모바일 보안 요약

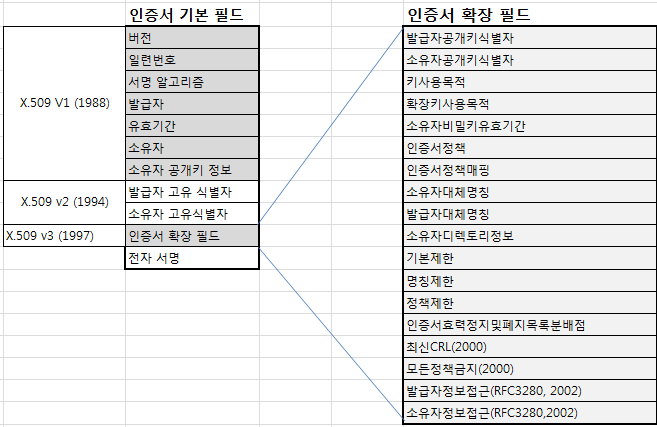
1. **기존환경과 모바일 환경에서의 보안위협 비교**
   1. 기존환경
      1. IT업체 우회 공격으로 주요 기반시설 침탈 및 대규모 공격
      2. 랜섬웨어
      3. IOT관련 위협
   2. 모바일 환경 보안위협
      1. 분실 및 도난
      2. 사회공학적기법(유용한 프로그램으로 위장한 악성프로그램)
      3. 취약점(어플리케이션 취약점, 모바일 플랫폼 취약점)
      4. 기존위협확대(사이버침해공격, 바이러스,웜) 및 신규 위협(무선랜, 블루투스, GPS 등 침해경로 다변화, 개방형 앱 안전성 보장 미흡
   3. 보안위협 비교

|  |  |  |
| --- | --- | --- |
| 보안위협 비교 | 모바일 기기 | 기존환경 예시: PC |
| 사용자/단말 | 분실/도난 가능성 높음 | 분실/도난 가능성 낮음 |
| 네트워크 | 대부분 무선기기 사용 | 유선망 & 무선망 사용 |
| 모바일Ddos |
| 응용서비스 | 위치/개인정보 유출 | 개인문서 유출 |
| 모바일 콘텐츠 | 모바일스팸 | 불법/유해콘텐츠 유통 |
| 불법/유해콘텐츠 유통 |

1. **모바일 악성코드 유포과정과 감염 시 증상**
   1. 유포과정
      1. 스마트폰 악성코드 WinCE/TerDial
         1. 3D Anti Terrorist Action 이라는 게임에 트로이 목마 형태의 악성코드
         2. **악성코드가 포함된 게임이 해외 유명 스마트폰 어플리케이션 공유 사이트에서 유포**
         3. **국내의 경우 윈도우 모바일 이용자 카페등의 커뮤니티에서 무료게임 공유형태로 유포**
      2. 게이니미(Geinimi, 10년 12월)
         1. 안드로이드 최초 봇넷 기능을 모바일 악성코드
         2. **중국 사설 안드로이드 마켓에서 다수의 유명앱을 리패키징하여 유통**
         3. 주기적으로 단말기 정보를 C&C로 유출하고 명령 다운받아 악성 행위 수행
   2. 감염 시 증상
      1. 개인정보 유출
      2. 장치 이용의 제한
      3. 부정과금 유발
      4. 모바일 DDOS
2. **스미싱- 개념, 각각의 특징 및 차이점, 사례, 공격기법 등**
   1. 개념
      1. SMS와 피싱(Phishing)의 합성어로 스마트폰 이용자들에게 URL이 포함 된 SMS를 전송하여 악성앱 설치를 유도한 후 스마트폰을 통제하여 개인정보 유출 및 금전적인 피해를 가하는 해킹 기법
   2. 특징 및 차이점
      1. 2012년도
         1. 최초의 스미싱 악성앱 탐지(주로 소액결제 인증문자를 가로채 금전적 이득 획득)
      2. 2013년도
         1. 공인인증서 탈취 악성앱 탐지
            1. 기기정보, 성명, 주민등록번호, 은행계좌번호, 공인인증서 등 금융정보 및 개인정보 탈취
      3. 2014년도
         1. 보호대책 우회기능 진화
            1. 버튼클릭, 캡차코드 입력 등 사용자 행위를 요구하는 방식으로 유포
            2. 백신앱 삭제, 원격제어를 통한 정보유출지 변경 등 보호조치 무력화
      4. 2015년도
         1. 앱 다운 및 삭제 방해 등 지능화
            1. 특정 전화번호를 입력해야만 다운, 관리자권한해제 방해를 통한 앱 삭제 방해
            2. 원격제어를 통한 문자 발송 등 악성 행위 표적화, 지능화
      5. 2016년도
         1. Drive by Download 형태로 진화
   3. 사례
      1. SMS 탈취 후 부정 결제
         1. 미리 확보된 피해자의 개인정보를 기반으로 스팸문자발송
         2. 피해자는 악성앱을 설치하고, 단말기 정보 및 설치 성공정보를 해커서버로 전송
         3. 해커는 게임 등 각종 구매사이트에서 소액결제 진행
         4. 구매사이트에서는 인증번호가 포함 된 SMS를 피해자에게 전송
         5. 악성앱은 수신 된 SMS를 피해자에게 보이지 않도록 조작 후 해커 서버로 전송(탈취)
         6. 해커는 탈취한 인증번호를 입력해 결제 성공
         7. 결제를 통해 확보한 사이버머니 현금화
   4. 공격기법
      1. SMS 탈취기법
      2. 공인인증서 탈취기법
      3. 감염된 스마트폰을 이용한 추가 스미싱 문자 유포
      4. Drive by Download 악성앱 유포
3. **대칭키암호와 공개키암호- 개념, 특성, 용도, 암호화방식 등**
   1. 개념
      1. 대칭키
         1. 통신을 하는 사람은 비공개 된 비밀키 공유, 암호문을 만드는 알고리즘 공개, 암호문 공개
      2. 공개키
         1. 암호화 키와 복호화 키가 서로 다름, 공개키만 공개, 속도가 느림
   2. 특성, 암호화 방식, 용도

|  |  |  |
| --- | --- | --- |
|  | 대칭키 암호방식 | 공개키 암호방식 |
| 특성 및 용도 | | |
| 암호화 속도 | 고속 | 저속 |
| 경제성 | 높음 | 낮음 |
| 전자서명 | 복잡 | 간단 |
| 암호화 방식 | 스트림암호 | 모르겠어요 |
| 블록암호 |  |
| 용도 | 무선환경 암호화 | 공인인증서, 전자서명 |

1. 공개키암호를 이용한 전자서명방식과 공인인증서 구조
   1. 공개키 암호를 이용한 전자서명 방식
      1. 전자문서 서명자 메지지 생성후 메시지 전송
      2. 메시지의 해쉬함수를 통한 해쉬값 생성
      3. 전자서명 알고리즘을 통한 개인키를 통한 서명 생성
      4. 서명 전송
   2. 전자문서 검증 확인
      1. 수신된 메시지의 해쉬함수를 통한 해쉬값 취득
      2. 수신된 서명을 공개키를 통한 복호화
      3. 메시지의 해쉬값과 복호화된 해쉬값을 비교하여 검증
   3. 공인인증서 구조 표 참조



1. **코드서명 기법 및 활용**
   1. 기법
      1. 프로그램을 다운받아 설치하기 전에 배포자, 개발자에 대한 신원확인을 통하여 프로그램의 위조나 변조에 대한 무결성을 검증하기 위하여 사용되는 기법
   2. 활용
      1. 어플리케이션을 위한 툴을 제공
      2. 개발자확인, 어플리케이션 데이터 공유, 마켓정책 준수확인
      3. 심비안
         1. 앱의 시스템 기능 제약용
         2. 사용 시스템 기능 레벨에따라 서명 & 테스팅 하우스에 제출
      4. IOS
         1. 앱의 출처 확인용
         2. 서명용 키는 Apple(CA)에서 발행
         3. Apple이 서명 검증 후 마켓에 업로드
2. **모바일 악성코드 분석방법 및 apk 구조** 
   1. 모바일 악성코드 분석방법
      1. 동적분석
         1. 설치 및 감염 상태 분석
         2. 원격지 차단 조치
         3. C2 주소 파악 및 트래픽 전송내용 분석
      2. 정적분석
         1. 디컴파일
         2. 소스레벨코드 분석
         3. 코드분석
         4. C&C 확인
   2. apk 파일의 구조
      1. AndroidManifest.xml : 어플리케이션에 대한 설명 및 실행권한 등의 정보를 지니는 XML 파일
      2. Classes.dex : Dalvik 가상머신에서 동작하는 바이너리 실행 파일
      3. /res : 컴파일되지 않은 리소스 파일(아이콘, 이미지, 음악 등)들이 포함된 폴더
      4. /META-INF : 배포시 인증서로 서명한 내용, APK파일내 폴더, 파일에 대한 SHA-1 해쉬값
      5. resources.arsc : 컴파일된 리소스파일
3. **IoT 보안위협**
   1. 센서/디바이스
      1. 저사양 디바이스 해킹(초경량, 저전력 디바이스를 위한 보안기술 적용 어려움)
      2. 디바이스 관리 취약점 증가(디바이스 수 증가에 따른 보안패치 적용, 모니터링의 어려움등
   2. 네트워크
      1. 무선네트워크 취약점
         1. 이종 무선네트워크 상호연동으로, 일정한 보안(인증,암호화)수준 유지 어려움
      2. 네트워크 트래픽 공격량 급증
         1. 대규모 디바이스로부터 발생하는 악성코드 감염 및 트래픽 폭증
   3. 플랫폼/서비스
      1. 공개 플랫폼 취약점
         1. Open API를 악용한 기기-서비스간 데이터 위변조 및 오작동 유발
      2. 개인정보 유출/프라이버시 침해
         1. 다양한 디바이스로부터 수집 된 단편적인 정보의 조합으로 새로운 개인 식별정보 생성
4. **BYOD 보안위협**
   1. 단말관점
      1. 분실 기기(자동 로그인 악용)
      2. 장기 미사용 기기 악용 계정 도용
      3. 문제점: 기기/사용자 식별 취약
   2. 접속환경 관점
      1. 공개 Wi-Fi 이용 접속
      2. 취약한 OS,SW 설치 기기 이용
      3. 문제점: 접속 환경 식별 불가
   3. 사용자 관점
      1. 악의적 내부 사용자
      2. 악성코드 감염 기기 원격 이용
      3. 문제점: 접속/이용 행위 분석 불가
   4. 개인 기기들이 기업 내부 인프라에 접속함으로 새로운 보안 위협 발생
      1. 데이터 유출
      2. 기업 내부 접근
      3. 직원통제 문제
      4. 보안 정책 수립 복잡
      5. 해킹/악성코드 감염
5. **클라우드 모델, 보안고려사항 등**
   1. 클라우드 모델
      1. SaaS(Software as a Service)
         1. 소프트웨어/어플리케이션을 제공하는 목적으로 만들어진 모델, 표준화 된 어플리케이션 프로세스 제공(icloud, Dropbox, One note 등)
      2. PaaS (Platform as a Service)
         1. 개발자가 자신의 어플리케이션을 개발, 테스트, 실행 할 수 있는 컴퓨팅 플랫폼 제공(Linux, Apache, PHP,MySQL)
      3. IaaS(Infrastructure as a Service)
         1. 서버, 스토리지, 네트워크 등 인프라 자원을 사용량 기반으로 제공, 기본 스토리지와 컴퓨팅 능력 제공(CPU, DISK 등)
   2. 보안고려사항
      1. 위협
         1. 새로운 공격경로(가상 네트워크를 통한 패킷, 스피닝, 가상머신간 해킹)
         2. 자원 공유로 인한 비인가자의 정보 접근
         3. 자원 집중화로 인한 대규모 피해 및 악용
         4. 보안 책임 소재 불분명 및 보안 정책 복잡화
         5. 법규 및 규제의 문제
      2. 위의 위협에 의해 보안 고려사항은 하기와 같다.
         1. 보안 강화를 위해 클라우드 플랫폼 활용: 통합 보안 로그 수집/분석
         2. 클라우드 이용자의 서비스 및 데이터 보호
         3. 기업 보호를 위해 SeaaS 활용
         4. 분야마다 클라우드 서비스 이용이 가능하도록 법률 제정