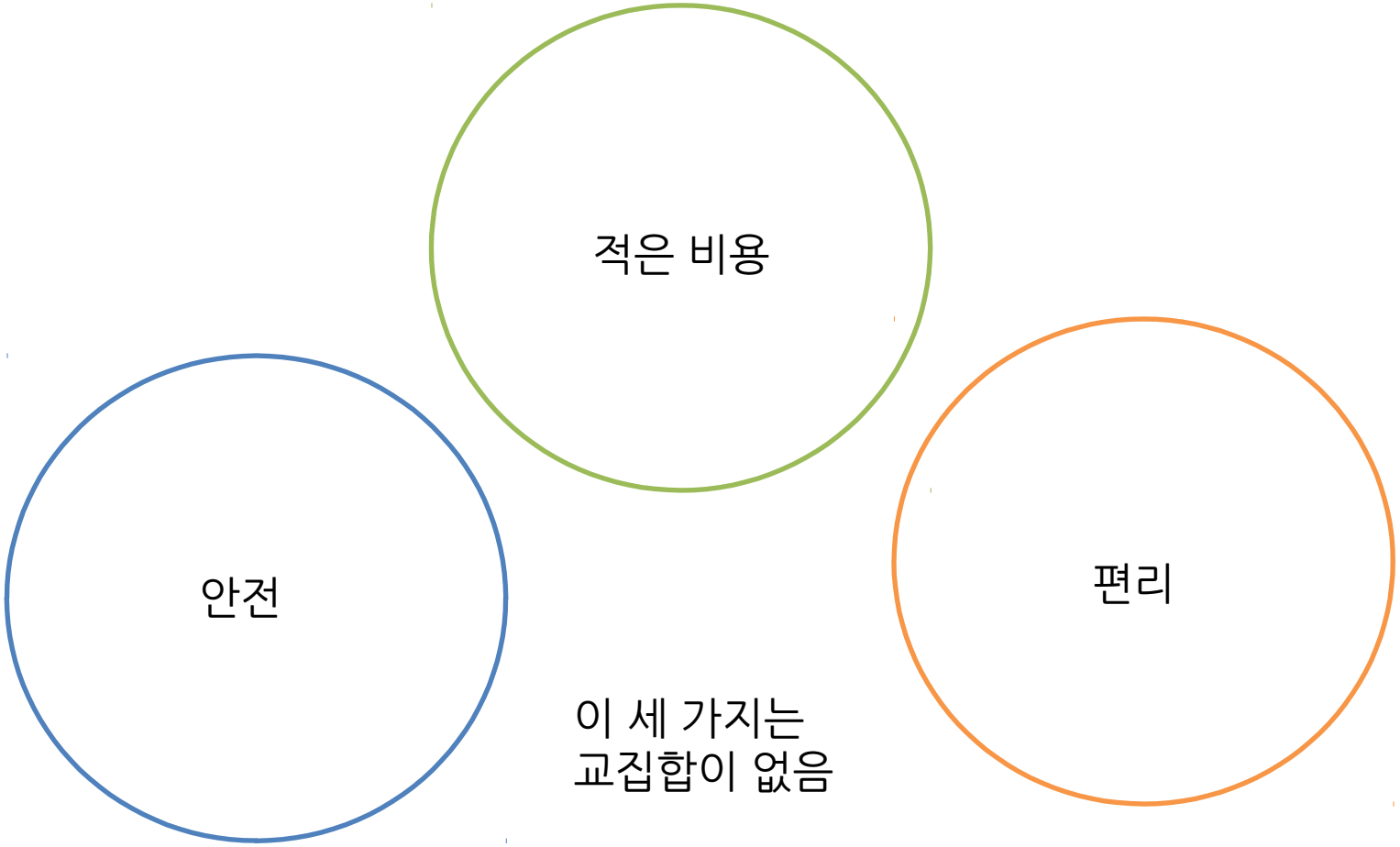
- 잘못된 관치적 접근이 벌어졌을 경우 시장이 왜곡된다 .
  - 이 말을 역시 “정부가 간섭하지 말라” 고 들으면 안 된다 .
  - 정부는 다양한 보안 활동이 지속적으로 이루어질 수 있도록 제도를 만들어야 한다 .
  - 이것을 곡해하여 정부가 특정 방법을 “인증” 하는 순간 보안체계는 무너짐 . 어차피 불안한 것이라면 정부가 인정하는 방식을 쓰려 할 것이다 . 실제로 그것의 보안성이 허약하더라도 말이다 .
  - 보안이 “모두 함께 지키는” 시스템의 안전이라는 사실까지 망각하게 되는 경우가 많다 .

한국적 보안의 특성

- 적은 비용에 , 안전하고 , 편리한 시스템을 구현 !



현실에서의 보안 문제



이 세 가지는
교집합이 없음

최강의 보안 ? 공인인증서

- 적은 비용에 : 공인인증서는 그냥 파일
  - 설사 유출되었다고 하더라도 유출된 사실을 알아내기가 매우 어려움
  - 현재까지 얼마나 많은 공인인증서가 유출되었는지조차 모름
  - 유일한 방패막은 개인 키 비밀번호인데 , 이를 무력화하려는 시도는 다양함

- 안전하고 ?
  - 근본적으로 PKI 기반 시스템이 갖고 있는 결함은 다 갖고 있음 . PKI 가 의미 없다는 것이 아니라 공인인증서는 변종 PKI 이기 때문에 , PKI 의 장점과 약점을 다 계승하고 있음 . 따라서 , 특별히 일반적인 PKI 체계에 비해서 안전하다는 말을 하기 어려움
  - 피싱 공격으로 인해 무력화될 가능성이 매우 높음 .

- 편리한 ?
  - 올인원 솔루션을 도입하기 위해 사용자의 컴퓨터에 “관리자” 권한으로 파일들을 마구 설치함 .
  - 그럼에도 불구하고 스마트폰은 루팅하면 금융거래 못 하게 함 . 이 두 사실은 상호 모순

현실에서의 공인인증서

- “국제 공인”으로 인정받지 못함 “한국만이 사용하는 방식”
  - 별도의 플러그인, 애플리케이션을 항상 사용해야 됨.
  - 별도의 플러그인, 애플리케이션을 동작시키면서 OS 보안을 무력화시켜야 한다.
  - 사실 OS의 보안은 강화되어 왔는데 한국적 보안은 계속 이를 낮추라고 요구한다.

- 과도한 “보안 프로그램의 백화점”
  - 사용자 입장에서 무엇인지도 모르는 프로그램들을 잔뜩 설치해야 한다.
  - 심지어는 웹 브라우저나 일반 통신의 기본적인 기능들도 별도의 프로그램을 써야 한다고 하며 “보안 프로그램”을 설치한다.
  - 이러한 프로그램은 매우 좋지 않은 사용자 경험으로 유도한다.
  - “보안을 위해 당신의 PC 보안을 일단 무력화하세요”
  - 이런 행위들은 해커들이 그대로 따라함, “귀하에게 보안 메일로 이번달 통신비를 알려드립니다” - 보낸 이가 해커가 아닌지 확인할 수 있는 방법이 있는가?

보안은 불편함으로부터 시작

- “편리한 보안”은 존재하지 않음
  - 일단 불편함. 그러나 한국적 보안은 이 불편함을 오해하고 있음
  - 보안을 위해 보안을 해제하고 ActiveX 를 관리자 권한으로 설치하고, 컴퓨터를 재부팅하고 종종 프로그램이 충돌하여 프로세스가 중단되는 것이 “보안을 위한 불편함” 이라고 생각함.
  - 그럼에도 불구하고, 올인원 프로그램으로 제공하니 얼마나 편리하냐고 강조함.
  - 사실 현재까지 한국적 보안은 무수히 많은 모순점들의 집합이 되어 있음.

- 진정 “불편한 보안”의 문제 - 한국이니까 발생하는 문제
  - “멋” 이 없다.
  - 전산보안임에도 보안 솔루션이 거의 없다.
  - 말로 먹고 사는 컨설턴트들에게 아까운 회사 비용을 지출해야 한다. 그리고 보안을 책임질 “을” 이 없다.
  - 소프트웨어를 전공하지 않은 이들도 프로세스를 이해할 수 있다. 극단적으로 은행장도 프로세스를 이해할 수 있다. (사기업에서 회장이 이해하는 프로세스와 이해하지 못하는 프로세스는 담당자의 피로도 차이가 매우 크다)

불편한 보안의 적용 예

- 인터넷 뱅킹 사고는 의도하지 않은 계좌 이체로 발생한다.
  - 한국적 해결책 : 일단 ActiveX 깔고, 공인인증서로 전자서명하면서 고객의 PC 정보도 수집하고, 전자서명은 인감과 같으니까 부인하지 못한다는 말로 겁준다. 그러나, 공인인증서가 생각보다 피싱에 약하니 보안카드나 OTP를 같이 쓰게 한다.

  - 불편한 보안 방식의 해결책 일부
  - 사전에 이체 가능하게 은행에 나와서 이체 대상 계좌를 등록하게 한다. 대부분의 고객들이 이체하는 계좌는 크게 많지 않다.
  - 이체 가능 계좌의 변동이 있을 경우 고객에게 통지한다.
  - 단, 고객의 편의를 위해 수익자가 명백한 이체거래(세금, 공과금 등)는 굳이 이체 대상 계좌를 등록하지 않아도 지불 가능하게 한다.
  - 고객의 동의 하에, 고객이 설정한 일정 금액 이하의 소액의 경우는 이체 대상 계좌에 속하지 않더라도 이체 가능하게 한다. 일정 금액 이하의 결정은 고객에게 충분히 정보 제공 후, 소액으로만 하도록 권고한다.
  - 과거 금융기록이 존재하지 않는 사람이나, 한때 신용상에 문제가 있는 사람이 첫 거래를 하는 경우 이체추심을 한다. 특히 일정 금액 이상의 현금이 불특정 다수로부터 유입될 경우 사고 계좌로 의심해 볼 필요가 있다.
  - 소비자를 대상으로 하는 사업체라 불특정 다수로부터 계좌 이체가 있는 경우, 해당 사업체의 신용을 평가하여 상한선을 두어 이를 허용한다. 가급적 불특정 다수를 대상으로 한 사업의 목적이라면 체크카드나 신용카드를 사용하도록 유도한다.
  - 기술적 보안 (OTP, 보안 카드, TLS 등)은 건전한 보안 통신을 유도하게 하는 도움 매체로 쓴다.

기술적 보안 , 사회적 보안

다케이코 이노우에 , 슬램덩크 中

사회적 프로세스가 기술 외적으로 완성된 상황에서 , 기술은 그 프로세스의 완성도를 높여 주는 역할을 수행한다 .

예를 들어 , SSL/TLS 라는 기술은 네트워크에서 누가 내가 통신하는 데이터를 훔쳐보지 못하도록 하는 기능을 하고 있다 . 그러나 , 나는 해커와 SSL/TLS 로 암호화 통신을 잘 수행하는 엉뚱한 상황을 맞을 수도 있다 .

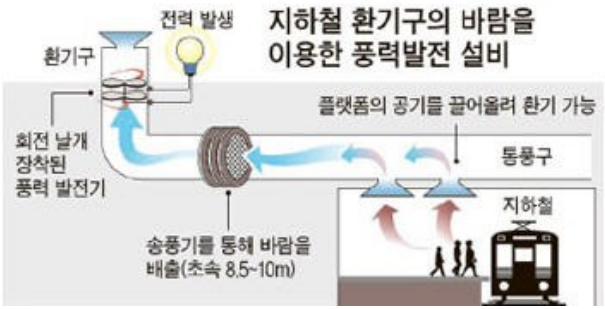
내가 통신하고자 하는 상대방이 해커가 아니라는 사실은 사회적으로 인지해야 한다 . 기술은 그 전제가 만족된 이후 , 전제를 충족하는 아주 좋은 솔루션을 제공할 것이다 .

한국적 보안은 , 내가 통신하고자 하는 상대방을 기술적으로 누구인지 맞추기 게임이었다 . 이 게임은 언제나 해커의 승리로 끝나게 된다 .

한국적 보안에서 강백호는 “왼손이 모든 것을 다 하는” 상태이다 .

환상에서 탈피 I

- 네트워크 저쪽에서 날아온 패킷 하나만으로 그가 누구인지 맞출 수 있는 사람은
  - 영적 존재다. 우리는 그를 신으로 받들어야 한다.
  - 하지만, 한국에서는 과학과 믿음의 영역이 구분되지 않는다.



2008 년 열역학 2 법칙마저 토론의 장으로 끌고 온
서울시 고객감동 창의경영 사례 발표회

- 깔끔한 솔루션 하나로 완벽한 보안시스템을 구축한다면 그보다 좋을 수 없다.
  - 하지만, 현실적으로 불가능하다. 인정하자.
  - 그렇기 때문에 매우 다양한 보안 방법을 연구하는 것이다. 하지만, 공인인증서 강제는 보안 시스템의 하향 평준화를 야기할 수 있다.

환상에서 탈피 II

- 어린 백성들이 뱅킹하고자 할 바 있어도 악성코드때문에 그 뜻을 펴지 못하니
  - 그래서 보안 솔루션, 방화벽, 키보드 보안, 기타 다각도의 정체 모를 프로그램을 설치하게 하면, 백성의 PC는 순수의 극치로 돌아갈 것으로 생각한다.
  - 그러나, 이런 방식으로는 거래 건전성을 지키지 못한다. 오히려, 악성코드가 엄청나게 상존해 있는 상황에서 해커들을 허탈하게 만드는 정책이 훨씬 유효하다.
  - 뱅킹 해킹했는데, 이체가능계좌가 없을 때 해커가 갖는 생각은?
  - 해커를 허탈하게 하는 정책적 측면은 무척이나 많다.
  - 이러한 방식은 전자서명을 거래증빙으로 고집하는 경우에 대한 사회적 해결책도 될 수 있다.

- 무조건 막아 막으면 돼. 전세계의 모든 악성코드를 다 막을 거야.
  - 그렇게 보안성이 좋다는 한국의 언론, 은행이 3월달에 어떤 상황을 맞았는지.
  - KISA와 모 음란 사이트의 숨바꼭질은 10년째 계속되고 있다.
  - 사용자의 컴퓨터의 청정을 증명하라 하지 말고, 거래의 건전성을 확립해 달라. 도청되는 전화기로도 민원서류를 신청할 수 있는 것이 올바른 프로세스다.

마치며

- 정부가 할 일은 해야 한다 .
  - 금융사 내부 시스템에 대한 정책적 보안 권고를 지속적으로 해야 한다 .
  - 현금인출기 지연인출과 같은 경우 매우 잘 한 정책이다 . 이런 정책은 더욱 정교하고 철저하게 만들어 내야 한다 .
- 정부가 하지 말아야 할 일은 안 해야 한다 .
  - 기술적 가이드라인은 제시하되 , 특정 솔루션을 “인증” 하는 행위는 안 된다 .
  - 기술적 솔루션을 안전하다고 홍보해서는 안 된다 . 기술 과신으로 치닫는다 .
  - 정부의 보안성 심사나 가이드라인은 최소의 규정으로 가야 하며 , 그것이 “가중처벌”의 기준이 아닌 면책의 기준이 되어서는 더욱 안 된다 .
- 인정할 부분은 인정해야 한다 .
  - 산업화 시대는 정부가 대기업 , 학계 , 연구소를 이끄는 선단의 맨 앞자리 역할을 했다 .
  - 정보화 시대는 산업계가 가장 빠르고 , 연구소 , 학계 , 정부 순으로 “느리다” 한국 정부가 잘못되었다는 것이 아니라 , 전 세계 어디도 “정부”가 느릴 수밖에 없는 구조다 .