

**Introduction to Software Security**

# **Overview of Computer Security** (1/2)

**Seong-je Cho**

**Computer Security & Operating Systems Lab, DKU**

# Sources / References

---

- Laurie Williams, CSC 515 Software Security, NC State
  - <https://sites.google.com/a/ncsu.edu/csc515-software-security>
- N. Vljajic, EECS 3482: Introduction to Computer Security, Yorku
  - [https://www.eecs.yorku.ca/course\\_archive/2016-17/W/3482/](https://www.eecs.yorku.ca/course_archive/2016-17/W/3482/)
- Nicholas Weaver, Computer Science 161: Computer Security, Berkeley
- Myrto Arapinis, Computer Security: INFRA10067, University of Edinburgh
  
- Fran Piessens – KU Leuven, Software Security Knowledge Area, Issue 1.0,
- Software Security, Meenakshi Mani, and Tanvi Shah

Please do not duplicate and distribute

# Contents

---

- Data vs. Information
- IT, Information System
- What is Security?
  - Information Security, Cyber Security, Computer Security
    - Software Security
- Some Famous Real World Threats/Attacks
- Why is Security important?

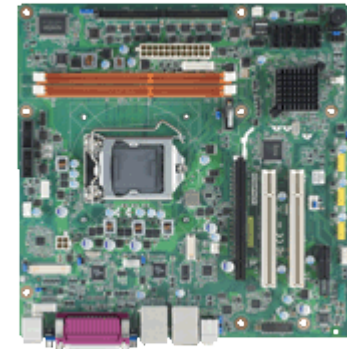
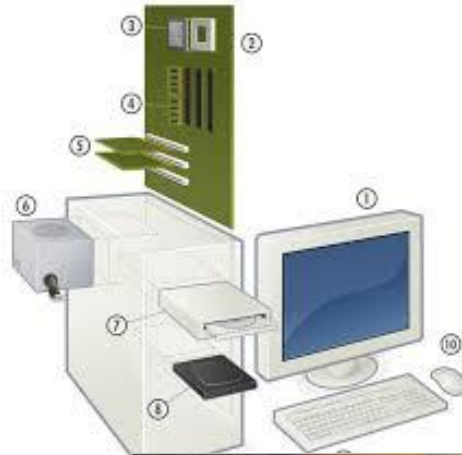
# **Data, Information, Information System**

# Introduction

- **Computer** – electronic device that can be programmed to carry out a set of arithmetic or logical operations automatically
  - A computer is an electronic device for storing and processing of data/information
  - A computer is an electronic machine that accepts data/information, processes it according to specific instructions, and provides the results as new information

- General-purpose

- Desktops, Servers
- Laptops (Notebooks), Tablets
- Smartphones (?)



# Introduction

## ● Computer

- an electronic device for storing and processing of data/information
- Special-purpose computer (Embedded devices)
  - Routers, AP, Smart-meter
  - Gaming consoles, Robot vacuums
  - Industrial controllers ...



## What Is an Embedded System?



# Data vs. Information

Data	Information
<ul style="list-style-type: none"> <li>• Raw facts</li> <li>• Unorganized</li> <li>• Unprocessed</li> <li>• Chaotic or Unsorted</li> <li>• <b>Input to a Process</b></li> </ul>	<ul style="list-style-type: none"> <li>• Useful &amp; Relevant</li> <li>• Organized</li> <li>• Processed</li> <li>• Ordered or Sorted</li> <li>• <b>Output of a Process</b></li> </ul>



01000111 11101100 10100001  
00111010 01011101 00001101

...

account balance: \$238,000.00

**In many organizations, information/data is seen as  
the most valuable asset !!!**

# Data & Information

**H** 한국경제

고양시, GPS 빅데이터 활용해 체납 차량 단속한다

경기 고양시는 지난달 구축한 'GPS 위치기반 빅데이터 영치시스템'을 활용, 자동차세 체납차량 단속을 3월 1일부터 본격적으로 시작한다고 27일 ...

**C** 조선비즈

KB국민카드, 빅데이터 분석 플랫폼 '데이터루트' 선보여

이 플랫폼은 대형 프랜차이즈 기업·중소기업·지방자치단체 등 누구나 카드 빅데이터를 온라인 환경에서 분석할 수 있는 것이 특징이다. 또 데이터 ...

**M** 매일경제

빅데이터는 옛말, 이젠 '딥데이터'가 경쟁력

데이터가 넘치는 '데이터 과잉' 시대가 되면서 스타트업들이 빅데이터를 넘어 '딥(deep)데이터'로 고개를 돌리고 있다. 남들도 수집할 수 있거나 허위...

2021. 11. 26.

**C** 조선비즈

빅데이터에 눈독 들이는 삼성·LG...조직개편에 M&A까지

삼성, CEO 직속 빅데이터센터 설치 아마존 출신 빅데이터 전문가를 센터장으로. LG, TV 데이터 분석 스타트업 알폰소 인수. TV와 콘텐츠 함께 판매 ... 5일 전



‘정보기술(IT) 개발자’ 영입 경쟁이 갈수록 치열해지고 있다. 한국 IT 1번지 판교역에 내리면 곳곳에 개발자를 채용한다는 내용의 광고물을 쉽게 만날 수 있다.

네카라쿠배는 네이버·카카오·라인플러스·쿠팡·배달의민족 등 국내 유명 IT 기업 앞 글자만을 따서 만들어진 용어. 인터넷 커뮤니티 디시인사이드 프로그래밍 갤러리에서 개발자 직군을 지원하는 취준생들이 가고 싶은 기업들을 묶어 부르며 유래했다. 실리콘밸리에서 핵심 IT 기업을 FAANG(페이스북·애플·아마존·넷플릭스·구글), MAGA(마이크로소프트·애플·구글·아마존) 등으로 줄여 부르는 트렌드가 국내에서도 나타난 것으로 볼 수



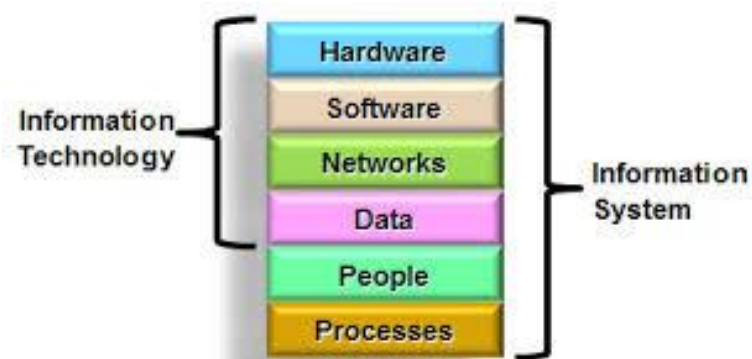
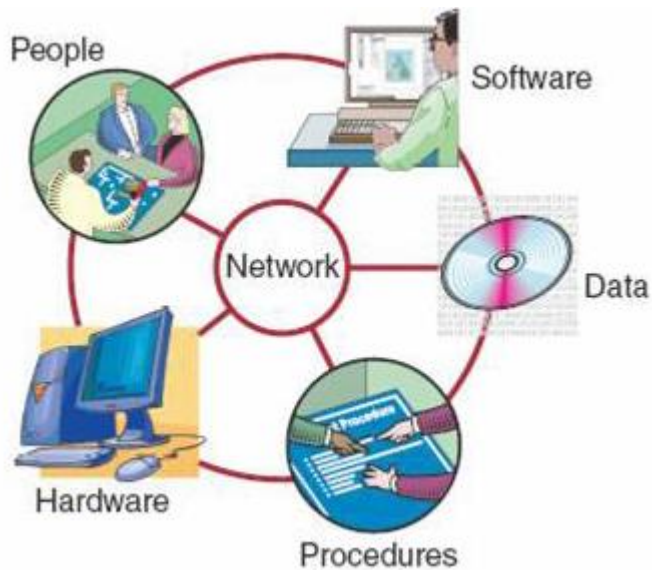
# Information Technology (IT)

---

- **Information Technology** – technology involving development & use of computer systems & networks for the purpose of processing & distribution of data/information
  
- **Categories of IT jobs:**
  - **IT engineer** - develops new or upgrades existing IT equipment (**software** or hardware)
    - SW developer + HW developer
  - IT administrator - installs, maintains, repairs IT equip./system
  - IT architect - draws up plans for IT systems and how they will be implemented
  - IT manager - oversees other IT employees, has authority to buy technology and plan budgets
  - **IT security specialist** - creates and executes security applications to maintain system security and safety

# Information System

- Entire set of **data, software, hardware, networks, people, and procedures** (processes, policies) that deal with processing & distribution of information in an organization
  - each component has its own strengths, weaknesses, and its own **security requirements**



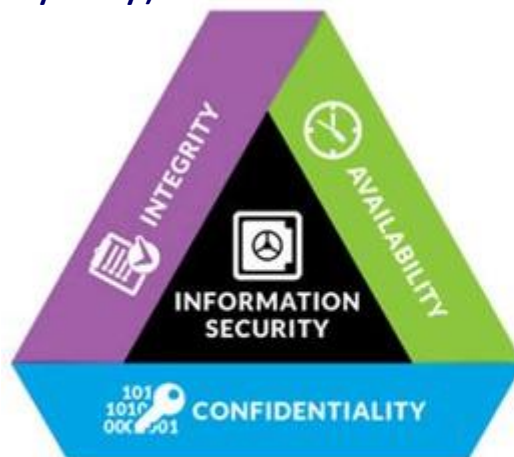
- **Information is**
  - stored on computer H/W,
  - manipulated by S/W,
  - Transmitted by communication,
  - used by people
  - controlled by policies

# **Security Attacks/Threats**

## **Cybersecurity, and Computer Security**

# What is Security?

- Security = State of being secure, free from danger (**threat**/risk/vulnerability)
- Security is to enforce a desired property *in the presence of an attacker*
  - Data confidentiality
  - Data and computation integrity
  - Availability
  - Authentication (Authenticity)
  - User privacy (Anonymity)
  - ...



- **Confidentiality** - protecting information from being accessed by unauthorized parties.
- **Integrity** - ensuring the authenticity of information—that information is not altered, and that the source of the information is genuine.
- **Availability** - information is accessible by authorized users.

Source: The Cyber Security Triad

<https://twitter.com/hcexecgroup/status/1271142535071584256>

# Information Security & Information Assurance

---

## ● Information Security

- The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
  - Source: NIST ([https://csrc.nist.gov/glossary/term/information\\_security](https://csrc.nist.gov/glossary/term/information_security) )

## ● Information Assurance

- The measures that protect and defend information and information systems by ensuring their availability, integrity, and confidentiality.
  - Source: CISA Cybersecurity Glossary (<https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#C>)

# Cybersecurity

---

- Prevention of damage to, protection of, and restoration of **computers**, electronic **communications** systems, electronic communications services, wire communication, and electronic communication, including **information** contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
  - The process of protecting **information** by preventing, detecting, and responding to **attacks**.
  - source: NIST Computer Security Resource Center ( <https://csrc.nist.gov/glossary/term/cybersecurity> )
- The activity or process, ability or capability, or state whereby **information** and **communications** systems and the information contained therein are protected from and/or defended against **damage**, **unauthorized use or modification**, or **exploitation**.
  - Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of **threat reduction**, **vulnerability reduction**, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including **computer network operations**, **information assurance**, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.
  - Source: CISA Cybersecurity Glossary ( <https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#C> )

# Types of Cyber Attacks

## Top cyber attack categories 2019

 **38%** **Crypto miners**

 **18%** **Banking**

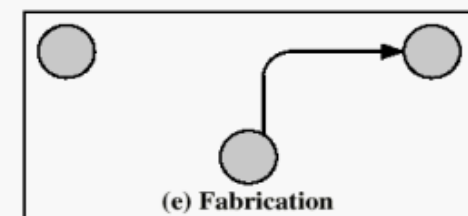
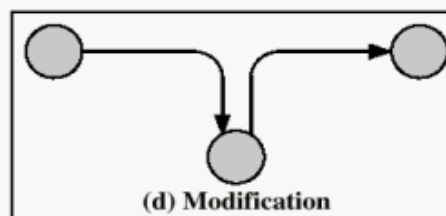
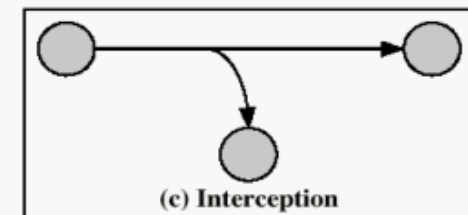
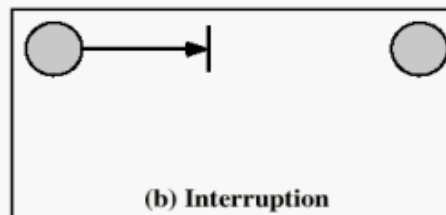
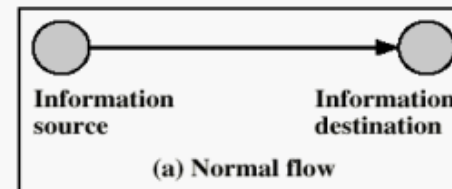
 **28%** **Botnet**

 **18%** **Infostealer**

 **27%** **Mobile**

 **7%** **Ransomware**

(Source: Check Point Cyber Security Report 2020)



# Threat Landscape 2020

- Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected
  - Malware > Web-based attacks > Phishing > Web application attacks > Spam > DDoS > Identity theft > Data breach > Insider threat > Botnets
  - Source: <https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020>



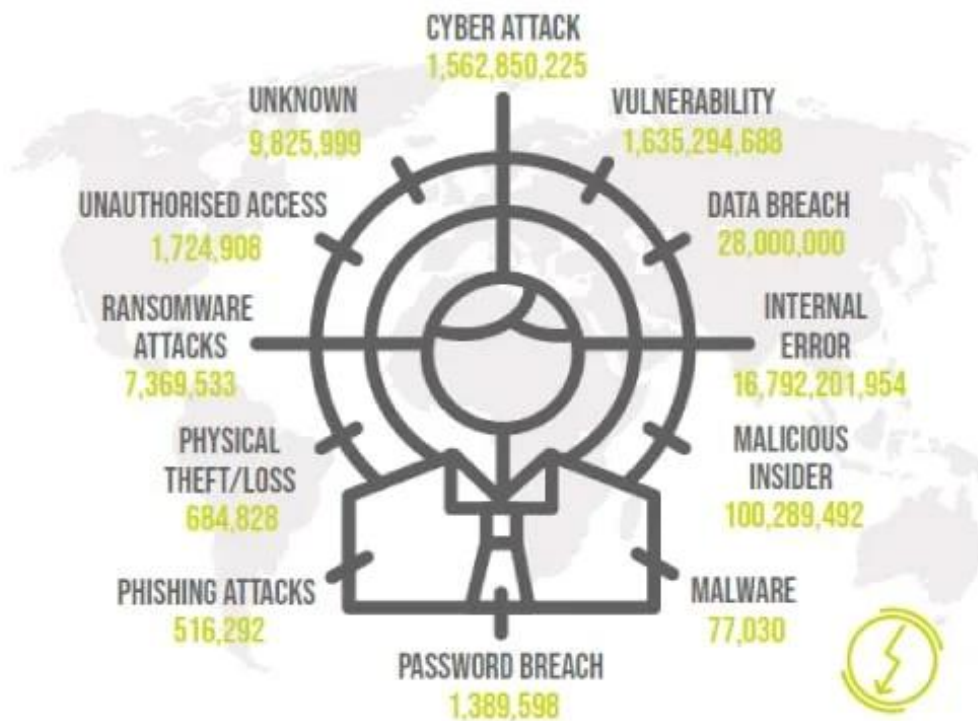


# Top cyber security attacks and breaches in 2021

2021 is considered one of the record-breaking years for **losing data** due to cyber-attacks and **data breaches** which are taking place in huge numbers.

As we all know how the implementation of technology is evolving these days, such as **AI and machine learning**, which helps countries grow at the fastest pace, but **malicious cyber attackers and data breaches are increasing** with their greatest tactics for accessing information.

- Source: Wissen hive (<https://www.wissenhive.com/blogs/top-cyber-security-attacks-and-breaches-in-2021>)



# What is Security?

---

- Security is to enforce a desired property *in the presence of an attacker*
- **Information Security** – practice of defending **information** from Unauthorized access (read, write, append),  
use,  
recording,  
disruption (분열, 혼란, 중단, 붕괴), – DoS (Denial-of-Service)  
destruction (Deletion), – DoS  
modification (Alternation, Tampering)  
...

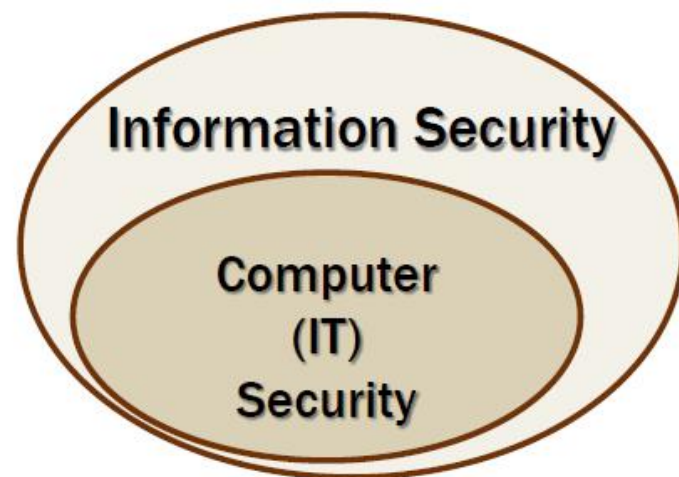
# What is Computer Security?

---

- **Computer security** is the protection of computer systems against adversarial environments
  - allow intended use
  - prevent unintended use
- **Computer Security** is the protection of computing systems and the data that they store or access
- ✓ We will try to understand:
  - why computer systems are insecure
  - how to build secure systems

# Computer Security vs. Information Security

- **Computer security** (aka IT security) is mostly concerned with information in 'digital form'
- **Information security** is concerned with information in any form it may take: electronic, print, etc.



# Computer Security

---

- **Computer security, cybersecurity or information technology security (IT security)** is

- the protection of computer systems and networks from the theft of or damage to their HW, SW, or electronic data, as well as from the disruption or misdirection of the services they provide.

(source: Wikipedia)

👉 In this class, **the three terms** (Computer security, Information security, Cybersecurity) **are used interchangeably**

- **Careers**

- Security analyst (Malware analyst)
- Security engineer
- Security architect
- Security administrator
- Chief Information Security Officer (CISO)
- Security Consultant/Specialist/Intelligence

# Definition of Software Security

# Software (SW)

- Application software
- System software
  - Operating systems
  - Device drivers
  - Utilities
  - ...

SW정책연구 "신규인력 35만3000명 필요"


코로나 이후 디지털 전환 수요 대비

홍 부총리 "8만9000명 추가 양성"

기업 단기훈련 등 중단기 지원 뒷받침


**정부, 2025년까지 SW인재 41만3000명 키운다**

발행일 : 2021.06.09 14:38 지면 : 2021-06-10  2면 English Translation

 이데일리


현대차, 소프트웨어 역량 강화에 12조원 투자

현대차는 이를 위해 소프트웨어 아키텍처 표준화와 제어기 무선 ... 한국과 해외 거점에 소프트웨어 전문 조직을 설립해 인력 확보·양성을 추진하는...

 동아일보


'미래차 SW인력' 국내 1000명도 안돼... 테슬라-GM은 4000명씩

테슬라의 SW 인력은 4000명이 넘는 것으로 알려져 있다. 일본 도요타는 올해부터 대졸자 신입 채용 전형에서 40~50%를 SW 계통 전공자로 채우기로 했다.

 지디넷코리아

"초·중·등 SW·AI 교과 수업시수 최대한 확보해야"

또 평생교육에서 성인의 다양한 SW·AI 역량 수준과 학습 동기, 산업 부문별 인력 수요를 고려한 교육 프로그램을 통합해 제공해야 한다는 내용을 제안에...

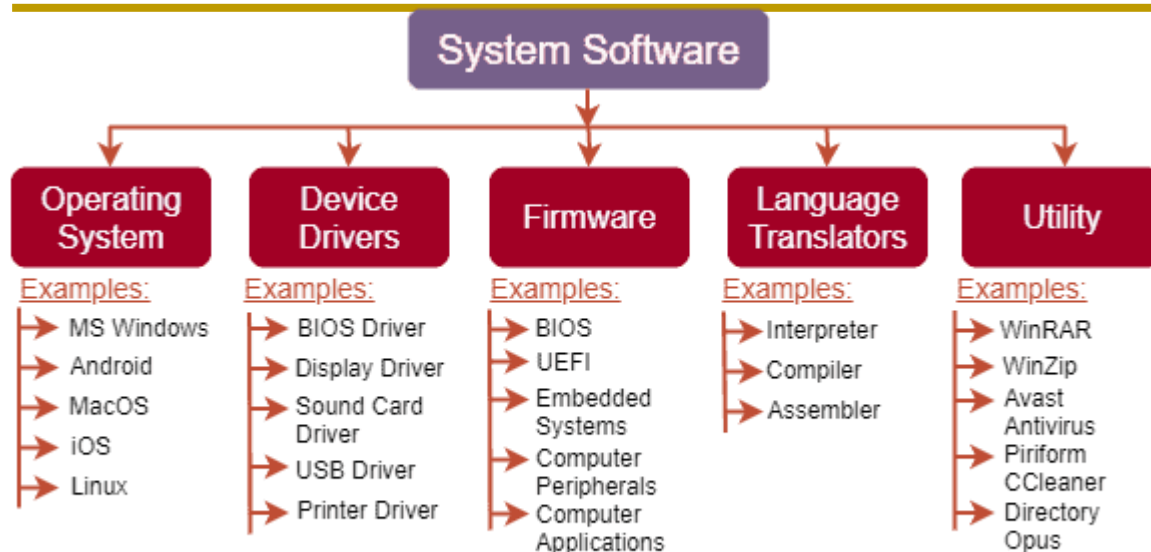
 아주경제

[제2차 SW인재 대란] ③ 네이버·카카오·3N "우리도 개발자 부족" 이구동성

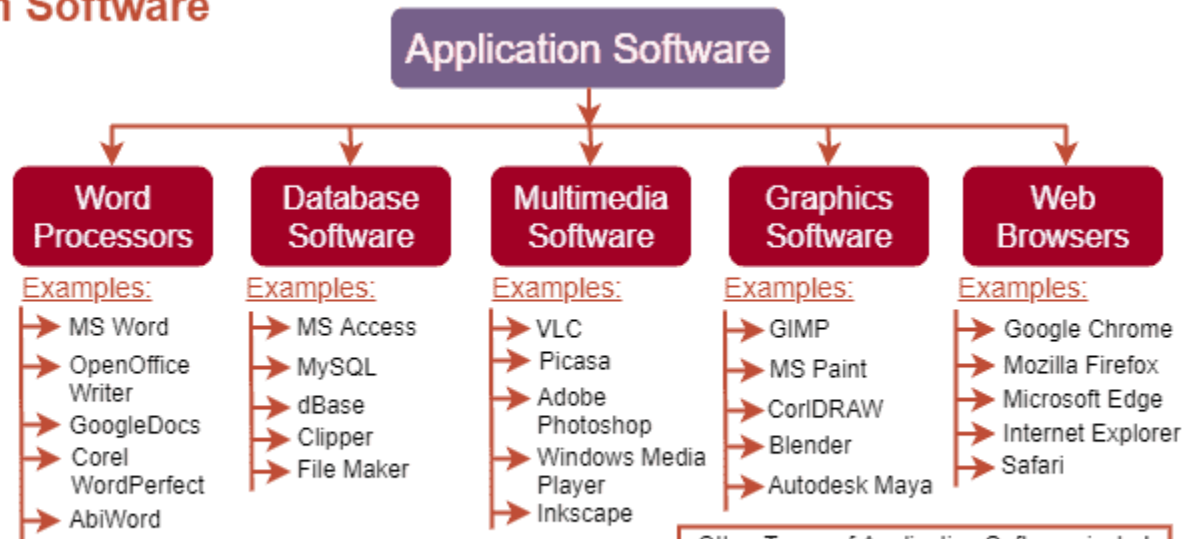
[제2차 SW인재 대란] ③ 네이버·카카오·3N "우리도 개발자 부족" 이구동성. 정명섭 기자 2021-06-28 00:15. 기사 공유; 폰트크기 조절.

2021. 6. 28.

# Types of Software



## Types of System Software



Other Types of Application Software include "Educational & Reference Software" and "Customized & Specific Purpose Software".

## Types of Application Software

Source: Tutorials Mate,  
Main Types of Software with Examples



# Software

**“Software is eating the world”, in all sectors.**

by Mark Andreessen, 2011.8.20

Founder of Netscape, renowned Venture Capitalist Andreessen-Horowitz

In the future every company will become a software company"

Nov 30, 2011, 01:58pm EST

## Now Every Company Is A Software Company

David Kirkpatrick Contributor  
Techonomy Contributor Group ①

### Software is Everywhere



Fall 2018 – University of Virginia

© Praphamontipong

2

Source: Software Testing Introduction CS 4501 / 6501 Software Testing, by Aron Russell

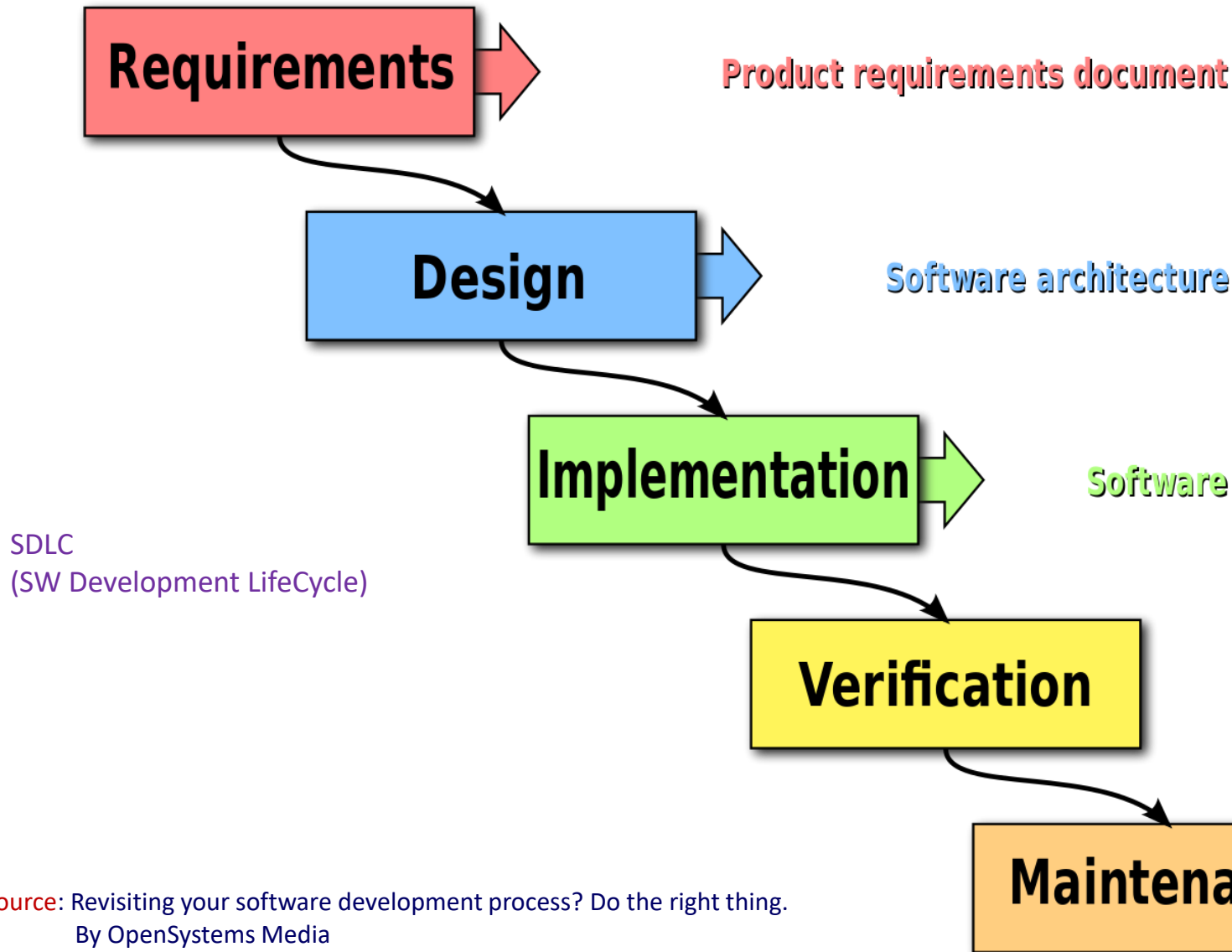
# Importance of Software

---

- The economies of ALL developed nations are dependent on software.
- More and more systems are software controlled
- Software engineering is concerned with theories, methods and tools for professional software development.
- Expenditure on software represents a significant fraction of GNP in all developed countries
- Software costs often dominate computer system costs. The costs of software on a PC are often greater than the hardware cost.
- Software costs more to maintain than to develop. For systems with a long life, maintenance costs may be several times development costs.
- Software engineering is concerned with cost-effective software development.

Source: SlidePlayer, Software Engineering & Mobile Apps

# SW Development Process



# A Building Process

**HOW DOES IT WORK . . . ?**

**Architects4Design** .com  
Contact us : 99009 46000



**STAGE : 1**  
**MEET OUR TEAM**



**STAGE : 2**  
**DISCUSS ABOUT YOUR  
REQUIREMENTS & BUDGET**



**STAGE : 3**  
**CONCEPT DESIGN**



**STAGE : 4**  
**PREPARE ESTIMATION &  
BOQ's for CONSTRUCTION**



**STAGE : 5**  
**PLAN SANCTION  
for CONSTRUCTION**



**STAGE : 6**  
**CONSTRUCTION**

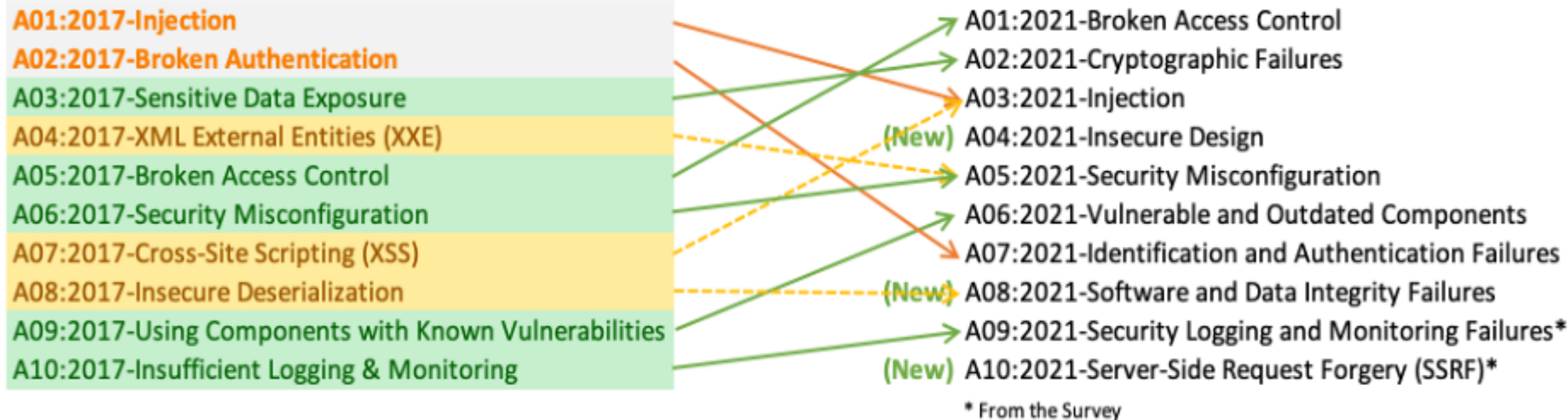
Source: <http://prabhakaranconstruction.com/gallery.php>

# Security risks in Software Development (Attacks on the SW)

## OWASP Top 10 Web Application Security Risks

2017

2021



## 2021 CWE Top 25 Most Dangerous Software Weaknesses

Rank	ID	Name	Score	2020 Rank Change
[1]	<a href="#">CWE-787</a>	Out-of-bounds Write	65.93	+1
[2]	<a href="#">CWE-79</a>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.84	-1
[3]	<a href="#">CWE-125</a>	Out-of-bounds Read	24.9	+1
[4]	<a href="#">CWE-20</a>	Improper Input Validation	20.47	-1
[5]	<a href="#">CWE-78</a>	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19.55	+5
[6]	<a href="#">CWE-89</a>	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19.54	0
[7]	<a href="#">CWE-416</a>	Use After Free	16.83	+1
[8]	<a href="#">CWE-22</a>	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.69	+4
[9]	<a href="#">CWE-352</a>	Cross-Site Request Forgery (CSRF)	14.46	0
[10]	<a href="#">CWE-434</a>	Unrestricted Upload of File with Dangerous Type	8.45	+5

# Software Security

---

- **By Laurie Williams – NC State**

- The idea of engineering software so that it continues to function correctly under malicious attack
  - SW Security  $\neq$  **Reacting** through “penetrate and patch”
  - SW Security  $\neq$  **Firewalling vulnerabilities**
- understanding, preventing, and mitigating software-induced security risks

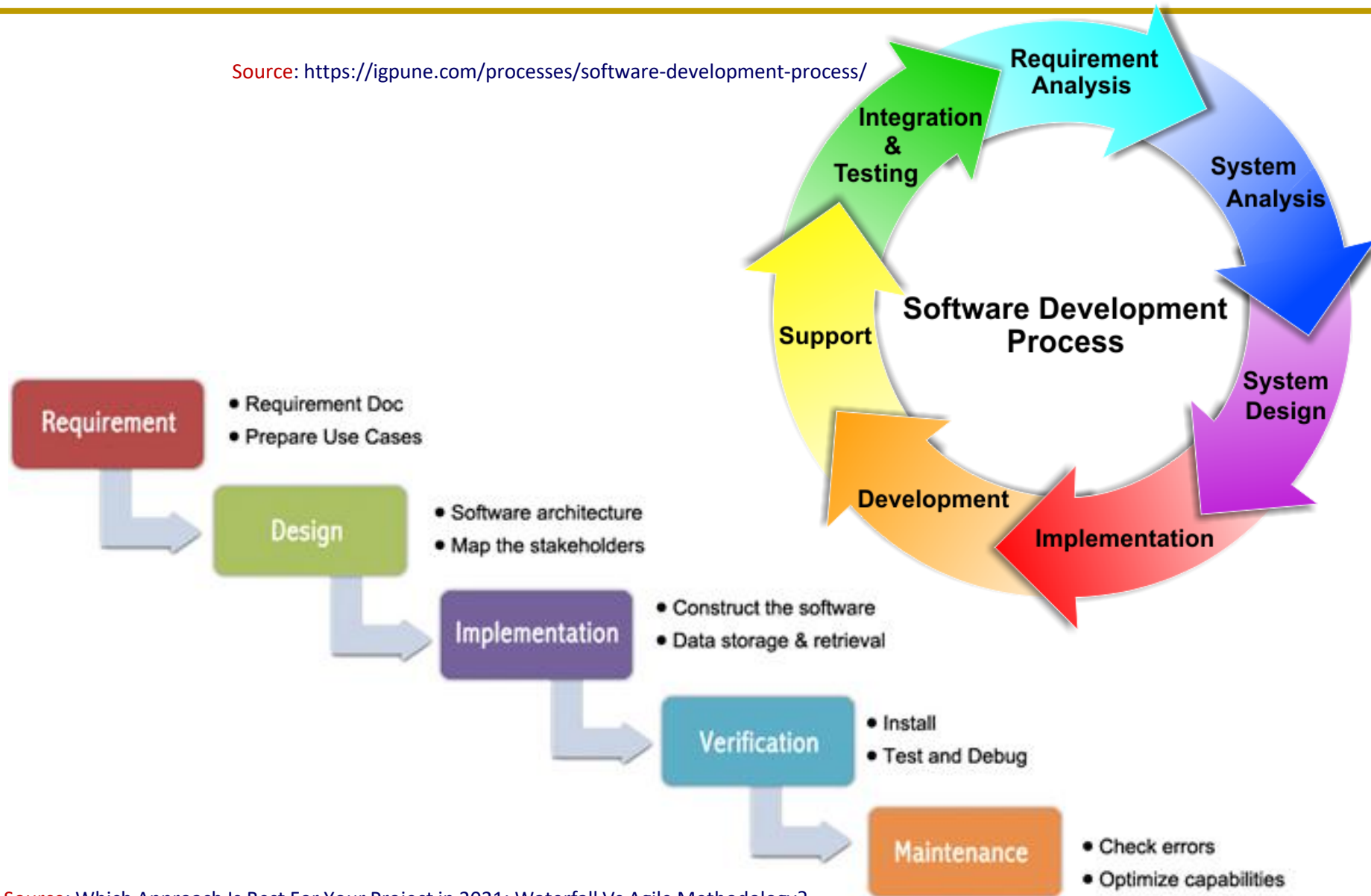
- **By Meenakshi Mani & Tanvi Shah**

- Its all about building secure software!
- The **process** of designing, implementing, and testing software **for security**
- Taking **the pro-active approach**: building security INTO the software as opposed to securing it after building it.



# Software Development Process

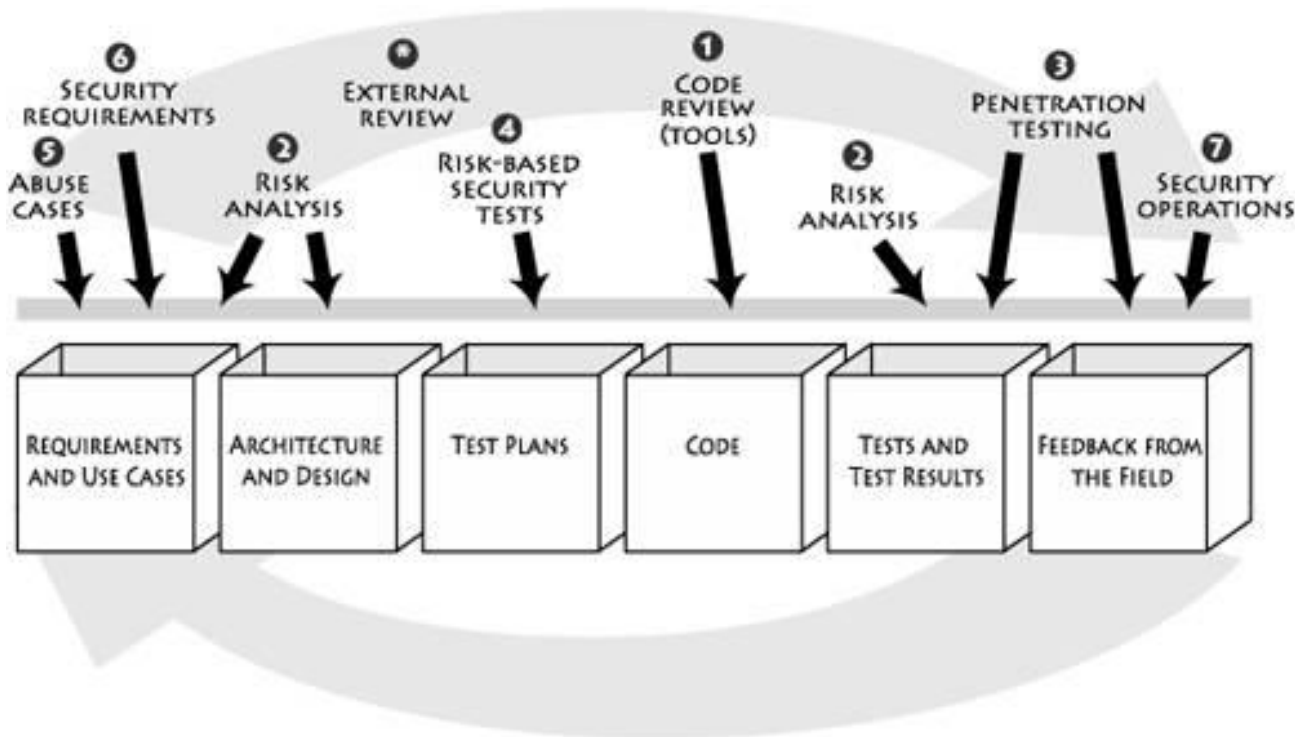
Source: <https://igpune.com/processes/software-development-process/>



Source: Which Approach Is Best For Your Project in 2021: Waterfall Vs Agile Methodology?

# Software Security

- Software security is an idea implemented to protect software against malicious attack and other hacker risks so that the software continues to function correctly under such potential risks. (source: Techopedia)
- Software Security: Building Security In





# Security Development Lifecycle (SDL) by Microsoft

- **The goals of SDL are twofold:**

- to reduce the number of security-related design and coding defects, and
- to reduce the severity of any defects that are left.

- **SD3+C**

- Secure by Design
  - means getting the design and code secure from the outset.
- Secure by Default
  - is a recognition that you never will.
- Secure in Deployment and Communication

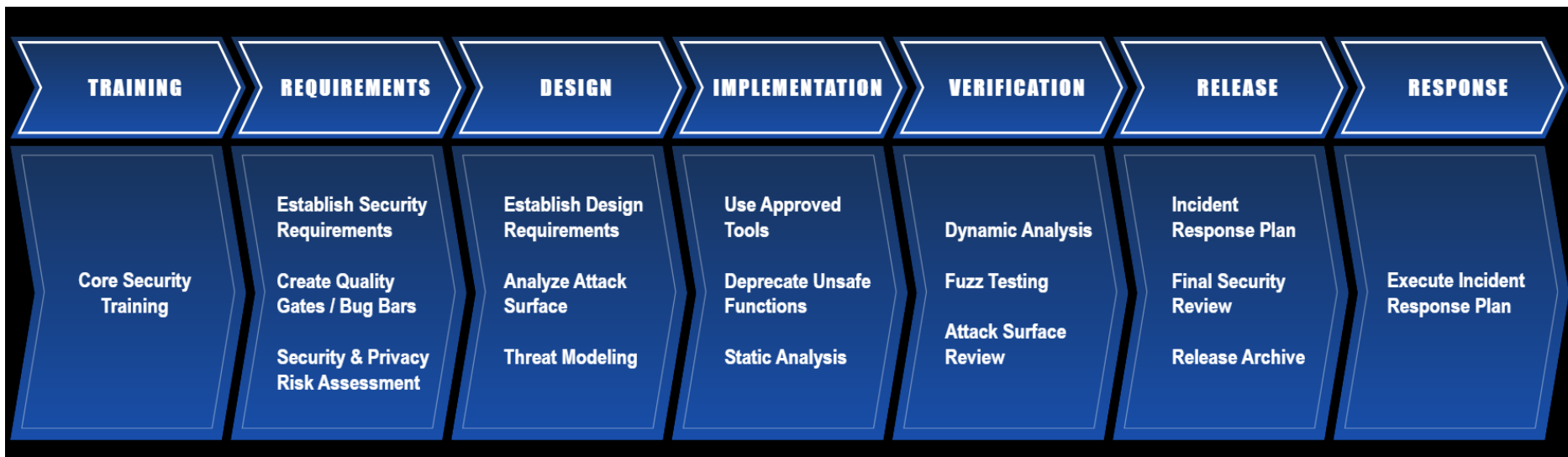
- **SDL adds security-specific checks and measures to any existing software development process.**



# Software Security

## ● Microsoft Security Development Lifecycle (SDL)

- A software development security assurance process
- Affects all steps in the lifecycle and the development culture
  - Training → Requirements → Design → Implementation → Verification → Release → Response
- Simplified SDL has 17 security practices (see figure below)
- Uses a build-security-in/secure-by-design-philosophy



Source: SDL app protection, PreEmptive, <https://www.preemptive.com/solutions/SDL-App-Protection>

👉 Software Security ≠ Security Software

# Other Software Threats

## Benign software (Goodware)

- System SW
- Application SW

## Malicious software (Malware)

- Ransomware
- Virus
- Worm
- Backdoors
- bots
- Trojan horse
- Rootkits
- Spyware

Potentially risky software  
= grayware = greyware  
Potentially Unwanted Applications (PUAs)  
= Potentially Unwanted Programs (PUPs)

- Adware
- Spyware
- ...



# Some famous real world attacks

Why is Security important?

# 사이버 위협 현황

- Log4j는 Java/Kotlin/Scala/Groovy 코딩 도중에 프로그램의 로그를 기록해주는 라이브러리로, 이클립스, IntelliJ IDEA, 안드로이드 스튜디오 등에 추가해서 프로그램 실행 시 자동으로 지정한 경로에 로그를 저장해주는 기능을 제공
  - Log4j 보안 취약점 사태 – 아파치 소프트웨어 재단의 Java 언어로 제작된 Log4j 라이브러리를 사용하는 대부분의 인터넷 서비스에서 매우 중대한 보안 취약점이 발견된 사건.
  - 출처: 나무위키
- Log4j는 JAVA를 기반으로 하고 있는데, Minecraft의 자바 버전에서 특정 메시지를 입력하면 상대 컴퓨터를 조종할 수 있는 현상이 일어났다. Log4j는 프로그램 개발 기록(로그)을 쉽게 관리할 수 있는 라이브러리(프로그램 기능 집합체)인데, 오픈소스라는 특성상 대다수 기업이 직간접적으로 활용했기 때문에 세계적으로 사태가 커졌다. MS는 지난 10일 긴급 업데이트로 진화에 나섰다.

CIO Korea

## 역대급 보안구멍 '로그4j' 막아라...개발자들의 고군분투기

12월 9일 아파치 재단(Apache Foundation)은 거의 모든 자바 애플리케이션에 사용되는 오픈소스 로깅 프레임워크 '로그4j(Log4j)'에서 발견된 치명적인...

2021. 12. 20.

보안뉴스

## 로그4j의 취약점이 보안 담당자들을 미치게 만드는 이유

[보안뉴스 문가용 기자] 보안 팀들이 로그4j(Log4j)에서 발견된 취약점 때문에 바쁘다. 단순 패치 적용만으로 끝나는 문제가 아니기 때문에 더 그렇다

2021. 12. 17.


H 한국경제

전세계 서버 뚫은 'Log4j' 공포 IT업계, SW 보안경쟁 불붙었다

티맥스소프트, 24시간 비상지원. LG CNS, 솔루션 긴급 업데이트 스패로우, 보안 진단서비스 제공. 전세계 서버 뚫은 'Log4j' 공포 IT업계, SW 보안...


2021. 12. 20.

# 사이버 위협/방어 현황

 보안뉴스


2022년에도 계속되는 로그4j 사태... 3가지 취약점 추가 공개

[보안뉴스 원병철 기자] 아파치재단이 로그4j(Log4j)에 대한 보안공지를 '다. ... CVE-2022-23302 : Apache log4j JMSSink 역직렬화 취약점

 지디넷코리아


MS·구글, Log4j 등 오픈소스 보안개선 앞장

MS·구글, Log4j 등 오픈소스 보안개선 앞장. 오픈소스 소프트웨어 공급망 보안 개선 알파오메가 프로젝트 참여. 남혁우 기자. 입력 :2022/02/11 14:56 수정:...

 매일경제

국내 은행에 매일 600건씩 사이버공격..."보안관제 강화해야"

15일 국민의힘 강민국 의원실이 금융보안원으로부터 제출받은 자료에 따르면 소매금융을 취급하는 국내 17개 은행이 2017~2021년 받은 사이버 공격은


 보안뉴스

우크라이나를 겨냥한 러시아의 사이버 공격 증가 중

액티늄의 공격은 2021년 10월 경부터 시작됐다고 하며, 각종 정부 기관에 더해 인권 및 구호 단체들까지도 공격의 대상이 되고 있다고 한다.

## McDonald's Cyber Attack Targets Data

Once McDonald's also became the successful victim of cyber-attack which involves the data extractions of numerous users. In countries like Taiwan and South Korea, the personal addresses, email addresses, and phone numbers of the customers get exposed. However, McDonald's managed to handle the situation at the time by confirming that the information volume which is exposed is small and we had appointed consultants to deal with the situation. But it is confirmed that it took McDonald's a week to stop cyber attackers from unauthorized access of their data.

 크립토프레스소 Cryptopresso

2028년까지 놀라운 성장을 보일 사이버 공격 시뮬레이션 도구 ...

2021년 유형별 글로벌 사이버 공격 시뮬레이션 도구 시장 세그먼트 비율(%). 온프레미스. 클라우드 기반. 애플리케이션별 글로벌 사이버 공격...

# Ransomware


- WannaCry ransomware



# Ransomware


"기아차 美법인, 랜섬웨어 공격받아...232억원치 비트코인 요구" [조선비즈, 2021.02.18](#)

**랜섬웨어, 온라인 교육 증가와 함께 교육 기관 겨냥...예방 대책은?**

박병화 기자 | 입력 2021-02-26 13:07 | 수정 2021-02-26 13:07  데일리시큐

2021년, 랜섬웨어 공격으로 최소 7천억 이상 랜섬머니 지불  
돼

지난해는 6억 달러(한화 약 7천149억원) 이상이 지불됐다고 밝혔다. 한편 사이버 위협 전문가들은 2020년과 2021년 실제 지불금액은 훨씬 더 높을 것이라...

 연합뉴스

작년 랜섬웨어 피해 76% ↑ ..."수상한 이메일 주의"

과학기술정보통신부에 따르면 지난해 랜섬웨어 해킹 피해 신고는 223건으로 재작년 127건보다 76% 늘었습니다. 지난달에도 최근 3년간 1월 평균인 5건의 4...


[연합뉴스 2022/02/09](#)

2022년 1월 랜섬웨어 피해 3.8배 늘었다! 랜섬웨어 침해사고

...

2022년 1월, 최근 3년 평균 동기간 대비 3.8배 급증 2021년 피해 기업 66%가 데이터 백업하지 않아 복구 어려움 과기정통부, '랜섬웨어 대응 3종...

[보안뉴스 2022.02.09](#)

 매일경제

[매일경제, 2022.02.25](#)

원자재 없고 랜섬웨어 터질라...러 침공에 국내 IT업계 진땀  
[러, 우크라 침공]

지난해 랜섬웨어 공격 건수가 크게 늘어난데다 전세계의 대러시아 제재에 러시아 정부 지원을 받는 해커들의 활동이 증가할 수 있기 때문이다. 이 같은...



# 비대면 환경의 보안 위협

## 비대면 환경 노린 해킹 ↑, 정부 23년까지 6,700억 원 투입...해결방법은


### 비대면(Untact) 환경의 보안위협

국내외 대표적인 보안기업들은 최근 앞 다투어 '2021년 보안전망 보고서'를 발표하면서 하나같이 '비대면 환경'을 보안이슈로 꼽았다. 이글루시큐리티는 '2021년 보안위협·기술 전망보고서'에서 코로나19를 계기로 디지털 전환과 기술 융합이 가속화되면서, 지금까지 경험하지 못했던 새로운 유형의 보안 위협이 빠르게 확산될 것으로 내다봤다. 포스트 코로나 시대, 비대면 플랫폼에서의 보안위협이 대두될 것이라는 전망이다. 비대면 플랫폼 사용이 증가하면서, 이를 노리는 사이버 공격 또한 지속적으로 발생 것이라는 설명이다. 이미 초대받지 않은 외부인이 들어와 화상 수업·회의를 방해하거나, 취약점을 익스플로잇해 비대면 애플리케이션을 장악하는 등의 공격이 잇달아 포착되고 있다. 또한, 다크웹을 통해 탈취된 사용자 계정 정보와 내부 정보가 판매될 가능성도 있어 추가 피해에 대한 대응방안 마련도 요구된다.

삼성SDS는 ▲비대면 환경을 노린 위협 증가 ▲랜섬웨어 고도화 ▲AI를 활용한 해킹 지능화 ▲산업설비에 대한 위협 본격화 ▲개인정보 등 민감 데이터 보호 중요성 증대 ▲클라우드 대상 공격 증가 ▲의료 분야 집중 공격 등을 주요 키워드로 꼽았다.


특히 비대면 업무환경 확대, 디지털 전환 가속화, 데이터 산업 활성화 등에 따라 사이버 위협도 더욱 증가할 것으로 예상되는 만큼 기업의 철저한 보안 대책 마련이 필요하다고 강조했다.

# 사이버 공격

 한국일보

우리 집 거실 흔히 '월패드 해킹'...똑똑한 아파트일수록 불안 커진다

월패드 해킹 촬영 이미지 유출' 의혹 증폭 불안한 시민들 급한 대로 '카메라 가리  
기' 이미 수년 전 홈네트워크 보안 취약 제기. 아파트 월패드의 위쪽...

 매일경제

2021. 12. 11.

[단독] 비밀번호 바뀌도...아파트 월패드, 해킹에 무방비

지난해 11월 사회적 문제가 된 월패드 해킹이란 각 가정 벽면에 부착돼 현관 출입문, 난방, 환기 등을 제어하는 홈IoT의 핵심 기구인 월패드를 해킹한...

4주 전

미국 텍사스에 위치한 '솔라윈즈'는 네트워크 모니터링 SW 전문 기업. 미국 국무부와 상무부를 비롯한 연방 기관이 핵심 고객. 미국 10대 통신기업 및 전 세계 유수의 대학도 솔라윈즈를 쓰고 있을 정도...

[아이뉴스24 안희권 기자] 지난해 말 발견됐던 미국정부기관을 겨냥한 솔라윈즈 사이버 공격은 역대 최대 규모였던 것으로 조사됐다.

**"美솔라윈즈 사이버공격, 최대규모로 매우 정교", 2021.02.16**

로이터 등의 주요 외신들에 따르면 브래드 스미스 마이크로소프트(MS) 사장은 14일(현지시간) 미국 주요 정부기관이 솔라윈즈의 소프트웨어 취약점을 이용한 해킹 공격으로 위험에 노출됐다고 말했다. 그는 이 해킹공격이 사상 최대 규모이며 가장 정교한 사이버 공격이었다고 평했다.

(도쿄=연합뉴스) 박세진 특파원 = 북한이 한국의 금융·인프라(사회기반) 등의 공공 분야에서 지난해 하루 평균 약 150만 건의 사이버 공격을 감행한 것으로 의심된다고 요미우리신문이 1일 서울발로 보도했다.

**"北, 한국 공공분야 일평균 150만건 사이버 공격"<요미우리>, 2021.02.01**

이 신문은 국가정보원이 작년 11월 국회에 보고한 내용과 한국 정부 관계자를 인용해 한국 공공 분야에서 받은 일평균 사이버 공격이 2016년 41만 건에서 작년에는 4배 수준인 162만 건으로 급증했다고 전했다.

## 2021 보안 위협 전망

AhnLab

타깃형 랜섬웨어 공격의 증가



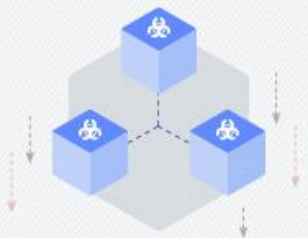
비대면 업무환경 보안위협 확대



다양해지는 악성코드 제작 언어



악성코드의 기능 모듈화



악성 앱 유포의 글로벌화



## 2022년 사이버위협 전망



01

Log4j 취약점 문제 장기화와  
공급망 보안위협



02

월패드 등 IoT 기기 대상  
사이버위협 증가



03

끝나지 않는  
랜섬웨어와의 싸움



04

디지털 대전환의 핵심 인프라,  
클라우드 보안 위협 증가



05

메타버스, NFT, AI 등  
신기술 대상 신종 위협 발생



06

사회적 이슈를 악용한  
스미싱, 해킹메일 지속



AhnLab

ESTsecurity

HAURI

INCA

NSHC

BITSCAN

과학기술정보통신부

보안뉴스

KISA 한국인터넷진흥원

# Benefits of Cybersecurity

---

- **Valuable information protection**
  - User data protection
  - Protection from data theft, Evade loss of crucial data
- **Improved privacy**
  
- **Protection of intellectual property**
- **Preventing financial frauds and embezzlement**
- **Prevention of cyber espionage**
- **Protects against malware attacks**
  
- **Risk mitigation**
  - Reduced hacking incidents
- **Recovery time is improved**

# Summary

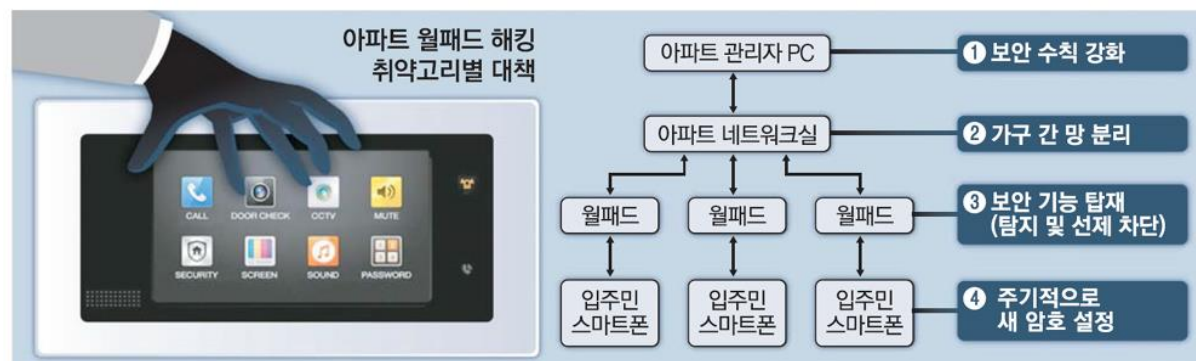
## ● Definition of

- Information, Information System
- Computer Security
- Software Security

☞ System Security, Network Security, Internet Security, Web Security, Mobile Security, ...

## ● Some famous real world attacks

- Ransomware
- 비대면 환경의 보안 위협
- Log4j 취약점 사태
- 비밀번호 바뀌도...아파트 월패드, 해킹에 무방비



Source: 비밀번호 바뀌도...아파트 월패드, 해킹에 무방비, 매일경제, 2022.02.02

# Appendix



# 국제해킹방어대회 '코드게이트 2022' 본선 진출 40개팀 발표


	General	University		Junior	
(자동진출)	PPP (USA) - codegate2020 winner				
1	Organizers (Multinational)	CyKor	고려대학교	kitsune	한국디지털미디어고등학교
2	Straw Hat (China)	해군 해난구조전대	송실대학교	Yo (Iran)	Issar school of art
3	More Smoked Leet Chicken (Russia)	lmssm99	서울과학기술대학교	Qyn (Netherlands)	Pontes Goese Lyceum
4	Kalmarunionen (Multinational)	GoN	카이스트	ash3r	선린인터넷고등학교
5	ZerOpts (Multinational)	PLUS	포항공과대학교	heegong	세명컴퓨터고등학교
6	The Duck (Korea)	psykor	고려대학교	K-ARMY	선린인터넷고등학교
7	CodeRed(Korea)	roKyC	고려대학교	Gyul	선린인터넷고등학교
8	본선 온라인 기원 (Korea)	CAT-Security	가톨릭대학교	Sechack	선린인터넷고등학교
9	WreckTheLine (Multinational)	KEEPER	부산대학교	B33nz1n0	인천효성고등학교
10		경희대 미남 해커들	경희대학교	CTF점음스기	한국디지털미디어고등학교
				고양이가 세상을 구한다	방산고등학교
				AIS	한국디지털미디어고등학교
				me2nuk	세명컴퓨터고등학교
				나는야 폭군 티라노사우르스	한국디지털미디어고등학교
				ursobad	
				(^o^)	제주제일고등학교
				DevDori	
					한국디지털미디어고등학교
					Montgomery Blair High School
					선린인터넷고등학교

코드게이트보안포럼은 '코드게이트 2022' 예선전에 총 48개 국 2,872팀이 참여한 가운데, 치열한 경쟁을 거쳐 총 40개 팀이 본선에 진출했다고 2일 밝혔다.

지난해 코로나19로 인해 개최가 취소되면서 2년 만에 치러진 이번 예선전은, 2월 26일부터 27일까지 ▲ 일반부 ▲ 대학생부 ▲ 주니어부로 나누어 온라인으로 진행되었다.


취약점 분석, 암호학, 리버싱 등 총 17개 문제가 출제되었으며, 문제별 배점을 고려하여 가장 높은 점수를 획득한 상위 팀이 진출하게 된다. 올해는 실제 사이버 전쟁에서 사용되는 운영체제(OS)의 취약점 문제를 비롯해 블록체인의 스마트컨트랙트, 대체불가토큰(NFT) 등 최신 사례를 반영한 기출문제로 실력을 겨뤘다.

# Software (SW)

 조선비즈

[스마트카 시대]⑤ “데이터 플랫폼 정비·소프트웨어 국산화 필수” - 조선비즈

하드웨어가 주를 이뤘던 내연기관차 시대와 달리 소프트웨어가 중심이 되는 스마트카 시대가 되면 필요한 인력부터 관련 기술, 법적 규제까지 모든 요소...

 아주경제

[제2차 SW 인재 대란] ① 20년 전 수준보다 10배의 파고... IT 넘어 전 산업에 개발자 부족

전통기업들, SW인재 확충해 비전 실현·위기 극복 '1차 SW 인재 대란' 뛰어넘는 인재부족 사태 맞아 모든 민간·공공 디지털 전환 "수십만 SW인재 필요"...

2021. 6. 28.

## 현대자동차 채용정보

[전략기술] UAM 소프트웨어 설계

경력모집기간 2020/04/29 ~ 2020/05/13

## 수행직무

· 임베디드 SW 설계 및 개발

- 항공(제어기/항공전자 시스템) 소프트웨어 아키텍처 설계/개발
- 항공 소프트웨어 플랫폼 및 프레임워크 설계/개발
- 항공 네트워크 소프트웨어 설계/개발(CAN, 1553, ARINC429, ARINC664 등)
- RTOS/non-OS 기반 항공 임베디드 어플리케이션 설계/개발

분산된 소프트웨어 역량 통합

합병시 확보되는 연구 인력 4000명

소프트웨어 중요성 갈수록 높아져

현대오토에버가 기술 고도화 책임

홈 헬스 케어 소프트웨어 시장, 2026년까지 대규모 성장 목격 | Delta Health Technologies, Netsmart Technologies, Kinnser 소프트웨어



# SW Engineer vs. SW Developer

SW Engineer	SW Developer
a professional who applies the principles of software engineering for designing, development, testing, maintenance, and evaluation of computer software. (is involved in the complete process)	a professional who builds software which runs across various types of computer  (Development is one aspect of the software project building process)
a team activity	primarily a solitary activity
works with other components of the HW system	writes a complete program
creates the tools to develop software	use readymade tools to build apps
tends to solve issues on a much larger scale	tend to do everything that engineers do but on a limited scale
The average salary for a Software Engineer is \$105,861 per year in the United States.	The average salary for a Software Developer is \$92,380 per year in the United States.

Source: Software Engineer vs. Software Developer: What's the difference?  
<https://www.guru99.com/difference-software-engineer-developer.html>

# Ransomware

"기아차 美법인, 랜섬웨어 공격받아...232억원치 비트코인 요구"

조선비즈, 2021.02.18

랜섬웨어, 온라인 교육 증가와 함께 교육 기관 겨냥...예방 대책은?


박병화 기자 | 입력 2021-02-26 13:07 | 수정 2021-02-26 13:07



## JBS Faced a Ransomware Attack

JBS USA was founded in the month of May after they became the victim of cyber-attackers which already infected some of the servers supporting its Canadian, Australian, and United States IT systems. The organization seized everything system which seems to be infected and then approached third-party consultants and law enforcement for setting the situation by working with internal IT support.

정보보호 리더 기업 7곳이 꼽은 2021년 3대 키워드, 랜섬웨어·비대면·클라우드

 데일리시큐

2021년, 랜섬웨어 공격으로 최소 7천억 이상 랜섬머니 지불  
돼

지난해는 6억 달러(한화 약 7천149억원) 이상이 지불됐다고 밝혔다. 한편 사이버 위협 전문가들은 2020년과 2021년 실제 지불금액은 훨씬 더 높을 것이라...

# 사이버 공격

국가기반시설 제어망에 대한 사이버 테러, OT 보안 전문 도구 통해 선제적 보안체계 구축 필요

## 사이버공격으로 가능해진 '양젓물 테러', 보안뉴스, 2021.02.22

[보안뉴스 이상우 기자] 올해 2월초, 미국 플로리다의 소도시 올즈마(Oldsmar)에 위치한 수처리 시설이 사이버 테러를 당했다. 해당 사이버 공격을 시도한 공격자는 데스크톱의 공유 소프트웨어인 팀뷰어(TeamViewer)를 통해 원격으로 제어시설에 접근해 주거용 및 상업용으로 사용되는 식수의 수산화나트륨 농도를 100배 이상 높이려고 시도했다. 쉽게 설명하면 해킹으로 '양젓물'을 우물에 풀려고 한 셈이다.

[아이뉴스24 안희권 기자] 지난해 말 발견됐던 미국정부기관을 겨냥한 솔라윈즈 사이버 공격은 역대 최대 규모였던 것으로 조사됐다.

## "美솔라윈즈 사이버공격, 최대규모로 매우 정교", 2021.02.16

로이터 등의 주요 외신들에 따르면 브래드 스미스 마이크로소프트(MS) 사장은 14일(현지시간) 미국 주요 정부기관이 솔라윈즈의 소프트웨어 취약점을 이용한 해킹 공격으로 위험에 노출됐다고 말했다. 그는 이 해킹공격이 사상 최대 규모이며 가장 정교한 사이버 공격이었다고 평했다.

(도쿄=연합뉴스) 박세진 특파원 = 북한이 한국의 금융·인프라(사회기반) 등의 공공 분야에서 지난해 하루 평균 약 150만 건의 사이버 공격을 감행한 것으로 의심된다고 요미우리신문이 1일 서울발로 보도했다.

## "北, 한국 공공분야 일평균 150만건 사이버 공격"<요미우리>, 2021.02.01

이 신문은 국가정보원이 작년 11월 국회에 보고한 내용과 한국 정부 관계자를 인용해 한국 공공 분야에서 받은 일평균 사이버 공격이 2016년 41만 건에서 작년에는 4배 수준인 162만 건으로 급증했다고 전했다.

# Cyber attacks stats 2021

---

## CYBER ATTACKS STATS 2021

- *By 2021, Cyber attacks will cost the world \$6 trillion*
- *By 2021 Companies have to expect ransomware attacks in every 6 seconds*
- *At present, 24,000 suspicious apps are deleted on a daily basis*
- *21% of files are not protected around the globe*
- *60% of frauds have mobile phone as their origin*
- *Average ransomware demand will be more than \$1000 by 2021*
- *90% of hackers are using encryption. Making it hard to track them*
- *It's expected that cyber-security awareness programs spending will reach \$10 billion by 2027*
- *Studies have revealed that 41% have loose end at their data protection system*
- *Only 25% of companies have standalone security department*

Source: What is the Importance of Cyber Security Tips in 2021

<https://www.testbytes.net/blog/cyber-security-tips-2021/>