SW 안전 그리고 SW 보안

2015년 12월 1일

고려대학교
최진영
choi@formal.korea.ac.kr

SPRi
소프트웨어정책연구소

순서

- 들어가기
- 소프트웨어 속성 (dependability)
- Software Safety
  - Software Safety Assurance
- Software Security
  - Software Security Assurance
- Secure Software (Safety + Security +…)
  - Software Assurance
- 결론

스마트 시대 : SW 중심 사회



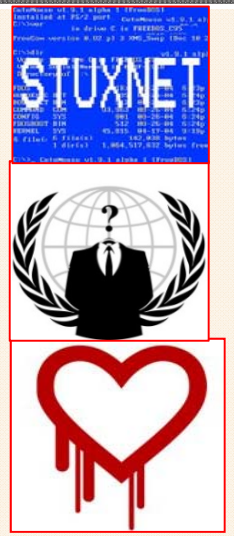









스마트 사회의 위협: SW Bug



- **(정상) 버그** :
  - 정상적 작동 중 설계/구현 등의 잘못으로 발생하는 버그.
  - SW 품질, 안전, 신뢰 등 문제 발생.

- **보안약점(취약점)** :
  - 정상적 작동 중 공격자가 악의로 활용할 수 있는 버그.
  - 사이버 공격에 악용

Dependability 속성

1. Availability (가용)
   - The ability of the system to **deliver services when requested**
2. Reliability (신뢰)
   - The ability of the system to **deliver services as specified**
3. Safety (안전)
   - The ability of the system to **operate without catastrophic failure**
4. Security (보안)
   - The ability of the system to **protect** itself against deliberate or accidental intrusion
5. Resilience (탄성)
   - The ability of the system to **resist and recover from damaging events**

Therac-25 사고

- AECL 방사선 암 치료기
- 1982년 SW 제어 서비스 시작
- 1985년 ~ 1987년 : 6번의 사고
- **3명 사망**
- SW 오류로 인명이 살상된 첫 케이스
- SW 공학에 Safety 개념 도입
- **Reliability ≠ Safety**
- IEC 62304 제정

  Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61508

- 모든 산업에 적용될 수 있는 기본 기능 안전 표준.
- 기능 안전 (functional safety) 정의

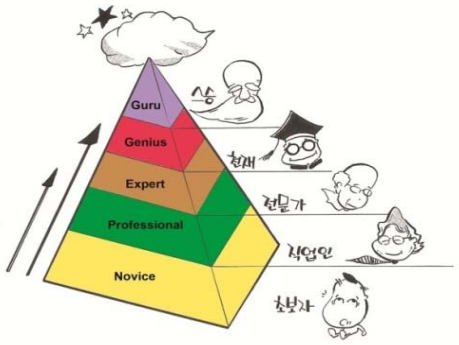
  "part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities."
- Safety life cycle 및 Safety Integrity Level (SIL) 소개
- 생명 주기 전반에서 발생할 수 있는 오류를 예방하기 위한 각 생명주기 단계별 기법을 명시
- 산업 별 기능 안전 표준의 기준

신용등급 과 SIL 등급

일반적 신용등급표

1	신용도 매우우량, 최상위 등급
2	신용도 매우우량, 상위 등급
3	안정적 신용거래 유지, 신용도 우량
4	신용도 우량하며, 단기연체 없음
5	신용도 보통이며, 장기연체 없음
6	장기연체 없으나, 약간 신용위험 존재
7	신용도 다소 우려, 기존거래 유지 가능
8	신용도우려되는 수준으로 부실화 진행
9	신용도 낮은 상태로 부실 요인 현재화
10	신용도 매우 낮은 상태, 신용 문제 발생

※ 7~10등급은 통상 저신용자로 분류



VS

국제 표준 – IEC 61508

전기/전자/프로그램 전자장비 기능 안전성 국제표준

- 소프트웨어 개발단계에서의 안전등급별 요구되는 활동

	Technique / Measure	SIL 1	SIL 2	SIL 3	SIL 4
1	Computer-aided specification tools	R	R	HR	HR
2a	Semi-formal methods	R	R	HR	HR
2b	Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	---	R	R	HR

Table A.1 – Software safety requirements specification

	Technique / Measure	SIL 1	SIL 2	SIL 3	SIL 4
7b	Semi-formal methods	R	R	HR	HR
7b	Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	---	R	HR	HR
8	Computer-aided specification tools	R	R	HR	HR

Table A.2 – Software design and development : Software architecture design

	Technique / Measure	SIL 1	SIL 2	SIL 3	SIL 4
1	Formal proof	---	R	R	HR
2	Probabilistic testing	---	R	R	HR
3	Static analysis	R	HR	HR	HR
4	Dynamic analysis and testing	R	HR	HR	HR
5	Software complexity metrics	R	R	R	R

Table A.9 – Software verification

파생 표준 및 기능안전

표준	DO-178C (12)	IEC 62304 (06)*	ISO 26262 (11)	IEC 61508 (98)	EN50128(01)
개정 일자	2012	2006	2011	1998	2001
분야	항공	의료기기	자동차	전기/전자/임베디드 시스템	철도
특징	-안전 수준 5등급	-class 3등급	-ASIL 4등급 -IEC 61508 기반	-SIL 4등급 -다른 SIL 사용 표준의 모태	-SIL 5등급 -IEC 61508 기반
테스팅	-정적 분석 -동적 분석	-정적 분석 -동적 분석	-정적 분석 -동적 분석	-정적 분석 -동적 분석	-정적 분석 -동적 분석
정형기법	-정형기법 권고 Level A 필수	-정적 분석	-정적 분석	-정형기법 권고 SIL 4 필수	-정형기법 권고 SIL 4 권고

* FDA 는 Assurance case 추진

보안 소프트웨어 표준 (Common Criteria)

- 보안 소프트웨어 (Security Software)
  - 기능목적이 보안 (예, 방화벽, 암호모듈 등)
- 소프트웨어 보안 (Software Security)
  - 소프트웨어 속성 (소프트웨어 내에 포함된 (제로데이) 취약점 밀도 등)

요구사항	EAL 5	EAL 6	EAL 7
보안 정책 모델	정형적	정형적	정형적
기능 명세	준정형적	준정형적	정형적
구조 설계	준정형적	준정형적	정형적
상세 설계	기술적	준정형적	준정형적
상호 관계	준정형적	준정형적	정형적

안전 공학 프로세스

- 프로세스 내 각 단계에서 리뷰와 확인을 하는 계획 기반 방식
- 목적: 오류 예방 (방지) 와 오류 검증
  - 해저드 분석
  - 안전성 분석
  - 정형 명세 및 정형 검증 (정형기법)
  - 정적 분석
- Safety life cycle 및 Safety Integrity Level (SIL) 소개
- 안전 리뷰 와 해저드 추적 및 확실한 식별 필요
- 애자일 방법론은 일반적으로 추천하지 않음.
- 규제기관은 시스템 개발 시 안전 공학 프로세스가 사용 되었는지 확인할 수 있는 명확한 증거를 요구할 수 있음.

ISO 26262 V&V

Verification(검증) and Validation (확인/검정)

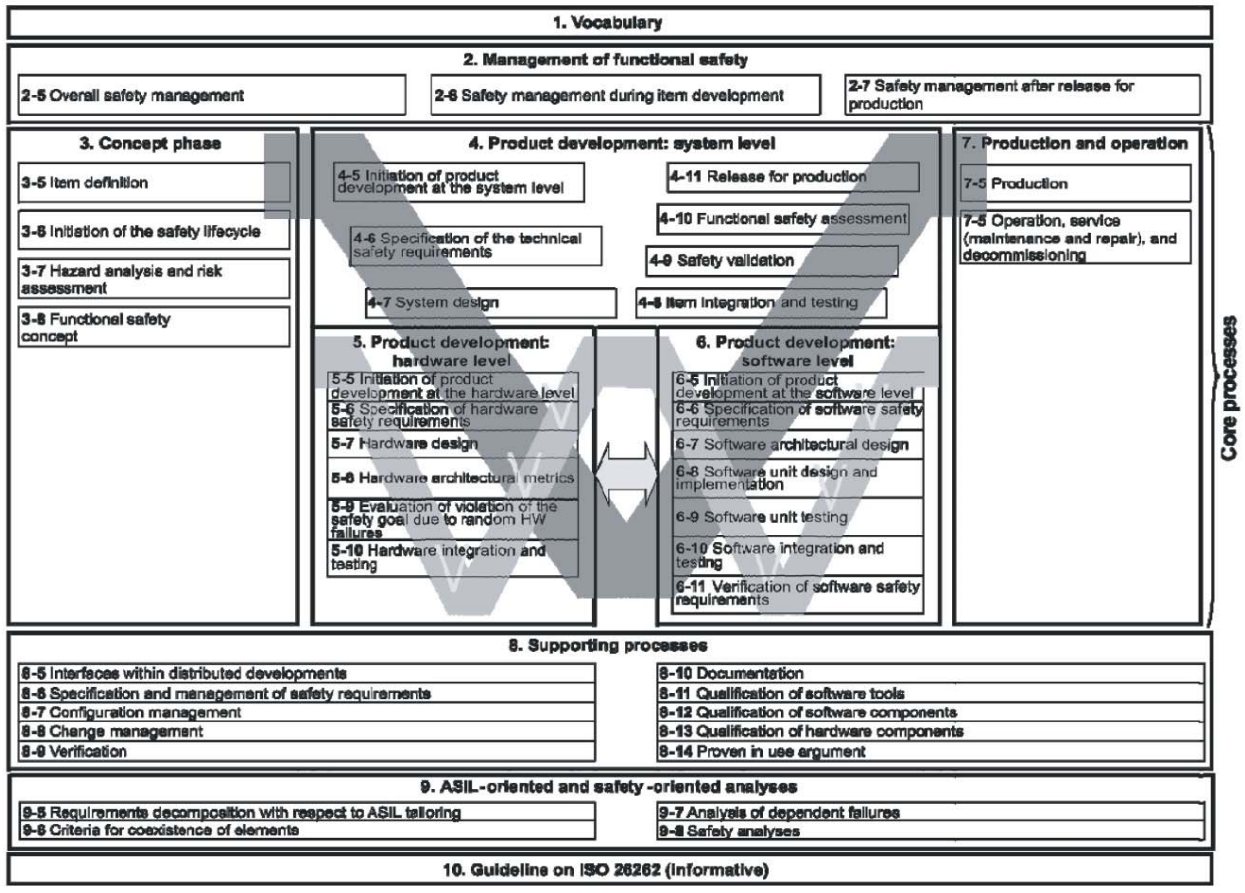


Figure 1 — Overview of ISO 26262

SW Safety Case

- "A documented body of evidence that a convincing and valid argument that a system is adequately safe for a given application in a given environment."

Chapter	Description
System description	An overview of the system and a description of its critical components.
Safety requirements	The safety requirements abstracted from the system requirements specification. Details of other relevant system requirements may also be included.
Hazard and risk analysis	Documents describing the hazards and risks that have been identified and the measures taken to reduce risk. Hazard analyses and hazard logs.
Design analysis	A set of structured arguments (see Section 15.5.1) that justify why the design is safe.
Verification and validation	A description of the V & V procedures used and, where appropriate, the test plans for the system. Summaries of the test results showing defects that have been detected and corrected. If formal methods have been used, a formal system specification and any analyses of that specification. Records of static analyses of the source code.

Software Vulnerability (취약점)

취약점이란, 소프트웨어 내에 있는

1. Bug, flaw, error, mistake, weakness (보안약점) 으로
2. 공격자가 이러한 weakness 에 접근 하여
3. 시스템의 정보보증을 위태롭게 함.

- wikipedia.com

In computer security, a **vulnerability** is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.[1] To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.

Software Weakness (보안약점)

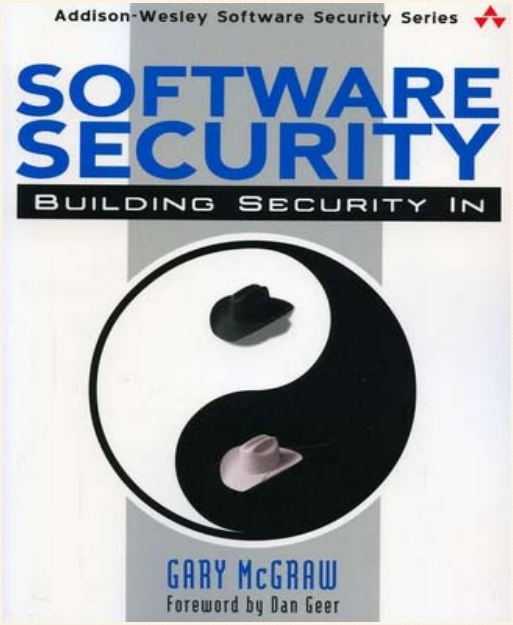
보안약점이란, 소프트웨어 내에 있는

1. 소프트웨어 구현, 코딩, 설계, 구조에 내포된
2. Bug, flaw, fault, error, mistake.

- cwe.mitre.org

Security Software vs. Software Security

VS.



Non Dependable Systems need Software Security

"뽐뿌 해킹사고는 웹 취약점 악용한 DB 공격 때문"

송고시간 | 2015/10/20 12:00

미래부 민관합동조사단, 조사 결과 발표…"SQL 인젝션 기법으로 개인정보 탈취"

(서울=연합뉴스) 정성호 기자 = 미래창조과학부는 지난달 11일 발생한 온라인 커뮤니티 '뽐뿌 커뮤니케이션'에 대한 해킹 사고를 조사한 결과 웹 취약점을 악용한 데이터 베이스(DB) 공격으로 정보 유출이 발생한 것으로 나타났다고 20일 밝혔다.

미래부 공무원과 민간 전문가로 민관 합동조사단을 꾸려 침해사고의 원인을 조사분석한 결과 해커는 3단계에 걸쳐 홈페이지의 구조·취약점을 파악한 뒤 'SQL 인젝션'을 통해 회원 약 196만명의 개인정보를 탈취한 것으로 조사됐다.

4월 12일	**농협** 인터넷뱅킹 등 서비스 중단(종합)(연합통신) **농협** 금융거래 중단.."**해킹** 아니냐" 항의 잇따라(MBC)	사고 발생 내부오류(공사),해킹부인
4월 13일	**농협** 전산망 중단…협력업체 직원 노트북서 장애 명령(YTN) **농협**, "협력사 직원 노트북서 시스템 장애명령" (머니투데이) [단독]**농협**, '최고관리자권한'빼앗겨…서버파괴(파이낸셜뉴스)	
4월 14일	좀비PC 한대에 **농협** `올스톱`…전산마비 사흘째 복구못해(매일경제)	
4월 15일	<**농협**, 전산망 관리 총체적 부실 드러나>(연합통신) [**농협**최악의전산사고] 전산장애 4대 의문점(서울신문) 검찰, **농협** 전산망 장애 '고의성'에 무게(헤럴드경제)	
4월 18일	'**농협** 사태' 노트북에 USB접속 흔적(종합)(연합통신) [종합]검찰, **농협** 전산망 사태 '외부 공격'에 무게(뉴시스) "**농협** 전산장애 100명이상 조전문가의 소행"(서울신문)	
4월 19일	**농협** "**해킹** 넘어선 고도의 사이버 테러 … 데이터 4억2000만 개 복원 중"(중앙일보) **농협**.**해킹**수사 3-4명 출국금지(MBC)	
4월 20일	**농협** '**해킹** 프로그램' 한 달 전부터 계획..수사 난항(MBC)	
4월 24일	**농협 해킹**, 디도스처럼 미궁 빠지나?(노컷뉴스)	
4월 26일	'**농협 해킹**' 일부 IP 中서 접속…검찰, 北과 연계 가능성 수사(한국경제) "北 해커부대, **농협** 전산망 마비 개입…" (국민일보) "**농협 해킹**, 북한 소행 가능성 크다"(중앙일보) **농협 해킹**이 北소행? "내·외부망 단절돼 불가능"(파이낸셜뉴스) 전산대란 **농협**, 북한 **해킹** 가능성 주장제기 "무리한 물타기" 비난여론(뉴스엔)	북한소행설 보도시작
4월 27일	오리무중 **농협** 사건, 왜 북한을 의심할까?(노컷뉴스) "**농협 해킹**, 북한 소행 정황 잡았다"(중앙일보)	재보선 선거일
4월 30일	**농협 해킹** 북한일 가능성 있다 "중국발 IP 상당수 일치"(한국	

Safety-Critical Systems need Software Security

- Stuxnet : 사이버 전쟁
- SCADA System : 사회 혼란, 인명 손실
- 인공심장 박동기 : 개인 공격

Stuxnet

From Wikipedia, the free encyclopedia

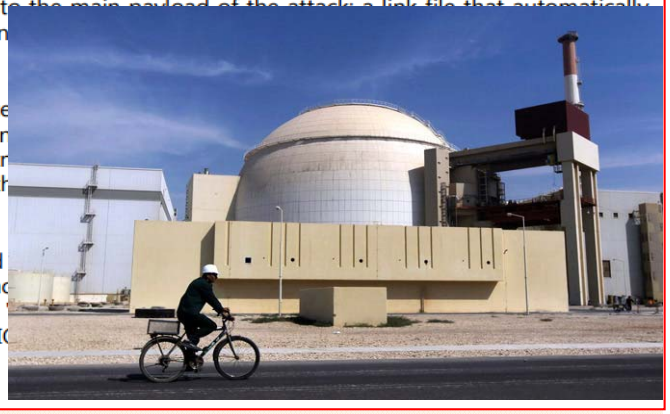
Stuxnet is a malicious computer worm believed to be a jointly built American-Israeli cyber weapon.[1] Although neither state has confirmed this openly,[2] anonymous US officials speaking to the Washington Post claimed the worm was developed during the administration of Barack Obama to sabotage Iran's nuclear program with what would seem like a long series of unfortunate accidents.[3]

Stuxnet specifically targets PLCs, which allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines, amusement rides, or centrifuges for separating nuclear material. Exploiting four zero-day flaws,[4] Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software. Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart.[5] Stuxnet's design and architecture are not domain-specific and it could be tailored as a platform for attacking modern SCADA and PLC systems (e.g., in automobile or power plants), the majority of which reside in Europe, Japan and the US.[6] Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges.[7]

Stuxnet has three modules: a worm that executes all routines related t
executes the propagated copies of the worm; and a rootkit componen
preventing detection of the presence of Stuxnet.[8]

Stuxnet is typically introduced to the target environment via an infecte
network, scanning for Siemens Step7 software on computers controllin
dormant inside the computer. If both the conditions are fulfilled, Stuxn
software, modifying the codes and giving unexpected commands to th
values feedback to the users.[9][10]

In 2015, Kaspersky's research findings on another highly sophisticated
Group, noted that the group had used two of the same zero-day attac
their use in both programs was similar. The researchers reported that
computer worms, at around the same time, indicates that the EQUATI
working closely together".[11]:13



Software Assurance (SwA) ?

Software Quality/Safety Assurance

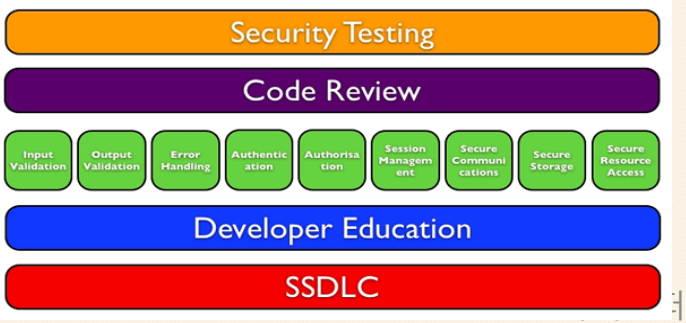
+

Software Security Assurance

"the level of confidence that **software is free from vulnerabilities**, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the **software functions in the intended manner.**" – CNSS IA Glossary, 2010

Secure Software

1. Dependable (기능성)
2. Trustworthy (보안성)
3. Resilient



Open Source SW Assurance

Open Source SW 믿고 사용할 수 있나?

- 일반적으로 기능성은 믿을 수 있으나,
- 보안성은 믿을 수가 없다. (Trustworthy)

오픈소스로 퍼지는 악성코드에 보안업체 골머리

Net Korea | 기사입력 2014-05-05 15:46

(지디넷코리아=손경호 기자) 악성코드는 수시로 변종이 등장한다.변종이 창궐하는 것은 악성코드 소스코드가 구글 안드로이드 운영체제(OS)처럼 오픈소스 형태로 공개되고 있는 것과도 무관치 않다. 소스가 공개되면 원래 악성코드 제작자 뿐만 아니라 다른 해커들도 손쉽게 소스코드를 구해 일부 내용을 바꿔 새로운 기능을 추가할 수 있다. 이렇게되면 탐지도 어려워진다.

2일 국내 보안업계 관계자들에 따르면 오픈소스 형태로 퍼지는 악성코드의 가장 대표적인 사례가 '고스트랫(Gh0st RAT)'이라는 해킹툴이다. 2007년께 처음 발견된 이 해킹툴은 사용자가 키보드로 입력한 정보를 가로채는 '키로깅, 분산서비스거부(DDoS) 공격, 파일 복사, 웹캠 화면 탈취 등 기능을 가졌다.

안랩 ASEC 블로그에 따르면 지난달 국내서 발견된 인터넷뱅킹용 악성파일 내에 고스트랫 기능이 추가됐다는 사실이 알려지기도 했다.

질문


ngiyabonga
danke
謝謝
teşekkür ederim
спасибо
dank je
thank you
gracias
tapadh leat
bedankt
hvala
mauruuru
mochchakkeram
dziękuję
go raibh maith agat
sagolun
sukriya
kop khun krap
aríngató
lakk
dakujem
grazie
мерси
tenima kasih
감사합니다
merci