10장. 악성 소프트웨어

10.3 바이러스 방어책

안티바이러스 방법

- 탐지(Detection):
  - 일단 감염되면 바이러스가 있는지 판단하고 위치를 파악
- 식별(Identification):
  - 일단 탐지되면 프로그램을 감염시킨 특정 바이러스를 식별
- 제거(Removal):
  - 특정 바이러스를 식별해냈으면 감염된 프로그램으로부터 바이러스의 흔적을 제거하고 원래 상태로 복구
  - 더 이상 퍼지지 않도록 차단

안티바이러스 소프트웨어 세대 (1)

- 제1세대:
  - 단순 스캐너(simple scanners)
    - 특징 의존(signature-specific) 스캐너
  - 다른 유형
    - 프로그램 길이 보관, 길이 변화 확인
- 제2세대
  - 발견 스캐너(heuristic scanners)
  - 발견 규칙집합(heuristic rules) 이용
    - 연관된 코드 단편 검색
      - 암호화 코드 시작 부분에서 암호화 키 검색
  - 무결성 검사
    - Checksum을 유지해서 변화 감지
    - 암호화된 해시함수 이용

안티바이러스 소프트웨어 세대 (2)

- 제3세대:
  - 활동 트랩(activity traps)
  - 바이러스 구조보다 동작을 보고 바이러스를 식별하는 메모리-상주 프로그램
  - 다양한 바이러스의 종류에 따라 특징이나 발견하는 방법을 따로 개발할 필요가 없음
- 제4세대
  - 다양한 기술을 섞어서 사용
    - 스캐닝 + 활동 트랩 + 접근제어
  - 풍부한 기능을 갖춘 방어(full-featured protection)

고도 안티바이러스 기술 (1)

- 유전적 복호화(GD: genetic decryption)
  - 빠른 스캐닝 속도로 가장 복잡한 폴리모픽 바이러스를 쉽게 탐지할 수 있음
  - 폴리모픽 바이러스가 포함된 파일이 실행될 때 바이러스는 자신을 복호화 해야만 하기 때문에 이 구조를 탐지하기 위해 실행파일이 GD 스캐너를 거치도록 함
  - GD 구성요소
    - CPU 에뮬레이터(CPU emulator):
      - 소프트 기반 가상 컴퓨터
    - 바이러스 특징 스캐너(Virus signature scanner):
    - 에뮬레이션 제어 모듈(Emulation control module):
      - 타깃 코드 실행을 제어

고도 안티바이러스 기술 (2)

- 유전적 복호화(GD: genetic decryption) (계속)
  - 동작 과정
    - 에뮬레이터에서 하나씩 타깃 코드 명령 수행
    - 복호화 루틴이 포함되어 있으면 해당 코드 번역
    - 주기적으로 제어모듈은 타깃 코드 스캔을 위해 인터럽트
  - 가장 어려운 문제
    - 각 번역을 얼마나 오랫동안 구동해야 하는가?
      - 에뮬레이션 기간이 길면 보다 많은 바이러스 탐지 가능
      - 자원 소모에 대한 사용자의 불평

고도 안티바이러스 기술 (3)

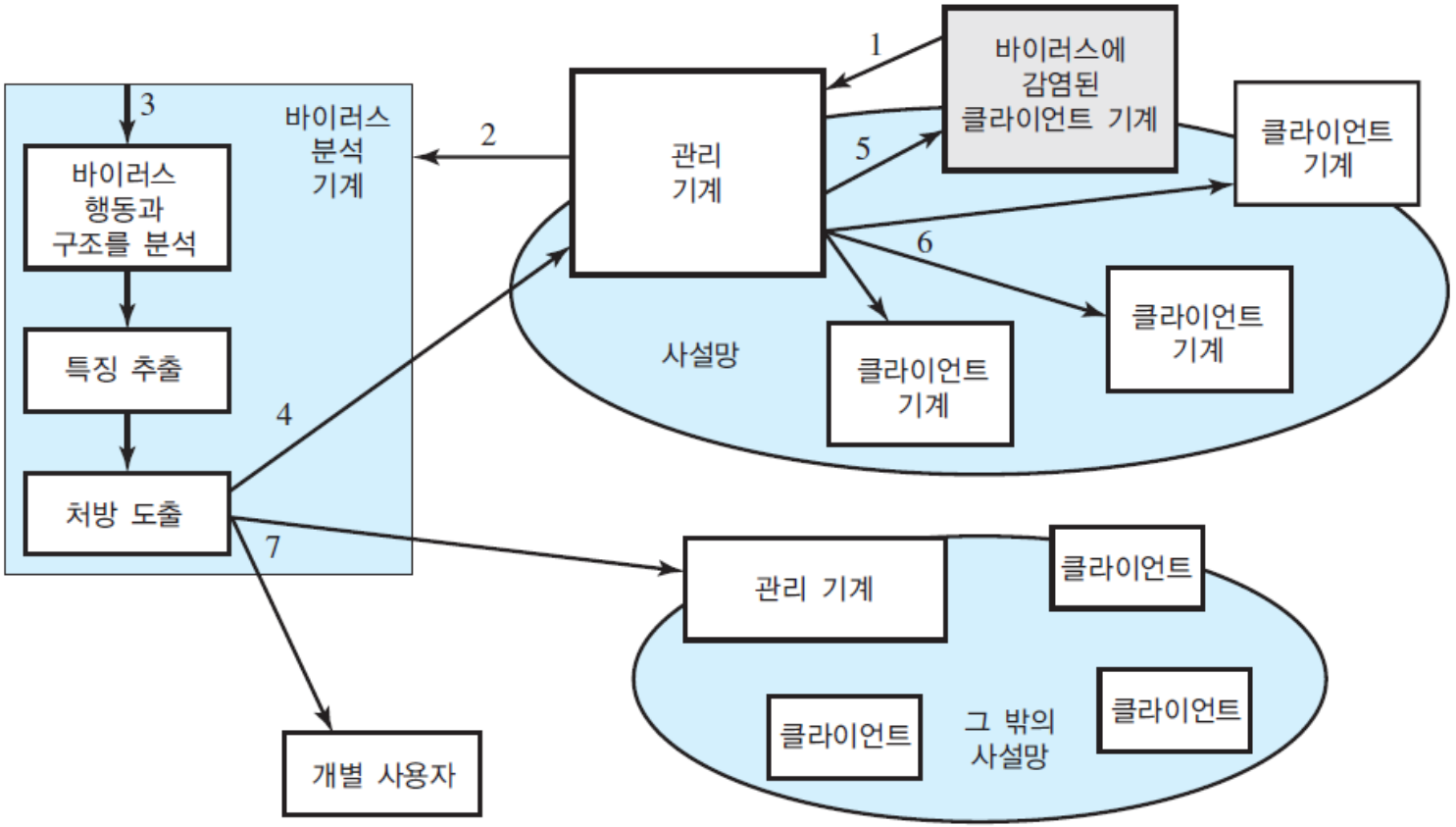
- 디지털 면역 시스템 (Digital immune system)
  - 바이러스 침해로부터 보호를 위해 IBM에 의해 개발된 종합적인 방법
  - 인터넷-기반 바이러스 확산방지 목적
  - 전통적인 바이러스
    - 상대적으로 느린 확산
    - 1달 주기로 안티바이러스 SW가 업데이트 되어도 문제 없었음
  - 바이러스 확산이 빨라진 원인은 인터넷 기술의 발전
    - 통합된 메일 시스템(Integrated mail systems):
      - MS의 아웃룩, 로터스사의 노트
    - 이동-프로그램 시스템(Mobile-program systems):
      - Java, Active-X

고도 안티바이러스 기술 (4)

- 디지털 면역 시스템 (계속)
  - 프로그램 에뮬레이션 기능 + 빠른 반응시간 제공
  - 새로운 바이러스가 한 기관에 나타나면
    - 자동으로 잡아내고, 분석하고,
    - 그것을 탐지하는 방법을 추가하고, 제거하며,
    - IBM 안티바이러스를 사용하는 다른 기관에 알림

고도 안티바이러스 기술 (5)

- 디지털 면역 시스템 (계속)



고도 안티바이러스 기술 (6)

- 디지털 면역 시스템 (계속)
  - 디지털 면역 시스템 운용 단계
    1. 각 PC의 모니터링 프로그램은 시스템 행동, 의심스런 프로그램의 변경 혹은 바이러스가 있다고 여겨지는 증상 등의 다양한 발견도구를 사용
       - 모니터링 프로그램은 감염되었다고 생각되는 모든 프로그램을 기관 내의 관리 기계로 전달
    2. 관리 기계는 표본 암호화 후 중앙 바이러스 분석기계로 전달

고도 안티바이러스 기술 (7)

- 디지털 면역 시스템 (계속)
  - 디지털 면역 시스템 운용 단계 (계속)
    3. 분석을 위해서 감염된 프로그램이 안전하게 구동되는 환경을 제공
       - 사용하는 기술
         - 에뮬레이션
         - 의심되는 프로그램이 실행되고 관찰할 수 있게 고안된 보호 환경 만들기
       - 바이러스분석 기계는 바이러스를 식별하고 제거할 수 있는 처방조치

고도 안티바이러스 기술 (8)

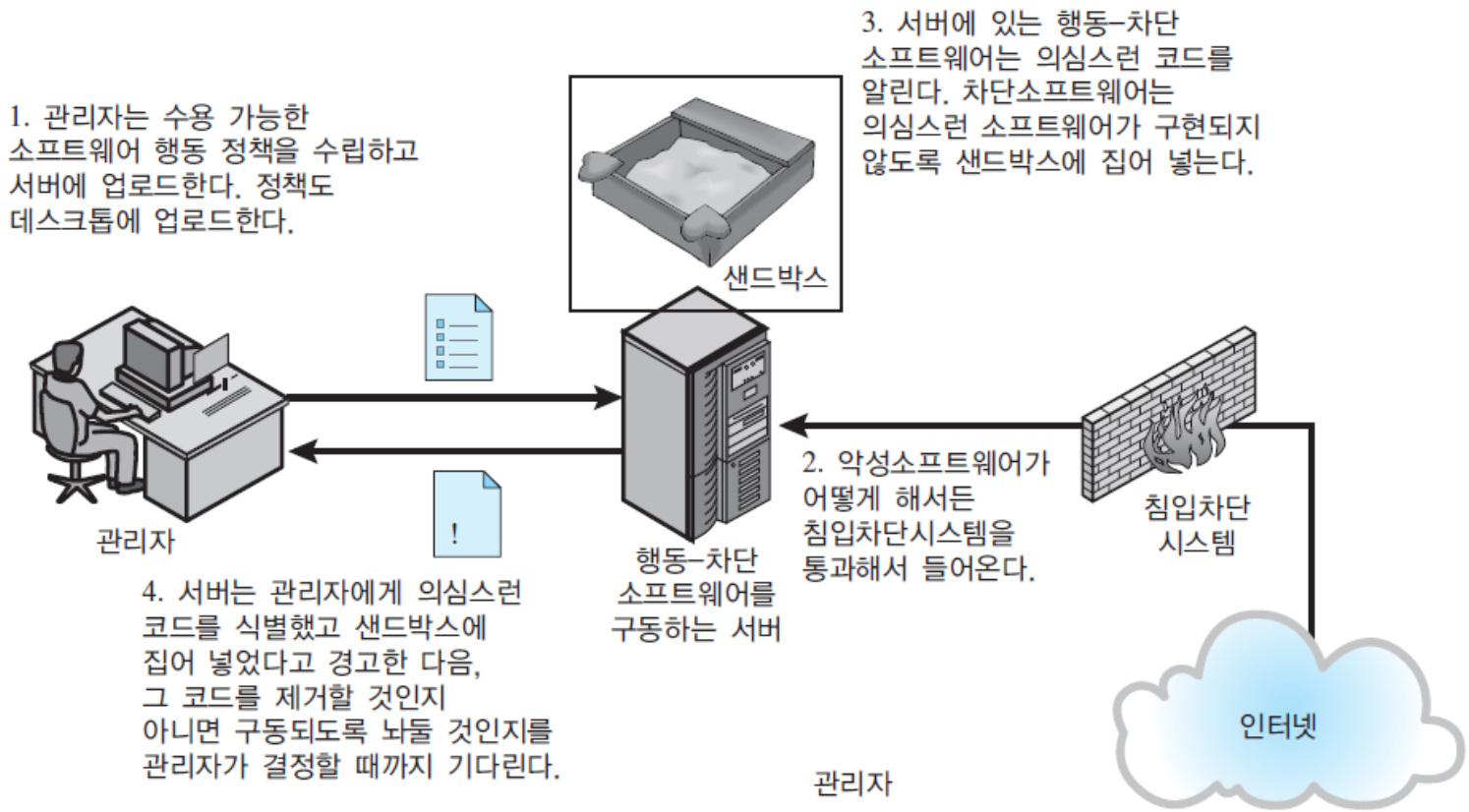
- 디지털 면역 시스템 (계속)
  - 디지털 면역 시스템 운용 단계 (계속)
    4. 처방으로 나온 것을 관리 기계로 전달
    5. 관리 기계는 처방을 감염된 클라이언트로 전달
    6. 처방을 기관 내의 다른 클라이언트에게도 전달
    7. 전 세계에 걸쳐 있는 가입자는 주기적으로 안티바이러스 업데이트를 수신하고 새로운 바이러스로부터 보호

행동차단 소프트웨어 (1)

- behavior-blocking software
- 악성 동작을 탐색하기 위해 호스트 컴퓨터의 운영체제에 집중적으로 관심을 갖고 프로그램 행동을 실시간으로 관찰
- 악성 동작이 시스템에 영향을 끼칠 기회를 주지 않고 사전에 차단
- 관찰 대상 행동
  - 파일을 열고, 읽고, 제거하고, 수정하려는 시도
  - 디스크 드라이브를 포맷하거나 다른 회복할 수 없는 동작을 하려는 시도
  - 실행 파일의 논리와 매크로의 스크립트를 수정하는 시도
  - 시작 설정(start-up setting) 같은 중요한 시스템 설정변경 시도
  - 실행 가능한 내용을 보낼 목적으로 전자메일을 작성하거나 인스턴트 메시징을 이용하는 클라이언트
  - 네트워크 통신 개시

행동차단 소프트웨어 (2)

- 행동차단 소프트웨어 동작



행동차단 소프트웨어 (3)

- 행동차단 소프트웨어는 의심스런 소프트웨어를 실시간을 차단
  - 안티바이러스 탐지기술을 통과했다 하더라도 최종적으로 운영체제에 잘 정의된 요청을 해야 함
  - 복잡한 논리와 무관하게 악성 동작 식별 가능
- 행동차단 소프트웨어만 동작하게 되면 제한적
  - 타깃 기계에서 동작이 어느 정도 이루어진 후에야 탐지됨