개인정보보안의 기초

(The Fundamental of Personal Information Security)

본 문서 의 내용은 원서 "How Personal & Internet Security Work" 의 내용 중 일부를 바탕으로 재구성되었습니다.

문봉교 (bkmoon@dongguk.edu)

유비쿼터스 컴퓨팅 및 보안 (UCS) 연구실

동국대학교 컴퓨터공학과

2011년 2월 10일

1장 신원도용 어떻게 이루어지나?

최근에 개인정보보안의 가장 잘 알려진 위협은 누군가의 사적인 정보를 훔쳐서 불법으로 사용하는 신원도용이다. 도용된 정보는 다양한 방법으로 사용되는데, 가장 단순한 예는 누군가의 신용카드나 은행계좌를 훔쳐서 사용하는 것이다. 하지만 이런 정보는 은행계좌를 새로 개설하거나 신용카드를 새로 발급받고 피해자의 이름으로 은행에서 대출을 받는데 사용될 수 있다. 이로 인해 피해자는 이를 회복하느라 몇 년을 고생하지만 범인은 흔히 처벌을 피해 간다. 신원도용은 또한 테러리스트나 특정국가내의 합법적 신원을 가지길 원하는 불법이민자들에게 이용될 수 있다. 최근 신원도용을 원하는 사람이 많아지면서 불법적으로 취득된 개인정보거래는 큰 돈벌이가 되고 있다.

- **그러면 개인신원정보가 어떻게 도난 당하는가?**

1. 신원도용이란 아주 광범위해서 신용카드를 훔치는 것에서부터 누군가의 운전면허번호와 주민등록번호를 가지고 다른 사람인 척 하는 것까지 많은 범죄행위가 이에 해당한다.

2. 신원도용의 일반적인 형태는 신용카드 도용인데, 신용카드 도용은 해커가 카드시스템에 침입해 정보를 유출하거나 신용카드전표 쓰레기 수납기를 뒤지는 등 많은 방법이 동원된다.

3. 신원도용은 일반적으로 여러가지 인터넷 사기로 이어진다. 예를들어 인터넷 피싱(Phishing)은 이메일을 통해 특정 웹페이지에 로그인하도록 유인하여 개인정보를 입력하게 한다. 이러한 정보중에는 보통 주민등록번호, 신용카드번호, 엄마의 이름 등이 들어간다.

4. 스파이웨어, 키로거(keylogger), 트로이목마 같은 프로그램이 컴퓨터에 몰래 설치되어 사용자의 개인정보를 빼내어 해커에게 보내거나 또는 사용자들이 입력하는 모든 키를 해커가 직접 보도록 할 수도 있다.

5. 일부 범죄자들은 물리적 신원도용이라는 아주 구식의 방법으로 신원정보를 훔쳐낸다. 그들은 지갑이나 핸드백을 훔쳐서 운

전면허증, 신용카드 등 내부에 있는 다른 신원정보를 사용한다.

6. 일반적으로 가장 흔한 신원도용방법은 신용회복사기이다. 사기꾼들은 해당개인의 신용불량을 회복시켜주는 권리청구서비스로 가장한다. 신용을 회복하기 위해 주민등록번호, 엄마의 이름, 생년월일, 신용카드번호, 은행계좌번호 등등의 개인의 모든 신원정보가 필요하다고 얘기한다.

7. 통계적으로 개인정보를 훔치는 대부분의 신용도용은 가족, 친구, 지인, 직장동료가 저지르는 경우가 많다.

8. 일부 범죄자들은 관리가 허술한 우편함을 노린다. 그들은 개인우편물을 훔쳐서 신용카드내역, 계좌정보, 고지서 등등을 찾아내어 여러 용도로 이를 사용한다. 예를들어, 범죄자들은 많은 관공서에서 이러한 고지서만 제시하면 따로 신원증명을 하지 않는다는 점을 잘 이용한다.

- **범죄자들은 도난 신원정보를 어떻게 사용하나?**

1. 범죄자들은 신용카드와 은행관련 정보를 빼내어 은행계좌에서 잔액을 모두 인출하거나 또는 훔친 신원정보를 사용하여 새로 은행계좌를 개설하고 신용카드를 만들고 금융기관으로부터 대출을 받을 수 있다. 범죄자는 자신의 실체가 드러나지 않을 것으로 생각하고 부도수표를 발행하거나 신용카드사용 대금을 갚지 않거나 또는 대출상환을 하지 않을 것이다.

2. 또한 훔친 신원정보를 거래하는 암시장이 성행하고 있다. 많은 개인신원정보 도둑들은 그 정보를 자신이 사용하지 않고 다른 사람에게 돈을 받고 팔아버린다. 일부 경우는 그저 다른 사람에게 개인적으로 팔기도 하지만 이윤추구를 위해 다른 사람에게 되파는 일을 하는 러시아 마피아 같은 갱단에게 팔기도 한다.

3. 훔친 신용정보는 돈세탁 같은 다양한 범죄행위에 사용되기도 한다. 돈세탁기법에는 누군가 주민등록번호 같은 훔친 신원정보를 사용하여 은행계좌를 개설한다. 돈은 그 계좌를 통해 세탁된다.

4. 훔친 신용정보는 불법이민자나 자신의 실제 신원을 감추고 특정국가의 신원으로 가장하려는 테러리스트들이 사용할 수 있다. 불법이민자나 테러리스트들은 다른 사람의 이름, 주민번호, 엄마의 이름 등의 신원정보를 부여 받게 된다. 불법이민자들이 이를 이용해 적법한 신원을 취득하여 합법적인 운전면허증을 받고 직업을 구하게 된다.

- **신원도용으로부터 보호하는 방법**

1. 피싱 유인공격에 응답해서는 안된다. 금융기관은 이메일로 자신의 계정에 로그인하라는 메시지를 보내지 않기 때문에 그런 이메일을 절대 클릭해서는 안된다. 대신 금융기관에 전화해서 문의하거나 이메일에 링크된 페이지가 아닌 공식 홈페이지에서 로그인해야 한다. 또한 불필요하게 주민번호를 노출해서는 안된다. 만일 웹사이트에서 요청한다면 해당금융기관에 한해서만 제공해야 한다.

2. 신용카드명세, 은행계좌정보, 주민등록번호가 들어있는 문서라면 그냥 버리지 말고 절쇄기에 넣어야 한다.

3. 여권, 주민등록증, 운전면허증을 지갑이나 핸드백에 휴대하지 말고 안전한 곳에 두어야 한다

4. 매달 신용카드 명세서와 은행계좌를 면밀히 살펴보고 의심이 가는 명세가 있는지 확인해야 한다. 온라인 사용내역을 확인할 수 있다면 매주 확인하는 것이 좋다. 온라인으로 신용카드를 사용할때는 암호를 사용하는 안전한 사이트에서만 사용해야 한다.

5. 스파이웨어 탐지 및 바이러스 백신 소프트웨어를 설치하고 사용해야 한다. 이것이 스파이웨어, 키로거, 트로이목마로부터 보호해준다.

2장 신용카드 보안은 안전한가?

많은 사람들은 지갑이나 가방을 잃어버렸을 때 또는 전화로 신용카드 정보를 알려주었을 때 신용카드가 도용되지 않을까 우려하고 있지만 실제로 발생한 대부분의 도용은 금융기관에 몰래 침입한 해커들이 신용카드번호를 훔친 경우이다. 또한 신용카드번호를 훔친 해커뿐만 아니라 금융회사에 근무하는 내부관계자들이 신용카드를 도용하는 사례가 많다. 한편 인터넷이 신용카드도용과 훔친 신용카드를 판매하는 중심지가 되고 있다. E-메일을 통해 신용카드정보를 제공하게 만드는 피싱(phishing)이라는 수법은 신용카드도용의 주된 방법중 하나이다.

- **신용카드정보의 유출**

1. 신용카드정보가 유출되는 가장 일반적인 경우는 가장 단순한 방법인 물리적 도난이다. 도둑이 신용카드가 든 지갑이나 핸드백을 훔치거나 카드만 훔치기도 한다.

2. 도둑은 명세서 쓰레기통을 뒤져서 취소된 거래내역에 대한 명세를 찾아낸다. 이 경우 신용카드는 없더라도 신용카드번호와 소지자의 이름 등을 알아내어 전화나 인터넷으로 신용카드를 사용할 수도 있다.

3. 서비스산업에 종사하는 사람들은 전화상으로 신용카드번호가 건네질 때 신용카드정보를 도용할 수 있다. 예를 들어, 호텔예약이나 음식점에서 당신의 신용카드정보를 복사하여 사용할 수 있다.

4. 인터넷은 신용카드정보를 훔치는 주요방법 중 한 곳이 되어버렸다. 사기꾼들은 물건을 파는 것처럼 가짜 판매 사이트를 설치하고 카드정보가 입력되면 그 정보를 도용한다.

5. 카드정보를 가로채기 위해 피싱사기가 많이 사용되었다. 피싱사기에서는 금융기관이나 카드회사에서 보내는 것처럼 가짜 이메일을 보내서 웹사이트에 로그인해서 카드정보를 입력하게 한다. 이런 사이트는 진짜처럼 보이도록 디자인 되었지만 실제

로는 사기꾼들은 카드정보를 훔치기 위해서 만든 가짜 사이트이다.

6. 신용카드 도용의 대부분은 실제로 카드를 훔친다기보다 카드정보를 가지고 있는 시스템을 해커가 공격하여 침입함으로써 이루어진다. 공격을 당해서 유출된 카드정보는 수십만에 이르고 어떤 경우는 수천만에 달한다. 일부는 회사내의 종사자가 카드정보를 훔치거나 범죄에 연루되기도 한다. 예를들어, Equifax, Experian, TransUnion 같은 신용조회기관으로부터 은행에 개인정보를 제공하는 Teledata Communications라는 회사의 내부관계자들이 자사의 데이타베이스에서 수만개의 카드정보를 훔친 경우도 있다. 사상 최대의 사건인 CardSystem Soliution이라는 회사에 해커가 침입하여 4천만개의 카드정보를 훔친 경우도 있다.

7. 신용카드정보를 가진 회사가 데이터를 부주의하게 다루다가 카드정보유출이 일어난 경우도 있다. 예를들어, 어떤회사는 개인의 신용카드정보를 저장해놓은 CD를 분실한 경우도 있다. Boston Globe는 신용카드정보를 다룰 자격이 없는 것으로 유죄 판결을 받은 적이 있다. 이 회사는 24만명의 가입자들의 카드정보를 출력하여 이걸로 운수업자와 판매상에게 배포된 신문을 포장하는데 사용했다. 카드정보를 담은 출력물은 390개의 운수업자와 2000개의 판매상에게 고스란히 보내졌다.

- **금융회사는 신용카드 부정사용을 어떻게 탐지하는가?**

1. 신용카드회사는 해마다 카드의 부정사용으로 인해 약 10억달러의 손실을 입고 있어서 잠재적 부정행위를 탐지하기 위해 자동화 시스템을 설치했다. 이 시스템은 고성능 컴퓨터에서 실행되는 인공지능(AI) 프로그램을 사용하는데, 종종 신경망으로 언급되는 이 시스템은 문제를 처리하고 해결하는데 사용되는 강력한 처리기들을 직렬로 연결한 거대한 집합체로 볼 수있다.

2. 많은 종류의 AI시스템들이 부정사용을 탐지해내는데, 이 시스템은 개별거래내역들을 전체 지출패턴과 비교하고, 이상하거나 변칙적으로 보이는 거래나 패턴을 찾아낸다. 가장 복잡한 일부 시스템들은 개별 신용카드 사용자의 지출 프로파일을 생성하

고 이 프로파일의 내용에 맞지 않는 거래들을 비교한다.

3. 개인의 모든 카드거래내역이 시스템에 자동으로 전달되어 각 거래는 개인별 프로파일과 비교되고 거래가 부정사용일 가능성을 측정한 수치가 매겨진다.

4. 낮은 수치를 보이는 대부분의 거래는 아무런 조치도 취해지지 않는다.

5. 일부 거래는 내역이 의심스럽다는 측정수치를 보이지만, 즉각적으로 아무런 조치가 취해지지 않고 비슷한 수치가 여러 번 나타나는 거래가 있으면 회사에서 조치를 취하게 된다.

6. 잠재적 부정사용을 나타내는 측정수치를 보이는 거래내역이 있으면 카드회사는 개인에게 연락하여 확인한다. 문제가 없으면 넘어가고, 만일 개인에게 연락할 수 없거나 개인이 부정사용 거래가 있다고 알려오면 그 카드는 즉시 취소되고 더 이상 사용할 수 없게 된다,

- **암시장 신용카드거래 추적**

1. 대부분의 도난신용카드는 훔친 범인이 사용하지 않고 방대한 인터넷 신용카드 암시장으로 들어간다. 도둑이 피싱사기나 금융기관을 해킹해서 카드번호가 도난당하면 바로 카드사용이 추적될 수 있다.

2. 카드는 갱단에 무더기로 팔리는데 주로 러시아 마피아가 카드번호를 사들이는데 상당히 개입되어 있다.

3. 갱단은 은밀한 회원제 웹사이트를 만들어놓고 거기다 신용카드번호를 올려놓는다. 일부 사이트는 가입비를 내야 하는 경우도 있다.

4. 이 사이트에는 수천개의 카드가 팔리고 있는데 각 카드는 잠재가치에 따라 가격이 매겨진다. 예를들어, 훔친 카드중에 청구주소를 변경할 수 있는 PIN번호가 있는 *Change of billing*을 나타내는 *cob*카드가 가장 가치가 있다. 일부 사이트에서

Discover Card cobs는 50달러에 팔리고 있는 반면, 일반적으로 사용제한이 없는 American Express cobs는 85달러에 팔린다.

5. 일부 사이트는 eBay처럼 운영하고 개인 판매자들이 매물로 내놓은 카드를 홍보한다. eBay에서처럼 팔려고 내놓은 카드들은 접수가 매겨진다.

6. 누군가 카드를 사고 싶으면 인스턴트 메신저를 이용해 대화를 할 수 있는데, 사람들이 익명으로 등록을 하기 때문에 주로 ICQ를 사용한다. 결재는 주로 e-gold사가 발행한 전자화폐인 e-gold가 사용된다. (Nevis의 카리브해 섬에 세워진 회사). E-gold는 거래에 관여한 사람들이 추적될 수 없도록 완벽한 익명성이 유지된다.

7. 불법카드를 구매한 사람은 카드를 실제 사용할 수 있는데 Cob의 경우 카드를 구매한 사람이 청구지 주소를 자신의 주소로 변경하고 구매한 물건을 자신의 주소로 받을 수 있다. 일부 경우, 자신의 실제주소가 노출되지 않도록 근처의 빈 아파트 같은 안전한 곳으로 주소를 바꾸고 물건이 언제 배달되는지 지켜보기도 한다.

3장 데이터 마이닝(data mining)의 위험성

데이터 마이닝은 방대한 양의 데이터를 검사하기 위해서 강력한 데이터 분석도구를 사용한다. 그리고 이를 통해 전에는 보이지 않거나 알려지지 않았던 새로운 패턴이나 관계를 찾아낸다. 데이터 마이닝은 또한 어두운 면을 가지고 있다. 즉, 사람들의 일상생활을 엿보는데 사용될 수 있으며 사람들의 위치추적 같은 상세한 사생활 정보를 만들어 낼 수도 있다. 이미 강력한 힘을 가지고 있는 정부가 데이터 마이닝을 사용하여 사람들의 사생활 정보를 만들어낸다면 더 위험해질 수도 있다.

- **데이터 마이닝의 원리**

1. 데이터 캐는 사람(마이너)은 우선 데이터를 수집한다. 가치있는 데이터가 수집되지 않으면 별로 의미가 없어지기 때문에 이 단계는 데이터 마이닝에서 아주 중요하며 시간이 많이 걸리는 작업이다. 데이터는 보통 상당히 많은 수의 데이터베이스에 저장되어 있다. 데이터가 단지 한 회사에서 채취된다면 정보수집에 사용된 데이터베이스의 수는 상대적으로 적어지게 된다. 하지만, 만일 연방정부가 복수의 연방 데이터베이스, 인터넷, 수많은 상업 데이터베이스로부터 정보를 수집한다면 엄청난 수의 데이타베이스를 뒤져야 한다.

2. 데이터가 수집되고 나면 잘 정리해야 한다. 많은 데이터베이스와 다양한 소스로부터 데이터를 수집할 경우 대개 데이터는 중복되거나 일부가 빠져있거나 부정확한 내용이 포함될 수 있다. 인간의 지시에 따라 미리 자동화된 프로그램이 이러한 데이타를 잘 정리한다.

3. 소프트웨어로 그 데이터를 검색해서 원하는 정보를 캐낼 수 있도록 데이터는 공통의 표준형태로 변환되어야 한다.

4. 데이터가 준비되고 변환되면, 해당 소프트웨어는 정보캐기를 시작한다. 성능이 뛰어날수록 정해진 시간내에 더 많은 데이터를 뒤져볼 수 있기 때문에 고성능 컴퓨터가 사용된다. 실제로 특정한 목적에 꼭 맞는 다양한 종류의 데이터마이닝 소프트웨

어와 기술이 존재한다. 숨겨진 관계를 찾아내는데 마이닝 기법을 쓰이는데 주로 Regression과 classification이라는 기술이 사용된다. 또한 명확하게 드러나지 않는 어떤 흐름을 찾는데도 사용될 수 있다.

5. 데이터 마이닝을 지원하기 위해 AI의 신경망(뉴럴네트워크) 기술이 사용될 수 있는데 신경망은 복잡한 문제를 풀기 위해 함께 동작하는 수많은 컴퓨터와 처리기들의 거대한 네트워크이다. 네트워크를 통해 신경망에 있는 각 컴퓨터마다 탐색할 특정 변수가 할당되어 대용량의 데이터를 탐색할 수 있다.

6. 일부 데이터마이닝 소프트웨어는 3차원 시각화 기술을 사용하여 데이타들 사이의 관계를 시각적으로 보여준다. 즉, 검사하는 정보에 대한 3차원 그래프를 만들어내어 보다 쉽게 데이터들간의 관련성을 알아낼 수 있다.

- **데이터 마이닝의 위험성**

1. 데이터 마이닝을 수행하는 대기업은 사람들에 대한 엄청난 정보를 수집한다. 주민번호부터 카드번호, 지출 패턴, 여행 습관, 개인금융정보에 이르기까지의 모든 정보를 수집하여 사적인 사업자에 판매를 한다. 사람들의 사생활이 판매되는 셈이다.

2. 데이터 마이닝 회사로부터 시스템을 해킹하거나 물리적으로 디스크를 훔쳐내어 정보를 유출시킬 수 있다. 이런 일이 벌어지면, 수백만명의 사람들이 신원도용의 위험에 빠지게 된다. 예를들어, 2005년 미국의 데이터 마이닝 거대기업인 ChoicePoint로부터 145,000명의 신원정보가 유출되었다. 유출된 정보엔 주민번호, 주소 및 다른 개인정보가 포함되어 있었다.

3. 미연방정부는 많은 데이터 마이닝 프로젝트를 수행하는데, 이중 많은 부분이 2001년 9월11일 세계무역센터와 펜타곤 공격이후 시작된 것이다. 비평가들은 이러한 프로젝트들 대부분이 사생활 침해의 우려가 있다고 걱정하고 있다. 미정부의 Total information awareness(TIA) 프로젝트는 수많은 정부기관, 개인 자료, 도서관 등등 다양한 데이터 자료로부터 정

보를 수집하여 많은 국민들의 상세한 프로파일을 만들어낼 수 있다.

4. 개인정보의 대규모 사용은 정부에 의해 의도적으로 잘못 다뤄질 수 있다는 우려가 제기되고 있다. 예를들어, 현정부를 비판하는 세력을 찾아내고 이들에 제재를 가하는데 사용될 수도 있다.

5. 또 다른 염려는 잘못된 판정의 문제이다. 예를들어, 플로리다에서 테러리스트 찾느라 승객들을 검색하는 시스템은 명확히 정도가 지나친 숫자인 120,000명을 통계적으로 테러리스트일 가능성이 있다고 표시했다. 일단 누군가 잠재적 테러리스트로 표시되면, 법적으로 추적될 수 있고 항공여행이 금지되고 직장에서 해고될 수도 있다.

6. 최근 불거진 페이스북 개인정보보안 취약점의 예로서 2010년 MIT 컴퓨터공학과 학부생 프로젝트가 대학윤리위원회에 회부된 사건을 들 수 있다. 그 내용은 페이스북에 공개한 개인의 인맥 및 개인정보에 '데이타 마이닝' 기법을 적용해 특정한 사람이 게이(동성애자)인지 아닌지를 판별해내는 일종의 공식을 만들어냈기 때문이다. 결국 기존 공개정보로부터 개인이 공개할 의도가 전혀 없었던 사생활 정보가 유출되어 공개되는 상황이 가능해진다는 것이다.

4장 직장감시와 사생활침해

미국내 직장감시는 상당히 일반적이며, 날마다 더 많이 이루어지고 있다. 고용주들은 많은 새로운 기술들을 이용하여 고용인들을 감시하고 있지만, 특히 고용인들의 컴퓨터와 인터넷을 모니터하고 있다. 즉, 고용인들이 일과 관련없는 웹사이트에 많은 시간을 소비하고 있지는 않는지 우려하고 있다.

- **직장내 감시가 어떻게 이루어지나?**

1. 미국내 일부 직장들은 Andrew Schulman이 작성한 privacy foundation study에 따라 연속적인 감시시스템을 설치하고 있다. 이런 종류의 감시를 수행하는 회사는 직장감시용 장비를 갖춘 중앙의 보안부서를 가지고 있다.

2. 숨겨진 폐쇄회로 카메라는 근로자들이 회사에 들어오고 나갈 때 마다 감시를 한다. 이 카메라는 사내 네트워크를 통해 컴퓨터나 다른 감시시스템에 연결되어있다. 그래서 보안 스탭들은 여러장소를 한번에 감시하고 녹화된 영상은 테이프나 컴퓨터에 저장된다. 일부의 경우는 작은 카메라로 근로자들의 컴퓨터 화면을 비추고 개개인이 어떤 작업을 하고 있는지 추적하기도 한다. 그러나, 컴퓨터를 이용하면 또 다른 방법으로도 훨씬 더 정확하게 감시할 수 있기 때문에 이런 방법이 일반적이지는 않다.

3. 고용주들은 불법으로 근로자들의 전화를 도청해서 모든 대화를 엿들을 수도 있다. 미국내에서 개인이 사적으로 대화를 도청하는 것은 법으로 금지되어 있지만, 1986년 ECPA는 일에 관계된 전화는 고용주가 들을 수 있도록 허용하고 있다. 직장내에서 이루어지는 모든 전화는 일에 관계된 것이라는데 논쟁의 여지가 있기 때문에 실질적으로 모든 전화가 도청 대상이 될 수 있다. ACLU는 해마다 미국내에서 대략 4억개의 통화가 고용주에 의해 도청되고 있다고 추정하고 있다.

4. 일부 고용주들은 회사차량에 GPS와 다른 추적장치를 달아서

회사차량을 사용하는 고용인들이 움직임을 추적하기도 한다 - 이 기술은 단지 차량의 위치를 알려주는 것 이상이다. 이것은 차량의 속도, 이동시간, 연료 소비량, 이동경로와 같은 정보뿐만 아니라 차량의 서스펜션에 센서장비를 부착해서 화물이 어디에서 실리고 내려지는지도 알 수 있다. 예를들어, 이것은 도난의 징표가 될 수 있는데 화물이 지정된 곳이 아닌곳에서 내려지는지를 알아낼 수 있다.

5. 대부분의 사람들은 일반적으로 휴대폰을 사용할 때 사용자의 위치와 움직임을 추적될 수 있다는 것을 깨닫지 못하고 있다. 고용주들은 이러한 정보를 사용해서 사외근무를 하는 고용인의 움직임을 추적할 수도 있다.

6. 벳지와 ID 태크도 직장내 고용인들의 위치를 추적하는데 사용될 수 있다. ID 카드는 약 15초마다 적외선 신호를 보내고 사무실에 내장된 센서들이 이 정보를 읽어서 고용인들의 움직임을 알리게 된다.

7. 아마도 가장 일반적인 직장내 감시는 고용인이 사용하는 인터넷과 컴퓨터 사용을 감시하는 것이다..

- **고용주는 어떻게 고용인의 인터넷사용을 감시하는가?**

1. 회사가 직장인들의 인터넷 사용을 감시하는 가장 흔한 방법중의 하나는 패킷 스니퍼(packet sniffers)를 사용하는 것이다. 패킷 스니퍼는 네트워크를 통해 흘러다니는 모든 데이터 패킷을 검사하고 로그파일로 저장할 수 있는 소프트웨어이다. 필터없는 스니퍼는 모든 패킷을 로그에 저장하지만, 필터를 사용한 스니퍼는 특정 패킷만을 뽑아서 저장한다. 예를들어, 특정 웹사이트로부터 네트워크로 보내지는 패킷들을 걸러내어 저장할 수 있다.

2. 패킷 스니퍼가 패킷을 로그파일에 저장한 후에 기술지원 스태프는 log같은 특정 소프트웨어를 사용하여 로그파일을 검사함으로써 방문한 페이지, 주고 받은 메신저 메시지, 고용인들이 써놓은 블로그 내용을 포함하여 고용인(직장인)의 인터넷 사용 행위를 알기 쉽게 정리해 낼 수있다.

3. Keystroke logger나 Keylogger 같은 보다 교활한 소프트웨어는 고용인들이 알지 못하는 사이에 몰래 컴퓨터에 Keylogger를 설치해 놓을 수있다.

4. 이 소프트웨어가 컴퓨터상에 설치되면 그 컴퓨터에서 입력된 모든 키의 내용을 특정한 사람에게 보내거나 특정한 로그로 저장할 수 있다. 즉, 모든 키입력이 기록되어 인터넷 사용뿐 아니라 모든 컴퓨팅 활동이 기록될 수 있다. 예를들어, Keylogger는 컴퓨터상에서 작성된 모든 문서의 내용을 그대로 기록할 수도 있다.

5. 고용주들은 또한 고용인의 이메일 사용을 감시할 수 있다. 회사서버를 통해 드나드는 모든 이메일을 저장하고 기록한다. 고용주들이 불법적으로 모든 고용인의 이메일을 볼 수도 있다.

5장 휴대폰이 해킹될 수 있을까?

휴대폰이 점점 복잡해지고 강력해지면서 바이러스나 해커의 공격에 점점 더 취약해지게 되었다. 휴대폰은 그 안에 개인정보를 더욱 많이 가지게 되었고 항상 네트워크에 연결될 수 있게 되었다. 즉, 통신을 위해 설계되고 만들어진 도구이기 때문에 침입자들이 휴대폰에 침입하기 위해 시도해볼 수 있는 부분도 더욱 많아지게 되었다.

- **휴대폰 해킹 위험**

1. 휴대폰을 복제하면 전자 identity를 훔칠 수 있어 이를 이용해 몰래 다른 사람의 전화를 사용하고 실제요금은 휴대폰 소유자가 내야 하는 상황이 발생할 수 있다.

2. 또한 휴대폰 감청꾼들이 통화내용을 몰래 듣고 개인과 회사의 사생활을 침해할 수 있다.

3. 요즘 휴대폰은 실제로 소형 컴퓨터로 볼 수 있다. 그래서 컴퓨터에서 바이러스를 퍼뜨리듯 휴대폰에서도 똑같이 바이러스가 감염될 수 있다. 즉, 바이러스는 휴대폰에서 또다른 휴대폰으로 감염될 수 있고 컴퓨터를 공격하듯 감염된 휴대폰을 공격한다.

4. bluebugging이라 불리는 기술을 쓰면 해커는 타인의 휴대폰을 완전히 손안에 넣을 수 있다. 해커는 휴대폰 소유자 몰래 휴대폰이 스스로 전화를 걸도록 할 수 있다. 예를들어, 해커는 전화기가 해커에게 전화를 걸게 할 수도 있고 감염된 휴대폰을 이용해서 다른 사람과의 통화내역을 엿들을 수도 있다. 즉, Bluebugger는 감염된 휴대폰으로 걸려오는 모든 전화를 자신의 전화로 돌릴 수 있다.

5. bluesnarfing이라고 불리는 또 다른 기술을 쓰면 해커는 휴대폰에서 주소록, 일정, 사진 같은 개인정보를 쉽게 빼낼 수 있다.

- Bluesnarfing의 원리

1. Bluesnarfing은 블루투스 기능이 있는 휴대폰에서 이루어진 가장 초기의 해킹공격중의 하나이다. 현재 최신 휴대폰에는 이런 공격은 동작하지 않고 Nokia6310i, Nokia7650, Nokia8910i, Ericsson R520m같은 예전의 휴대폰상에서 주로 발생했다. 해커는 먼저 공격에 사용할 일반적으로 Bloover (bluetooth와 Hoover의 합성어 vacuum cleaner가 먼지를 흡입하는 것과 같은 방법으로 정보를 빨아들인다는 뜻)라 불리는 소프웨어를 다운받는다. 일부 버전은 휴대폰에 설치될 수 있지만 보통 해커가 랩탑에 이 소프트웨어를 설치한다.

2. 이 소프트웨어는 발견 모드(discovery mode)에서 근처 블루투스 장치를 스캔한다. 간혹 블루투스 장치의 양쪽이 모두 동의해야만 서로 연결될 수 있는 경우도 있지만 대부분 발견모드에 있는 블루투스 장치는 원하는 휴대폰에 연결할 수 있다.

3. 이 소프트웨어는 일반적으로 블루투스 장치용 Bluetooth OBEX 프로토콜을 사용하여 연결하는데, 전형적으로 정보를 보낼때 사용되는 push 프로파일을 사용하여 연결한다. 해커는 이 소프트웨어를 사용해서 일부 초기 휴대폰의 OBEX 프로토콜 구현의 보안결함을 악용해 폰북파일 (telecom/pb.vcf)이나 일정파일 (telecom/cal.vcs) 같은 흔한 파일명에 대해 get 요청을 함으로써 폰북정보, 일정정보, 및 다른파일들을 빼낼 수 있었다.

4. 해커는 휴대폰 사용자 몰래 파일을 변경할 수도 있다.

5. 해커는 또한 이 소프트웨어를 이용해 주변의 다른 휴대폰들을 다운시키게 하는 불순한 메시지를 무차별적으로 보낼 수 있다.

- Paris Hilton의 휴대폰이 어떻게 해킹되었나?

1. 최근 가장 심각했던 휴대폰 보안사고는 B급 유명인인 힐튼호텔의 상속녀 패리스 힐튼의 휴대폰으로부터 주소록 및 개인정보가 유출된 해킹 사건이다. 그녀의 개인휴대폰에 저장되어 있

던 주소록과 사진이 인터넷 웹에 올려진 것이다. 패리스는 Side kick II 스마트폰의 폰북안에 모든 연락처를 저장해 놓았었다.

2. 주소록 정보와 사진 데이터는 패리스가 가입되어있던 T-mobile 서비스에 주기적으로 백업된다. 그래서 그녀의 폰에 저장된 모든 개인정보는 T-mobile서비스에서도 이용될 수 있다.

3. T-mobile서비스는 고객이 T-mobile 서버에 백업된 자신의 개인정보에 접근해서 e메일을 읽을 수 있도록 해준다. 이때 고객들은 자신만의 비밀번호를 사용하여 T-Mobile 서버상의 자신의 정보에 접근할 수 있다. 일반적으로 고객이 비밀번호를 잃어버릴때를 대비하여 사이트는 "비밀 질문" 을 제시한다. 고객이 비밀질문에 답변하면 패스워드를 알려주고 고객은 자신의 계정을 다시 사용할 수 있다.

4. 패리스 힐튼의 경우, 선택한 비밀질문은 "What is your favorite pet' s name?" 이였다. Ms. Hilton은 공개적으로 그녀의 애완동물 Chihuahua의 이름을 Tinkerbell이라고 여러번 얘기했었다. 침입자는 힐튼이 비밀질문으로 "Tinkerbell"을 사용했을 거라고 추측했고 그 계정에 접근하는데 성공했다.

5. 침입자가 그녀의 계정에 접근한 후에 그녀의 모든 개인정보를 내려받아 웹에다 게시했다.

6. 실제로 그녀의 개인정보가 이런식으로 유출되었는지는 확실하지 않다. 한편 Hilton의 개인계정을 통해서가 아니라 누군가가 T-mobile 서버를 직접 해킹하여 정보를 빼냈다고 믿는 사람들도 있다.

6장 Biometrics란 무엇인가?

오늘날 사람들은 직장이나 보안시설에 들어가기 전에 개인의 신원을 확인 받아야 한다. 또한 많은 컴퓨터와 네트워크는 사람들이 먼저 신원인증을 받아야만 사용할 수 있도록 허용한다. 바이오 메트릭스는 사람들의 목소리, 지문, 홍채, 심지어 혈관의 구조 같은 유일한 신체적 특성을 이용하여 신원인증을 하게 된다. 전형적인 바이오 메트릭스 시스템은 신원을 인증할 사람의 신체적 특성을 검사하는 센서, 인증 정보를 저장하는 컴퓨터, 그리고 저장된 정보와 센싱한 정보를 검사하여 인증여부를 결정하는 컴퓨터로 이루어진다.

- **홍채 Scanning의 동작원리**

1. 홍채 scanning 시스템은 홍채사진을 사용하여 누군가의 신원을 증명하기 위한 방법이다. 일부 사람들이 망막 scanning이라는 예전의 기술을 홍채 scanning과 혼동하는 경우도 있지만 망막 scanning은 홍채 scanning 만큼 정확하지 않고 불편해하는 사람들이 많다.

2. 홍채사진을 찍기 위해서는 CCD(charged-coupled device) 디지털 카메라가 사용된다. 이 카메라는 2가지 종류의 빛을 사용하는데 가시광선과 근적외선이다. 근적외선은 눈동자가 아주 어둡게 보이도록 하여 홍채가 더 잘 보이게 하기 때문에 홍채사진을 찍는데 특히 적합하다.

3. 사람이 스캐너로부터 약 3~10인치 정도 떨어진 거리에서 카메라는 홍채사진을 찍을 수 있다.

4. 신원등록시 카메라는 홍채사진을 컴퓨터로 보내어 수백 가지 특징을 분석하고 여기서 파악한 특징을 기반으로 신원을 확인할 수 있는 유일한 코드를 만들어낸다.

5. 신원확인시 컴퓨터는 카메라로 스캔된 사람의 코드와 일치하는 유일한 코드를 찾기 위해 데이타베이스를 검색한다. 일치하는 코드가 발견되면, 그 사람은 신원은 확인된 것이고 출입허

가를 받는다. 일치하는 코드가 없으면 출입이 거부된다.

- **지문 ID의 원리**

1. 모든 사람의 지문은 유일한 나선모양의 골의 형태로 이루어져 있다. 지문이 서로 유사하긴 하더라도 일란성 쌍둥이의 지문조차 동일하지 않다. 그래서 지문 ID를 사용하면 사람들의 출입 시 신원확인이 가능해진다.

2. 그 과정은 우선 지문 스캐너에 손가락을 올려놓으면 스캐너는 CCD를 사용해서 지문의 사진을 찍는다.

3. CCD는 지문의 반전된 영상을 얻는데, 이때 사진의 어두운 부분을 더 밝게 되고 밝은 부분이 더 어둡게 된다.

4. 영상을 저장하기 전에 CCD는 영상이 선명한지 확인한다. 영상의 어두운 부분의 평균치와 다른 여러가지 특징을 확인한다. 영상 충분히 선명하지 않으면 선명한 영상을 얻을 때까지 사진을 다시 찍어 확인한다.

5. CCD는 영상을 저장하고 소프트웨어로 영상을 검사한다. 실제로 전체 영상을 보지않고 지문의 유일한 부분인 minutae라 불리는 부분을 검사한다. 예를들어 능선이 끝나는 부분이나 2개로 갈라지는 부분을 검사한다.

6. 알고리즘은 minutae를 검사하고 다른 지문 minutae 기록들과 비교한다. 충분한 수의 minutae 일치가 발견되면, 그 지문이 동일한 것으로 결정한다. 그렇지 않으면 일치하지 않는 것으로 판정한다.

7장 RFID와 사생활침해

RFID(radio frequency identification)는 제품조달 사이클에서 상품이 어디로 이동하는지 추적하기 위해서 만들어진 무선주파수통신 기술이다. RFID 태그들이 제품과 포장지에 삽입되고 RFID 리더가 태그로부터 해당정보를 읽어내는 방식이다. 이 정보는 네트워크나 인터넷을 통해 중앙 데이터베이스와 응용프로그램에 전달된다. 응용프로그램은 이 정보를 모아서 제조업체에게 제품의 판매현황이나 이동경로를 알려줄 수 있다.

- **RFID의 동작원리**

1. RFID 태그(카드 또는 트랜스폰더라 불리는)는 제품 라벨이나 제품내에 부착되기도 한다. 이 태그에는 제품을 유일하게 구분해주는 제조날짜, 제품번호 같은 정보를 포함한다.

2. RFID 태그는 3개의 요소로 구성되는데, 안테나 역할을 하는 코일, 실리콘칩(처리기, 제품정보저장용 메모리, 무선송수신기를 포함), 그리고 코일과 칩을 부착해놓은 부분이다.

3. RFID 리더는 RFID 태그로부터 정보를 읽기 위해 사용하는데 RF무선 주파수 전자기파장을 발생시킨다.

4. RFID 태그는 리더의 전자기파장내에 들어오면, 태그는 유도전류를 얻어 자신의 메모리내에 있는 데이터를 RFID 리더로 전송한다. (일부 RFID 태그는 능동적이라 리더로부터 전원을 받지 않고 데이터를 전송할 수도 있다.)

5. 리더는 유무선으로 네트워크에 연결되어 있고 수집한 정보를 중앙컴퓨터로 전송한다. 이 컴퓨터는 제품발송의 전체 과정을 추적하기 위해 사용된다. 예를들어, 리더는 창고에 두고 제품을 출하할 때마다 발송정보를 전송한다.

6. RFID 리더는 공급망을 따라 여러군데 설치되어 그때그때 태그로부터 정보를 읽어 중앙컴퓨터로 전송한다. 이런 식으로 제조업체는 제품이 언제 배달되는지 즉시 알 수 있다.

7. 상점에 있는 RFID 리더는 상품이 창고에서 진열대로 옮겨져서 팔리는 과정을 추적할 수 있다. 쇼핑객이 카트를 끌고 출구로 가면 리더는 자동적으로 판매처리를 하게 되어 계산대에서 줄을 설 필요가 없게 된다.

- RFID가 당신의 일상을 어떻게 추적하는가?

1. RFID가 사생활침해에 관여하고 있음을 암시하는 열쇠는 RFID가 제품 식별을 위해 유일한 ID 번호를 가지고 있다는 것이다. 코카콜라 캔처럼 동일한 종류의 상품에 똑같은 코드를 가지는 바코드와 달리 RFID는 동일한 상품이라도 다른 RFID 태그를 가진다. (각 상품이 개별 일련번호를 가지고 있음을 의미한다.) 이것은 상품이 어디에 있든지 개별 상품을 추적할 수 있다.

2. RFID 기술발전이 사생활을 중요하게 생각하는 사람들에겐 걱정스러운 일이 되었다. 신기술 RFID칩은 종이판지틈에 끼워넣거나, 금형을 뜨기전에 플라스틱속에 집어넣거나, 의류 이음매에 넣어 꿰매거나 포장용기에 통합해 버릴수도 있다. 게다가 전도체 잉크를 사용해서 RFID 칩과 안테나를 어디든 인쇄할 수 있다. 이것은 누군가가 전혀 알아채지 못하고 RFID 칩이 있는 상품을 사서 입거나 가지고 다니게 된다는 뜻이다.

3. RFID리더는 원거리에서도 태그를 읽을 수 있어서 제품을 만들거나 판매한 회사 이외에 다른 개인이나 회사가 이 태그들을 읽을 수도 있다. 따라서 이론적으로 사람들이 RFID 태그가 있는 물건을 가지고 공공장소나 상점에 들어갈 때 RFID 리더를 가진 사람은 당신의 사생활에 대한 많은 상세정보를 얻을 수 있게 된다. 그러므로 RFID 태그가 붙어있는 옷을 입거나 책같은 물건을 가지고 있다면 상점직원이나 누군가가 당신의 사생활을 손쉽게 속속들이 알아낼 수 있다.

4. 음식과 약물 관리본부는 처방전에 RFID 태그를 사용해서 소비자들이 병원이나 약국에서 처방을 받을 때 올바른 투약법을 받는걸 확인하도록 했다. 하지만 개별 알약에 초소형 RFID 태그를 새겨 넣을 수 있기 때문에 RFID 리더를 가진 제 3의 사람이 특정인이 어떤 처방의 약을 먹고 있는지 쉽게 알아낼 수

있어 사생활을 중요하게 생각하는 사람들은 사생활 침해를 우려하고 있다.

5. 일부 정부기관은 여권과 운전면허증 같은 신분증에 RFID 태그를 집어넣자고 제안한다. 사생활보호 옹호자들은 이렇게 되면 RFID 리더를 사용해서 지나다니는 사람들에 대한 이름, 생일, 현재 주소 및 유사정보 같은 엄청난 개인정보를 일어낼 수 있게 된다고 우려하고 있다.

6. 의료목적으로 사람의 체내에 RFID를 이식하는 문제를 걱정하는 목소리도 있다. 현재 RFID는 가축에 이식되어 그들의 움직임을 추적하고 또한 멸종위기의 야생동물에게 이식하여 그들의 서식처를 추적하기도 한다. 전자사생활정보센터(EPIC)같은 단체는 RFID 칩을 의료목적으로 사람에게 이식하려는 움직임이 있다고 얘기한다. 이 칩은 개인 식별 및 병명, 증상, 투약 약물 같은 의료정보를 포함하게 될 것이라고 한다. RFID 리더를 가지고 사람들의 이런 정보를 얻어낼 수 있게 된다.

7. 여러 개의 RFID 태그로부터 수집된 정보는 개인정보와 함께 데이타베이스에 저장될 수 있다. 그래서 개인정보로 인식되고 있는 입고 있는 옷, 먹는 음식, 투약 약물, 건강 상태 등을 포함하는 개인에 대한 총체적인 프로파일이 만들어질 수 있다.

8장 당신의 위치는 어떻게 추적될 수 있나?

현대사회의 잘 알려진 모토에 "달릴 수는 있어도 숨을 수는 없다"는 말이 있다. 예를들어, 당신이 휴대폰 사용자라면 통신서비스 회사가 당신의 대략적인 위치를 알아낼 수 있는 다양한 방법이 있다. 또한 GPS(global positioning system)는 소름이끼칠 정도의 정확성을 가지고 당신의 구체적인 위치를 집어낼 수도 있다.

- **GPS의 동작원리**

1. GPS의 동작원리를 이해하기 위해서, 먼저 삼각측량법을 이해해야 한다. 이 기술을 이용하면 3개의 지점으로부터 자신의 위치까지의 거리를 측정하여 현재 자신이 있는 위치를 정확하게 알아낼 수 있다.

2. 즉, 당신이 보스턴이 중심이 되는 원주상의 어디엔가 보스턴에서 75마일 떨어진 곳에 있다고 하자. 이제 당신이 뉴욕으로부터는 170마일 되는 지점에 있다고 하면, 뉴욕이 중심이 되는 2번째 원을 그릴 수 있다. 이제 당신은 2개의 원이 만나는 2지점중(A 또는 B) 한군데 있음을 알 수 있다. 마지막으로 당신의 위치가 Hartford로부터는 20마일 되는 곳이라는 것을 안다고 하면, Hartford가 중심이 되는 3번째 원을 그릴 수 있고 당신의 정확한 위치를 알아낼 수 있다.

3. GPS 시스템에서는 지구상의 특정지점으로부터의 거리가 아니라 지구를 둘러싸고 있는 위성으로부터 거리를 이용한다. 그래서 한 개의 위성으로부터의 거리를 알면 당신은 그 위성 주위의 원이 아닌 구면 위의 어디엔가 있게 된다. 이러한 3개의 구면은 2개의 지점에서 교차하고 당신의 위치는 이론적으로 2개가 된다. 그러나 2개의 점 중 하나는 우주공간에 있게 되어 위성으로부터의 거리를 사용하여 당신의 위치를 결정할 수 있다. 하지만 보다 정밀한 위도 같은 정보를 얻기 위하여 4개의 위성으로부터의 거리를 측정할 필요가 있다.

4. 실제로 당신의 위치를 알아내기 위해서는 GPS 단말기가 필요

하다. 이 단말기는 4개의 위성으로부터의 거리를 계산하고 이를 기반으로 지구상의 당신의 실제 위치를 불과 몇 피트 오차 범위 이내로 알아낼 수 있다.

5. 현재 24개의 GPS위성이 지구궤도를 돌고 있다. 이 위성들은 지구상의 어느 위치에서도 언제든지 4개의 위성이 보여지도록 잘 분포되어 있다. 이 위성들은 2개의 주파수(1575.42Mhz와 1227.60Mhz)를 이용해 끊임없이 지상으로 신호를 보내오고 있다.

6. GPS수신기 내부에는 위성의 현재 위치를 알려주는 위성운행서가 있다. 이 수신기는 하나의 위성에 신호를 맞추고 위성으로부터의 신호가 자신까지 도달하는데 걸리는 시간을 측정한다. 전자기파의 속도(186,000 mps)를 알고 있기 때문에 위성으로부터의 거리를 계산할 수 있다.

7. 수신기는 다른 3개의 위성에 대해서도 동일한 계산을 한다. 다음단계에서 지구상의 당신의 위치에 대한 위도와 경도를 계산하여 알려준다.

8. GPS 수신기는 또한 지도를 포함하고 있어서 당신이 지도상의 어디에 있는지 직접 볼 수 있고 당신의 위치를 계속 추적할 수도 있다. 이런 기능은 운전중 차량의 위치를 보여주는 차량항법시스템에 사용되고 있는데, GPS가 지도뿐 아니라 거리와 방향에 대한 데이터베이스 정보와 결합되어 운전할 때 진행방향을 바꿀 수 있도록 방향을 지시한다.

- **휴대폰 위치추적의 원리**

  1. 최신 휴대폰은 GPS수신기를 내장하고 있어, 휴대폰 사용자의 위치가 추적될 수 있다. 그러나 휴대폰은 이동통신 사업자의 기지국 기반시설을 이용하여 GPS수신기 없이도 추적될 수 있다.

  2. 당신이 휴대폰으로 전화를 할 때, 전화기는 가장 강한 신호를 보내는 기지국을 찾는다.

3. 휴대폰은 기지국에 연결한다.

4. 기지국은 이 정보를 이동통신회사의 홈위치등록기(HLR)에 보낸다. HLR은 시스템내의 모든 휴대폰 사용자의 위치를 기록하고 각 사용자가 전화를 걸 때 어느 기지국을 사용했는지 기록한다.

5. HLR은 사용된 기지국을 알고 있기 때문에 전화건 사람의 대략적인 위치를 알 수 있다.

6. 일부 경우, 한 개의 기지국은 3개내지 6개의 섹터로 구분된다. 각 섹터는 방향성 안테나를 사용한다. HLR은 휴대폰이 어느 섹터에 있는지 알아내어 휴대폰 사용자의 위치를 훨씬 더 정확하게 알아낼 수 있다.

7. 하나의 기지국에서 다른 기지국으로 옮겨갈 때, HLR은 사용자가 움직이고 있다는 것을 알아채고 새로운 위치를 추적할 수 있다.

8. 전화를 걸지 않을 때 조차 기지국은 휴대폰의 위치를 추적할 수 있다. 휴대폰의 전원이 켜져 있으면, 휴대폰은 가장 가까운 기지국을 찾아서 자신의 위치를 알린다. 누군가가 이 휴대폰 사용자에게 전화를 걸려면 이 전화기가 어느 기지국을 통해서 통신망에 연결되어 있는지 알아야 하기 때문에 이런 절차가 필요하다. 전화를 걸 때처럼 휴대폰이 기지국에 위치를 등록할 때도 HLR로 동일한 정보가 보내진다.

9장 DNA 검사 및 사생활침해

- DNA 검사의 원리

1. 범죄수사에서 DNA를 검사하는 방법은 여러가지가 있는데 주로 RFLP(restriction fragment length polymorphism)을 사용해서 범죄현장의 DNA와 용의자의 DNA가 일치하는지 검사한다. 우선, 혈액, 타액, 정액, 피부조직, 머리카락 등으로부터 용의자의 DNA를 채취한다. DNA는 세포의 핵에서만 발견되기 때문에 이런 자료로부터 채취되어야 한다. 범죄현장에서 DNA가 발견되면 먼지와 잔해로부터 오염될 우려가 있기 때문에 깨끗이 관리해야 한다. 어떤 경우엔 DNA는 범죄현장의 천, 의류 또는 그 밖의 다른 곳에서 채취할 수도 있다.

2. 대부분의 유전물질은 사람마다 변하지 않으므로, RFLP라 불리는 DNA 검사는 사람마다 DNA내의 유전물질이 다르다는데 초점이 맞춰져 이루어진다.

3. 이러한 DNA 조각들은 "restriction enzymes" 라는 효소를 사용하여 DNA부터 추출된다. Enzymes는 DNA의 어느 면이든 잘라서 RFLP를 분리해 낸다.

4. DNA 조각의 길이는 사람마다 다르기 때문에 RFLP의 길이는 DNA 매칭의 기초가 된다. 그러나 RFLP는 눈에 보이지 않을 정도로 너무 작아서 일치하는지 검사를 하기전에 gel electrophoresis라는 과정을 통해 상대적 크기를 시각적으로 묘사해 놓아야 한다. DNA를 gel mold 상태로 두고 전기충전이 가하면 DNA는 음의 전기를 띠게되어 양의 전기를 띤 mold의 반대편으로 끌린다. 비록 육안으론 볼 수 없지만 DNA 조각들은 점차 움직여서 명확한 사다리 형태를 남긴다. 이 형태를 가시화하기 위해 방사능검사와 X-ray 필름을 사용해서 패턴 사진을 찍는다. (로잘린 프랭클린의 X선 회절).

5. 현장에서 발견된 DNA 패턴이 용의자 또는 희생자의 DNA 패턴과 같은지 일치 여부를 검사한다. 4 ~ 5번의 방사능검사와

x-ray 사진이 촬영된다. 모든 검사에 대해 용의자의 DNA가 범죄현장에서 발견된 DNA와 일치하게 되면 용의자는 체포된다.

- **DNA 분석자료의 위험**

1. 여러가지 이유로 사람들의 DNA 분석 자료가 구축되고 있다. 그것들이 모두 범죄문제와 관련된 것은 아니다. 예를들어 누군가 자신이 어떤 유전병에 대한 유전자를 보유하고 있는지 알기 위해 DNA 검사를 할 수도 있다.

2. 사생활 보호론자들은 DNA 분석자료가 폭넓게 사용될 경우의 위험성을 우려하고 있다. 그들의 가장 큰 우려는 DNA 분석자료가 방대한 데이터베이스에 통합되어 정부나 회사에서 사용될 수 있다는 것이다.

3. 한가지 걱정스러운 일은 고용주들이 DNA 분석자료에 접근하길 원한다는 것이다. 만일 고용주들이 어떤 고용인이나 지원자의 DNA분석자료에 접근하여 해당인물이 특정 병에 더 잘 걸리기 쉽다는 것을 알게 되면 그들은 그 사람을 뽑지 않을 수도 있고 부서를 이동시키거나 심지어 해고할 수도 있다.(예, 정신과 치료경력이 있으면 현역으로 가지 못하는 경우)

4. 또 다른 우려는 건강보험회사가 특정 유전병이나 질환에 걸리기 쉬운 사람들이 보험에 가입하는 것을 거절하는 것이다.

5. 사생활 보호론자들은 또한 법집행관들이 적절하지 않게 DNA 분석자료를 사용하는 것이다. 예를들어 분석자료에서 특정 유전자를 가진 사람들이 쉽게 범죄행위를 저지른다고 언급하면서 지속적으로 그들을 감시하거나 저지르지도 않은 범죄에 대해서 체포를 하거나 할 수도 있다.

6. 또 다른 우려는 데이터베이스 정보가 입찰자에게 팔려서 사람들의 일상에 대한 개인적인 개성들이 상품으로 팔리게 되는 것이다.

10장 공항검색과 테러리스트

- **공항 검색스캐너의 원리**

1. 대부분의 공항 금속 탐지기는 파동유도-pulse induction(PI)로 알려진 기술에 기반을 두고 있다. 이 시스템에서 탐지기의 양쪽면에 있는 전선 코일이 각각 전송기와 수신기의 역할을 담당한다.

2. 코일은 짧고 강한 전류파동을 생성하고 이 전류 파동은 순간적인 자기장을 만들어 낸다. 일부 시스템은 초당 1000번의 파동을 생성하기도 하지만 전형적으로 코일은 초당 100번의 파동을 만들어 낸다.

3. 만일 금속 조각이 탐지기내에 있으면, 파동은 파동의 반대편에 있는 물체에 자기장을 생성한다.

4. 각 파동의 끝에서 파동은 자신의 극성을 뒤집어서(양은 음으로 음은 양으로) 아주 날카로운 전기적인 뾰족한 그래프를 만들어낸다. 금속이 탐지기내에 있으면 금속의 자기장에 있는 여분의 에너지 때문에 그래프의 뾰족함이 더 커진다. 이 뾰족한 그래프는 몇 ms(마이크로 세컨드) 지속한다.(마이크로 세컨드는 백만분의 1초이다). 이 뾰족함은 reflected pulse라는 또 다른 전류를 만들어내고 약 30 ms동안 지속하면서 코일을 통과한다. 금속이 탐지기내에 있을 때 금속이 그래프의 뾰족함을 더 증폭시키므로 reflected pulse도 더 커진다.

5. 금속탐지기는 reflected pulse의 길이를 측정하는 샘플링 회로를 가지고 있다. 이 회로는 reflected pulse의 길이를 금속이 없을 때의 파동의 정상길이와 비교한다. 만일 파동이 길어지면, 금속이 존재한다는 걸 나타낸다.

6. 샘플회로는 reflected pulse에 대한 정보를 integrator라는 장치에 보낸다. 이 integrator는 샘플링 회로가 보낸 약한 신호를 증폭해서 비프음을 울리는 오디오 장치로 보내서 금속이 탐지되었다는 것을 알린다.

- **공항 테러리스트 추적시스템의 원리**

1. 누군가가 테러리스트인지 또는 잠재적 테러리스트인지 확인하기 위해 승객들을 투시하는 다양한 방법이 있다. 논쟁의 여지가 있는 (CAPPSII)라는 방법 및 아직 실전에 적용되고 있지는 않지만 유사한 프로그램을 사용하는 제안들이 있다. 이 프로그램은 사람들의 사생활보호 권리와 시민의 자유를 침해한다고 비판을 받고 있다.

2. 승객이 항공편 예약을 하면 승객은 현재 공개되어있는 자신의 정보보다 더 많은 정보를 제공해야 한다. 승객은 자신의 이름 전체, 생년월일, 집주소 및 집전화번호를 제공해야 한다.

3. 항공사 예약시스템은 그 정보를 CAPPSII 시스템에 보낸다.

4. CAPPSII 시스템은 상업적인 신용기관이 제공하는 정보를 포함하여 여러기관으로부터 제공된 데이터베이스를 검색한다. 연방기관과 주기관으로부터의 정보와 CIA, FBI와 NSA와 같은 수사기관으로부터의 정보도 이에 해당한다.

5. CAPPSII 시스템은 해당 승객에 대한 점수를 계산해서 그 사람을 green, yellow, red 중 하나의 범주로 분류한다. 이 분류는 다시 항공예약시스템에 보내진다. 그 사람이 탑승수속을 하고 탑승권을 받으면 그 탑승권에는 그를 green, yellow, red중 하나로 식별할 수 있는 암호 데이터가 포함되어 있다.

6. green으로 분류된 사람은 보통 검색을 받는다. Yellow로 표시된 승객은 검색봉으로 훑거나 다른 검색방법을 이용해 추가적인 검색을 받는다.

7. Red로 표시된 승객은 법집행관이 직접 보고 질문을 하고 기다리게 하거나 체포한다.

11장 전자감시와 사생활침해

- NSA 에쉴론(Echelon) 스파이 시스템

1. NSA의 Echelon 시스템의 세부내용은 일급비밀로 세상의 모든 전화, 이메일, 인터넷, 팩스, 그밖의 다른 전자적 통신을 가로채서 해석하는 일을 한다. 동작방법에 대한 정확한 원리는 비밀로 되어 있기 때문에 정확히 알 수는 없지만 공개된 자료에 기반을 두고 일반적인 동작개요를 알 수 있다.

2. 대부분의 국가에서 사용하는 국제통신위성(Intelsats)의 국제위성 접시안테나를 통하여 감청시스템이 배치되어 있다. Intelsat들은 적도상공의 궤도에 떠서 안정적으로 돌고 있는데, 각 위성은 동시에 수만개의 전화, 이메일, 인터넷, 팩스 및 다른 전자적 통신을 처리한다. 담당 부분은 여러 개의 위성들에 배치되는데 타겟 위성에서 모든 통신을 가로챈다.

3. Intelsat들은 세상의 통신 트래픽의 전부는 아니지만 많은 부분을 전송한다. 그 밖에 해저 케이블, 유선통신시스템, 이동통신 네트워크, 지역통신위성 등이 또한 존재한다. Echelon은 여러가지 방법으로 이러한 시스템들을 감시한다. 예를들어, Echelon은 바다와의 경계지점에서 직접 해저케이블을 감시하며 전파경로를 따라 일부 지점에서 감청시스템을 배치해서 이동통신망을 감시한다.

4. Echelon이 가로챈 데이터는 암호화된 통신과 비암호 통신 두가지로 구분되는데, 암호화된 통신은 고성능 컴퓨터로 보내서 암호를 풀어 암호이전의 원래 데이터로 해석해낸다.

5. 각각의 통신 데이터는 감청센터의 특정용어사전 컴퓨터에 보내진다. 이 용어검색용 컴퓨터는 일반적인 수퍼컴퓨터와 유사한데 모든 통신 메시지를 뒤져서 시스템에 미리 프로그램된 특정용어를 찾아내는 고성능 컴퓨터이다. 예를들어, 핵이나 생물학적 무기산업에서 사용되는 특수용어, 테러리스트 지도자의 이름 등등이다. 각 컴퓨터가 사용하는 사전은 다양한 종류의 용어들이 있는데, 일부는 대외첩보국이 NSA로 보낸 것이다.

예를들어, 영국첩보국이 IRA에 관련된 용어들을 Echelon에 포함하도록 요청할 수도 있다. 어떤 용어를 포함한 통신데이타는 영구적으로 Echelon 시스템에 입력되고 특별한 코드가 주어진다. 용어코드 이외에 다른 코드도 가진다. 예를들어, 통신데이타를 처리하는 용어사전 컴퓨터의 이름인 카우보이 같은 것이다.

6. 키워드를 가진 통신 데이터는 암호화된 안전한 통신로를 통해 지역 Echelon본부로 보내진다. 여기서 통신전문가들이 그때그때 유용한 정보를 가지고 통신데이타를 샅샅이 뒤져서 미국내외의 쓸모있는 정보를 찾아내 첩보국에 넘긴다.

- FBI의 카니보어(carnivore) 시스템

1. 지금은 없애버렸지만 FBI는 이메일 들여다보기, 방문사이트 보기와 같은 사람들의 인터넷 사용을 감시하기 위해 carnivore라는 시스템을 사용했었다. Carnivore의 데이터수집 부분은 패킷감시 소프트웨어를 구동시킨 펜티엄기반의 시스템이 사용되었다. 이 컴퓨터에는 키보드나 모니터가 달려있지 않았고 ISP에 있는 어느 누구도 사용할 수 없었다.

2. 이 컴퓨터는 전용선과 56K 모뎀을 이용해 FBI 사무실에 연결되었다. FBI는 pcAnywhere라는 기존 프로그램을 사용해 Carnivore 소프트웨어와 컴퓨터를 원격으로 제어하였다. 전용선은 인터넷에 연결되지 않았고 모든 데이터는 pcAnywhere의 암호화 기능과 그 밖의 다른 프로그램을 사용해 암호화되었다.

3. FBI는 특정인에 대한 도청허가증을 부여 받아 감시할 권한이 있는데, 이 허가증을 가지고 해당인물에 대한 특정한 종류의 정보만을 수집할 수 있었다(예, 이메일). FBI는 Carnivore 소프트웨어의 필터를 사용해 그들이 원하는 정보만 검사하고 그 외의 다른 모든 정보는 걸러내었다. 예를들어, FBI는 필터를 사용해 특정인물이 주고받는 패킷만을 감시하거나 이메일이나 웹사용만을 검사했다.

4. 이더넷 감시장치는 목적 ISP에 설치하는데 이 장치는 보통의

방법대로 데이터 트래픽이 ISP를 통해 전달되게 놔둔다. 그러나 ISP를 통해 흘러다니는 모든 데이터 패킷의 복사본을 만들어 Carnivore 컴퓨터에 보낸다.

5. Carnivore 컴퓨터는 모든 패킷을 검사하고 필터링을 해서 패킷을 걸러낸다. Carnivore의 감시 대상인 패킷들은 2GB 착탈식 드라이브에 저장된다.

6. 착탈식 드라이브는 FBI에 전달되고 그 안에 담긴 데이터는 보통 두가지 소프트웨어를 통해 검사된다. Packeteer와 CoolMiner이다. Packeteer는 모든 패킷을 다시 모아서 CoolMiner가 사용할 수 있는 형태로 만든다. CoolMiner는 이메일 메시지와 HTTP 프로토콜 사용해서 보낸 데이터만을 검사하기 위해서 사용된다. FBI는 CoolMiner를 사용해서 보낸 메일 및 받은메일 같은 모든 감시대상을 재구성할 수 있다.

- **애국조례(patriotic regulations)의 사생활침해**

1. 논쟁의 여지가 있는 애국조례는 일부 사생활침해의 위험성을 내포한다.

2. 애국조례하에서는 어떤 특정인이 범법행위를 했다는 증거가 없어도 정부는 그사람의 도서관 사용기록을 조회할 수 있다. 그리고 그의 기록이 조회되었다는 사실을 알려주지도 않는다. 사실 이조례는 도서관 사서가 특정인의 기록조회를 본인에게 알려주는 것을 금하고 있다. 만일 알려준다면 사서는 감옥에 가게 된다.

3. 애국조례는 또한 범죄사실이 없어도 정부가 특정인의 의료기록을 조회할 수 있도록 한다. 물론 기록조회사실을 본인에게 알려주지도 않는다. 실제로 이 법에 의하면 의료전문가들은 기록조회사실을 알려주어서도 안된다. 의료전문가가 이 법을 어기면 역시 감옥에 가게 된다.

4. 애국조례는 정부가 당신의 은행, 신용기관, 다른 금융기관으로부터의 다양한 금융거래내역을 살펴볼 수 있다. 물론 기록이 조회되었다는 사실을 알리지도 않으며 조회사실을 본인에게

알리는 사람은 감옥에 가게 된다.

5. 애국조례에 의거하여 정부가 상당한 법적 근거나 법원명령 없이도 다양한 인터넷 통신내역을 볼 수 있다. 예를들어, 당신이 구글상에서 검색하는 웹서핑 습관에 대한 자세한 내용을 조회할 수도 있다.

6. 이 조례에 의하면 정부는 당신도 모르게 당신의 집을 검색할 수도 있다. 정부는 당신 몰래 당신의 집과, 사무실에 들이닥쳐서 사진을 찍고 정보를 수집해 갈 수도 있다.

12장 도청과 거짓말 탐지기

- **도청의 원리**

연방, 주, 지방의 법집행기관에서 합법적으로 허용되는 도청은 CALEA에 의해 이루어진다. 하지만 누군가의 통화에 끼어들어 몰래 듣기를 원하는 불법도청자들은 CALEA보다 아주 다양한 저급 기술을 사용한다. 불법도청이 이루어지는 전형적인 방법과 CALEA가 불법도청을 하는 전형적인 예는 다음과 같다.

1. 전화선내의 구리선들 중에 하나는 빨간색 절연피복이고 다른 하나는 녹색인데, 전화상에서 수신하는 목소리와 말하는 사람의 목소리를 음파로 표현하는 교류가 흐르고 있다.

2. 누군가 가정으로 연결된 전화선을 잘라서 녹색과 빨강색의 피복을 벗겨서 그 위에 다른 전선을 겹쳐 잇고 또 다른 전화에 연결하거나 음성녹음기를 연결하면 기존의 전화연결은 영향을 받지 않고 아무도 모르게 대화는 도청될 수 있다.

3. 전화를 엿듣기 위해 전화접속박스에 도청기가 사용될 수 있다. 접속박스는 보통 옥외 기둥위에 있는데 가정의 전화선을 주전화선에 연결한다.

4. 또한 전화기내부에 무선도청장치를 둘 수도 있다. 이 장치는 전화선에 연결되어 있고 전화기내의 신호를 집밖의 무선수신기로 보내고 이 신호는 다시 원거리에서 엿듣고 있는 누군가에게 보내진다.

- **합법도청의 원리**

CALEA는 도청허가를 받은 법집행관들이 통신사업자들을 통해 전화대화를 엿듣고 전화내역에 대한 정보를 얻을 수 있도록 허용한다.

1. 판결전에 법집행관들이 통신사업자들에게 가서 도청이 필요한

이유를 설명한다. 판사의 승인이 나면 합법적 문서나 명령이 통신사업자에게 전달된다.

2. 통신사업자의 특별한 권한이 있는 사람이 승인받은 CALEA 도청을 위해 특별히 설치된 시스템에 로그인 한다. 여러 개의 제조업체가 만든 다양한 시스템들이 있지만, 대부분이 전화망을 구성하는 라우터와 스위치들를 감시한다.

3. 전화네트워크상의 모든 통화는 디지털 스위치와 라우터를 거친다. 감시를 위해 사용된 시스템은 모든 통신이 지나가는 네트워크의 중심에 연결된다.

4. 감시 시스템은 통화에 대해 두개의 주요한 정보를 얻을 수 있는데, 실제 목소리전송 자체(call content information -CCC)와 전화번호와 통화참가자와 같은 각 통화와 관련된 데이터(CDC)들이다.

5. CCC와 CDC정보는 특별한 보안 라우터를 통해 법집행국에 보내진다.

6. 연방통신위원회는 Skype와 같은 VoIP를 사용한 인터넷상의 컴퓨터끼리 직접 통화하는 PC-to-PC 통화도 CALEA의 감시의 대상이라고 규정하고 있지만, 이러한 통화를 도청할 수 있는 어떠한 기술적인 방법도 아직 없다.

- **거짓말 탐지기의 원리**

1. 일반적으로 거짓말 탐지기는 두가지가 있는데 요즘엔 별로 사용되지 않는 구식기술인 아날로그 탐지기와 새로운 방식의 가장 많이 사용되는 디지털 거짓말 탐지기이다.

2. 거짓말 탐지기 테스트를 받을 때, 질문에 대한 응답자의 생리학적 반응을 측정하기 위해 응답자에게 여러개의 튜브와 선이 부착된다. 또한 호흡율을 측정하기 위해 공기가 채워진 두개의 고무 튜브(pneumographs)가 응답자의 복부와 가슴주위에 부착된다. 거짓말을 하면 보통 높은 호흡률을 보인다. 즉, 가슴과 복부의 근육이 확장할 때, 그 튜브내의 공기를 미세하게 내

보내게 된다. 아날로그 거짓말 탐지기에서 튜브는 폐에 부착되는데 다른 한쪽은 기계 팔에 연결된다. 이 기계 팔은 이어서 잉크달린 펜에 연결되고 펜은 두루마기 종이에 호흡률을 기록한다. 디지털 거짓말 탐지기에서는 내뿜어진 공기를 측정하고 변환기가 이를 디지털 신호로 변환하여 컴퓨터에 입력한다. 컴퓨터는 이 정보를 사용해서 그 사람의 호흡률을 계산한다.

3. 혈압과 심장박동을 측정하기 위해 혈압측정용 가압대가 오른팔 위쪽에 부착된다. 가압계와 거짓말 탐지기는 튜브로 연결된다. 아날로그 거짓말 탐지기에서 튜브는 폐에 부착되고 두루마기 종이에 호흡률과 혈압을 기록하는 잉크펜에 연결된다. 디지털 거짓말 탐지기에서 변환기는 이 정보를 디지털 신호로 변환하여 컴퓨터 입력한다. 컴퓨터는 이 정보를 사용해서 혈압과 심장박동율을 계산한다. 보통 거짓말을 할 때 혈압과 심장박동율이 높아진다.

4. 전자피부작용이라고 불리는 피부 전기저항(GSR)은 실제로 사람의 손가락끝에 있는 땀의 양을 측정하는 것이다. 이론적으로 누군가 스트레스 상황에 놓이면 땀을 많이 흘린다. 검류계가 2개의 손가락 끝에 연결되고 피부에 전류가 통하는 비율을 측정한다. 피부는 땀이 많을수록 전류가 더 잘 통한다. 아날로그 탐지기에서는 변동이 두루마기 종이에 기록되고 디지털 탐지기에서는 컴퓨터에 기록된다. 일반적으로 거짓말할 때 GSR이 더 크다.

5. 거짓말 탐지기를 다루는 검사관은 피실험자에게 일련의 질문을 한다. 조사할 범죄에 관한 질문뿐 아니라 대조표준용 질문도 한다. 대조용 질문은 범죄에 관한 질문에 대한 대답과 비교할 기준으로 검사관이 사용하는 일반적인 질문이다. 테스트가 끝났을 때 검사관은 결과를 해석하고 피실험자가 특정한 질문에 대해 거짓말을 했는지 여부를 보고한다. 거짓말 탐지기 결과들은 잘못 해석될 수도 있고 피실험자가 이 검사를 속이는 기술을 사용할 수도 있다. 예를들어, 검사전에 진정제를 복용하거나 손가락 끝에 땀 억제제를 바르거나 하는 것들이다. 이러한 이유로 매우 엄격한 지침하에 시행된 검사결과는 이외에는 보통 법정에서 받아들여지지 않는다.