

SW개발보안

소프트웨어보안 소개

목차

- 세상을 바꾼 소프트웨어
- 소프트웨어와 보안
- 국내 SW관련 법제도
- 주요 보안 취약점 소개



세상을 바꾼 소프트웨어

생각보다 빠른 시대 변화 모습 (인쇄)



생각보다 빠른 시대 변화 모습 (인쇄)



생각보다 빠른 시대 변화 모습 (인쇄)



생각보다 빠른 시대 변화 모습 (결제)



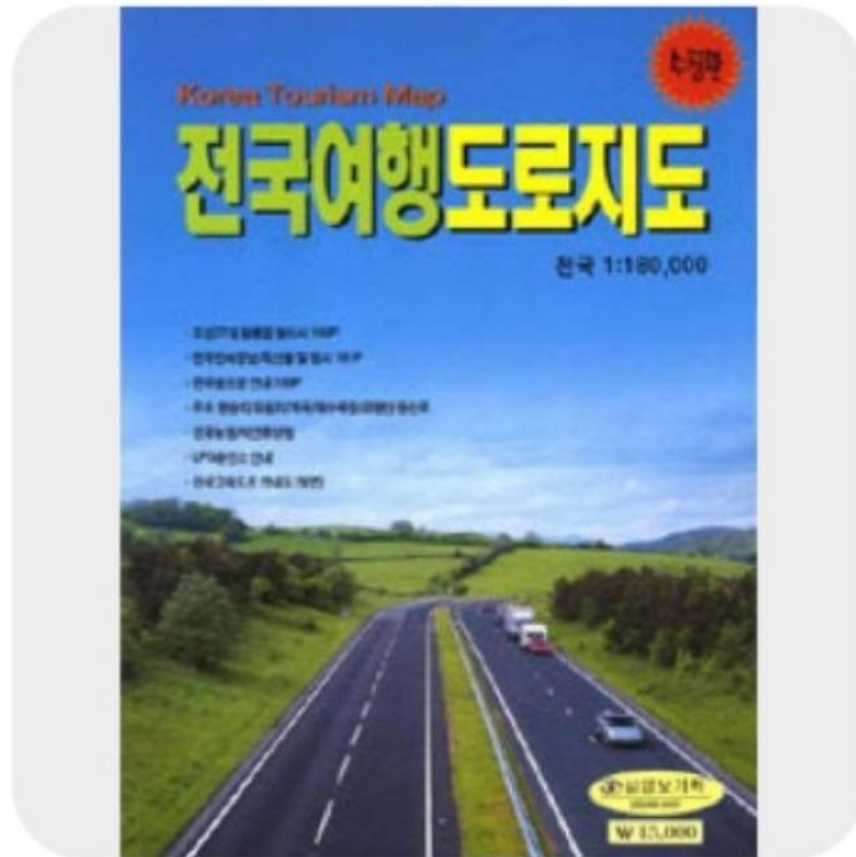
생각보다 빠른 시대 변화 모습 (결제)



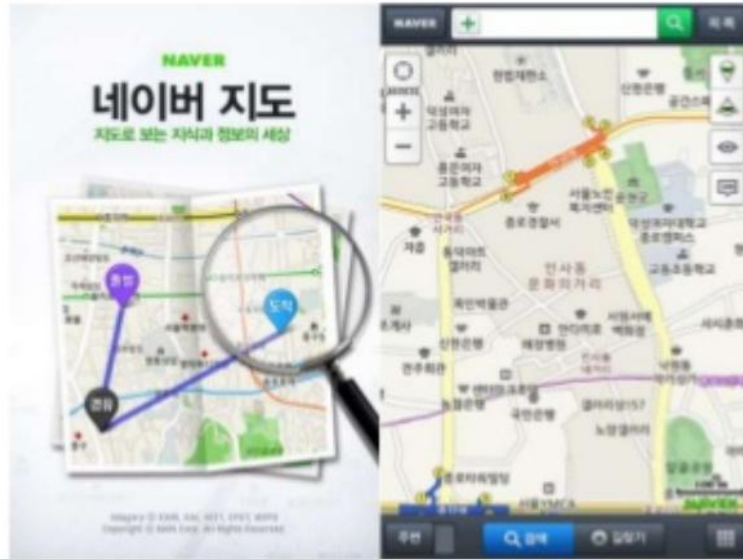
생각보다 빠른 시대 변화 모습 (결제)



생각보다 빠른 시대 변화 모습 (여행)



생각보다 빠른 시대 변화 모습 (여행)



생각보다 빠른 시대 변화 모습 (여행)



생각보다 빠른 시대 변화 모습 (통신)



생각보다 빠른 시대 변화 모습 (통신)



세상을 바꾼 소프트웨어

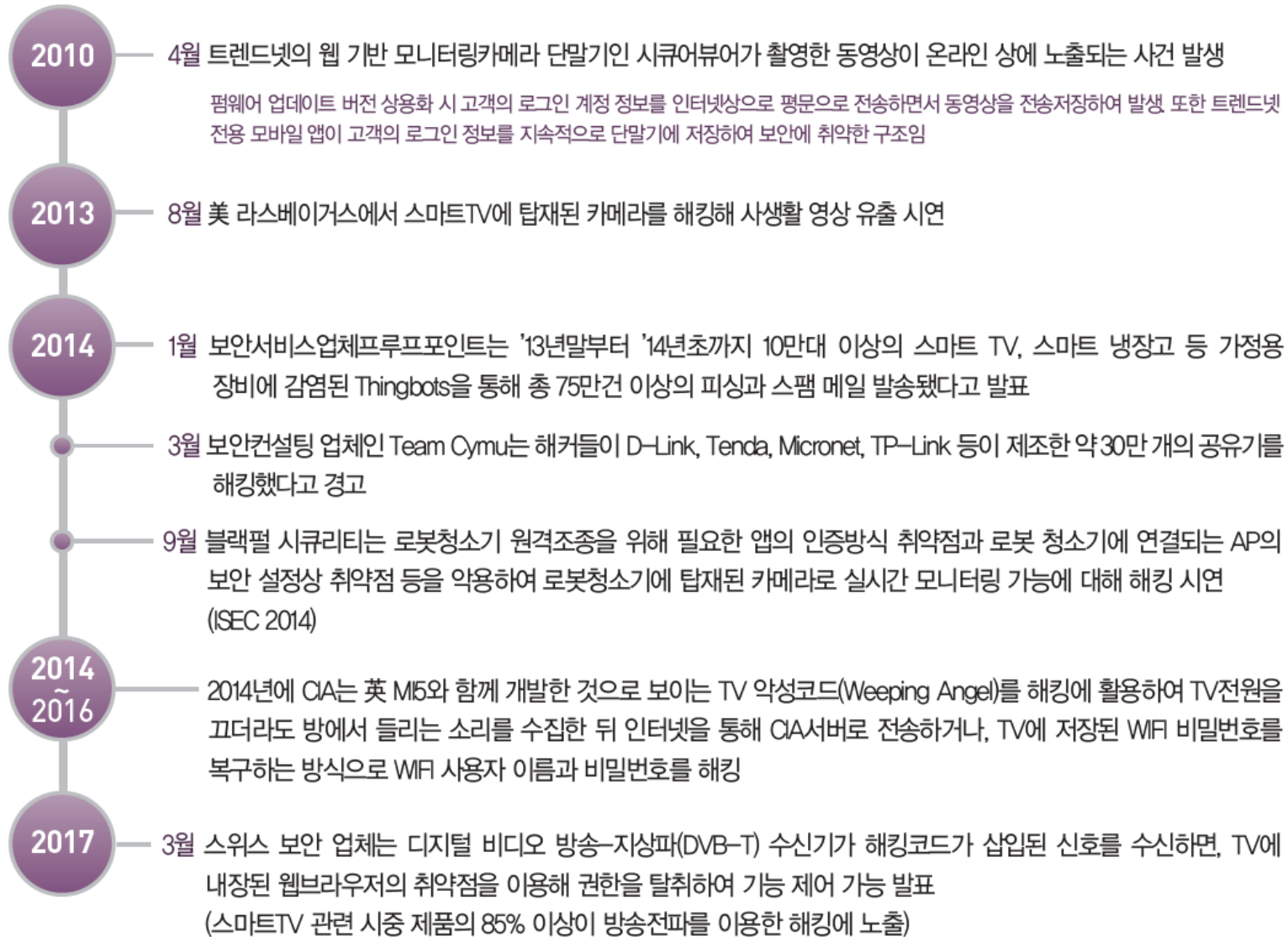


<https://youtu.be/UgxrSW9i1ns>



소프트웨어와 보안

IoT 제품 관련 보안사고 동향



융합산업과 소프트웨어보안 문제

- 'зомби PC'에서 'зомби 기계'로 확대
 - 4차 산업혁명과 함께 모든 사람과 인터넷이 연결되는 '초연결', '클라우드' 기반 소프트웨어 산업사회가 다가옴
 - 보안이 취약한 사물인터넷 기기로 봇넷이 확대 (예: 2016 Mirai botnet)
 - 2021년경에는 스마트 의료기기, 자율주행차, 웨어러블 디바이스 등 IoT기기 보급률이 약160억개에 달할 것으로 예상



**Hackers Remotely Kill
a Jeep on a Highway**

<https://youtu.be/MK0SrxBC1xs>

융합산업과 소프트웨어보안 문제

- 인공지능 소프트웨어 기술을 악용한 사이버 범죄 증가
 - 인공지능을 이용하여 보안 시스템이 탐지 못하는 악성코드를 작성하고, 네트워크 침입을 위한 탐색과 공격을 자동화
 - 인공지능을 이용하여 자동으로 피싱을 시도 (예: Deepfake)
 - 공격과 방어를 하려는 인공지능 알고리즘의 대결이 치열해질 것으로 보임



'Deepfake' videos become new weapon in security

https://youtu.be/a_uSo30k5eg

융합산업 속 소프트웨어 위협

- 초연결과 SW사회 도래

- 인공지능 기계가 사람을 대신 → 기계는 SW가 운영함
- 모든 조직은 개발 운영상의 비용 절감을 목적으로 SW를 클라우드로 이전하고, 데이터는 가치를 더해가고, SW는 데이터를 생산하며, 4차 산업혁명에서 SW요구사항은 홍수처럼 밀려들 것임
- 사물인터넷, 자율주행차 등 초연결 사회가 오고 모든 사물에 운영 소프트웨어가 탑재 되면 융합 보안은 매우 중요해짐

- 소프트웨어 보안 위협

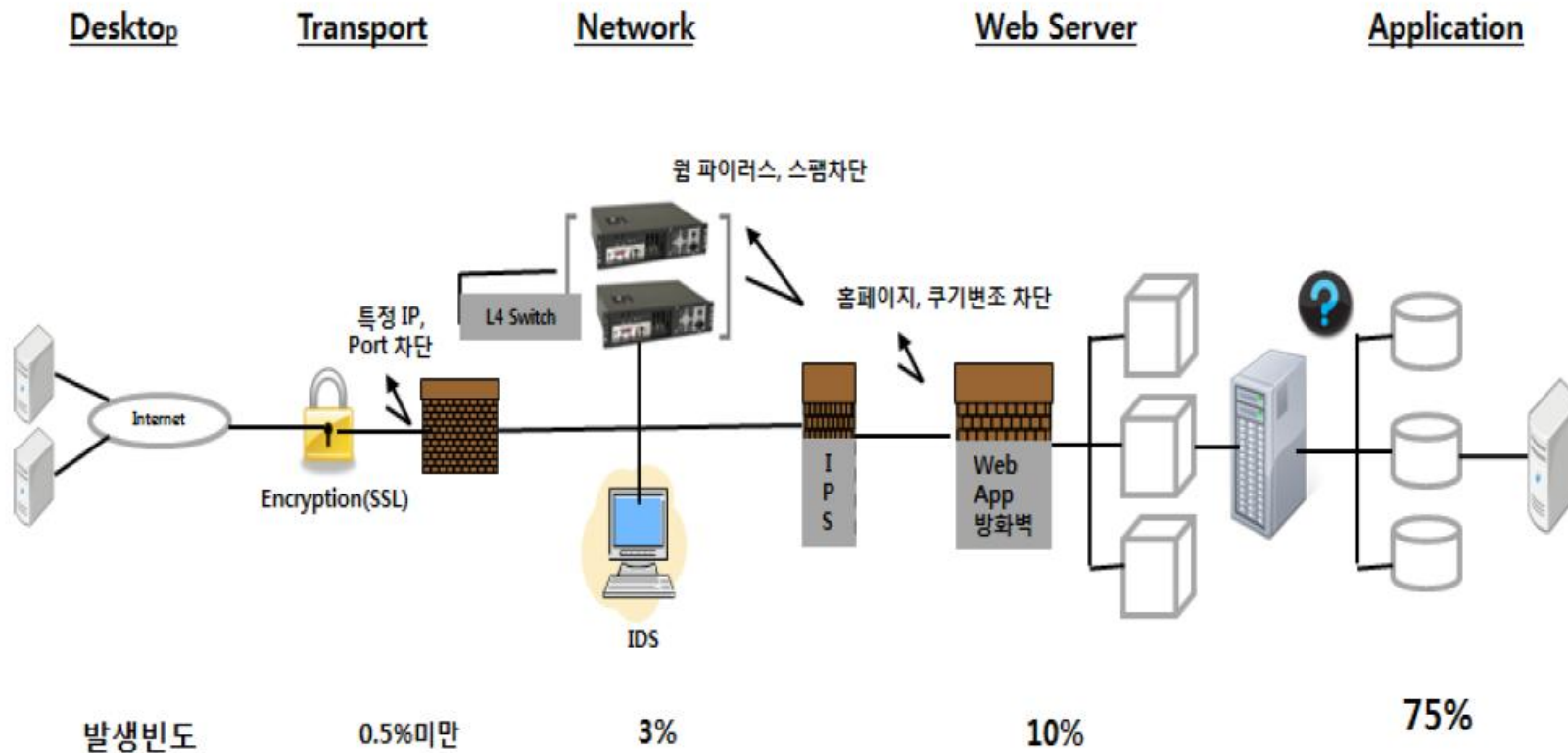
- SW가 사회 전 영역에서 핵심 역할을 수행 할 것으로 예상
- 따라서 SW취약점이 보안 침해사고의 루트로 이용될 수 있음
- 점점 더 복잡해지는 SW설계상 오류가 안전사고 유발 가능

소프트웨어 보안이란?

- Security, as part of the software development process, is an ongoing process involving people and practices, and ensures application confidentiality, integrity, and availability. Secure software is the result of security aware software development processes where security is built in and thus software is developed with security in mind.
- Security is most effective if planned and managed throughout every stage of software development life cycle (SDLC), especially in critical applications or those that process sensitive information.
- The solution to software development security is more than just the technology.

소프트웨어 보안이 중요한 이유

- 가트너에 의하면 소프트웨어 보안침해사고의 75%는 취약점을 내포하는 응용프로그램에 의해 발생되었다고 보고됨



소프트웨어 보안의 중요성

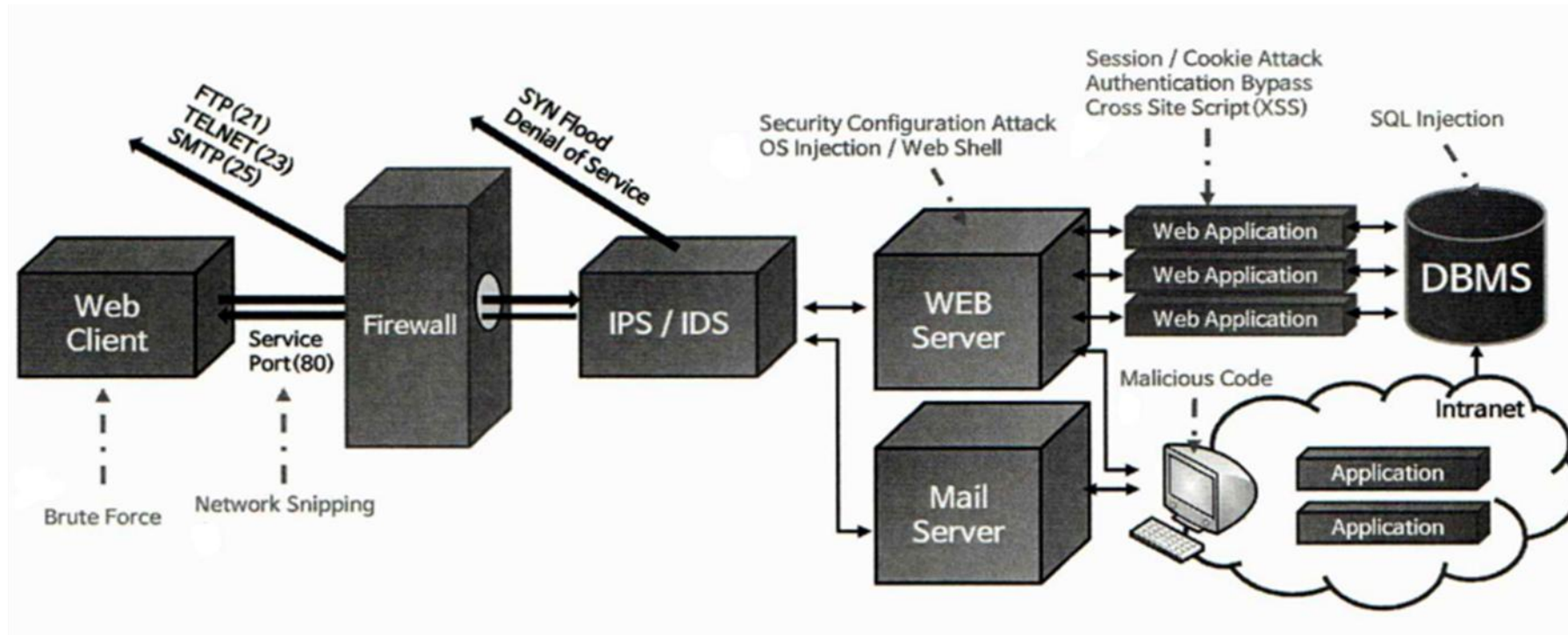
Vulnerabilities By Types/Categories

CVEdetails.com assigns types/categories to vulnerabilities using CWE ids and keywords.

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2015	1037	1104	221	776	152	6	249	50	8	46	379
2016	1180	1173	97	497	99	12	87	41	16	33	519
2017	2478	1542	505	1500	281	155	334	109	57	97	936
2018	2083	1731	503	2041	569	112	479	188	118	85	1248
2019	1205	2029	544	2387	487	126	560	137	103	121	907
2020	1217	1872	465	2201	436	110	415	119	131	100	812
2021	1663	2529	742	2724	548	91	520	126	192	133	677
2022	1863	3368	1788	3403	728	95	769	126	230	146	779
2023	1658	2219	2118	5125	762	112	1392	125	242	179	592
2024	1780	2522	2650	7456	944	257	1435	112	373	121	127
2025	380	535	699	2407	224	80	612	23	127	27	0
Total	16544	20624	10332	30517	5230	1156	6852	1156	1597	1088	6976

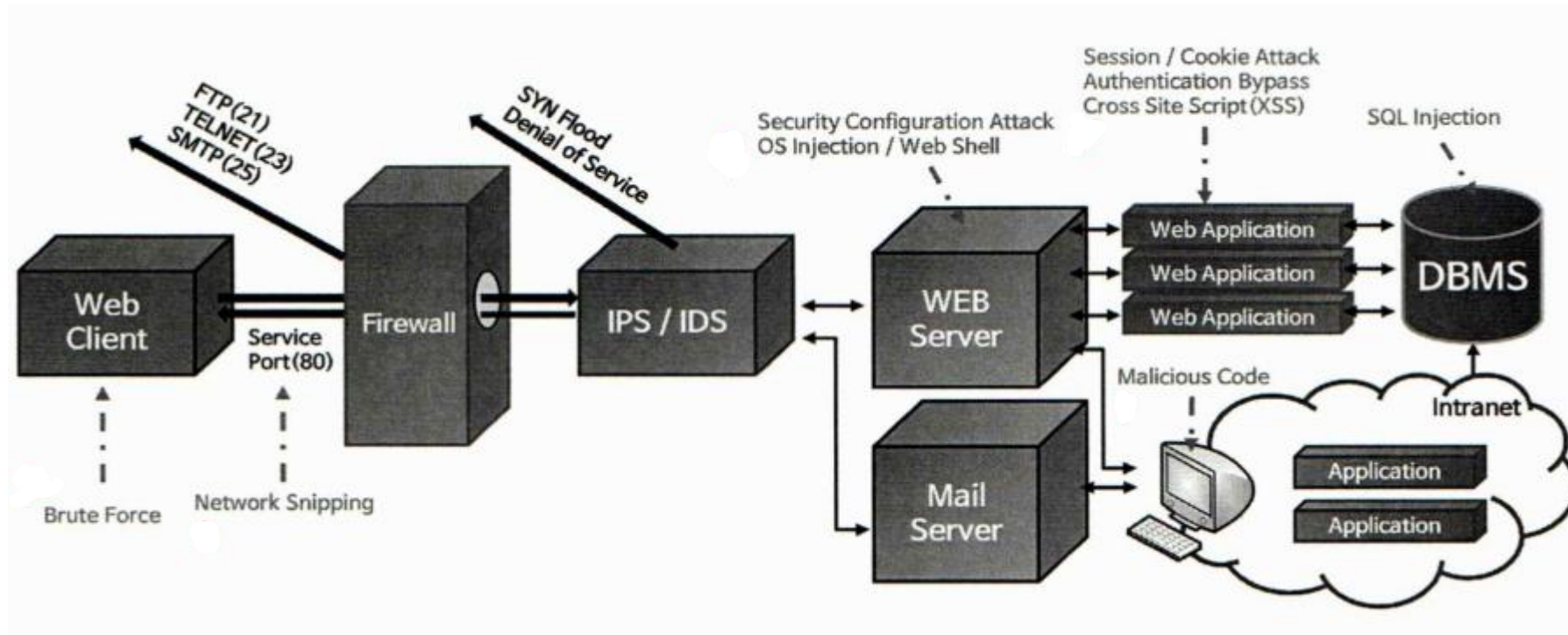
소프트웨어 보안의 필요성

- 방화벽, IDS 등의 다양한 보안솔루션을 통해 DoS, SYN Flood 등의 공격을 막고 있음
- 웹 서비스(HTTP)를 위해 80번 포트가 오픈되어 있어 대부분의 공격이 웹 서비스를 타겟으로 함
- 웹 서버 공격을 통해 웹 어플리케이션 뿐만 아니라 내부망 시스템까지 장악



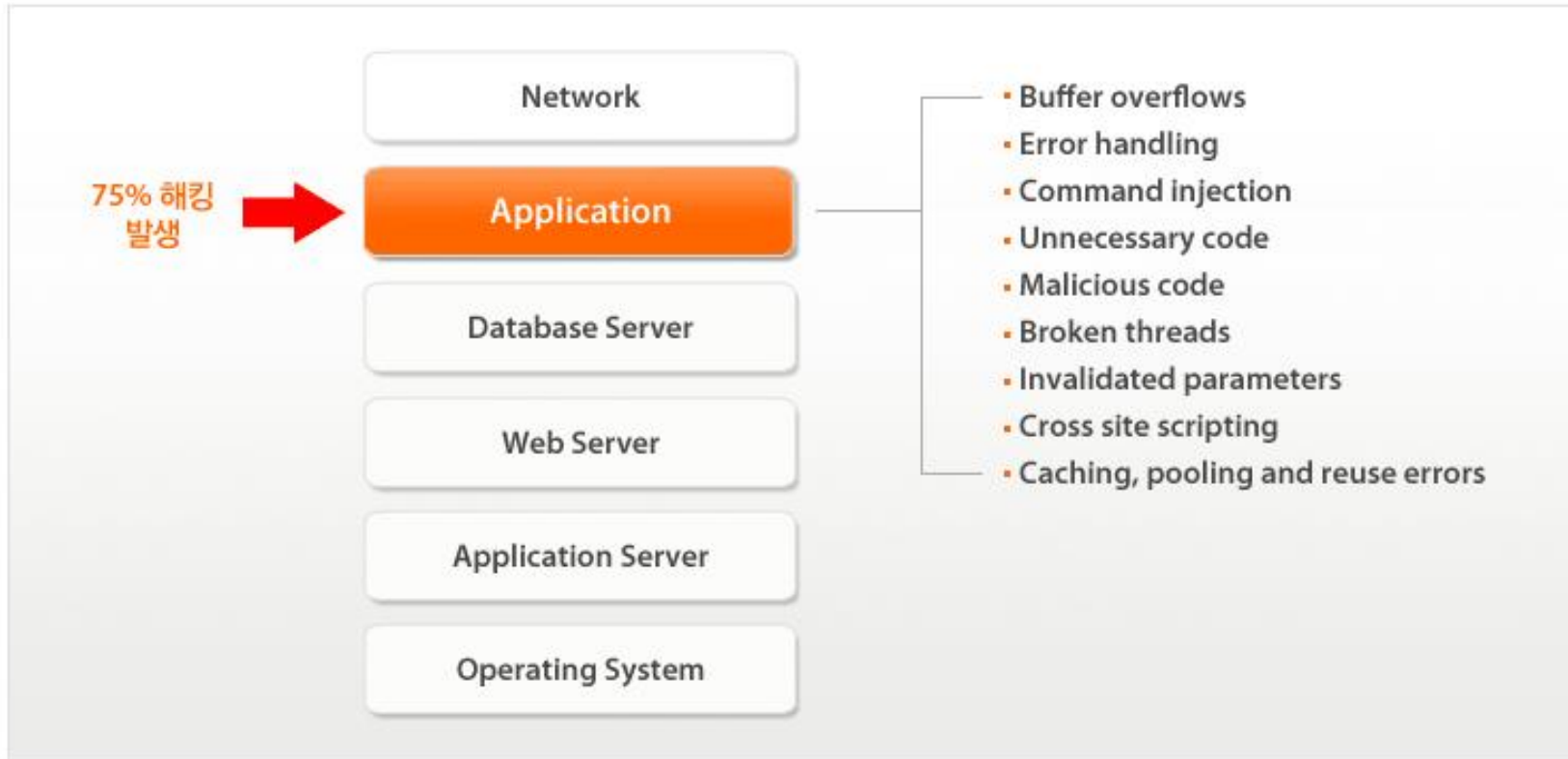
소프트웨어 보안의 필요성

- 다양한 보안솔루션이 구축되어도 HTTP를 통한 공격에 무방비 노출될 수 있으므로 네트워크를 통해 접근 가능한 모든 어플리케이션은 보안성을 고려한 소프트웨어 설계 및 구현 필요



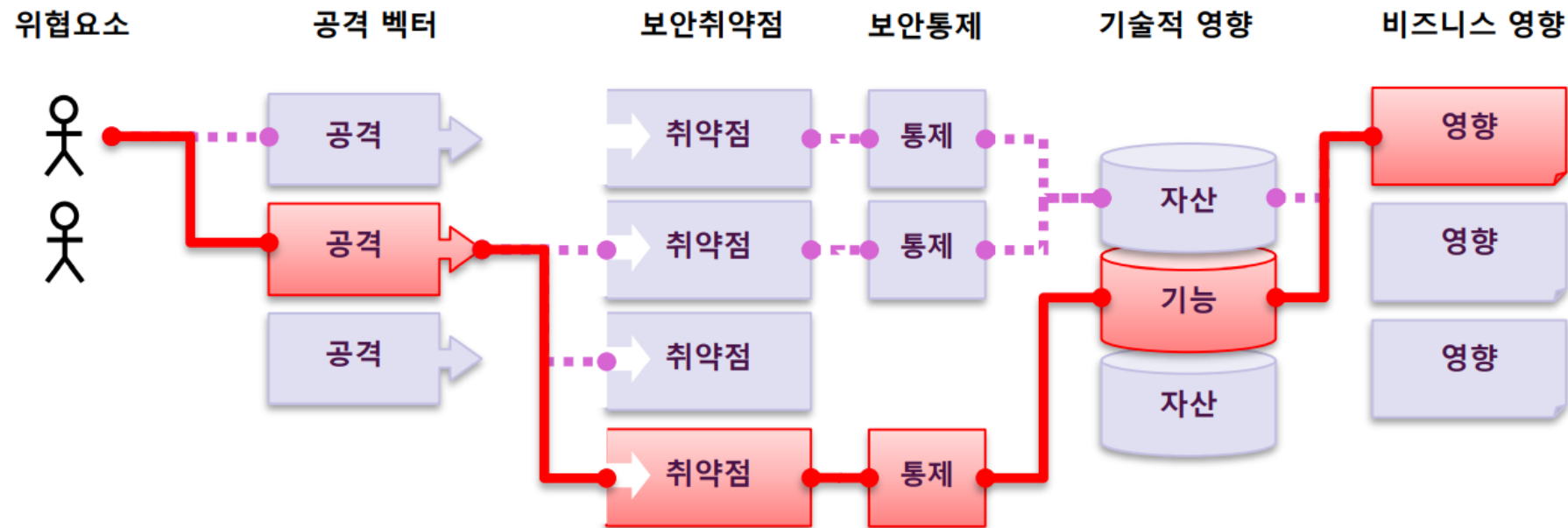
소프트웨어 보안의 필요성

- 보안사고의 75%는 응용프로그램 취약성에서 발생된다



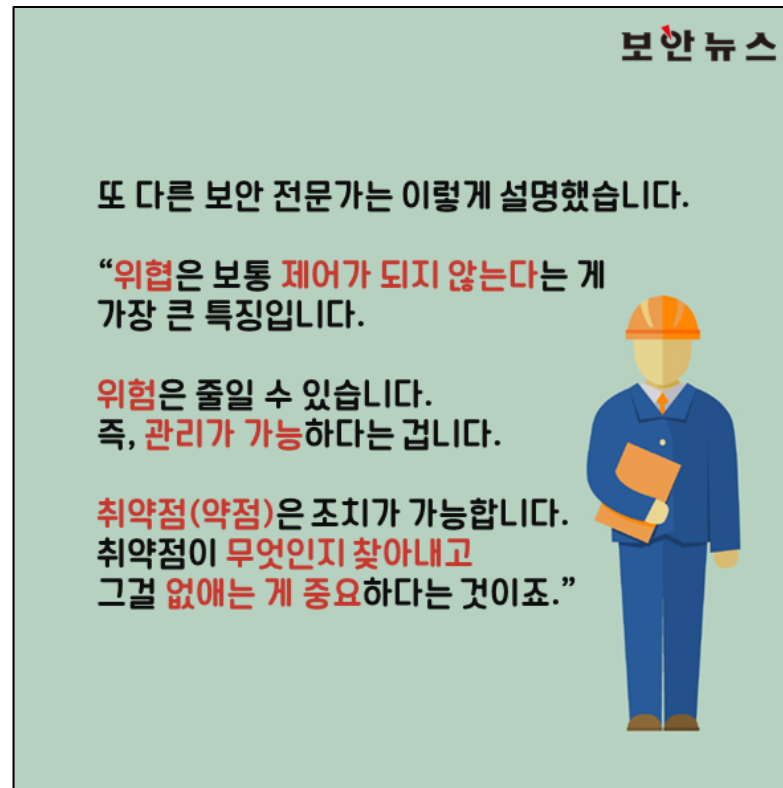
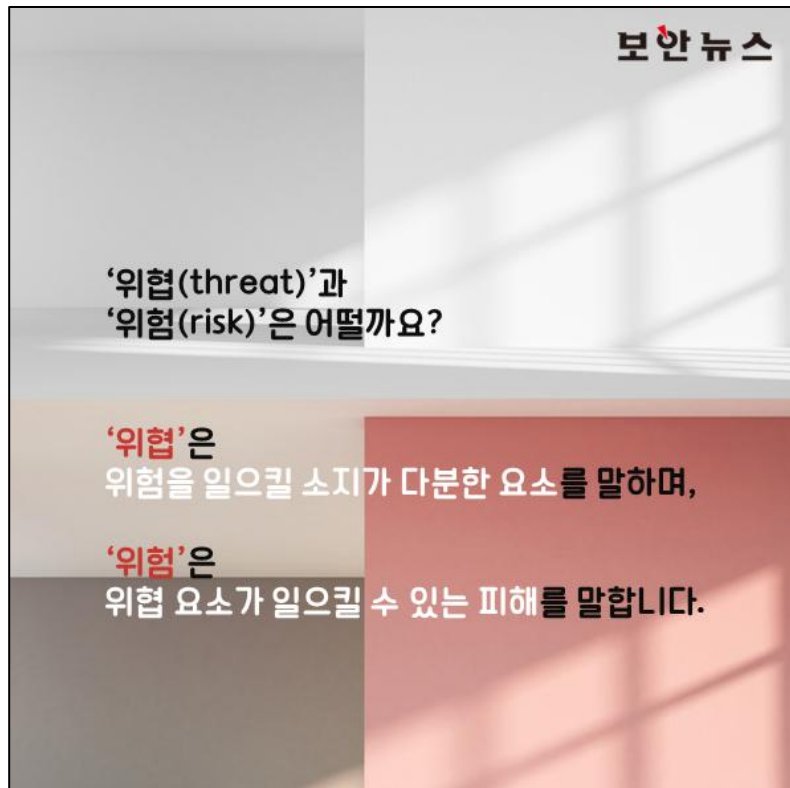
보안 위협 유입 경로

- 공격자는 소프트웨어의 약점(weakness)를 이용하여 소프트웨어 또는 시스템을 통제(control)함
- 공격에 사용된 소프트웨어의 약점은 취약점(vulnerability)으로 분류됨



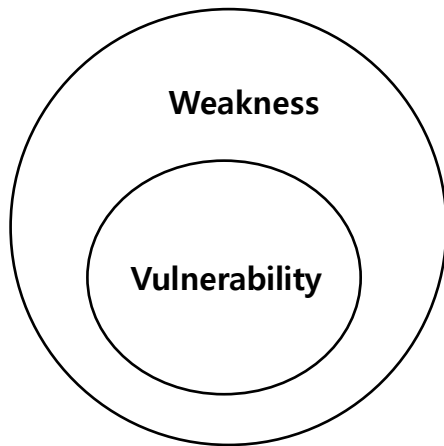
위협 vs. 위험

- 위험(Risk)은 위협(Threat)이 발생시킬 수 있는 잠재적 피해(Loss or Damage)를 의미한다
- 위협은 제어가 되지 않는 경우가 많지만, 위험은 관리가 가능하다



취약점 vs. 약점

- 취약점(Vulnerability)
 - 해킹 등의 외부 공격을 통해 **보안사고의 원인**이 되는 소프트웨어 또는 시스템의 보안 약점
 - MITRE에서 CVE(Common Vulnerabilities and Exposures)의 이름으로 관리
- 약점(Weakness)
 - 의도하지 않은 데이터의 변경 및 접근, 프로그램 실행 중단, 허용되지 않은 부정확한 액션 등을 수행할 수 있게 만드는 일종의 **소프트웨어의 결함**으로, 취약점을 발생할 수 있는 원인 제공
 - MITRE에서 CWE(Common Weakness Enumeration)의 이름으로 관리



취약점 vs. 약점

보안 뉴스


사실 보안 전문가 여러분에게는
‘약점’보다는 **‘취약점’**이란 말이 더 익숙하시겠지만,
이 둘은 사전적으로 **다른 의미**입니다.

‘약점’은
개발 단계에서 발생하는
보안 관련 오류이고,

‘취약점’은
운영 단계에서 발생하는
보안 관련 오류이기
때문입니다.

물론 현장에서는
엄격하게 구분해서 쓰지는 않습니다.

보안 뉴스

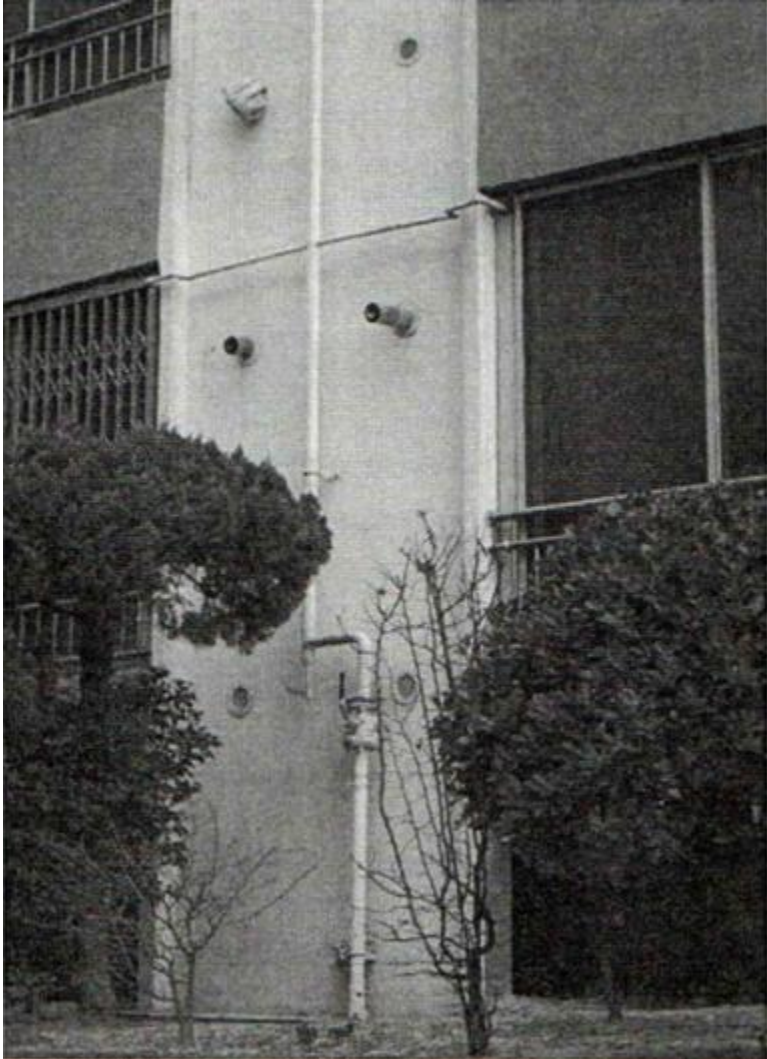


한 보안 전문가는

“보안 **약점**은 weakness로
‘공격에 활용될 여지가 있는 오류’
즉, 이론상 존재하는 위험 요소를 말하고,

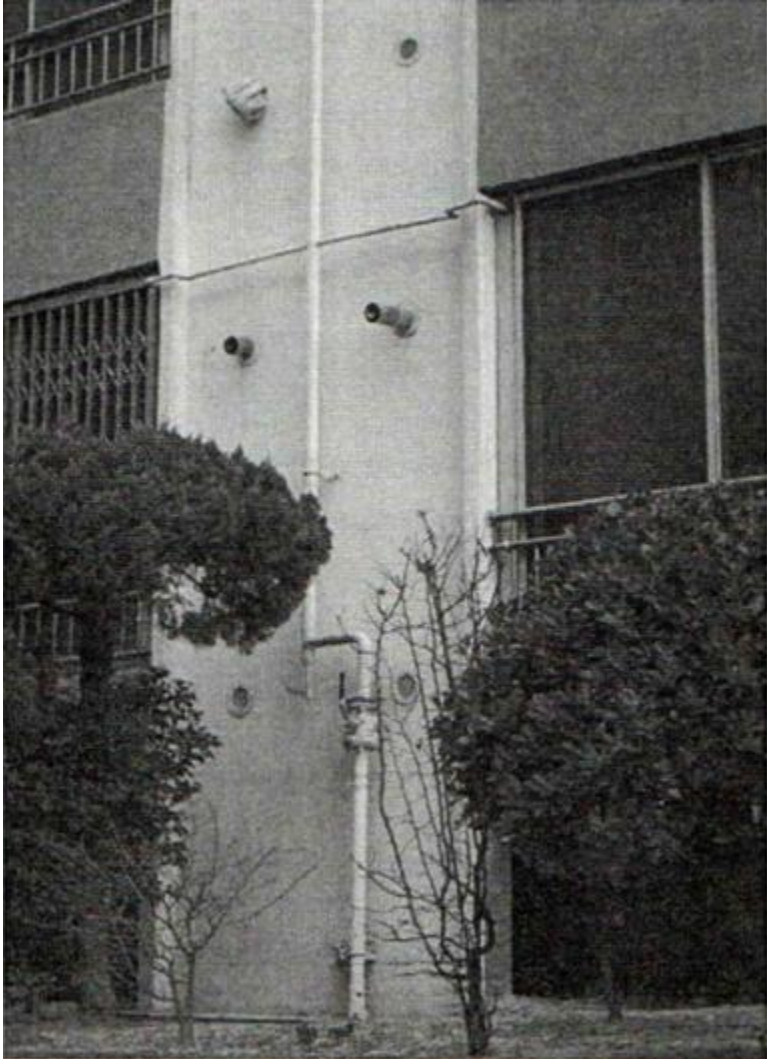
보안 **취약점**은 vulnerability로
‘실제로 공격 구현이 가능한 오류’
즉, 구현이 실제로 가능한 것”이라고
설명했습니다.

취약점 vs. 약점



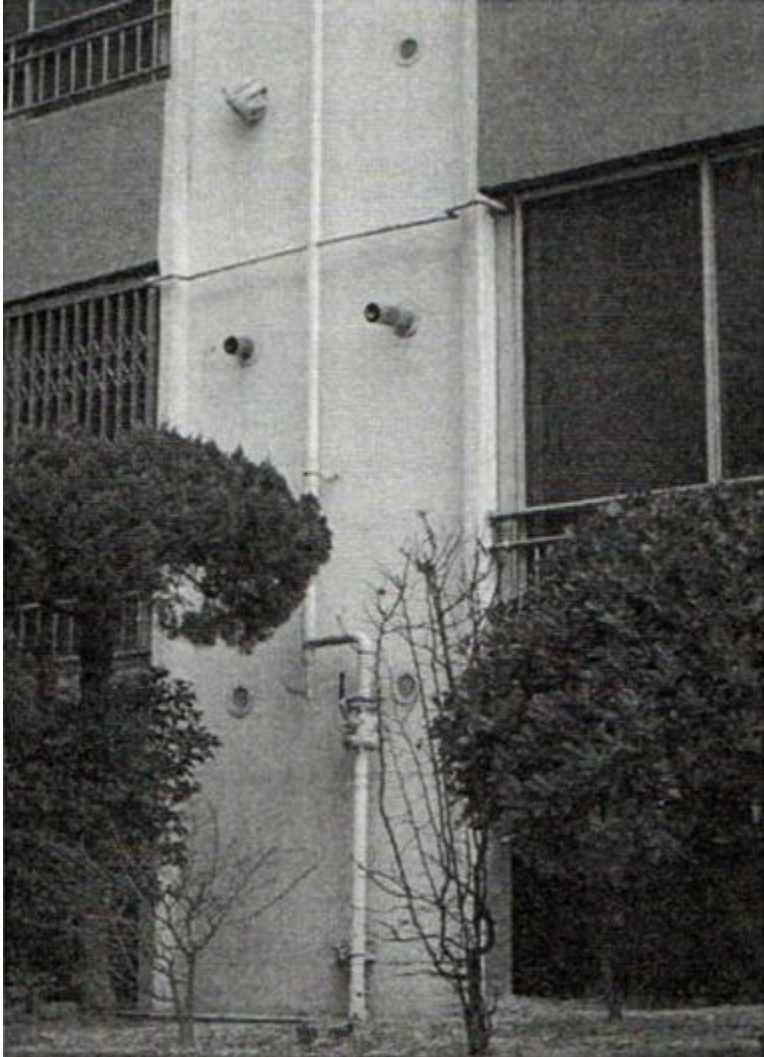
- 이 아파트의 보안 약점은?

취약점 vs. 약점



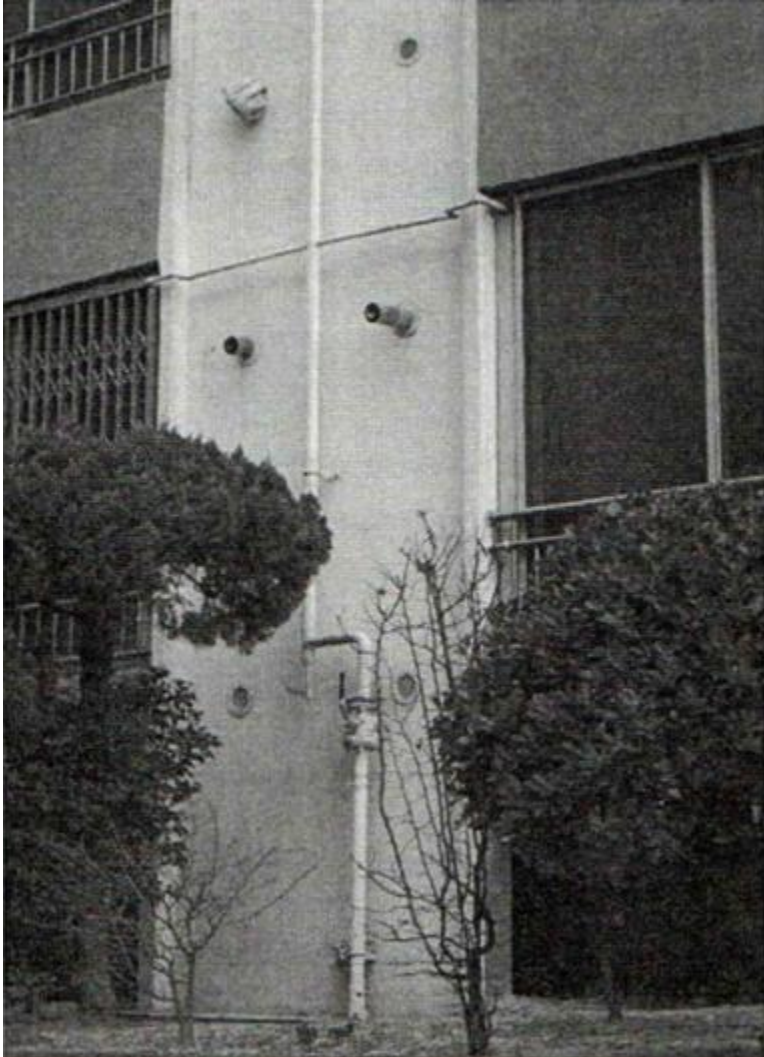
- 이 아파트의 보안 약점은?
 - 외부로 노출된 가스 배관
 - 방범창이 없는 열린 1층 창문

취약점 vs. 약점



- 이 아파트의 보안 약점은?
 - 외부로 노출된 가스 배관
 - 방범창이 없는 열린 1층 창문
- 이 아파트의 보안 취약점은?

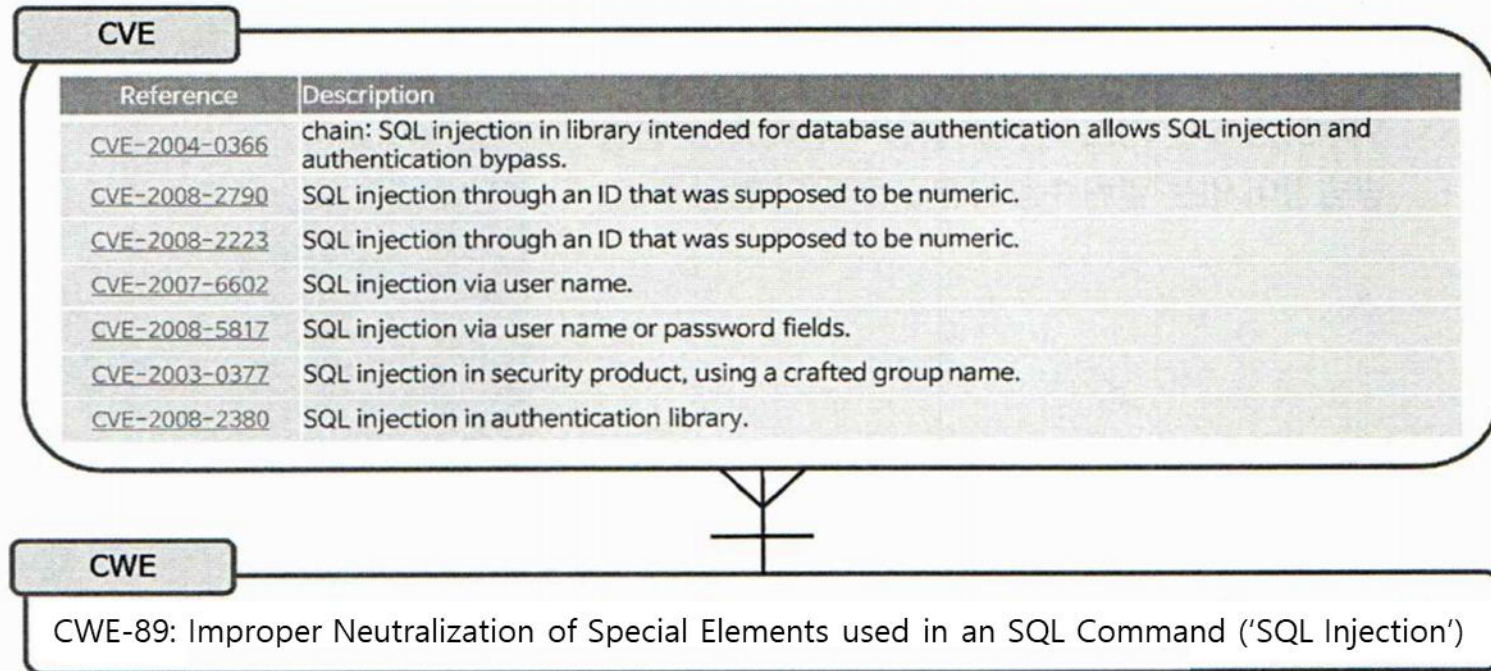
취약점 vs. 약점



- 이 아파트의 보안 약점은?
 - 외부로 노출된 가스 배관
 - 방범창이 없는 열린 1층 창문
- 이 아파트의 보안 취약점은?
 - 외부로 노출된 가스 배관을 통한 베란다 무단 침입
 - 방범창이 없는 열린 1층 창문으로 무단 침입

취약점 vs. 약점

- 하나의 보안 약점은 다수의 취약점의 원인이 될 수 있음
- CVE는 각 제품의 보안 취약점에 대한 분류 체계, CWE 는 보안 취약점의 원인이 되는 소프트웨어의 결함(보안 약점) 분류 체계



취약점 vs. 약점

CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

Other :

[Microsoft Bulletins](#)

[Bugtraq Entries](#)

[CWE Definitions](#)

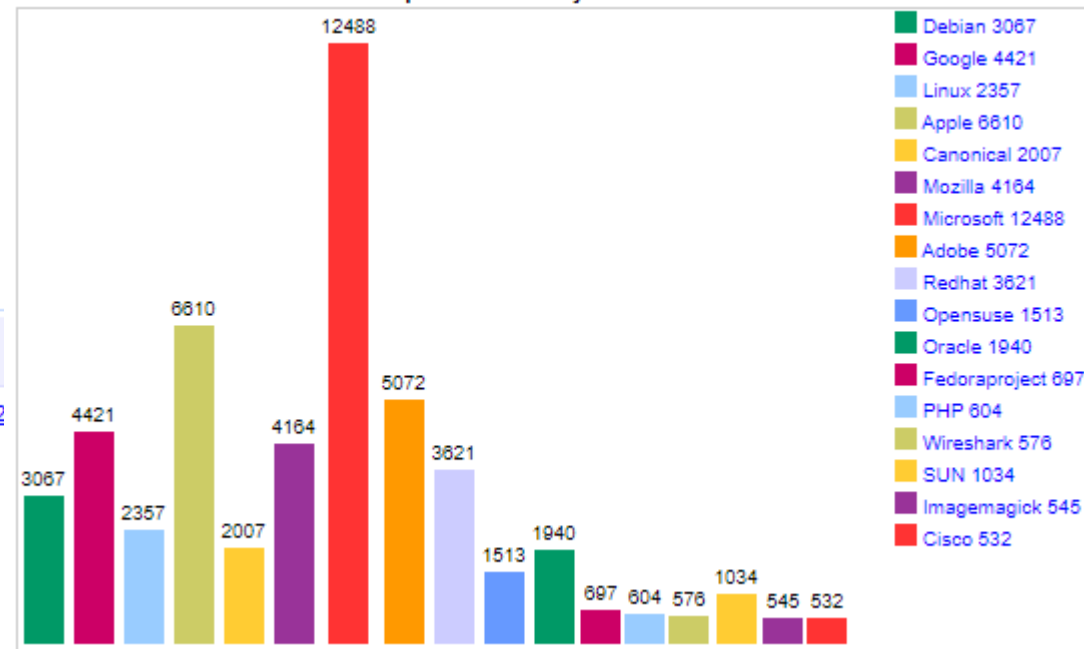
[About & Contact](#)

Top 50 Products By Total Number Of "Distinct" Vulnerabilities

Go to year: [1999](#) [2000](#) [2001](#) [2002](#) [2003](#) [2004](#) [2005](#) [2006](#) [2007](#) [2008](#) [2009](#) [2010](#) [2011](#) [2012](#) [2013](#)

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	3067
2	Android	Google	OS	2563
3	Linux Kernel	Linux	OS	2357
4	Mac Os X	Apple	OS	2212
5	Ubuntu Linux	Canonical	OS	2007
6	Firefox	Mozilla	Application	1873
7	Chrome	Google	Application	1858
8	Iphone Os	Apple	OS	1655
9	Windows Server 2008	Microsoft	OS	1421
10	Windows 7	Microsoft	OS	1283
11	Acrobat Reader Dc	Adobe	Application	1182
12	Acrobat Dc	Adobe	Application	1182
13	Windows 10	Microsoft	OS	1111
14	Flash Player	Adobe	Application	1078
15	Windows Server 2012	Microsoft	OS	1050
16	Enterprise Linux Desktop	Redhat	OS	1039
17	Internet Explorer	Microsoft	Application	1030

Total Number Of Vulnerabilities Of Top 50 Products By Vendor



CVE-2007-6602

공격방법

취약점이 발견된 소프트웨어 및 버전명

CVE-ID

CVE-2007-6602

[Learn more at National Vulnerability Database \(NVD\)](#)

• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

SQL injection vulnerability in app/models/identity.php in NoseRub 0.5.2 and earlier allows remote attackers to execute arbitrary SQL commands via the username field to the login script.

References

Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

취약점이 발생한 지점(기능)

인증 vs. 인가

- 인증(Authentication)
 - 자신의 신원을 주장하는 사람이 맞는지 확인 및 검증하는 절차
- 인가(Authorization)
 - 검증된 사용자에게 자원 접근에 대해 어느 정도의 권한과 서비스를 허용할 것인가에 대한 접근권한 여부와 수준을 결정하는 절차
- 예제)
 - 회사에 들어가기 위해서는 회사 직원이라는 것을 검증하기 위해 지문 또는 사원증을 통해 본인임을 인증한다.
 - 회사 전산실에 들어가기 위해서는 전산실에 출입하여 자원 접근이 가능할 수 있도록 권한을 인가 받아야 한다.
 - 회사 뒷문을 통해 몰래 출입할 수 있다면?
 - 인증 우회(Authentication Bypass)
 - 회사 전산실에 들어갈 권한이 없음에도 불구하고 내 사원증으로 전산실 출입이 가능하다면?
 - 부적절한 인가(Improper Authorization)



국내 SW보안 관련 법·제도

국내 보안 관련 법/제도

- 개인정보 보호법
 - 개인정보의 안전성 확보 조치 기준
 - 표준 개인정보 보호지침
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률
 - 바이오 정보 보호 가이드 라인
- 위치정보의 보호 및 이용 등에 관한 법률
 - 위치정보의 보호 및 이용 등에 관한 법률위치 정보의 관리적, 기술적 보호조치 가이드
- 행정자치부 권고 비밀번호 작성 규칙
- 국가정보원 국내 권고 암호알고리즘
- 행정기관 및 공공기관 정보시스템 구축 운영 지침
- 클라우드컴퓨팅서비스 정보보호에 관한 기준

“개인정보보호법” 및 “개인정보의 안전성 확보 조치 기준”

- 개인정보 정의
 - “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함)
- 개인정보는 크게 **민감정보** 및 **고유식별정보**로 구분함
- 민감정보의 정의 (“개인정보 보호법” 제23조 및 “개인정보 보호법 시행령” 제18조)
 - 사상신념, 노동조합, 정당의 가입탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 **사생활을 현저히 침해할 우려가 있는 개인정보**
 - 유전자검사 등의 결과로 얻어진 유전정보나 “형의 실효 등에 관한 법률” 제2조 제5호에 따른 범죄경력 자료에 해당하는 정보
- 고유식별정보 정의 (“개인정보 보호법” 제23조 및 “개인정보 보호법 시행령” 제19조)
 - **주민등록번호**
 - 여권번호
 - 운전면허번호
 - 바이오 정보(지문, 홍채 등)

“개인정보보호법” 및 “개인정보의 안전성 확보 조치 기준”

- 접근 권한의 관리
 - 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 함
- 비밀번호 관리
 - 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 **비밀번호 작성규칙을 수립**하여 적용하여야 함
- 접근통제 시스템 설치 및 운영
 - 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 함
 - 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한
 - 개인정보처리시스템에 접속한 IP주소등을 분석하여 불법적인 개인정보유출 시도를 탐지

“개인정보보호법” 및 “개인정보의 안전성 확보 조치 기준”

- 개인정보의 암호화
 - 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말함
 - 바이오정보: 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보
- 개인정보를 정보통신망을 통하여 송수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 함
- 비밀번호 및 바이오정보는 암호화하여 저장하여야 함
- 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 함
- 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 함
- 접속기록의 보관 및 위변조방지
 - 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관 관리하여야 함
 - 개인정보취급자의 접속기록이 위변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 함

“개인정보보호법” 및 “개인정보의 안전성 확보 조치 기준”

유형	개인정보
인적사항	성명, 주민등록번호, 주소, 본적지, 전화번호 등 연락처, 생년월일, 출생지, 이메일 주소, 가족관계 및 가족구성원 정보 등
신체적 정보	(신체정보) 얼굴, 지문, 홍채, 음성, 유전자정보, 키, 몸무게 등 (의료·건강정보) 건강상태, 진료기록, 신체장애, 장애등급, 병력(病歷) 등
정신적 정보	(성향정보) 도서·비디오 등 대여기록, 잡지구독정보, 물품구매내역, 웹사이트 검색내역 등 (내면의비밀 등) 사상, 신조, 종교, 가치관, 정당·노조가입여부 및 활동내역 등
재산적 정보	(개인금융정보) 소득, 신용카드번호, 통장계좌번호, 동산·부동산 보유내역, 저축내역 등 (신용정보) 개인신용평가정보, 대출 또는 담보설정 내역, 신용카드 사용내역 등
사회적 정보	(교육정보) 학력, 성적, 출석상황, 자격증 보유내역, 상벌기록, 생활기록부 등 (법적정보) 전과·범죄 기록, 재판 기록, 과태료 납부내역 등 (근로정보) 직장, 고용주, 근무처, 근로경력, 상벌기록, 직무평가기록 등 (병역정보) 병역여부, 군번, 계급, 근무부대 등
기타	전화 통화내역, IP주소, 웹사이트 접속내역, 이메일 또는 전화 메시지, 기타 GPS 등에 의한 개인위치정보

* 상기 내용은 한국인터넷진흥원의 개인정보보호 소개 내용을 발췌함

“개인정보보호법” 및 “개인정보의 안전성 확보 조치 기준”

■■■ 암호화 적용 기준 요약표 ■■■

구 분			암호화 기준
정보통신망, 보조저장매체를 통한 송신 시	비밀번호, 바이오정보, 고유식별정보		암호화 송신
개인정보처리 시스템에 저장 시	비밀번호		일방향(해쉬 함수) 암호화 저장
	바이오정보		암호화 저장
	고 유 식 별 정 보	주민등록번호	암호화 저장
		인터넷 구간, 인터넷 구간과 내부망의 중간 지점(DMZ)	암호화 저장
		여권번호, 외국인 등록번호, 운전면허 번호 내부망에 저장	암호화 저장 또는 다음 항목에 따라 암호화 적용여부 · 적용범위를 정하여 시행 ① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과 ② 암호화 미적용시 위험도 분석에 따른 결과
업무용 컴퓨터, 모바일 기기에 저장시	비밀번호, 바이오정보, 고유식별정보		암호화 저장 ※ 비밀번호는 일방향 암호화 저장

“개인정보보호법” 및 “개인정보의 안전성 확보 조치 기준”

- 제47조(개인영상정보의 안전성 확보를 위한 조치) 영상정보처리기기운영자는 개인영상 정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 법 제29조 및 령 제30조 제1항에 따라 안전성 확보를 위하여 다음 각 호의 조치를 하여야 한다.
 1. 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립시행, 다만 “개인정보의 안전성 확보조치 기준 고시” 제2조 제4호에 따른 ‘소상공인’은 내부관리계획을 수립하지 아니할 수 있다.
 2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
 3. 개인영상정보를 안전하게 저장 전송할 수 있는 기술의 적용(네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일 저장 시 비밀번호 설정 등)
 4. 처리기록의 보관 및 위변조 방지를 위한 조치(개인영상정보의 생성일시 및 열람할 경우에 열람 목적, 열람자, 열람 일시 등 기록관리 조치 등)
 5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치
- 제2조 (용어의 정의)
 - “개인영상정보”란 영상정보처리기기에 의하여 촬영처리되는 영상정보 중 개인의 초상, 행동 등과 관련된 영상으로서 해당 개인을 식별할 수 있는 정보를 말한다.

클라우드컴퓨팅서비스 정보보호에 관한 기준

- **제3조(관리적 보호조치)** ①클라우드컴퓨팅서비스 제공자는 클라우드컴퓨팅서비스의 안전성 및 신뢰성 확보를 위하여 다음 각호의 사항을 포함한 관리적 보호조치를 취하여야 한다.
- **제4조(물리적 보호조치)** ①클라우드컴퓨팅서비스 제공자는 중요 정보와 정보처리시설 및 설비 보안을 위하여 다음 각 호의 사항을 포함한 물리적 보호조치를 취하여야 한다.
- **제5조(기술적 보호조치)** ①클라우드컴퓨팅서비스 제공자는 클라우드컴퓨팅서비스의 안전성 및 신뢰성 확보를 위하여 다음 각 호의 사항을 포함한 기술적 보호조치를 취하여야 한다.
- **제6조(공공기관용 추가 보호조치)** ①클라우드컴퓨팅서비스 제공자가 “전자정부법” 제2조 제3호에 따른 공공기관에게 클라우드컴퓨팅서비스를 제공하는 경우에는 그 서비스의 안전성 및 신뢰성 확보를 위하여 다음 각 호의 사항을 포함한 보호조치를 추가로 취하여야 한다.



주요 보안 취약점 소개

OWASP Top 10

- Open Web Application Security Project
- 가장 많이 발생하는 어플리케이션 취약점을 3년 주기로 배포
- CAPEC, CWE 등을 기반으로 주로 발생하는 취약점을 10개로 선정하여 OWASP Top 10으로 발표
- OWASP Top 10 분류
 - Web Application
 - Mobile
 - IoT(Internet of Things)
 - Cloud

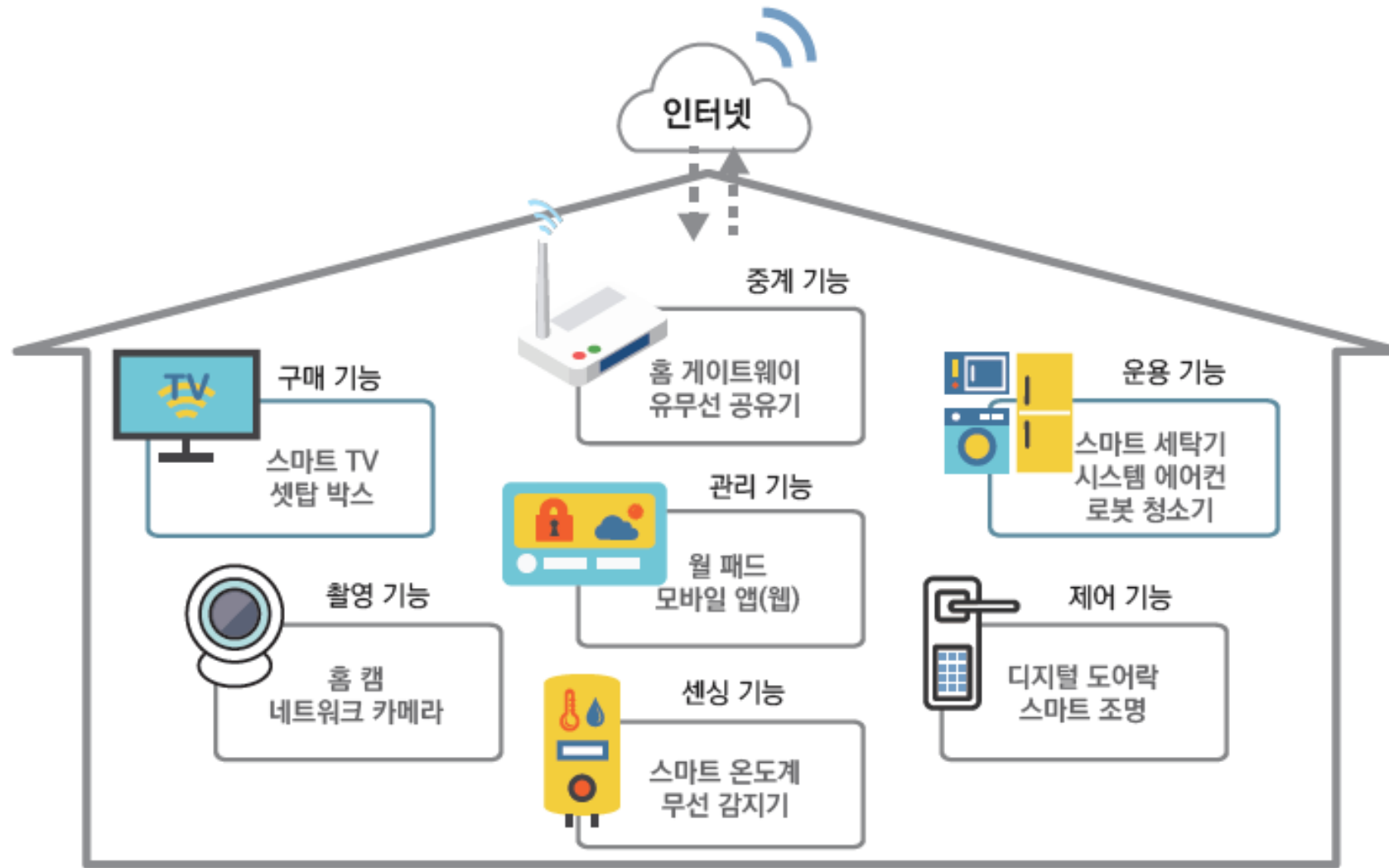
OWASP IoT Top 10

1. 안전하지 않은 웹 인터페이스
 - 기본비밀번호 사용, 크로스사이트스크립팅(XSS), SQL삽입, 취약한 세션 관리, 계정 잠금 부재 등
2. 불충분한 인증/인가
 - 취약한 패스워드 조합, 취약한 인증, 권한 상승, 부적절한 인가 등
3. 안전하지 않은 네트워크 서비스
 - 버퍼오버플로우, 서비스 거부(DoS), UPnP 포트 오픈
4. 취약한 통신
 - 중요정보 평문 전송, 취약한 SSL/TLS라이브러리 사용, SSL/TLS설정 미흡
5. 프라이버시 문제
 - 불필요한 개인정보 수집

OWASP IoT Top 10

6. 안전하지 않은 클라우드 인터페이스
 - 기본비밀번호 사용, 계정 잠금 부재, 중요정보 평문 전송
7. 안전하지 않은 모바일 인터페이스
 - 기본비밀번호 사용, 계정 잠금 부재, 중요정보 평문 전송
8. 불충분한 보안 설정
 - 취약한 패스워드 조합, 감사로그 설정 부재 등
9. 안전하지 않은 소프트웨어/펌웨어
 - 검증 절차 없는 파일 다운로드, 업데이트 파일 평문 전송, 중요정보가 포함된 펌웨어
10. 취약한 물리적 보안
 - USB포트를 통한 소프트웨어 접근, 스토리지 장치 제거 가능

홈 가전 IoT 보안가이드



출처: "홈 가전 IoT 보안가이드" - 한국인터넷진흥원

홈 가전 IoT 보안가이드

유형	세부 설명	대상제품
센싱	(정의) 열, 빛, 온도, 압력, 습도 등 여러 종류의 물리적인 양이나 변화를 감지, 검출하거나 판별, 계측한 정보를 전송하는 제품 (보안성) 센싱 정보의 무결성 및 진위 여부, 인가된 수신자 (보안위협) 센싱 정보 위·변조, 위장	스마트온도계 등 센서
제어	(정의) 등록된 센서로부터 전송된 정보 또는 인가된 사용자의 조작 명령에 따라 통제하고 조정하는 제품 (보안성) 제어 명령어의 무결성 및 진위 여부, 인가된 사용자 접근, 인증정보 기밀성 및 무결성 (보안위협) 제어 명령어 위·변조, 위장, 인증정보 유출·도용	디지털 도어락, 스마트 전력 차단기, 스마트 조명 스위치 등 제어 제품
중계	(정의) 홈 네트워크의 맥내망과 사업자망을 상호 접속하거나 중계하는 제품으로, 홈·가전 IoT 제품의 송·수신 데이터를 중계하는 역할 수행 (보안성) 홈·가전 IoT 제품으로 송신하는 데이터의 기밀성 및 무결성, 송수신 데이터 저장 금지, 인가된 송·수신자, 정책설정을 위한 인가된 사용자 접근, 인증정보 기밀성 및 무결성 (보안위협) 중계 데이터 유출 및 위·변조, 위장	홈게이트웨이 등 네트워크 제품

홈 가전 IoT 보안가이드

유형	세부 설명	대상제품
구매	<p>(정의) 양방향 통신을 기반으로 홈쇼핑 또는 영화 등 콘텐츠 구매 기능을 제공하는 제품</p> <p>(보안성) 인가된 사용자 접근, 구매에 필요한 중요 정보(인증정보, 개인정보, 금융정보 등)의 기밀성 및 무결성</p> <p>(보안위협) 중요정보 위·변조, 위장</p>	스마트TV, 셋탑박스 등 구매 기능을 제공하는 제품
촬영	<p>(정의) 댁내에 설치된 네트워크 카메라를 통하여 영상을 촬영하여 저장하거나 촬영한 영상정보를 네트워크 통신채널로 전송하는 제품</p> <p>(보안성) 개인영상(정지영상 포함)의 기밀성, 인가된 사용자의 저장 영상 접근, 인가된 수신자, 인증정보 기밀성 및 무결성</p> <p>(보안위협) 개인영상 유출, 위장</p>	홈캠(웹캠) 등 영상촬영 제품
관리	<p>(정의) 네트워크 통신을 이용하여 다양한 유형의 홈·가전 IoT 제품을 관리(설정·조회·제어 등)하는 제품</p> <p>(보안성) 등록된 관리대상 제품(센싱, 제어 등 유형 제품), 인가된 사용자 접근, 인증정보 기밀성 및 무결성</p> <p>(보안위협) 위장, 보안설정 임의 변경</p>	월패드, 모바일 앱(웹) 등 관리기능 제공 제품
운용	<p>(정의) 홈·가전제품의 고유 기능을 수행하는 제품으로 네트워크에 연결되어 원격으로 관리 기능</p> <p>(보안성) 인가된 사용자 접근</p> <p>(보안위협) 위장, 임의 접근·사용</p>	스마트 냉장고, 스마트 세탁기, 시스템 에어컨 등

홈 가전 IoT 보안가이드

보안항목	보안요구사항	관련 주요 보안위협
소프트웨어 보안	<ul style="list-style-type: none">• 시큐어코딩• 알려진 보안취약점 점검 및 제거• 최신 3rd party 소프트웨어 사용	<ul style="list-style-type: none">• 소프트웨어 결함 등 보안약점으로 인한 보안취약점 원인 제공• 알려진 보안취약점 악용• 3rd party 소프트웨어의 보안취약점 악용
물리적 보안	<ul style="list-style-type: none">• 물리적 인터페이스 차단	<ul style="list-style-type: none">• 물리적 보안 취약
인증	<ul style="list-style-type: none">• 인증 및 접근통제• IoT 제품간 상호 인증	<ul style="list-style-type: none">• 인증 메커니즘 부재• 강도가 약한 비밀번호• 접근통제 부재

홈 가전 IoT 보안가이드

보안항목	보안요구사항	관련 주요 보안위협
암호화	<ul style="list-style-type: none">• 안전한 암호 알고리즘 사용• 안전한 암호키 관리• 안전한 난수 생성 알고리즘 사용	<ul style="list-style-type: none">• 취약한 암호알고리즘• 취약한 암호키 길이• 낮은 엔트로피
데이터 보호	<ul style="list-style-type: none">• 안전한 통신채널• 저장 및 전송 데이터 보호• 개인정보 보호	<ul style="list-style-type: none">• 전송데이터 보호 부재• 인증정보, 암호키, 개인정보 등 중요정보 평문 저장
플랫폼 보안	<ul style="list-style-type: none">• 설정값 및 실행코드 무결성 검증• 안전한 업데이트• 감사기록	<ul style="list-style-type: none">• 데이터 무결성 부재• 펌웨어 업데이트 취약점• 보안사고 추적 불가능

CWE/SANS Top 25

- CWE에 등록된 약점(weakness) 중 가장 널리 알려진 소프트웨어 약점 Top 25를 배포
- SANS연구소, MITRE 등의 보안기관 및 전문가들로 구성
- CWE(Common Weakness Enumeration)를 통해 보안 약점 관리 및 공유
- <https://www.sans.org/top25-software-errors/>

SANS

Train and Certify

Manage Your Team

Resources

Focus Areas

Get Involved

About

CWE/SANS TOP 25 Most Dangerous Software Errors

CWE/SANS Top 25

Rank	ID	Name
1	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
3	CWE-20	Improper Input Validation
4	CWE-200	Information Exposure
5	CWE-125	Out-of-bounds Read
6	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
7	CWE-416	Use After Free
8	CWE-190	Integer Overflow or Wraparound
9	CWE-352	Cross-Site Request Forgery (CSRF)
10	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
11	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
12	CWE-787	Out-of-bounds Write

CWE/SANS Top 25

13	CWE-287 🔗	Improper Authentication
14	CWE-476 🔗	NULL Pointer Dereference
15	CWE-732 🔗	Incorrect Permission Assignment for Critical Resource
16	CWE-434 🔗	Unrestricted Upload of File with Dangerous Type
17	CWE-611 🔗	Improper Restriction of XML External Entity Reference
18	CWE-94 🔗	Improper Control of Generation of Code ('Code Injection')
19	CWE-798 🔗	Use of Hard-coded Credentials
20	CWE-400 🔗	Uncontrolled Resource Consumption
21	CWE-772 🔗	Missing Release of Resource after Effective Lifetime
22	CWE-426 🔗	Untrusted Search Path
23	CWE-502 🔗	Deserialization of Untrusted Data
24	CWE-269 🔗	Improper Privilege Management
25	CWE-295 🔗	Improper Certificate Validation

클라우드 컴퓨팅 해킹 사고

해킹에 뺨 맞은 클라우드... '보안 의구심' 확산 (2019.7.31, 한국경제)

30일(현지시간) 월스트리트저널(WSJ), CNBC 등에 따르면 캐피털원은 해커 침입으로 미국인 1억 명, 캐나다인 600만 명 등 총 1억600만 명의 개인정보가 유출됐다. 이름, 주소, 전화번호 등 신상정보와 신용점수, 신용한도 등 각종 금융 관련 데이터가 노출된 것으로 알려졌다. 8만 건의 은행 계좌번호와 100만 건의 캐나다 사회보험번호 등도 유출돼 피해가 확산될 가능성이 있다.

...중략...

캐피털원의 데이터를 빼낸 해커는 웹 서버의 방화벽 취약점을 뚫고 데이터에 접근한 것으로 확인됐다. WSJ는 “부실하게 구성된 방화벽을 통해 해커가 시스템에 침입한 것으로 조사됐다”고 보도했다. 캐피털원과 클라우드 서비스 제공사인 아마존은 “이번 사건은 클라우드 서비스를 사용한 것이 문제라기보다는 데이터와 관련된 시스템 관리가 제대로 이뤄지지 못했던 것”이라며 “이런 유형의 (방화벽) 취약성은 클라우드뿐만 아니라 사내 데이터센터 환경에도 공통적으로 적용된다”고 해명했다.

<https://www.hankyung.com/it/article/201907313937i>

클라우드 설정 오류로 이메일 27억, 출생신고서 80만 노출! (2019.12.11, 보안뉴스)

지난 주 보안 전문가 밥 디아첸코(Bob Diachenko)는 27억 개가 넘는 이메일 주소를 공개된 엘라스틱서치 DB에서 발견한 바 있다. 이중 10억 개 정도에는 평문으로 된 비밀번호까지 부착되어 있었다. 이메일 주소의 도메인들은 텐센트(Tencent), 시나(Sina), 소후(Sohu), 넷이즈(NetEase) 등 중국 업체의 것이었다. 물론 야후, 지메일 등 다른 나라의 것도 섞여 있긴 했다. 알고 보니 2017년에 발생한 대규모 정보 유출 사건 후 다크웹에서 거래되던 품목들이었다.

...중략...

영국의 모의 해킹 전문 업체인 피두스 인포메이션 시큐리티(Fidus Information Security)에 소속된 연구원들도 이런 DB를 이번 주 찾아냈다. 미국 출생신고서 사본 80만부가 저장된 AWS S3 버킷을 발견한 것이다. 출생신고서 및 사망신고서 사본을 취급하는 한 기업의 것이었다. 해당 DB는 비밀번호조차 걸려있지 않은 채 인터넷을 향해 문을 활짝 열고 있었다. 재미있게도 이 DB에 저장되어 있던 94000개의 사망신고서 사본은 열람이 불가능한 상태였다.

...중략...

DB 내 출생신고서들은 2017년생의 것부터 저장되어 왔으며, 이름, 생년월일, 주소, 이메일 주소, 전화번호, 기타 다른 개인정보 등을 포함하고 있었다. 피두스의 총괄인 앤드류 마빗(Andrew Mabbitt)은 “S3 관련 프로젝트를 진행하다가 해당 DB를 우연히 발견했다”고 밝혔다. “전체 공개로 설정되어 있어서, 누구라도 URL만 있으면 접속할 수 있는 상태였습니다.”

<https://www.boannews.com/media/view.asp?idx=85119>

클라우드 컴퓨팅 보안 위협

번호	보안 위협
1	데이터 유출
2	잘못된 설정 및 부적절한 변경 제어
3	클라우드 보안 아키텍처 및 전략 부족
4	불충분한 ID, 자격 증명, 액세스 및 키 관리
5	계정 하이재킹
6	내부자 위협
7	안전하지 않은 인터페이스 및 API
8	약한 제어 영역
9	메타스트럭처 및 응용구조의 실패
10	제한된 클라우드 사용 가시성
11	클라우드 서비스의 남용 및 악의적 사용

<https://cloudsecurityalliance.org>