Introduction to Software Security

Security Threats

Seong-je Cho

Computer Security & Operating Systems Lab, DKU

References

- Microsoft STRIDE chart
  - https://www.microsoft.com/security/blog/2007/09/11/stride-chart/
- Common Vulnerabilities & Exposures (CVE)
  - https://cve.mitre.org/
- The Open Web Application Security Project (OWASP)
  - https://owasp.org/
- Information Security: Principles and Practice*, 2nd edition by Mark Stamp, Wiley, 2011*
- *N. Vlajic, CSE 3482*: Introduction to Computer Security, Yorku
- *L. Williams*, CSC515 Software Security, NC STATE
- *V. Kemerlis*, CSCI 1650 – Software Security and Exploitation
  - https://cs.brown.edu/courses/csci1650/lectures.html

Contents

- Threats in Alice's online Bank and their protection
  - The cast of characters: Defenders, Clients, Attackers/Adversaries, …
- Types of Security Threats
  - Interception / Modification / Interruption / Fabrication / Repudiation
  - STRIDE
- Main Components of Security Threats
- Software Security Threats

Security Threats

The Cast of Characters

- Alice and Bob are the good guys

- Trudy, and Darth are the bad guy
- Trudy is our generic “intruder”

Alice's Online Bank (AOB)

- Alice opens Alice's Online Bank (AOB)
- What are Alice's security concerns?
  - What types of security threats are there?
- If Bob is a customer of AOB, what are his security concerns?
- How are Alice and Bob concerns similar? How are they different?
- How does Trudy view the situation?

What type of attacks can adversaries perform in this situation?

Types of Security Threats

- Trudy tries to know Bob's account number/balance, PIN, …
- Trudy tries to withdraw money from Bob's account
  - Trudy tries to change Bob's account balance
  - Trudy tries to improperly change his own account balance if he opens a savings account
- There may be too many transactions to provide normal services

☞ In this section, we consider security threats is very similar to security attacks

- Security Threats ≈ Security Attacks

은행에 대한 사이버 위협/공격

- 15일 신한은행 겨냥 디도스 공격 발생, (디지털투데이, 2021.01.15)
  - 디도스 공격에 은행 홈페이지 접속시간 지연

- 금융 해킹공격 연평균 7회..디도스공격이 최다, (파이낸셜뉴스, 2020.10.05)
  - 유형별로 보면 여러 대의 컴퓨터가 특정사이트를 마비시키려고 한꺼번에 공격하는 디도스(DDos) 공격이 23건으로 가장 많았고, 정보유출 7건, 시스템 위변조 5건, 악성코드 감염 2건이다.
  - 한국거래소, 케이뱅크, 카카오뱅크, 11번가가 디도스 공격을 받았다. 지지자산운용은 내부정보가 유출됐고, 페퍼 저축은행은 인터넷망 웹메일 서버 침해(악성코드)가 발생한 것으로 드러났다.

- 5년간 전자금융 침해사고 37건…홍성국 의원 "케뱅·카뱅·거래소도 공격받아" (한국금융, 2020.1005)

2020	시스템위변조	저축은행	페퍼저축은행	인터넷망 웹메일 서버 침해(악성코드) 발생
2020	정보유출	금융투자	지지자산운용	서버 침해 발생으로 내부자료 유출
2020	DDoS공격	전자금융업자	11번가	홈페이지에 대한 DDoS공격
2020	DDoS공격	은행	카카오뱅크	모바일 뱅킹에 대한 DDoS공격
2020	DDoS공격	은행	케이뱅크	인터넷 뱅킹에 대한 DDoS공격
2020	DDoS공격	금융투자	한국거래소	홈페이지에 대한 DDoS공격

은행에 대한 사이버 위협/공격

순번	연도	유형	업권	금융회사	개요
1	2016	시스템위변	금융투자	흥국자산운용	홈페이지 웹쉘 업로드
2	2016	정보유출	금융투자	NH투자증권	내부 코드서명용 인증서 외부 유출
3	2016	DDoS공격	전자금융업자	쿠팡 ((구)포워드벤쳐스)	DDoS공격으로 접속 지연
4	2016	시스템위변	전자금융업자	한국스마트카드	웹 소스 내 스크립트 위변조
5	2016	DDoS공격	전자금융업자	쿠팡 ((구)포워드벤쳐스)	TCP Syn Flooding 공격으로 서비스 일시 접속 불가
6	2016	정보유출	금융투자	유진투자선물	상속인 조회 서비스 관련 데이터 유출
7	2017	정보유출	금융투자	한국투자증권	iNoble 관리자 사이트 해킹
8	2017	시스템위변	금융투자	흥국자산운용	녹취시스템 랜섬웨어 감염
9	2017	악성코드감	은행	우리은행	DR센터 퇴직연금교육관리시스템 악성코드
10	2017	정보유출	전자금융업자	갤럭시아 커뮤니케이션즈	외부메일서버 해킹
11	2017	악성코드감	전자금융업자	페이게이트	개인PC 바이러스 감염으로 내부정보 유출
12	2017	DDoS공격	금융투자	한국거래소	DDoS공격 발생(Armada collective)
13	2017	DDoS공격	은행	산업은행	DDoS공격 발생(Armada collective)
14	2017	DDoS공격	은행	국민은행	DDoS공격 발생(Armada collective)
15	2017	DDoS공격	금융투자	유진투자선물	DDoS공격 발생(Armada collective)
16	2017	DDoS공격	은행	하나은행	DDoS공격 발생(Armada collective)
17	2017	DDoS공격	금융투자	흥국증권	DDoS공격 발생(Armada collective)
18	2017	DDoS공격	금융투자	이베스트 투자증권	DDoS공격 발생(Armada collective)
19	2017	DDoS공격	금융투자	교보증권	DDoS공격 발생(Armada collective)
20	2017	DDoS공격	금융투자	리딩투자증권	DDoS공격 발생(Armada collective)
21	2017	DDoS공격	전자금융업자	에스케이플래닛	DDoS공격 발생(Armada collective)
22	2017	DDoS공격	금융투자	골든브릿지증권	DDoS공격 발생(Armada collective)
23	2017	DDoS공격	금융투자	IBK투자증권	DDoS공격 발생(Armada collective)
24	2017	DDoS공격	금융투자	유화증권	DDoS공격 발생(Armada collective)
25	2017	DDoS공격	금융투자	SK증권	DDoS공격 발생(Armada collective)
26	2017	DDoS공격	은행	대구은행	DDoS공격 발생(Armada collective)
27	2017	DDoS공격	은행	전북은행	DDoS공격 발생(Armada collective)
28	2017	정보유출	은행	산업은행	CISCO 네트워크 장비공격
29	2017	시스템위변	신용정보업	BNK신용정보	홈페이지 위변조 사고 발생
30	2018	정보유출	은행	우리은행	인터넷뱅킹 부정접속 발생
31	2018	DDoS공격	여신전문업	국민카드	DDoS공격으로 앱카드 장애

전자금융 침해사고 현황(2020.8월 기준 최근 5년간 연도별, 유형별, 업권별 전자금융 침해사고 현황).

출처 : 인포스탁데일리, 2020.10.05

iNoble: 한국투자증권의 멤버십 서비스

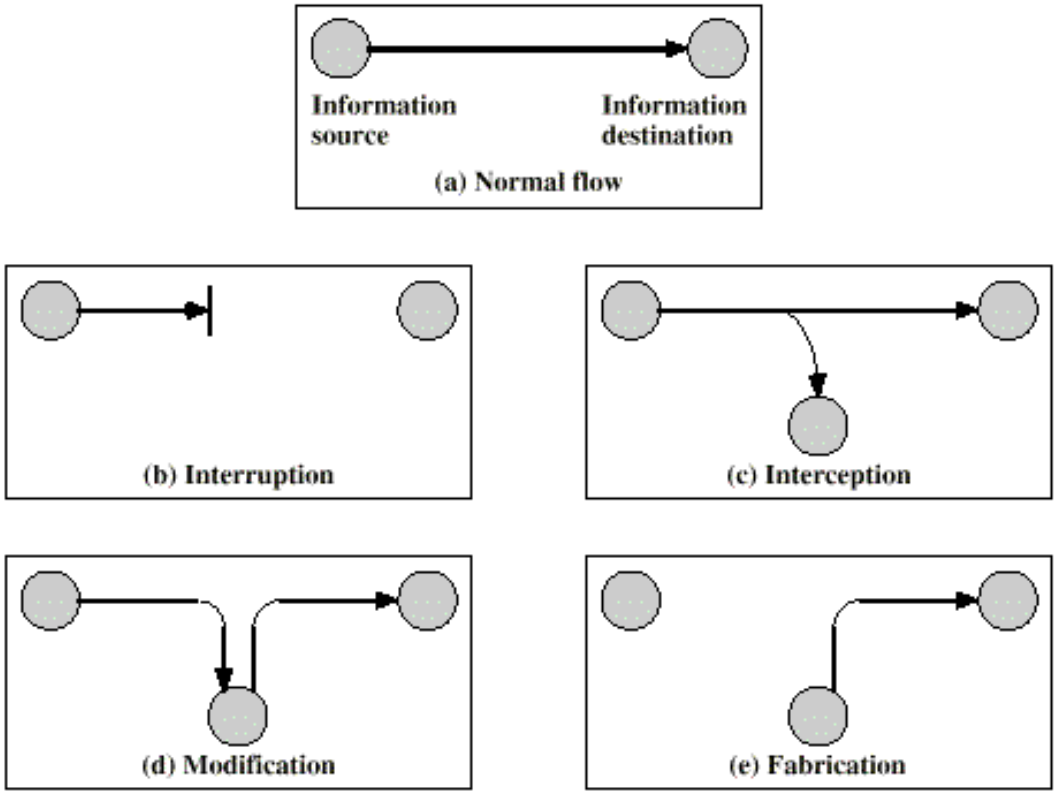
Amada collective: 해커 그룹

Types of Security Threats

- **Interruption:** asset is lost or unavailable (e.g., DoS / DDoS attacks)
- **Interception:** unauthorized access (e.g., wiretapping, illegal copying)
- **Modification:** changes/alteration into DB/program file
  - Patient data tampering, Modify communication, Band's firmware modification, Repackaged Android apps
- **Fabrication:** insert spurious transaction, illegally add entry to passwd file or DB

Which is the hardest threat to be detected?

Which threats can be prevented by Block-chain?



Examples of Threats and Attacks

What type of threat are the followings related to?

- Eavesdropping on communication, Wiretapping telecommunications networks, …
- Packet sniffing to capture data from/to network
- Key logging to capture data from/to a computer system
- Illicit copying of files or programs
- User / Credential counterfeiting, Email spoofing, Fake message, …
- Destruction of SW or HW, Cutting a communication line
- Flooding: TCP flood (SYN flood), Ping flood, …
- Occupying target server's resources: A fork bomb (rabbit virus), Repetitive file creation, Deadlock condition, …

Examples of Threats and Attacks

What type of threat are the followings related to?

- Changing information stored in data files or DB
- Altering programs so they perform differently
- Reconfiguring system HW or network topologies
- Website defacement
  - an attack on a website that changes the visual appearance of a website or a web page
- Replaying previously intercepted messages
- Spoofing a web site or other network service (e.g., DNS spoofing)
  - Pharming

✓ Phishing, Smishing, Vishing (voice or VoIP phishing), Telephone scam, …

Microsoft STRIDE model

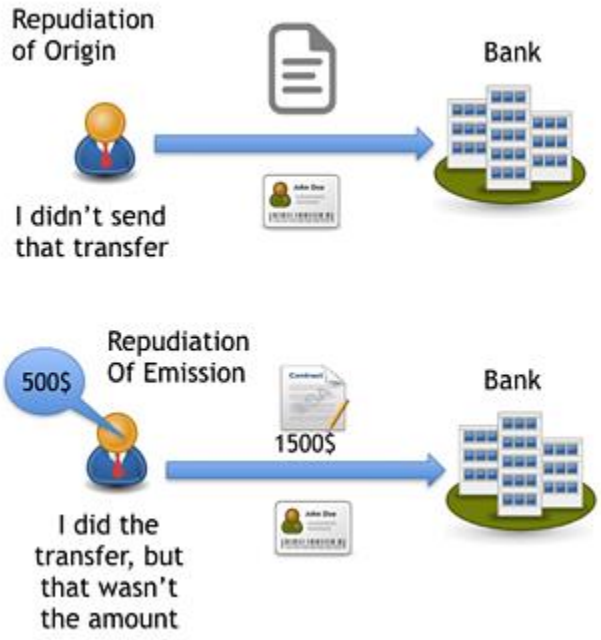
Threat	Definition	Example
Spoofing	An attacker tries to be something or someone he/she isn't	Phishing attack to fool user into sending credentials to fake site
Tampering	An attacker attempts to modify data that's exchanged between your application and a legitimate user	Message integrity compromised to change parameters or values
Repudiation	• An attacker denies performing an malicious action or doing something. • Delete access logs	Illegitimately claiming a transaction was not completed
Information disclosure	An attacker can read the private data that your application is transmitting or storing	Unencrypted message sniffed off the network
Denial of Service	An attacker can prevent your legitimate users from accessing your application or service	System flooded by requests until web server fails
Elevation of Privilege	An attacker is able to gain elevated access rights through unauthorized means	Attacker changes group membership. Rooting

Repudiation (부인, 잡아뗌)

- Repudiation
  - Attackers claim to not be responsible for an action
  - Attackers deny performing an action without other parties having any way to prove otherwise

- Example
  - Repudiation on the accountability of user (access, location, management, security)

Why do banks need Non-Repudiation of Origin and Non-Repudiation of Emission?

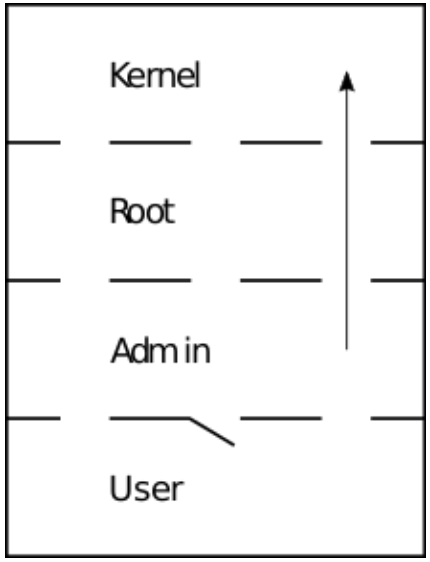


Elevation of Privilege

Privilege Escalation

- The exploitation of a bug or flaw that allows for a higher privilege level than what would normally be permitted.
- the act of exploiting a bug, a design flaw, or a configuration oversight in an OS or software application to gain elevated access to resources that are normally protected from an application or user.
- an attack that involves gaining illicit access of elevated rights, or privileges, beyond what is intended or entitled for a user.

- Allowing access to someone without proper authorization
- Unprivileged user gains privileged access to compromise the system
- Effectively penetrated and become part of the trusted system

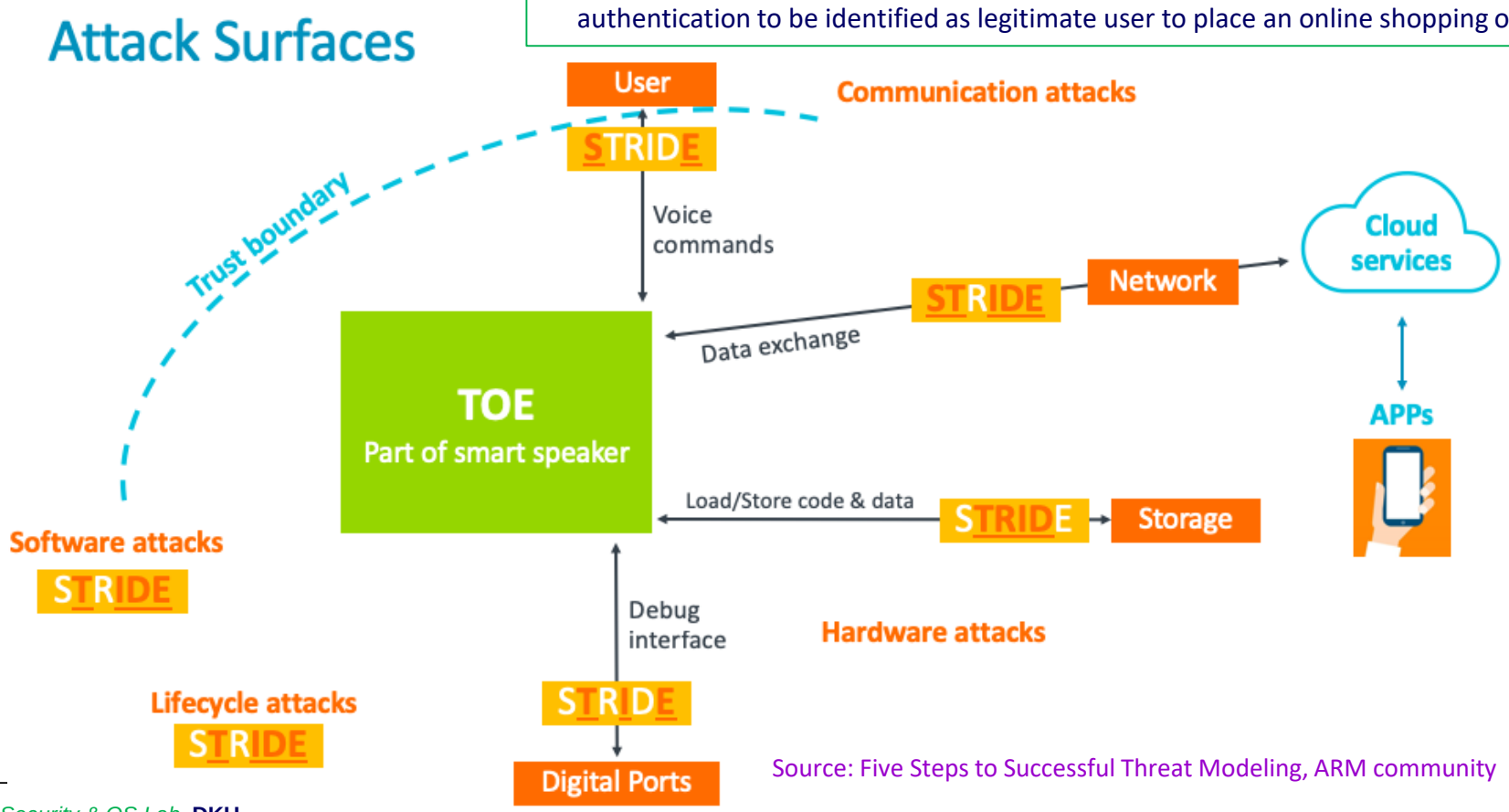


STRIDE threat model

- Identify potential adversaries, the attack surface and threats
  - ToE (Target of Evaluation)

If we take the user interface as an example of an entry point, potential communication attacks via voice commands could include:

- Spoofing -- an unauthorized person masquerading as the legitimate user to access the device
- Escalation of privileges, or an attacker who is trying to breach the voice ID authentication to be identified as legitimate user to place an online shopping order



Source: Five Steps to Successful Threat Modeling, ARM community

STRIDE threat model

- After you have identified your vulnerabilities and your threats, you can then consider how the threats directly affect each of your assets

Assets vs Threats

Firmware

Code injection(T) Reverse engineering(I)
Break secure state(TIE)
FW corruption(TD) Escalation of privilege(IE)

Configuration

Tamper config(T) Impersonation (SI)
Device disconnected(TD)
Unauthorized access(IE)

Certificates & Keys

Replace firmware certificate(TE)
Side channel analysis(I)
Corrupt Certificate(TD)

Voice records

Tamper records(T)
Impersonation (SI)
Unauthorized access(IE)

Credentials

Admin Impersonation (SRIE)
Replace credential(T)
Side channel analysis(I)
Unauthorized access(TIE)

Event Logs

Tamper system time(TR) Impersonation (SI)
Suppress/Erase critical events(TR)
Unauthorized access(IE)

Network communication

Impersonation (SRIE)
Tamper package(T)
MITM(RI)

Device resources

Debug port abuse(TI)
Eavesdropping buses(I)
Abuse resources(DE)

S : Spoofing of user identity
T : Tampering
R : Repudiation
I : Information disclosure
D : Denial of service (D.o.S)
E : Elevation of privilege

Source: Five Steps to Successful Threat Modeling, ARM community

Components of Security Threats

Security Threat

- any action/inaction that could cause disclosure, alteration, loss, damage or unavailability of a company's/individual's **assets**

- Three main components of a security threat:
  - **Target** [**Asset with vulnerability**]: organization's asset that might be attacked
    - Data & information, SW, HW, network service, system resource, etc.
  - **Agent** [**may or may not be present**]: people/organizations originating the threat – **intentional** or **non-intentional**
    - employees, ex-employees, hackers, commercial rivals, terrorists, …
  - **Event**: action that exploits target's vulnerability
    - **malicious**/ **accidental** destruction or alteration of information, misuse of authorized information, etc.

Vulnerabilities

- CVE (https://cve.mitre.org/) defines a **vulnerability** as:
  "A weakness in the computational logic (e.g., code) found in SW and HW components that, when exploited, results in a negative impact to confidentiality, integrity, or availability.
  - an occurrence of a weakness within a product, in which the weakness can be used by a party to cause the product to **modify or access unintended data**, **interrupt proper execution**, or **perform incorrect actions**
  - ☞ Weakness = a type of **mistake** that could contribute to the introduction of vulnerabilities

- ✓ Mitigation of the vulnerabilities in this context typically
  - involves coding changes, but
  - could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety)."

- ✓ All vulnerabilities in the NVD have been assigned a CVE identifier and thus, abide by this definition.

Source: https://nvd.nist.gov/vuln

Vulnerabilities

최악의 보안 취약점 'Log4j', 남은 이슈와 보안담당자들의 과제

- 보안뉴스, 2022-03-14

KISA의 'Log4j 위협 대응 보고서 v1.0' 살펴보니...개요와 원인, 취약점 악용 방식 등 정리

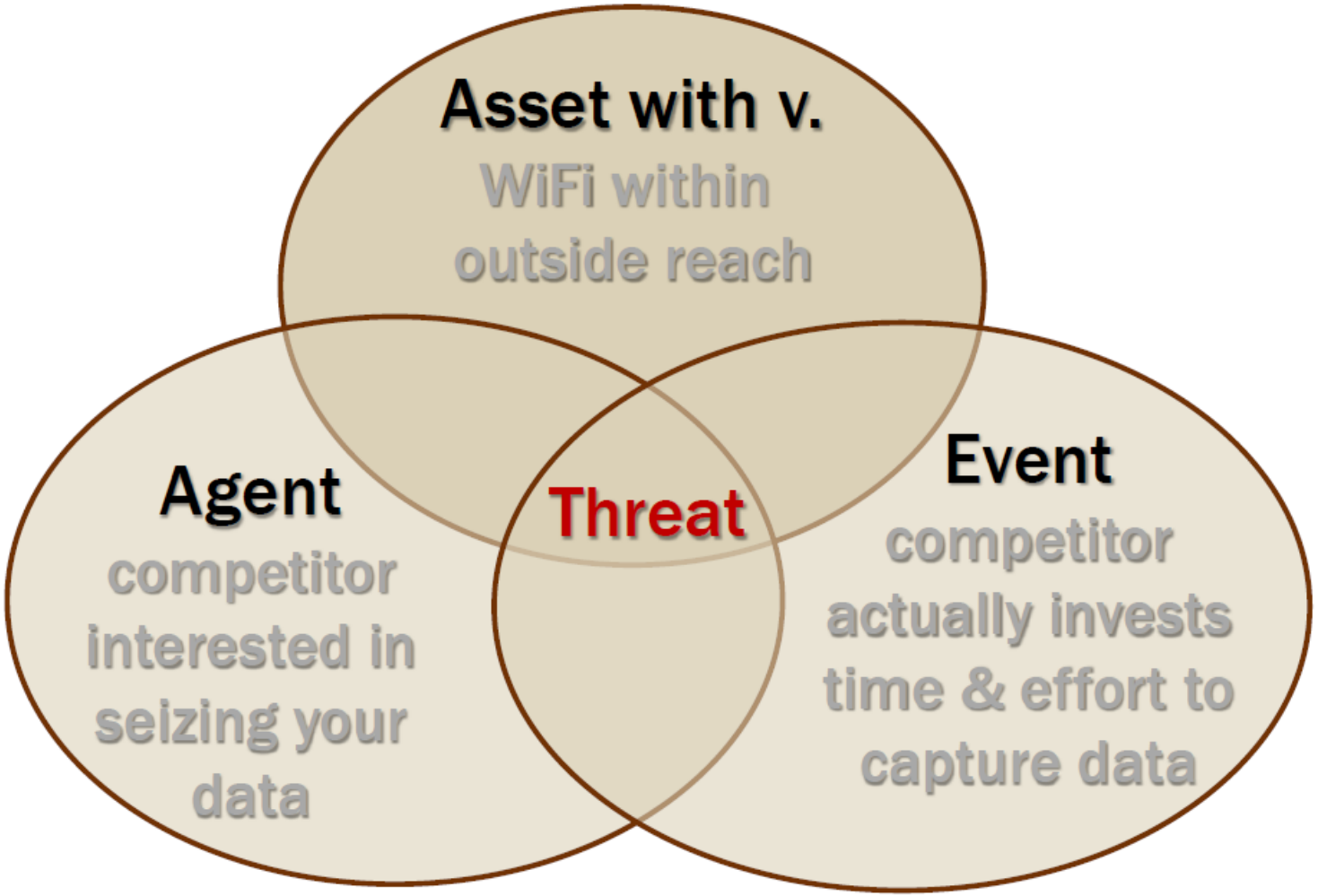
주요 이슈 △보안 업데이트는 여전히 진행중 △취약점 식별 및 내부 침투 확인 어려움 등

보안담당자들의 과제 △보안장비 정책 설정 △주요 시스템 모니터링 강화 △로그 관리 철저 등

	CVE 번호	취약점 내용	CVSS Score	패치 발표 날짜
1	CVE-2021-44228	원격코드 실행 취약점	10.0	2021-12-06
2	CVE-2021-45046	원격코드 실행 취약점	9.0	2021-12-13
3	CVE-2021-4104	1.x에서 발생하는 원격코드 실행 취약점	7.5	지원 종료
4	CVE-2021-45105	서비스 거부 취약점	5.9	2021-12-18
5	CVE-2021-44832	원격코드 실행 취약점	6.6	2021-12-28
6	CVE-2022-23302	1.x에서 발생하는 원격코드 실행 취약점	8.8	지원 종료
7	CVE-2022-23305	1.x에서 발생하는 SQL Injection 취약점	9.8	지원 종료
8	CVE-2022-23307	1.x에서 발생하는 원격코드 실행 취약점	9.8	지원 종료

Log4j 최초 취약점 발견 이후 추가 취약점 발견 및 보안 패치 현황[자료=KISA]

Example: Threat in WiFi network



NO EVENT ⇒ NO THREAT !!!

Examples of Threats

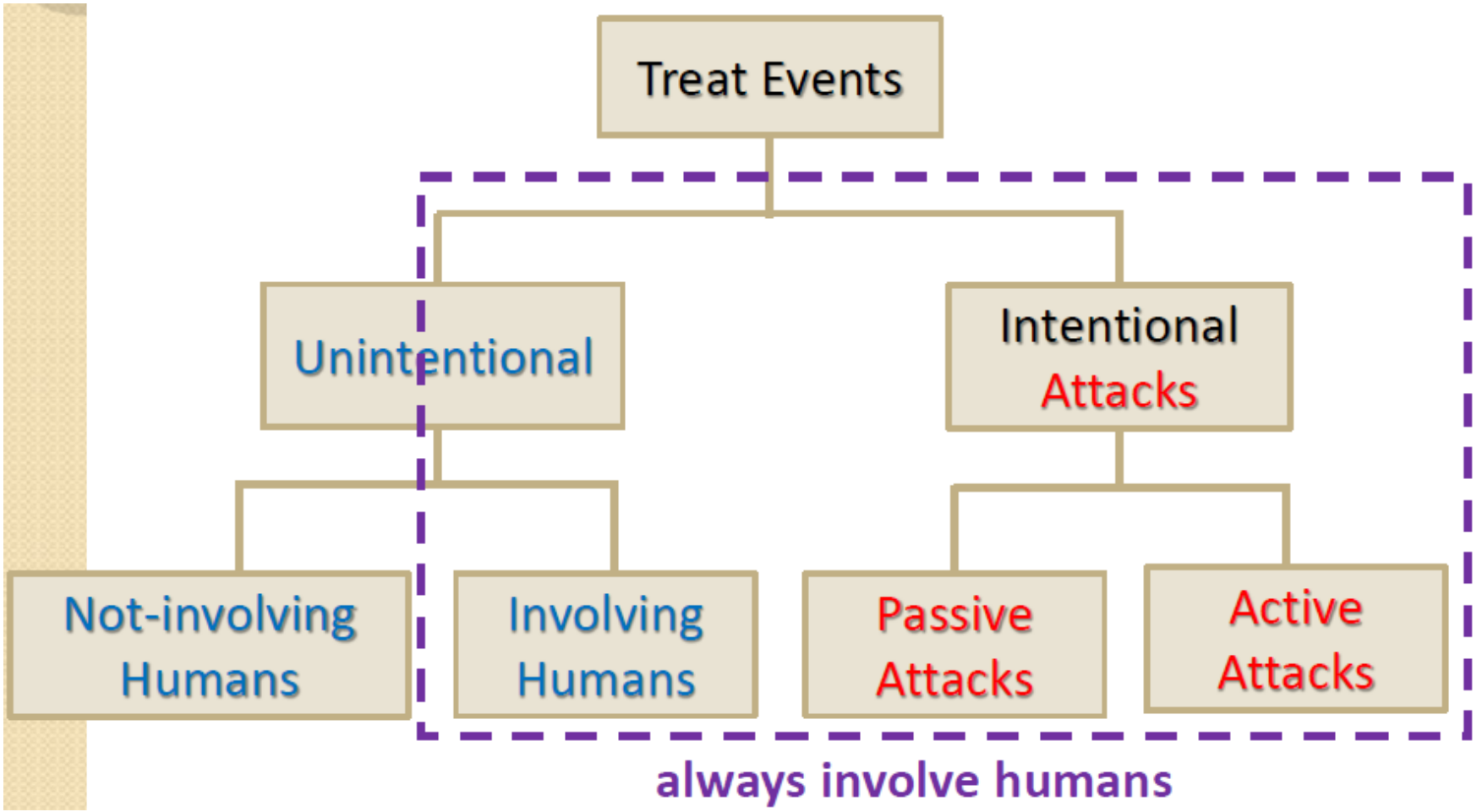
- **Threat without Agent**
  - **Asset with vulnerability: Data on a server, Not backuped!**
  - **Event: Flood or fire in the server room**

- **Outsider vs. insider, deliberate vs. accidental**
  - **Asset with vulnerability**
  - **Agent: outsider or insider**
    - Example of insider agent: SysAdmin has added a new software to the system and has forgotten to change the password
  - **Event: deliberate or accidental**

DBMS, IP camera
Default password

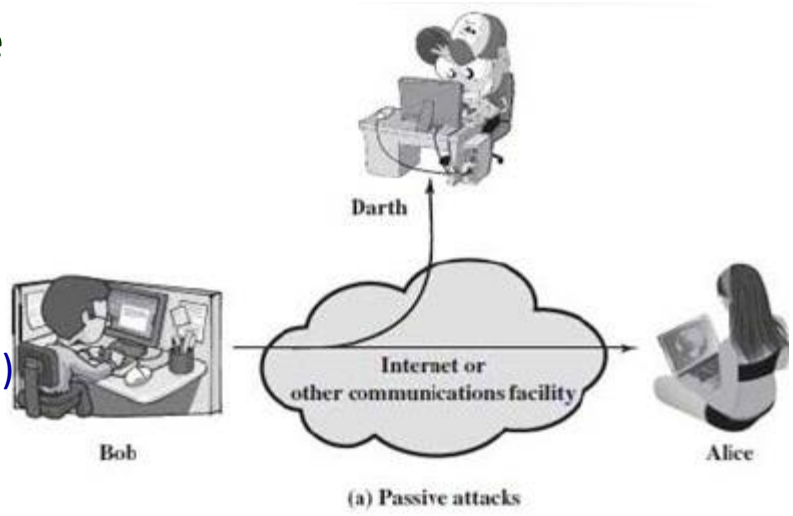
- **Attack**
  - **Asset with vulnerability**
  - **Agent executed threat event deliberately → Attack**
  - **Event: deliberate**

Categories of Threat Events



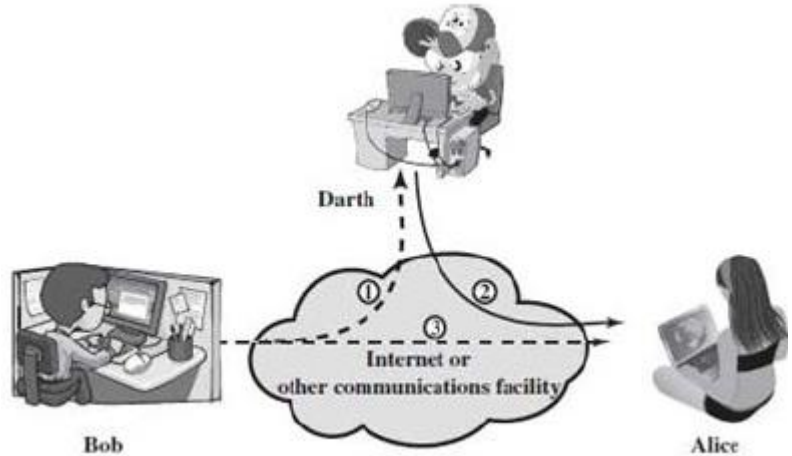
Threat Events: Intentional Attacks

- Passive Attack – attempts to learn or make use of info. from the system but does not affect system resources
  - compromises Confidentiality
  - Examples:
    - Release of message content (traffic interception)
    - Traffic analysis (monitoring of transmission)



(a) Passive attacks

- Active Attack – attempts to alter system resources or affect their operation
  - compromises Integrity or Availability
  - Examples:
    - Data modification
    - DoS
    - Masquerading (impersonation)
    - Replay : Capture of a data unit and its subsequent retransmission



(b) Active attacks

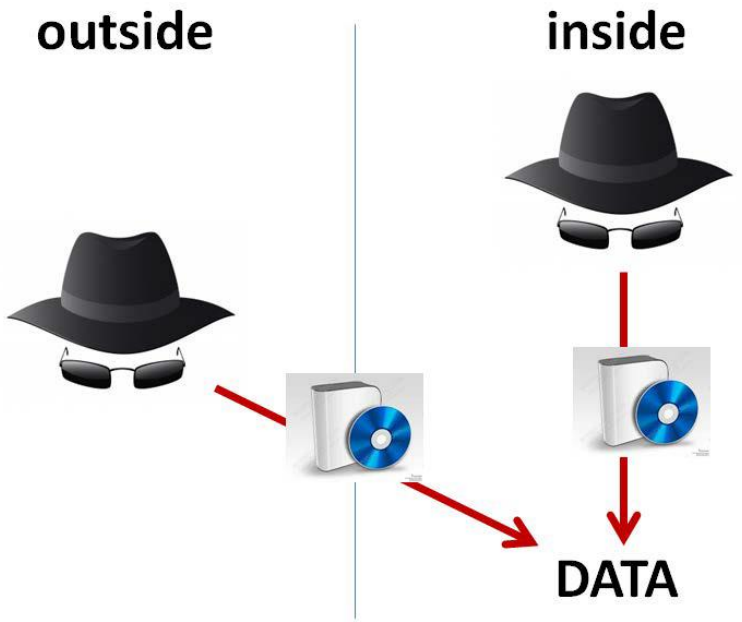
Passive Attack: Traffic analysis

- Though the contents of the transmission can be protected (using encryption), one can learn about the location and identity of the communicating hosts as well as the frequency and length of the messages being exchanged.
- All incoming and outgoing traffic of the network is analyzed, but not altered.

- Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.
- The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged.
- This information might be useful in guessing the nature of the communication that was taking place.

Threat Events: Software Attacks

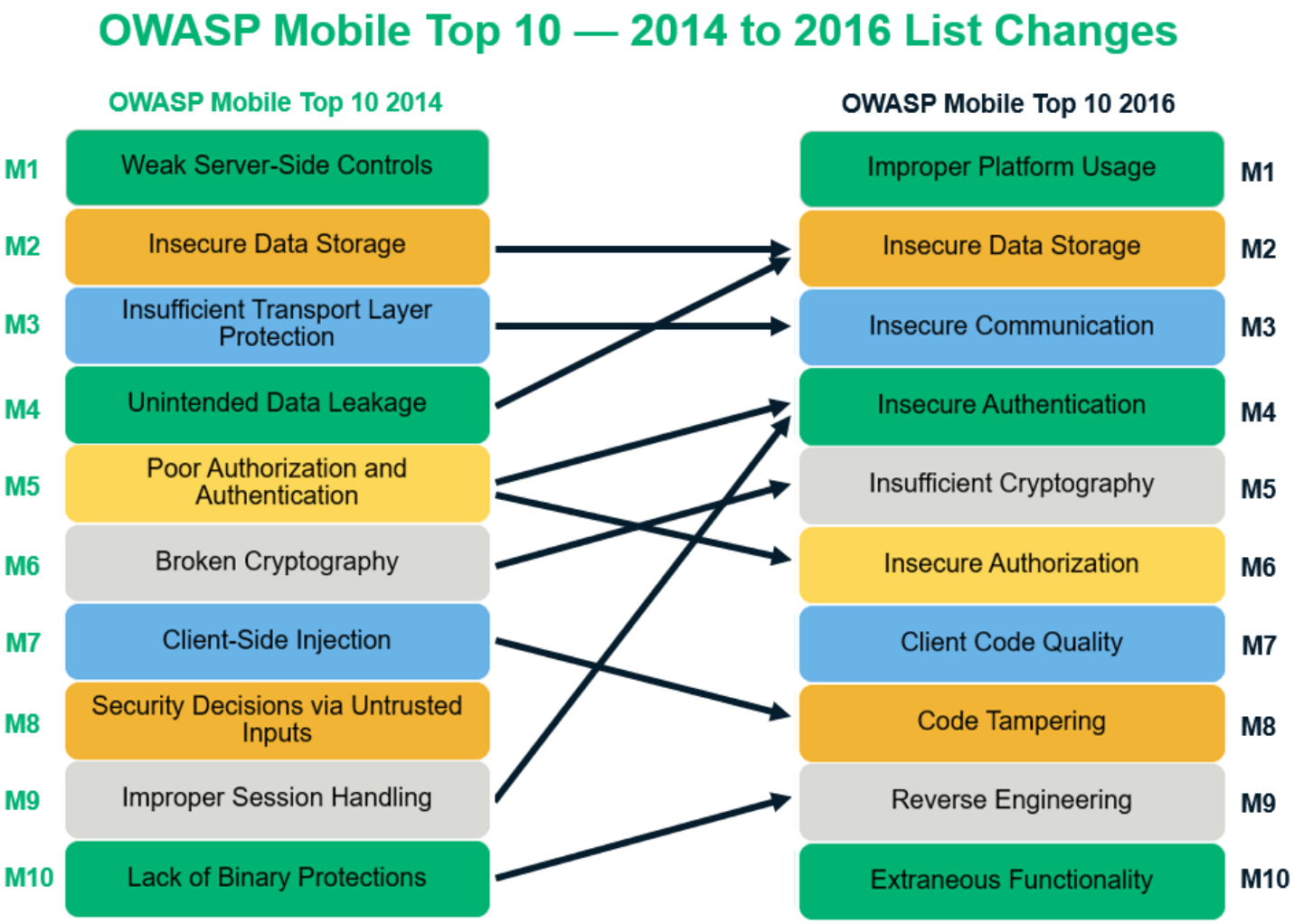
- Deliberate Software Attacks
  - a deliberate action aimed to violate / compromise a system's security **through the use of specialized software**
  - Types of attacks:
    - a) Use of Malware
    - b) Password Cracking
    - c) DoS and DDoS
    - d) Spoofing
    - e) Sniffing
    - f) Man-in-the-Middle
    - g) Phishing
    - h) Pharming



OWASP Top 10 Mobile Risks

This helped us to analyze and re-categorize the OWASP Mobile Top Ten for 2016.

The top ten categories 2016 are more focused on Mobile application rather than Server.



OWASP IoT Top 10 List of Vulnerabilities

- IoT Top 10 2018 Mapping Project

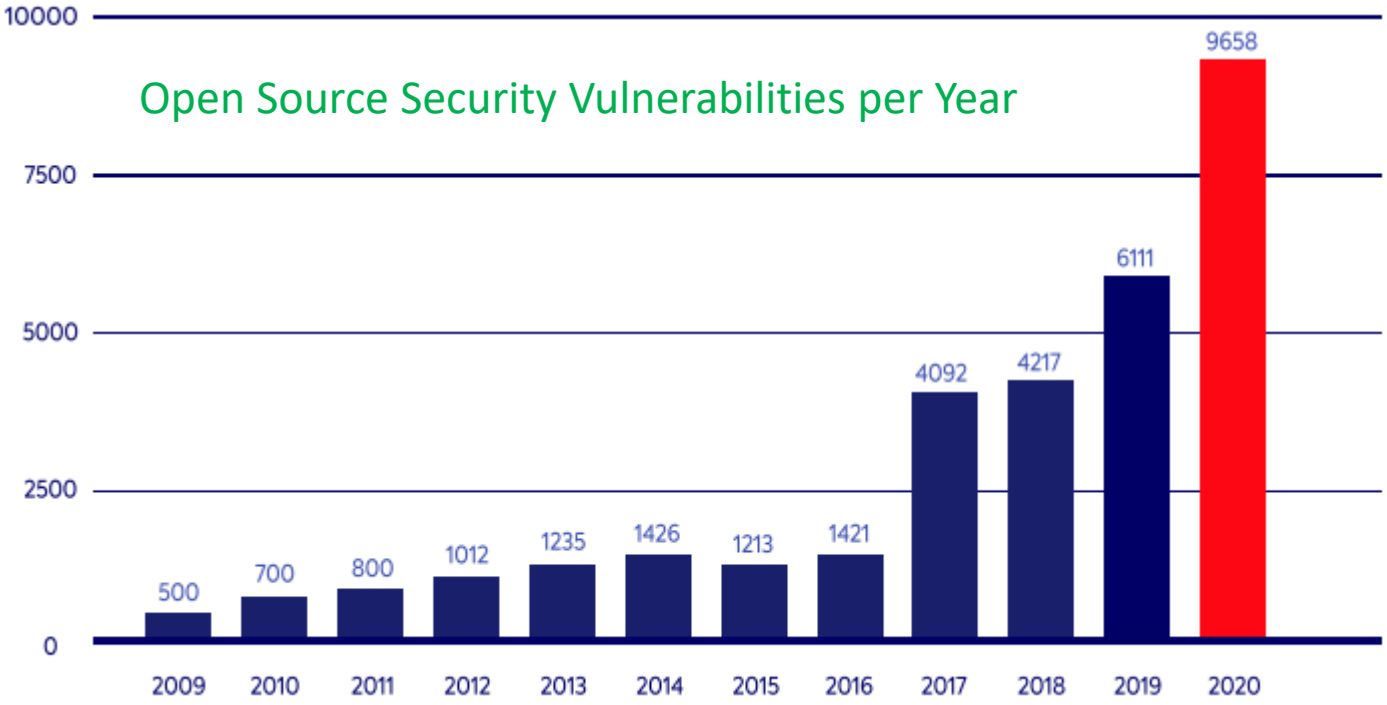
OWASP IoT Top 10 2014	OWASP IoT Top 10 2018 Mapping
I1 Insecure Web Interface	I3 Insecure Ecosystem Interfaces
I2 Insufficient Authentication/Authorization	I1 Weak, Guessable, or Hardcoded Passwords I3 Insecure Ecosystem Interfaces I9 Insecure Default Settings
I3 Insecure Network Services	I2 Insecure Network Services
I4 Lack of Transport Encryption/Integrity Verification	I7 Insecure Data Transfer and Storage
I5 Privacy Concerns	I6 Insufficient Privacy Protection
I6 Insecure Cloud Interface	I3 Insecure Ecosystem Interfaces
I7 Insecure Mobile Interface	I3 Insecure Ecosystem Interfaces
I8 Insufficient Security Configurability	I9 Insecure Default Settings
I9 Insecure Software/Firmware	I4 Lack of Secure Update Mechanism I5 Use of Insecure or Outdated Components
I10 Poor Physical Security	I10 Lack of Physical Hardening

Software Security Threats

Security Issues of Software

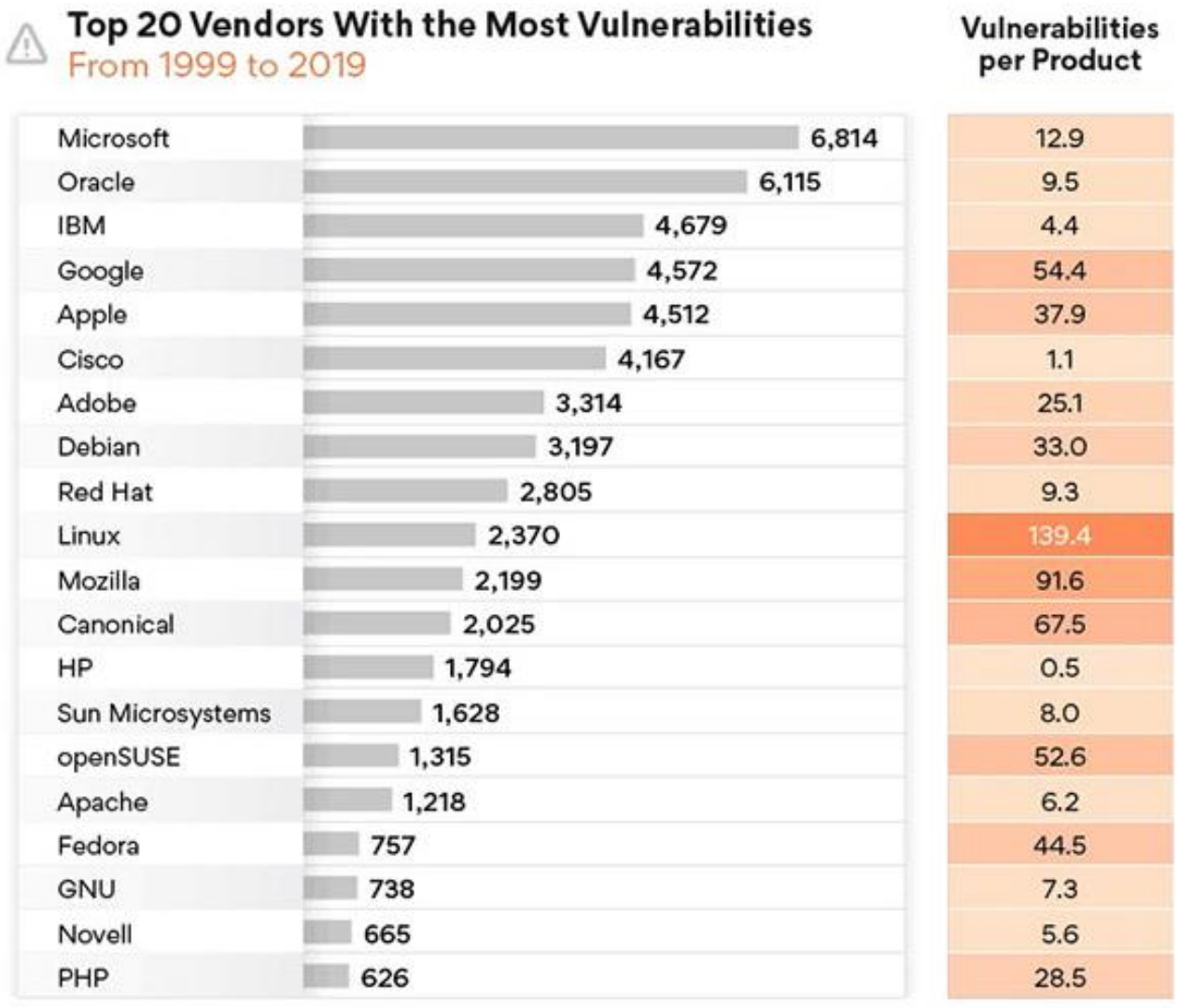
- **Cryptography, protocols, and access control are implemented in software**

- **What are security issues of software?**
  - **Most software is complex and buggy**
  - **Software flaws lead to security vulnerabilities**
  - **How to reduce flaws in software development?**



Source:
"The Number of Known Open Source Security Vulnerabilities Continues to Skyrocket ",
April 14, 2021, WhiteSource

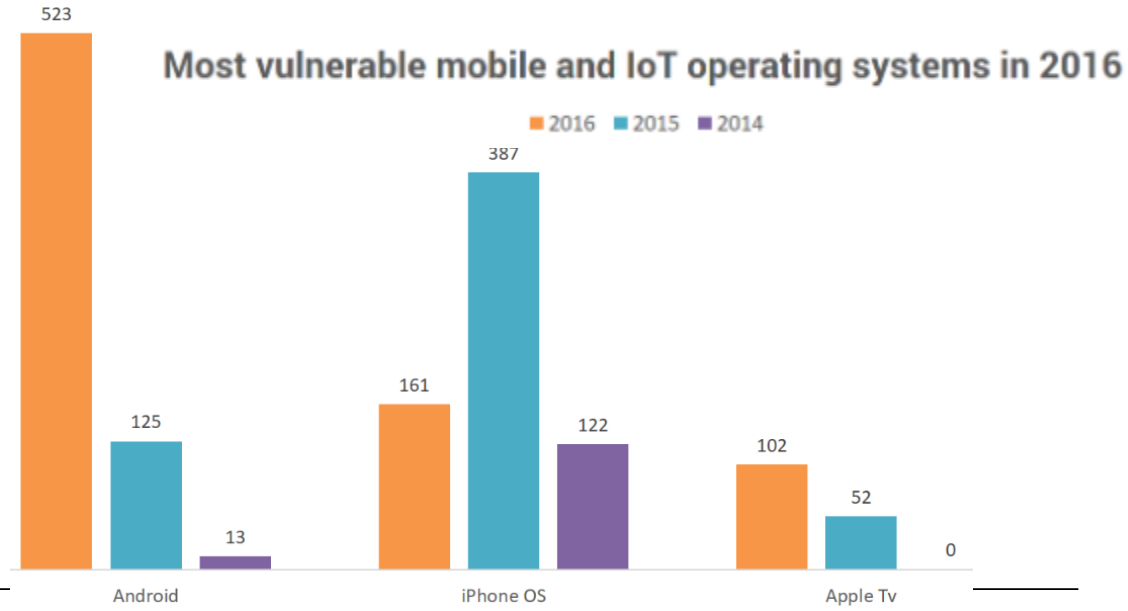
Software vendors contain the most vulnerabilities



Source: “This is the operating system containing the most holes in a decade”, TipsMake.com

Threats related to Software

- **Operating systems enforce security**
  - For example, authentication, authorization, accountability (audit log), …
- **OS: large and complex software**
  - Win XP has 40,000,000 lines of code!
  - OSs are subject to bugs and flaws like any other software
  - Many security issues specific to OSs
  - Can you trust an OS completely?



Source: https://heimdalsecurity.com/blog/most-vulnerable-software-2016/

Top 20 Products with the Most Technical vulnerabilities Over Time

1999–2019	
Debian Linux	3,067
Android	2,563
Linux kernel	2,357
Mac OS X	2,212
Ubuntu	2,007
Mozilla Firefox	1,873
Google Chrome	1,858
iPhone iOS	1,655
Windows Server 2008	1,421
Windows 7	1,283
Adobe Acrobat Reader DC	1,182
Adobe Acrobat DC	1,182
Windows 10	1,111
Adobe Flash Player	1,078
Windows Server 2012	1,050

2019	
Android	414
Debian Linux	360
Windows Server 2016	357
Windows 10	357
Windows Server 2019	351
Adobe Acrobat Reader DC	342
Adobe Acrobat DC	342
cPanel	321
Windows 7	250
Windows Server 2008	248
Windows Server 2012	246
Windows 8.1	242
Windows RT 8.1	235
Ubuntu	190
Fedora	184

SOURCE: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S NATIONAL VULNERABILITY DATABASE

Source: "This is the operating system containing the most holes in a decade", TipsMake.com

Software Cracking (by Wikipedia)

- **Software cracking** is the modification of software to remove or disable features, especially copy protection features (including protection against the manipulation of software, serial number, hardware key, date checks and disc check) or software annoyances like nag screens and adware.

- A **crack** refers to the means of achieving, for example a stolen serial number or a tool that performs that act of cracking.
  - Some of these tools are called keygen, patch, or loader.
  - A keygen is a handmade product serial number generator that often offers the ability to generate working serial numbers in your own name.
  - A patch is a small computer program that modifies the machine code of another program.
    - This has the advantage for a cracker to not include a large executable in a release when only a few bytes are changed.
  - A loader modifies the startup flow of a program and does not remove the protection but circumvents it.
    - A well-known example of a loader is a trainer used to cheat in games.

모바일 앱 보안

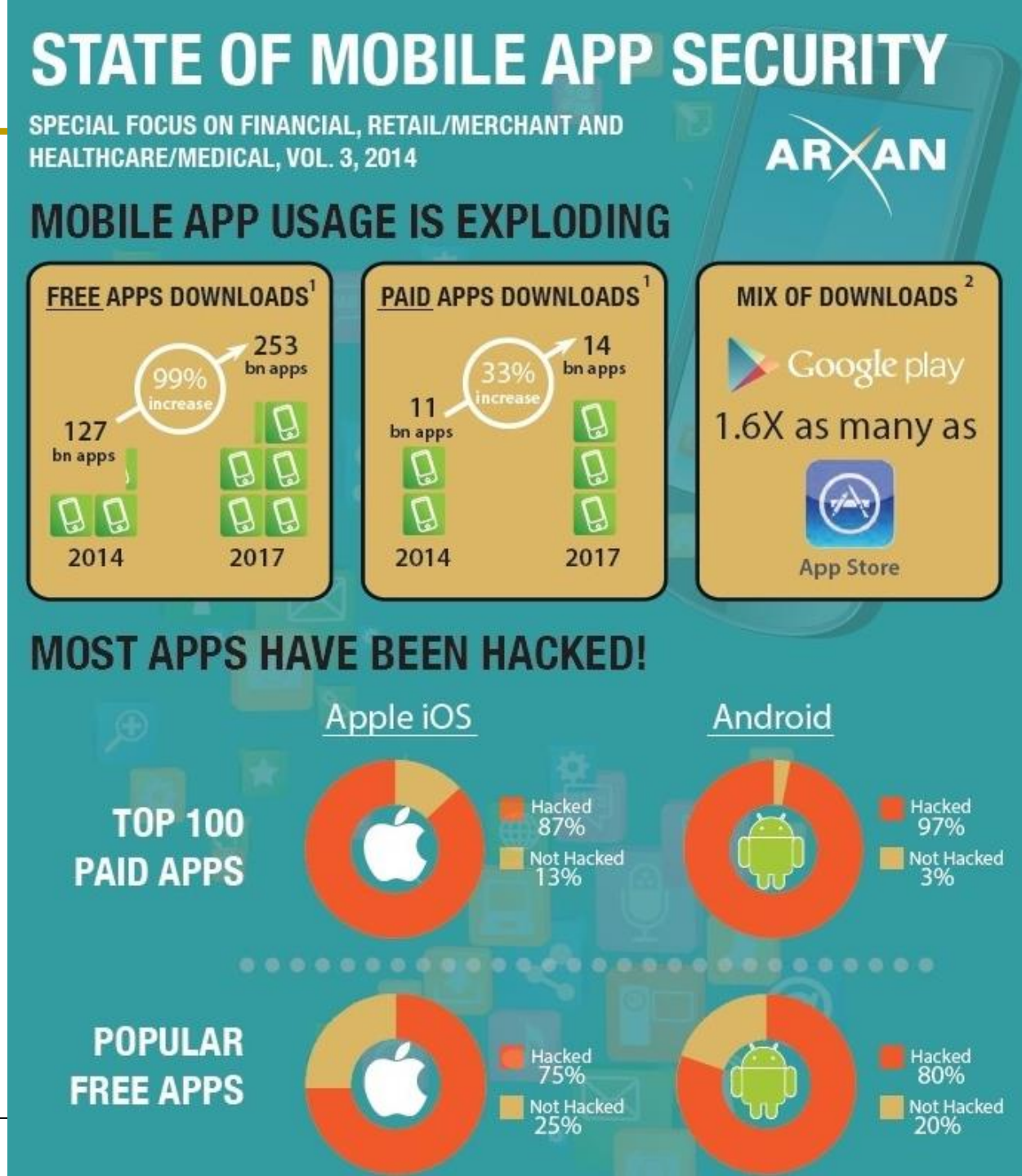
출처: Arxan Technology
2015년 2월 보고서

앱 해킹은 다음 3단계로 구성

1. **공격 대상과 exploit을 정의**
2. **코드를 역공학**
3. **코드를 변조**

- **결과**
  - 소스코드/IP 도용
  - 광고 제거/교체
  - 악성코드 삽입
  - Free pirated copies

- 이러한 과정은 무료 및 저가의 해킹도구로 쉽게 수행 가능



M7~M9 of OWASP Mobile Top 10

- **M7: Poor Code Quality**
  - Threat Agents include entities that can pass untrusted inputs to method calls made within mobile code. These types of issues are not necessarily security issues in and of themselves but lead to security vulnerabilities. For example, buffer overflows within older versions of Safari (a poor code quality vulnerability) led to high risk drive-by Jailbreak attacks. Poor code-quality issues are typically exploited via malware or phishing scams.

- **M8: Code Tampering**
  - Typically, an attacker will exploit code modification via malicious forms of the apps hosted in third-party app stores. The attacker may also trick the user into installing the app via phishing attacks.

- **M9: Reverse Engineering**
  - An attacker will typically download the targeted app from an app store and analyze it within their own local environment using a suite of different tools.

Threats related to Software

- **Some software is intentionally evil**
  - **Malware (Malicious Software)**
    - **computer viruses, worms, ransomware, spyware, bot, etc.**
- **How does the malware work?**
- **What can Alice and Bob do to protect themselves from malware?**
- **What can Trudy do to make malware more "effective"?**

Summary

- **Types of Security Threats,**
  Microsoft STRIDE model
  - Interruption (DoS)
  - Interception (Information disclosure)
  - Modification = Tampering
  - Fabrication (Spoofing)
  - Repudiation
  - Elevation of privilege
- Three main components of a security threat
  - Target (Asset), Agent, Event
- OWASP Top 10 Mobile Risks
- OWASP Top 10 IoT Vulnerabilities
- Software Security Threats

Appendix

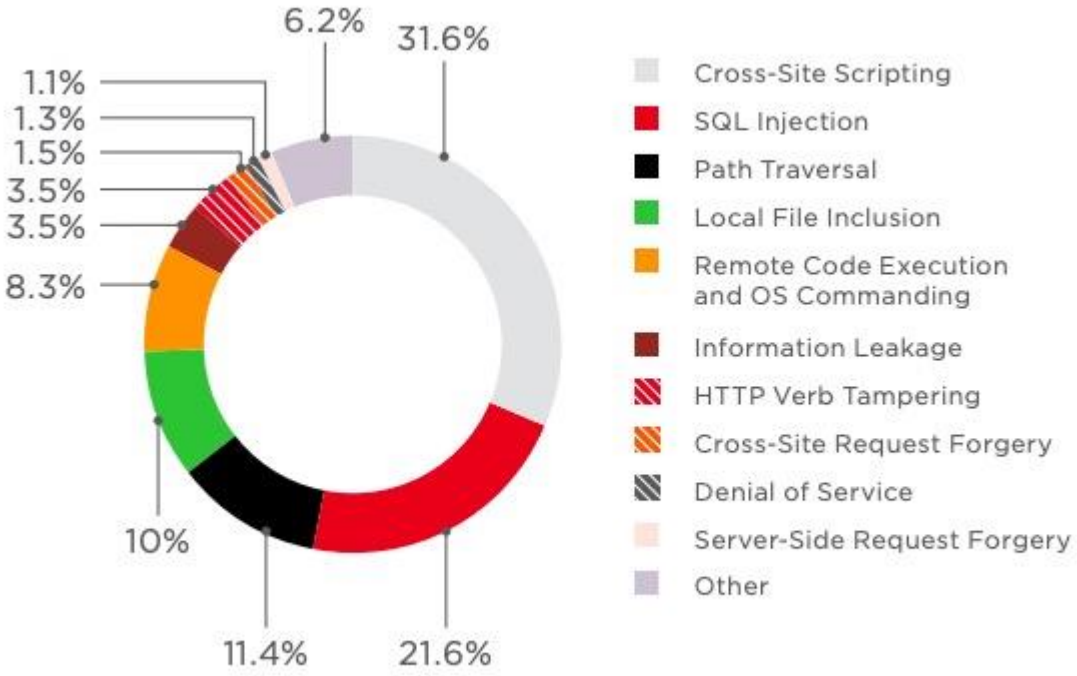
OWASP Cloud Top 10 Risks

- R1. Accountability & Data Risk
- R2. User Identity Federation
- R3. Legal & Regulatory Compliance
- R4. Business Continuity & Resiliency
- R5. User Privacy & Secondary Usage of Data
- R6. Service & Data Integration
- R7. Multi-tenancy & Physical Security
- R8. Incidence Analysis & Forensics
- R9. Infrastructure Security
- R10. Non-production Environment Exposure

- https://owasp.org/www-pdf-archive/OWASP_Cloud_Top_10.pdf

Software is NOT secure

- Web application attack statistics: 2017 in review



Source: https://www.ptsecurity.com/ww-en/analytics/web-application-attack-statistics-2017/

Real-life examples of Cyber Attacks

집 안 사생활 몰래 훔쳐봤다…IP 카메라 악용 막으려면?

어린 자녀나 반려동물을 키우면서 '집에 CCTV'를 설치하는 경우가 많습니다. **IP카메라**라고도 부르는 이 CCTV로 집안 곳곳을 언제든 들여다볼 수 있는데, 범죄에 노출될 수 있는 만큼 주의가 필요.
A씨는 사무실에 인터넷과 연결만 하면 실시간으로 영상을 볼 수 있는 IP 카메라를 설치했는데, 한 달쯤 뒤 접속 기록을 살펴보다가 낯선 IP 주소를 확인.곧바로 경찰에 신고했고 수사 결과 IP 카메라를 설치했던 기사가 휴대전화 앱으로 A 씨 모습을 훔쳐본 사실이 드러났습니다. IP 카메라는 촬영 기기가 휴대전화 앱과 연동돼 아이디와 비밀번호를 입력하면 CCTV 화면을 실시간으로 볼 수 있는데 처음 설정된 비밀번호를 바꾸지 않는 사람이 많다는 점을 악용해 범죄를 저지른 겁니다.
-- SBS뉴스 (2020.10.15)

보안 장치 없이 IP 노출시키고 있는 카메라 6천 대, 러시아에서 발견돼

> 보안을 위해 설치한 감시 카메라가 오히려 보안의 위협이 될 수 있다는 연구 결과가 나왔다. 러시아 내에서만 비밀번호도 없이 인터넷에 그대로 연결된 카메라 6천 대가 나온 것이다. 하지만 인터넷에 연결된 카메라 자체의 수는 한국이 더 많다고 하니, 이 역시 점검해 봐야 할 상황이다.

Avast에 의하면 러시아 내의 CCTV 카메라 6300여 대가 공공 인터넷에 아무런 보호 장치 없이 노출되어 있어 누구나 접속할 수 있다고 한다. IP 주소들만 알면 아무나 접속해 영상 장치를 통해 주변을 감시할 수 있게 된다는 뜻이다.
아무런 보호 장치가 없다는 건, 최소한의 로그인 절차도 없다는 뜻이다. 사용자 이름이나 비밀번호를 몰라도 접속이 가능하거나, 비밀번호가 1234나 user, admin 등 디폴트로 설정되어 있어 없는 것과 마찬가지 상태인 것을 말한다. -- 보안뉴스 (2021.03.15)

Real-life examples of Cyber Attacks

- **Crack이란 보호 기술이 적용된 상용 소프트웨어를 불법으로 사용하기 위해 보호 방식을 제거하는 프로그램이나 행위.**
- **Keygen: 소프트웨어 불법 사용을 목표로 특정 소프트웨어에 대한 CD키나 등록 번호를 만들어 내는 프로그램**

컴퓨터에 크랙·키젠 잘못 깔았다간 나도 모르게 모네로 채굴하는 좀비PC 된다

안랩에 따르면 공격자는 먼저 한글로 작성된 피싱 사이트를 제작해 크랙 프로그램을 검색하는 이들을 유인했다. 이후 크랙과 유사하게 파일을 만들어 다운로드를 유도하고 이용자 몰래 악성코드를 심었다.

해당 악성코드는 이용자들의 PC에 암호화폐 '모네로(Monero)'를 채굴하는 마이너(Miner)를 설치한다. 이 악성코드는 감염 PC의 절전모드, 대기모드 진입 기능을 비활성화 해 지속적으로 PC자원을 소모하며 암호화폐를 채굴한다. PC 활동을 실시간으로 확인할 수 있는 모니터링 프로그램이 실행되면 자동으로 채굴을 멈추기 때문에 사용자가 악성코드 실행 여부를 파악하기 어렵다. -- Block Media, 2020.06.29