Introduction to Software Security

1st Homework (1번 과제)

Computer Security & OS Lab
Dept. of Software Science, DKU

Cho, Seong-je (조성제)

Spring, 2020

1번 과제 목적

- 실제 생활에서 꼭 필요한 컴퓨터 보안 기능/서비스 등을 익힌다.
- 온라인 뱅킹 시, 안전한 금융 거래 방식을 사용한다.
- 악성 프로그램으로부터 내 PC를 보호한다.
- 방화벽의 개념을 이해한다.
- Network firewall과 Anti-malware SW와의 차이점을 파악하여 설명한다.

“1번 과제”는 다음 3가지에 대해 조사/정리

크게 3가지 사항에 대해 조사하여 정리

1) 국내 은행들의 인터넷 뱅킹에서 적용하고 있는 보안 기능/기술/서비스 등을 조사하여 정리.
   - 공인 인증서 (accredited certificate)
   - 키보드 보안 프로그램 (anti-keylogger 등)
   - OTP (one time pad) Token

2) 국내 백신 소프트웨어의 주요 원리 및 기능 등을 조사하여 정리
   - 악성 프로그램(malware)인지 아닌지 어떻게 파악하는지?
   - 새로운 유형의 악성 프로그램을 탐지하기 위해 사용하는 방식은?

3) 방화벽(firewall)에 대한 원리 및 기능 등을 조사하여 정리
   - Windows Defender 등의 개인 PC 방화벽 포함
   - 방화벽의 주요 목적은 무엇인지? 어떻게 그 목적을 달성하는지?

과제 내용 1)에 대한 추가 설명

1) 국내 은행들의 인터넷 뱅킹에서 적용되고 있는 컴퓨터보안 기능/기술/서비스에 대해 조사하여 정리하시오.

- 최소한 다음 4가지에 대해는 조사해야 함.
  - 인터넷 뱅킹 서비스 관련하여 어떠한 사이버 위협들이 존재하는지?
  - 공인 인증서 (accredited certificate)의 용도는 무엇인지?
  - 키보드 보안 프로그램 (anti-key logger 등)의 목적 및 기능은 무엇인지?
  - OTP (one time pad) Token의 목적 및 기능은 무엇인지?
- 다음 보안 기능/서비스들에 대해서도 조사하여 정리
  - 피싱방지 서비스 (anti-phishing service)
  - 전자금융사기 예방 서비스 (Online and mobile banking fraud prevention, 또는 Anti-fraud technologies in online banking)

과제 내용 2)에 대한 추가 설명

2) 국내 백신 SW들의 동작 원리 및 기능을 조사하여 정리하시오.

- 백신 소프트웨어 = Anti-virus SW 또는 Anti-malware SW
  - Malware = Malicious software = Malicious program
- 대표적인 백신 SW 제품으로 V3 Pro/Lite, Alyac, ViRobot 등이 있음

- **최소한 다음 내용에 대해 조사하여 정리해야 함**
  - 악성 프로그램들 중, Adware, Spyware, Ransomware, Backdoor 에 대해 설명하시오.
  - 백신 SW가 악성 프로그램(malware)인지 아닌지 어떻게 탐지하는지?
  - 새로운 유형의 악성 프로그램을 탐지하기 위해서는 사용하는 방식은?
  - 다음 두 가지 경우(①과 ②) 중에서 어떤 경우가 더 나쁜 상황인지? 그리고 그 이유를 같이 설명하시오.
    ① 악성 프로그램을 정상 프로그램으로 탐지하는 경우
    ② 정상 프로그램을 악성프로그램으로 탐지하는 경우

※ 조사가 어려우면, 할 수 있는 만큼 조사하여 정리하면 됩니다.

과제 내용 3)에 대한 추가 설명

3) 방화벽(firewall)에 대한 동작 원리 및 기능 등을 조사하여 정리하시오.

- 방화벽의 예는 다음과 같음
  - 네트워크 방화벽, 개인 PC 방화벽, Windows Defender, …

- **최소한 다음 내용에 대해 조사하여 정리해야 함.**
  - 방화벽의 원리 및 주요 기능은?
  - 방화벽을 적용하여 DoS 또는 DDoS 공격을 방어할 수 있는가?
    - 있다면, 어떤 방식으로 DoS 또는 DDoS 공격을 방어하는가?
  - 네트워크 방화벽과 백신 SW와의 차이점은?

보고서 작성 시 포함 내용

- **보고서 표지에 포함될 내용**
  - 과목명(SW보안 개론), 분반 표시(2분반 또는 3분반),
  - 과제번호 및 제목 (1번 과제: 인터넷뱅킹, 백신SW, 방화벽 조사 정리)
  - 성명, 학번
  - 제출일

- **보고서 내용에 포함될 내용**
  1) 앞서 설명한 ①인터넷뱅킹에서 적용되는 보안 기능/기술/서비스, ②백신 SW의 동작 원리 및 기능, ③ 방화벽의 동작원리 및 기능을 정리
  2) 참고한 교재/자료/문서/논문 등이 있으면, 위 ①, ②, ③ 별로 구분하여 표시하여 보고서에 포함
  3) Discussion
     - 1번 과제 수행하면서 어려운 점
     - 다음 과제에서 조사해 보고 싶은 내용
     - 이번 강의에서 배우고 싶은 내용

과제물 수행 방식

- 개인 과제
  - 개별적으로 조사하여 보고서로 정리
  - No Cheating
- 신뢰할 만한 교재/자료/문서/논문/사이트를 활용
  - 보고서 작성 시에, 참조(참고)한 교재/자료/문서/논문/사이트 정보를 포함하여 기술
  - Trusted websites: https://scholar.google.com/ , Scicece.gov, NIST – Glossary, …
- Deadline
  - 4월 7일까지

과제물 제출

- 과제 보고서를 인쇄본(hardcopy) 또는 이메일로 파일로 제출

- 이메일에 파일 첨부로 TA(조교선생)에게 제출 시,
  - 이메일 제목: "SW보안개론(분반) 1번 과제 제출"
    - 2분반 이메일 제목: SW보안개론(2) 1번 과제 제출
    - 3분반 이메일 제목: SW보안개론(3) 1번 과제 제출
  - 보고서 파일 이름은 "ISS(분반)_HW1_이름_학번_mmdd" 형식으로
    - **예시) 3분반 홍길동 (32165678), 제출일이 4월 2일이면 →**

      "ISS(3)_HW1_홍길동_32165678_0402"
  - TA
    - **조재희 (jehee1204@gmail.com), 미디어센터 505호**

- 인쇄본: 미디어센터 505호, 또는 학과사무실(조성제교수 사물함)로 제출