Introduction to Software Security

Security Goals

Seong-je Cho

Computer Security & Operating Systems Lab, DKU

References

- Microsoft STRIDE chart
  - https://www.microsoft.com/security/blog/2007/09/11/stride-chart/
- *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
- Goals of Computer Security
  - Confidentiality / Integrity / Availability
  - Extended CIA Framework
    - Authentication / Authorization / Non-repudiation
- Example of CIA
- Think like an Intruder

Alice's Online Bank (AOB)

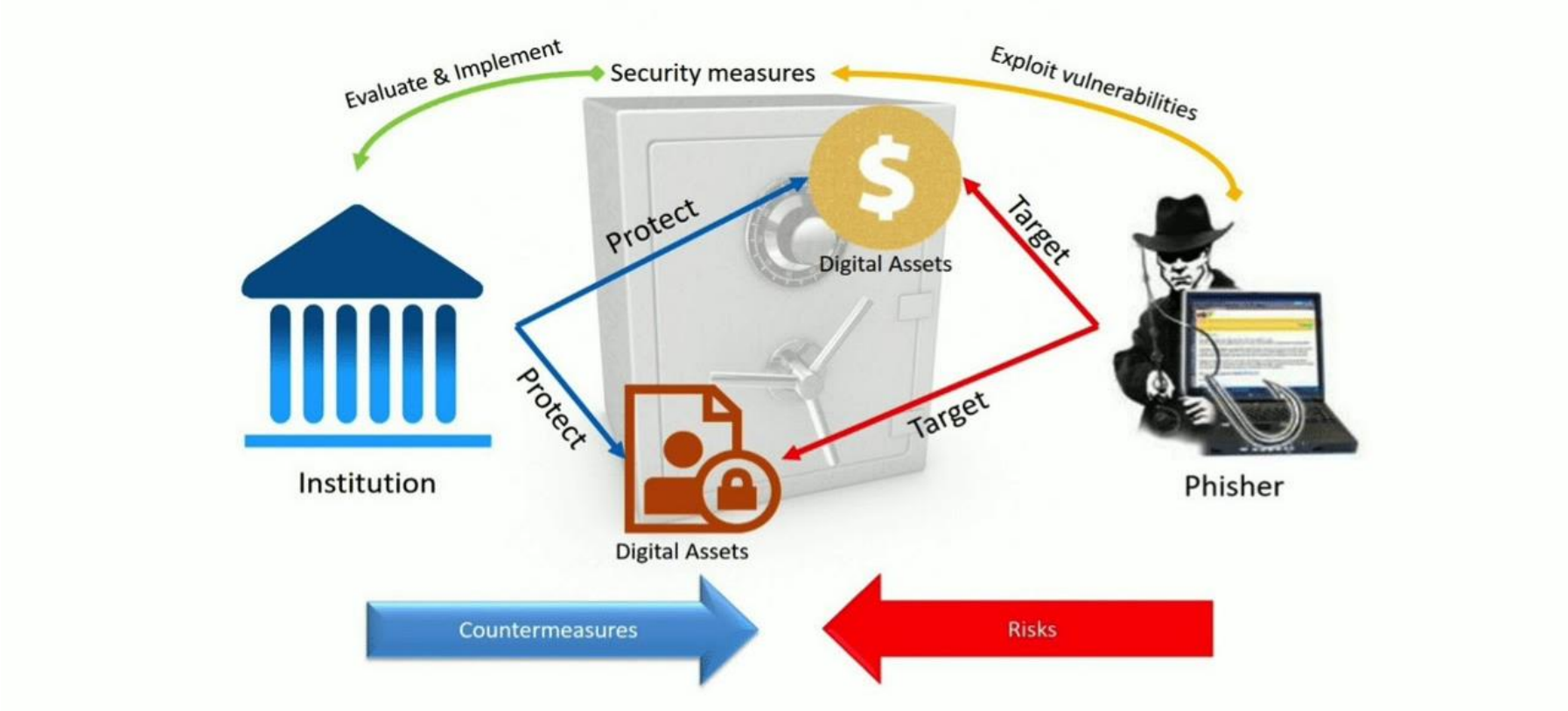
- Alice opens Alice's Online Bank (AOB)
- What are Alice's security concerns?
  - What types of security threats are there?
- If Bob is a customer of AOB, what are his security concerns?
- How are Alice and Bob concerns similar? How are they different?
- How does Trudy view the situation?

What type of attacks can adversaries perform in this situation?

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

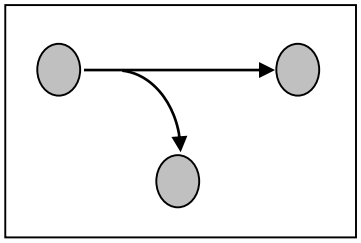
Threats vs. Countermeasures



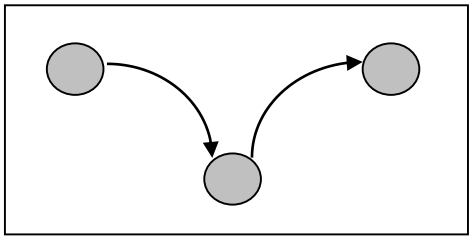
Security Goals

Key Security Goals : C.I.A.

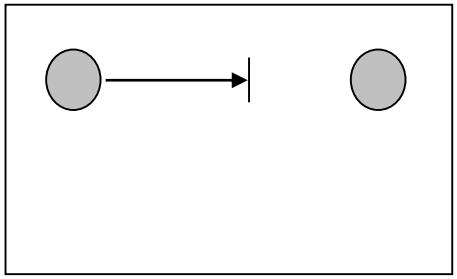
- **Confidentiality**
  - AOB must prevent Trudy from learning Bob's account balance
  - Confidentiality: prevent unauthorized reading of information



- **Integrity**
  - Trudy must not be able to change Bob's account balance
  - Bob must not be able to improperly change his own account balance
  - Integrity: prevent unauthorized writing of information

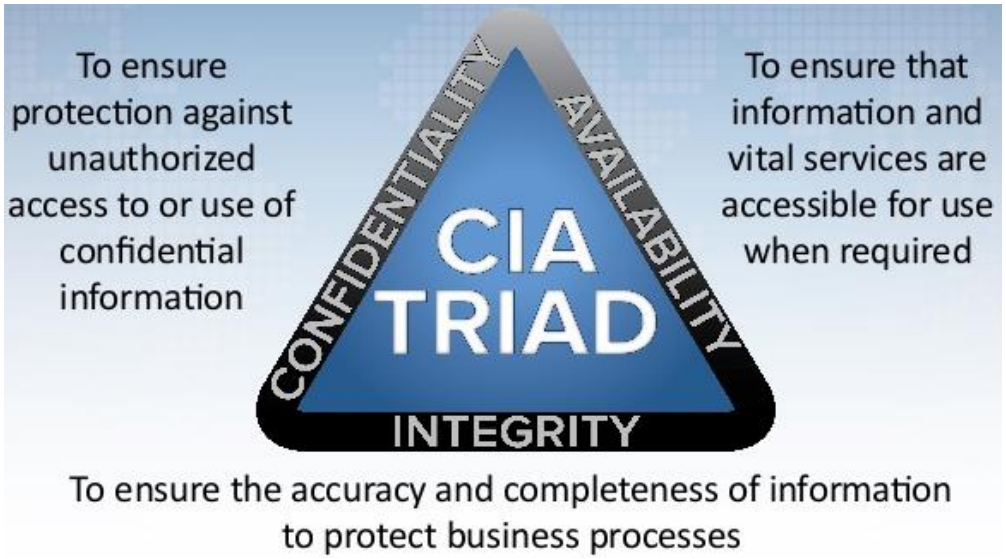


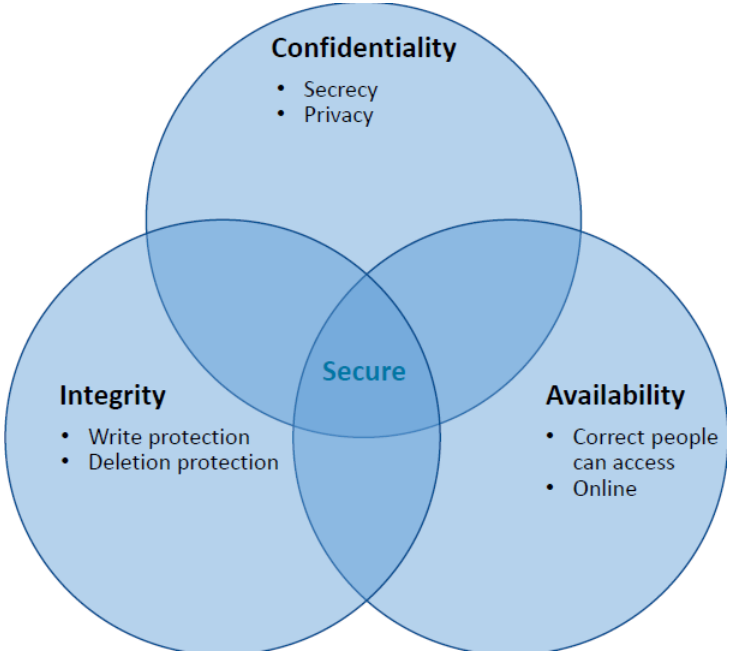
- **Availability**
  - AOB's data and service must be available when needed
  - Alice must be able to make transaction
    - If not, Bob'll take his business elsewhere
  - Availability: Data is available in a timely manner when needed
  - Availability is a "new" security concern
    - In response to denial of service (DoS)



Key Security Goals

- **C.I.A. Triangle** – 3 key characteristics of information that must be protected by computer security:
  - **Confidentiality** (**Secrecy**) - only authorized parties can read(see) private information
  - **Integrity** - information is changed only in a specified and authorized manner (by authorized users)
  - **Availability** – data and service is accessible to authorized users whenever needed





An information systems is secure if it supports C.I.A.

Beyond CIA

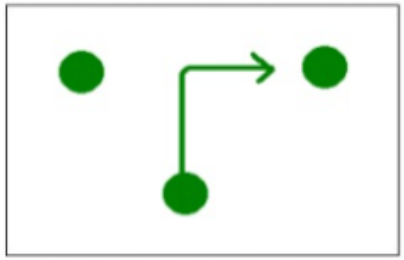
- **CIA are only beginning of the Info Sec.**
- **Case 1: when Bob logs on his computer/smartphone,**
  - **How does Bob's computer know that "Bob" is really Bob and not Trudy?**
  - **Bob's password must be verified**
    - **This requires some clever** authentication

    ☞Authentication: **"Who are you?"**

    » Authentication can prevent **fabrication** (spoofing) attacks

    ✓ **Entity authentication** – validating user/machine identity

    ✓ **Message authentication** – validating whether a message came from the user/machine/source who claims to have sent it



Fabrication

  - **What are security concerns of passwords?**
  - **Are there alternatives to passwords?**
    - **Accredited Certificate** (공인인증서)
    - **Biometrics: …**
    - **…**

Beyond CIA

- **CIA may not be enough.**

- **Case2: when Bob logs into AOB via network**
  - **how does AOB know that "Bob" is really Bob?**
  - **As before, Bob's password is verified → Authentication**

  - **Unlike standalone computer case, network security issues arise**
    - ☞ **Wiretapping, Packet sniffing**

  - **What are network security concerns?**
    - **Protocols are critically important**
    - **Crypto also important in protocols**

Beyond CIA

- **Once Bob is *authenticated* by AOB, then AOB must restrict actions of Bob**
  - **Bob can't view Charlie's account info**
  - **Bob can't install new software, etc.**

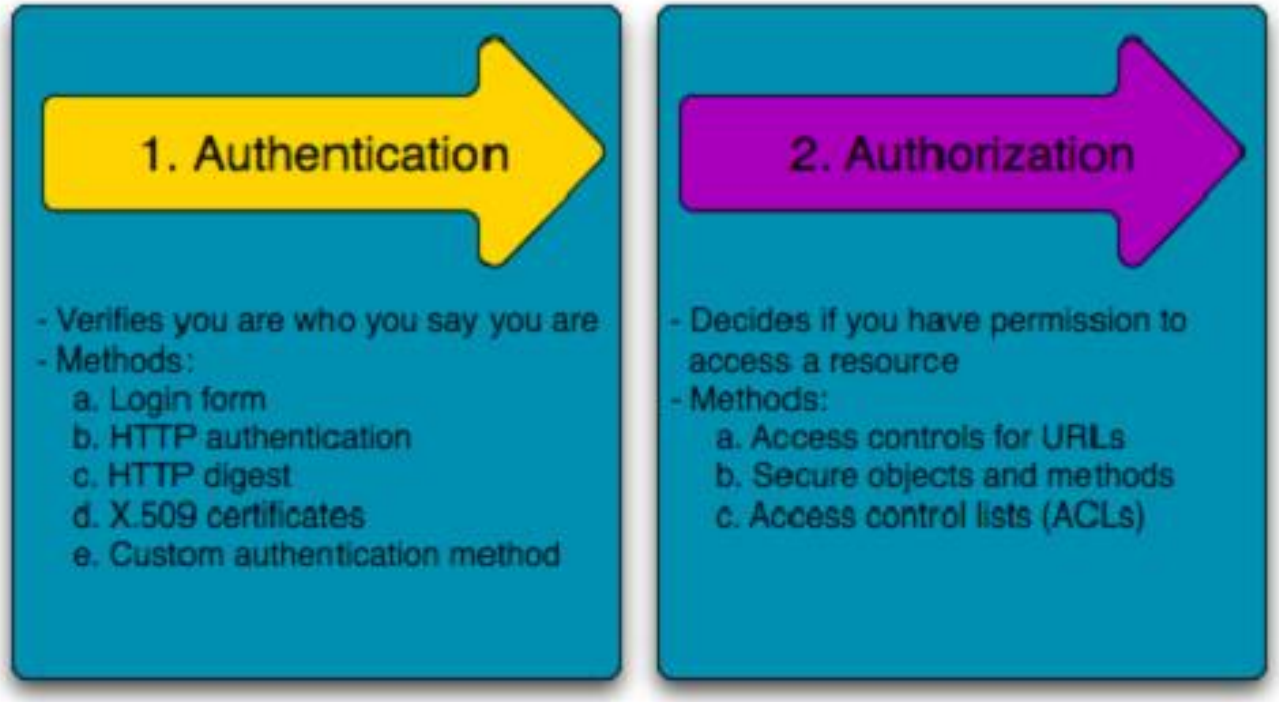
- **Enforcing these restrictions is known as authorization**
  - **Authorization** (권한 부여, 인가):
    "What permissions do you have?"

☞ **Access control includes both authentication and authorization**
  - Access control validates the permissions a user claims to have on a resource

AUTHENTICATION	AUTHORIZATION
Process of confirming the truth of an attribute of a single piece of data claimed true by an entity	Process of specifying access rights/ privileges to resources related to information security
Checks a person's details to identify him	Checks a user's privileges to access resources
Verifies user's credentials	Validates user's permissions
Occurs before authorization	Occurs after authentication
Ex: A student can authenticate himself before accessing the Learning Management System of a University	Ex: He can access lecture slides and other learning material of the courses based on the permissions given to him

Source: https://pediaa.com/difference-between-authentication-and-authorization/

Authentication vs. Authorization



Source: https://medium.datadriveninvestor.com/authentication-vs-authorization-716fea914d55

- **Multi-user systems:**
  - Admin (Root, Super-user), Normal user, Guest
  - Owner, Guest
  - Different Access rights (Permissions)
    - Create, Read/View, Write, Delete, Execute, …
    - ✓ Naver (카페), Band, Kakao (일반채팅, 비밀채팅, 오픈채팅), Gmail, …

Extended C.I.A. Triangle

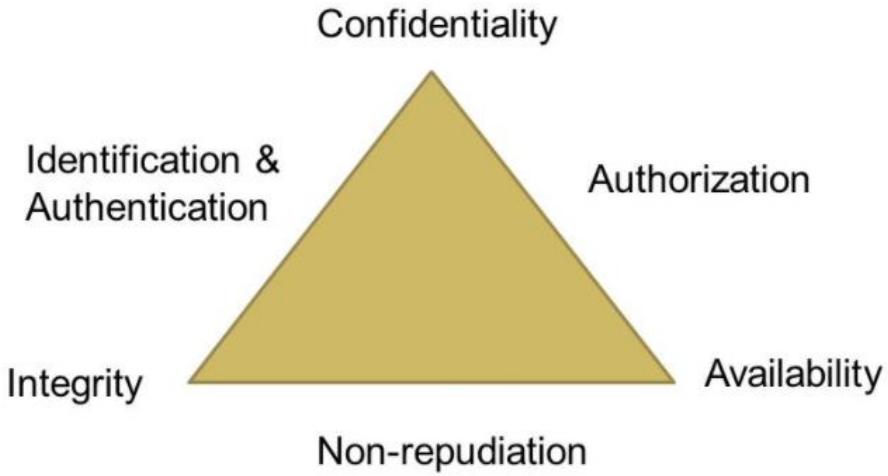
- security experts feel that additional concept need to be added to the CIA triad:
  - **Authentication** (Authenticity) – "Who are you"
    - Validate a system is accessing by the right person
    - verify that each user and data origin are authentic and accurate
  - **Authorization** (권한부여, 인가) - "What you can do"
    - Are you allowed to do that?
      - » Check users' permissions to access data.
    - security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features.

Extended C.I.A. Triangle

- security experts feel that additional concept need to be added to the CIA triad:
  - **Non-repudiation** ("You did that")
    - Actions of an entity should be uniquely traced back to that entity.
    - It is the prevention of either the sender or the receiver denying a transmitted message.
  - **Accountability** - being able to trace actions of an entity (uniquely to that entity)
    - **Accountability** means that the system is able to provide audit trails of all transactions.
    - Actions are traceable to those responsible

audit trail: 감사 이력/추적/기록

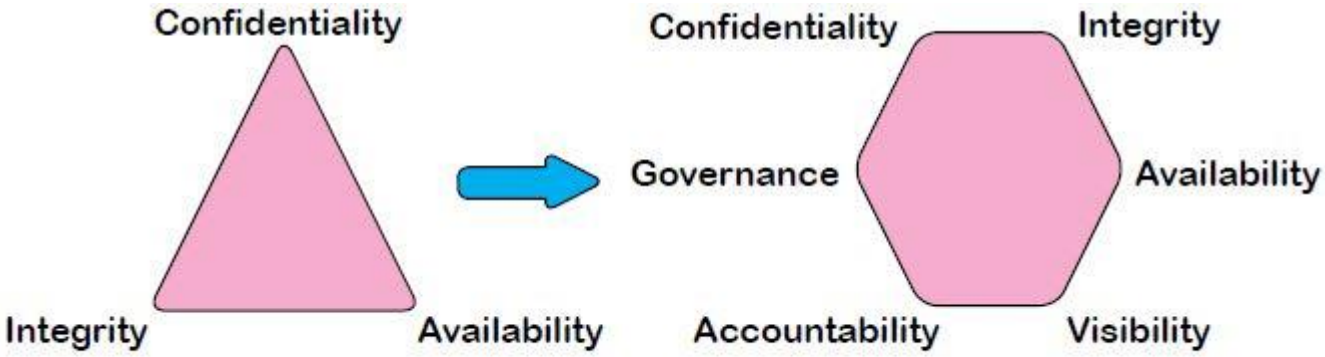
Extended CIA Framework



- **The Pillars of Information Security**

Source: http://computersecurty.blogspot.com/2013/09/the-pillars-of-information-security.html

- **Futuristic Approach to Ensuring Data Security in Clouds**



Source: http://www.bluekaizen.org/futuristic-approach-to-ensuring-data-security-in-clouds/

STRIDE vs. AINCAA

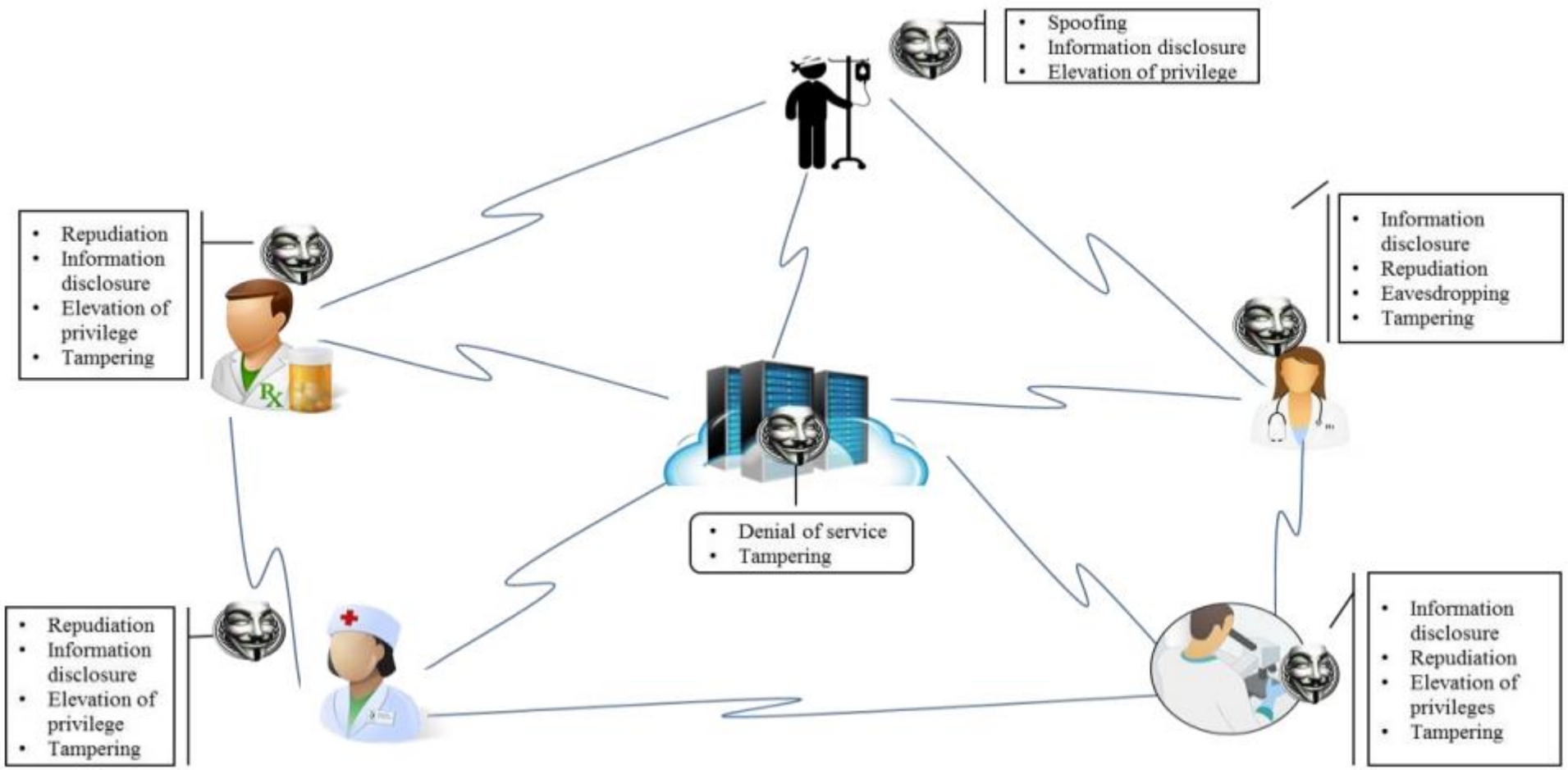
	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

- [Source] Threat Modeling: 12 Available Methods, DECEMBER 3, 2018, Nataliya Shevchenko
  https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html

Standard Mitigations against STRIDE

Threat	Mitigations	Approaches (Techniques)
Spoofing	Authentication	To authenticate principals: • Cookie authentication • Kerberos authentication • PKI systems such as SSL/TLS and certificates To authenticate code or data: • Digital signatures
Tampering	Integrity	• Windows Vista Mandatory Integrity Controls • ACLs • Digital signatures
Repudiation	Non Repudiation	• Secure logging and auditing • Digital signatures
Information disclosure	Confidentiality	• Encryption • ACLs
Denial of Service	Availability	• ACLs • Filtering • Quotas
Elevation of Privilege	Authorization	• ACLs • Group or role membership • Privilege ownership • Input validation

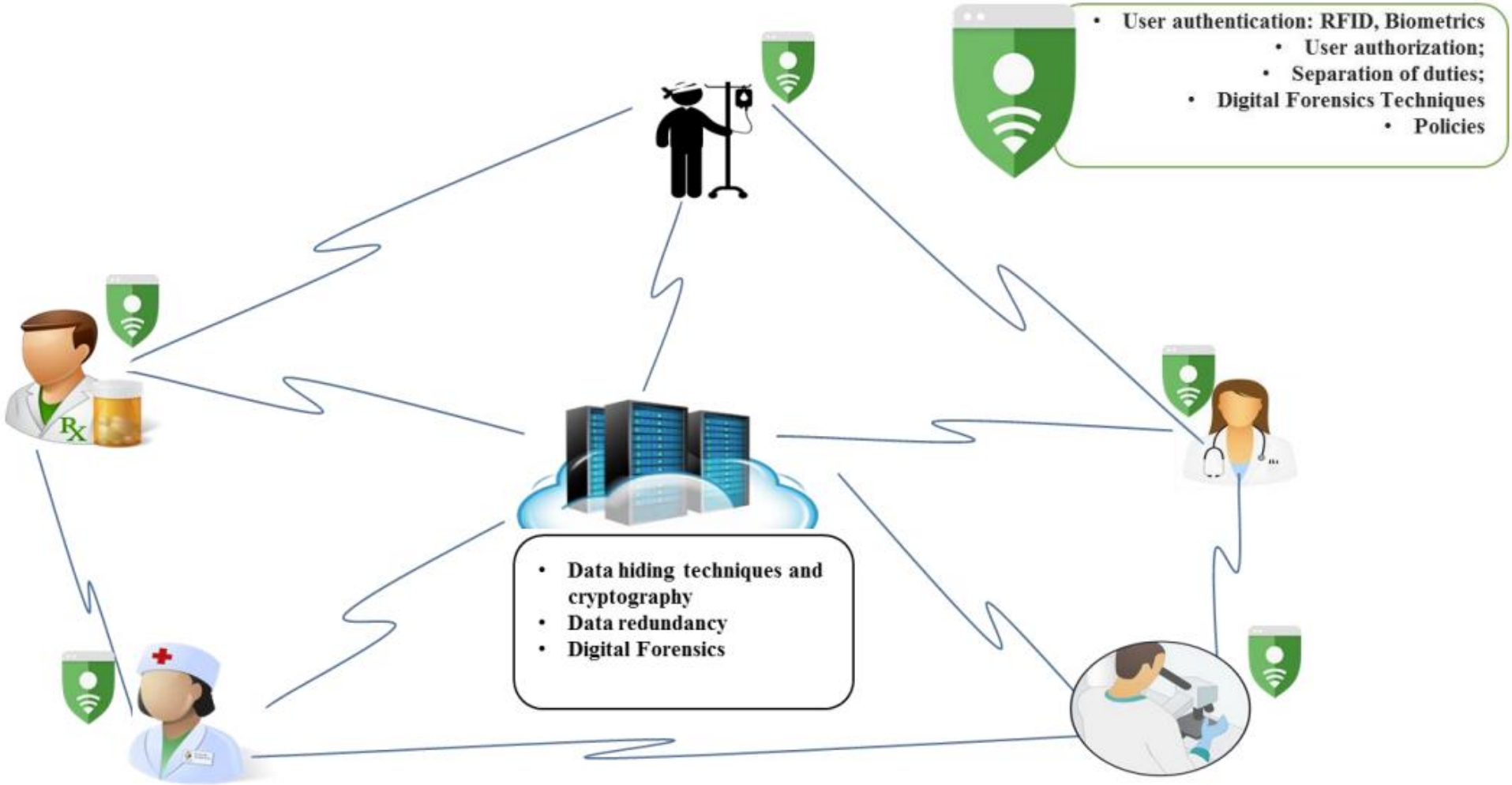
Threat model for an EHS



EHS = Electronic health Systems

Source: Alhassan, John K., et al. "Threat modeling of electronic health systems and mitigating countermeasures." (2016).

Countermeasures to identified threats

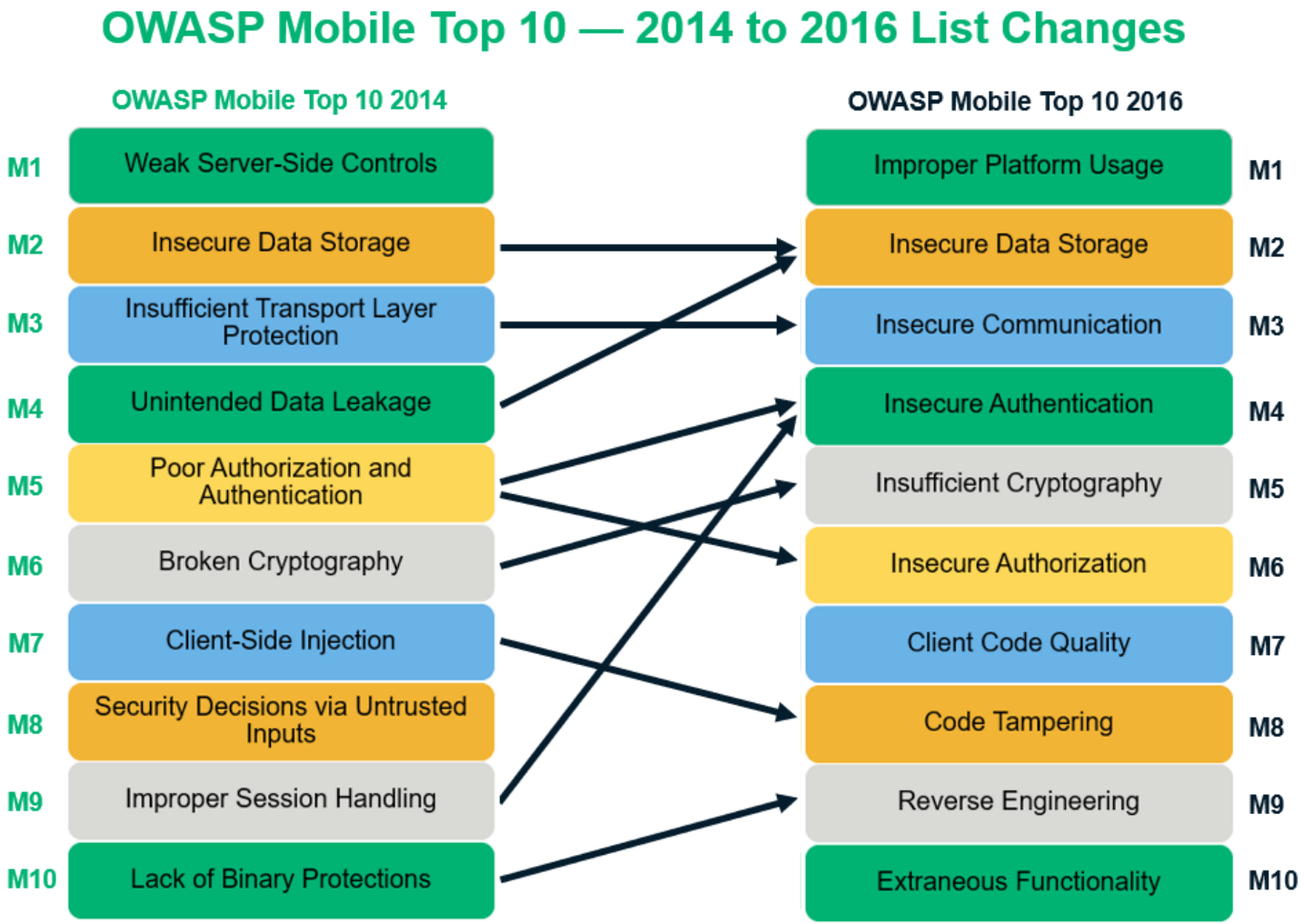


- Authentication. Integrity, Non-repudiation, Confidentiality, Availability, Authorization

Source: Alhassan, John K., et al. "Threat modeling of electronic health systems and mitigating countermeasures." (2016).

Defenses? against OWASP Top 10 Mobile Risks

Which countermeasures are there for protecting mobile systems against security risks?



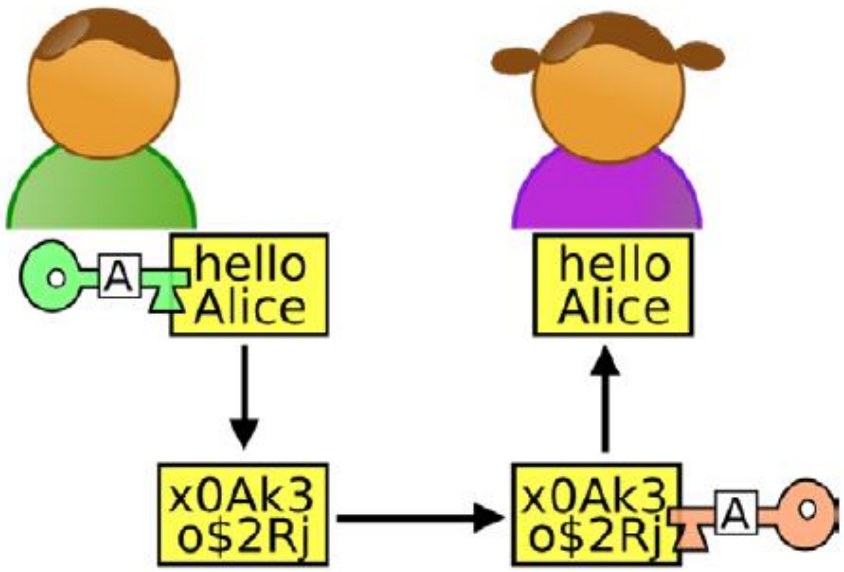
Examples of C.I.A.

Example: DATA CONFIDENTIALITY

- **Student grade** – an information asset of high importance for student.
  - In US, release of such information is regulated by **Family Educational Rights and Privacy Act**(FERPA).
  - Grade information should only be available to students, their parents and employees that require this information to do their job.
  - In Canada, the same issue is regulated by **Personal Information Protection and Electronic Documents Act** (PIPEDA).

Example: How to ensure data confidentiality?

- cryptography
  - AES
  - RSA



- strong access control
  - Never access, No read, No view

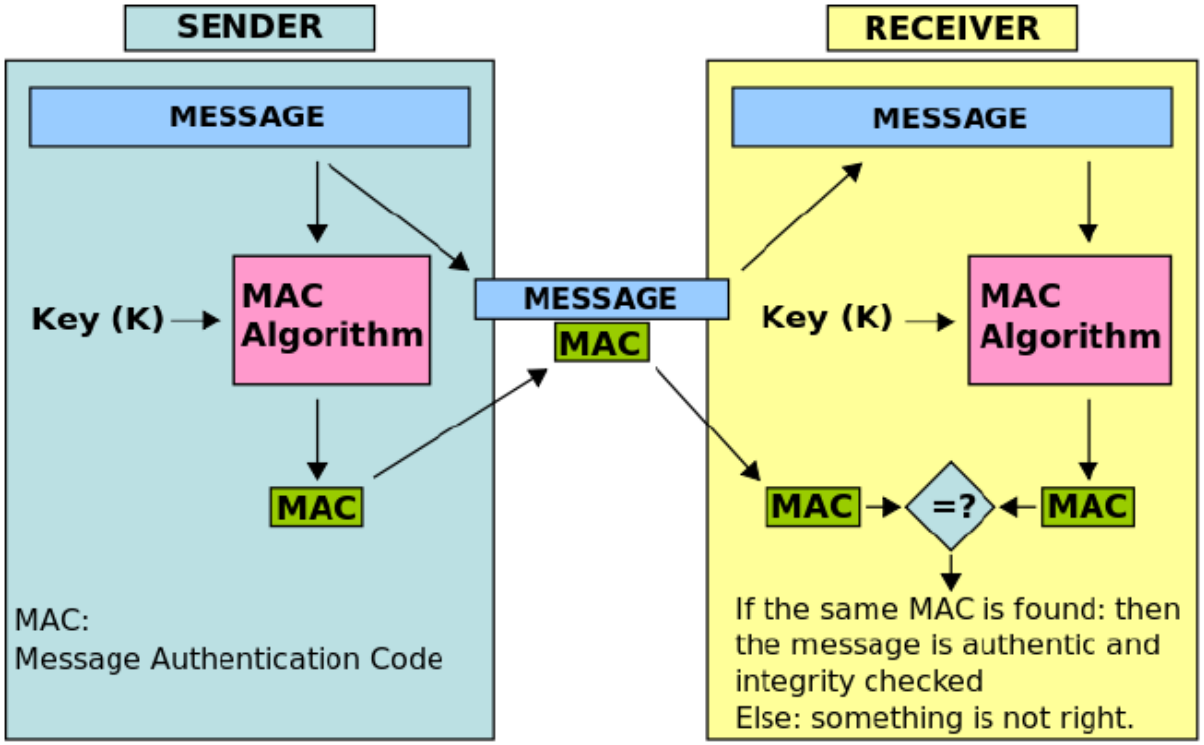
- limiting number of places where data can appear
  (e.g., cannot be stored on an USB, 공개 웹 사이트에 게시 금지)

Example: DATA Integrity

- **Patient information in a hospital** – the doctor should be able to trust that the information is correct and current.
- Inaccurate info could result in serious harm to the patient and expose the hospital to massive liability.
  - In US, **Health Insurance Portability and Accountability Act** (HIPAA) regulates the collection, storage, and transmission of sensitive personal health care information.
  - Hospital is responsible for safeguarding patient information against error, loss, defacing, tampering and unauthorized use.
    (Ontario's Personal Health Information Protection Act -PHIPA)

Example: How to ensure data integrity?

- **strong access control** - prevents attacks on data integrity
  - No write, No append
- **Cryptographic hashing**
  - Detects attacks on data integrity
  - MAC, SHA-256

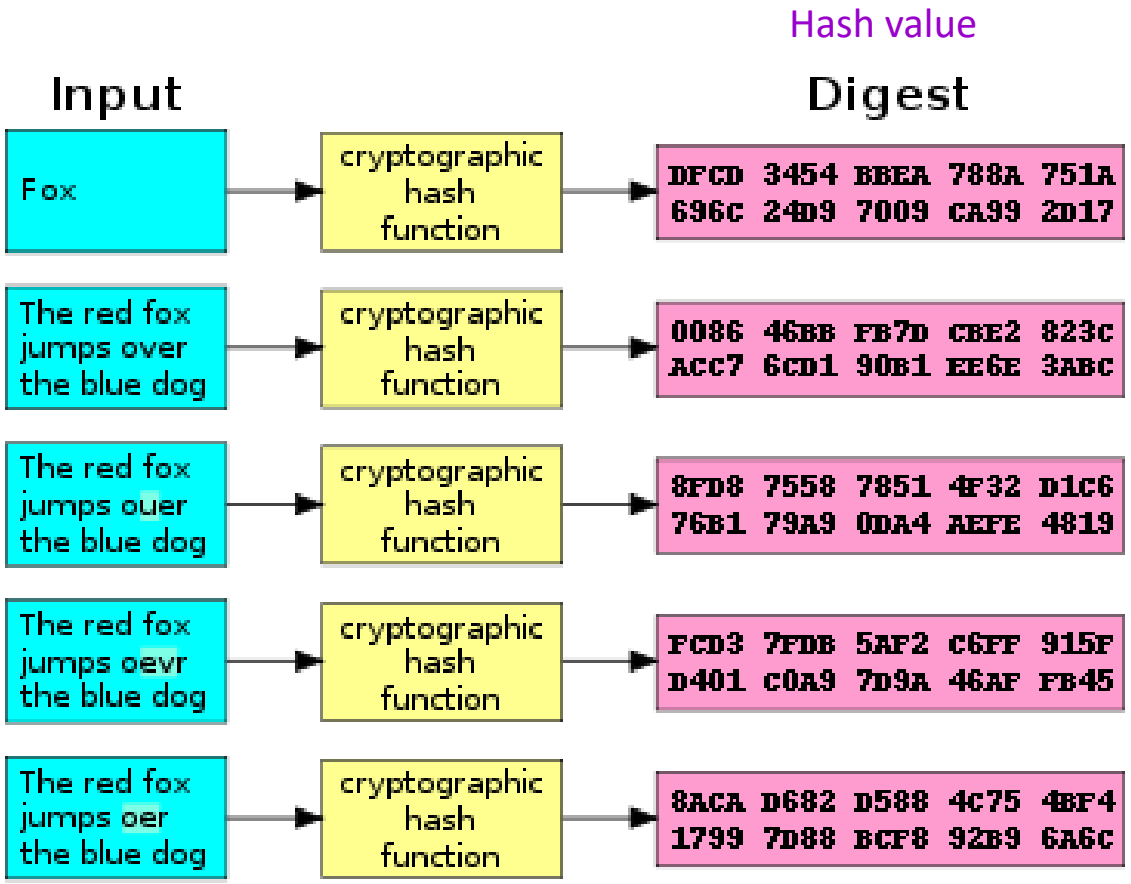


- **documenting system activity** - who did what and when
  - detects attacks on data integrity

Example: How to ensure data integrity?

- **Cryptographic Hash Function**
  - **MD5, SHA-256, SHA-512, …**

  - One-way function
  - Avalanche effect



Source: Wikipedia

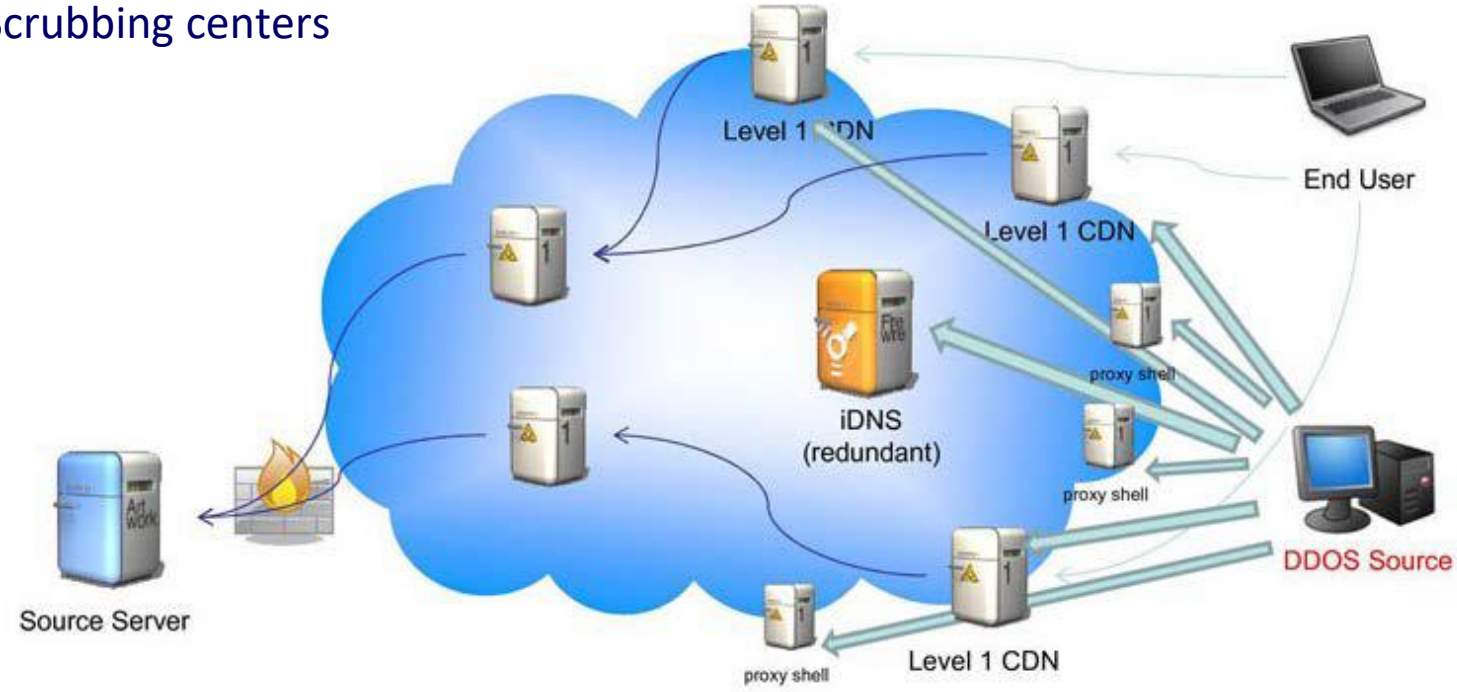
Example: DATA Availability

- **Accessible and properly functioning web site** – a key asset for an e-commerce company.
  - E.g., a DDoS attack could make the site unavailable and cause significant loss in revenue and reputation.

  - In US, **Computer Fraud and Abuse Act** (CFAA) applies to DoS-related attacks.
  - In Canada, DoS activities are regulated under **Criminal Code of Canada, Section 342: Unauthorized Use of Computer**

Example: How to ensure data availability?

- **anti-DDoS system** (in case of attack that attempt to prevent access by blocking the bandwidth/server):
  - e.g., Content Delivery Networks (CDNs),
    Scrubbing centers



- **well established backup procedure** (in case of attacks that attempt to prevent access by destroying data)

Example: CIA of different IT components

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Computer and Network Assets, with Examples of Threats.

Think like an Intruder

Think Like Trudy

- In the past, no respectable sources talked about “hacking” in detail
- It was argued that such info would help hackers

- Recently, this has changed
  - Books on network hacking, how to write evil software, how to hack software, etc.

- Good guys must think like bad guys!
- A police detective
  - Must study and understand criminals
- In Computer security
  - We want to understand Trudy’s motives
  - We must know Trudy’s methods
  - We’ll often pretend to be Trudy

Think Like Trudy

- Is all of this security information a good idea?
- "It's about time somebody wrote a book to teach the good guys what the bad guys already know." — Bruce Schneier

- We must try to think like Trudy
- We must study Trudy's methods
- We can admire Trudy's cleverness
- Often, we can't help but laugh at Alice and Bob's stupidity
- But, we cannot act like Trudy

Think Like Trudy

- **"우리 회사 뚫어주세요"...모의해킹 수요 급증** (한국경제, 2021.01.03)
  - 피싱 이메일을 직원들에게 보내고, 사내 네트워크 망을 불시에 공격하는 등 훈련 목적의 '모의해킹' 수요가 최근 크게 증가한 것으로 파악됐다. 모의해킹은 랜섬웨어 등 실제 일어나는 침해사고를 재연하는 훈련이다.
  - 보안장비 및 솔루션의 취약점을 찾아내고 개선점을 도출하기 위해서다.
  - 신종 코로나바이러스 감염증(코로나19) 등으로 동요하는 사람들의 심리를 이용하는 '사회공학적 공격'에 대비해 임직원의 보안의식을 높이려는 목적도 있다.
  - 보안회사에 소속된 화이트 해커가 고객사에 파견돼 모의해킹 업무를 수행하는 게 일반적이다.
  - 자사 제품 및 서비스의 취약점을 신고하면 포상금을 주는 기업도 늘어나고 있다

2020년 발생한 주요 사이버 보안 사고

4월	스타일쉐어	개인정보 유출
5월	잡꾸미기	개인정보 유출
6~8월	LG전자 SK하이닉스	업무 정보 유출
11월	이랜드그룹	점포 시스템 마비 고객정보 유출
	KAIST	개인정보 유출

자료: 업계

악성메일 공격 모의훈련 시나리오

1단계	화이트해커가 인터넷 검색, SNS 등서 임직원 메일주소 수집
2단계	'[긴급] 보안 패치 업데이트' 등의 제목으로 피싱 메일 발송
3단계	임직원이 악성메일 다운로드
4단계	악성파일이 감염 PC 정보 및 저장된 파일 수집·암호화
5단계	부서별 감염률 그래프 등 훈련 결과 보고서 제공

자료: SK인포섹

"해커들의 '창'은 기업 및 기관의 '방패'보다 항상 빠르게 진화한다"
"피해를 최소화하기 위해선 모의훈련 등으로 맷집을 키우는 게 중요하다"

Think Like Trudy

- [플랫폼] "모의해킹으로 숨은 보안구멍 찾기...그게 저희 임무죠“ -- (매일경제, 2021.03.31)

LG CNS 화이트해커 조직 `RED팀` 3인 인터뷰

사후대응보다 사전예방 초점
직접 해커가 돼 취약점 찾아내

보안 패치 수립 등 컨설팅까지
짧게는 며칠, 길게는 두달 걸려

해커에 가장 쉬운 구멍은 `사람`
이메일·SNS 링크 열땐 신중히

레드팀이란 `공격조`를 뜻하는 군사용어
레드팀이라는 이름처럼 시스템의 취약점을 직접 해킹해 보여주는 것이 특징이다. 서 팀장은 "사후 대응이 아닌 사전 예방을 위해서는 **실제 해커들이 사용하는 방법**으로 모의 해킹을 하는 게 중요하다"며 "우리는 고객 승인 하에 **해커들과 동일한 기술·방법으로 해킹해 취약점을 찾아** 설명해주고 대응법을 알려준다"고 설명했다. 예를 들어 클라우드 전환 때 정보관리자 권한을 잘못 설정하면 스마트팩토리 설비가 랜섬웨어에 감염되는 것처럼 해커들이 실제로 어떻게 공격하는지, 해킹 시 어떤 피해를 입게 되는지 피부에 와 닿게 설명해준다.

카카오페이는 정보보호 담당자 영입에 나섰다. 전자금융기반시설 취약점 점검 기준에 따른 보안성 진단 및 개선 업무, 대내/외 서비스 취약점 점검 및 모의해킹 등 보안성 검토, 신규 서비스 기획 단계의 보안기술 적용 검토, 소스코드 보안성 검토 및 안전한 프로그래밍을 위한 개발자 가이드 등의 업무를 담당한다. 3년 이상의 업무 경험과 금융 분야 취약점 진단/보안성 심의 내용 및 절차를 이해하고, 분석/평가 결과에 따른 개선 방안을 제시할 수 있어야 한다.

현대차·농협은행·카카오페이 등 금융·자동차기업 보안인력 채용 나섰다 -- (보안 뉴스, 2021.03.01)

현대자동차는 소프트웨어 차량 보안 책임연구원을 모집한다. 차량 보안에 있어 자동차 그룹 전체의 컨트롤타워 역할을 하는 부서로 차량 보안사고 대응과 차량 보안 신규 위협 연구, 그리고 실차 점검을 기반으로 한 프로세스 개선 등의 업무를 수행한다. 경력 2년 이상에 학사 이상 학위, 디바이스 보안 관련 프로젝트 경험이 있어야 한다.

침투 테스트 = 윤리적 해킹

- **"해커에서 침투 테스터로의 변신" 침투 테스트의 기초와 요구 사항** (2017.11.23, ITWorld)
  - '윤리적 해킹(ethical hacking)'으로도 불리는 침투 테스트(Penetration test): 기본적으로 보수를 받고 합법적으로 컴퓨터나 기기에 침투하는 일
  - 전문 침투 테스터는 서면으로 범위와 목적을 합의해야 한다.
    - 테스트의 범위에 포함되는 컴퓨터 자산들은 무엇인가? 모든 컴퓨터가 포함되는가? 아니면 특정 애플리케이션이나 서비스, 운영체제 플랫폼, 모바일 기기, 클라우드 서비스만 해당되는가?
    - 전문 해커(레드 팀)가 방어 담당자(**블루 팀**) 모르게 침투를 시도하는 테스트인가? 아니면 진짜 해커들이 사용하는 방법으로 기존의 탐지 및 방어 체계를 테스트하는 테스트인가?
    - 침투 테스트가 블랙박스(침투 테스터가 관련 시스템이나 애플리케이션에 대해 모르는 상태에서의 테스트)인가? 아니면 화이트박스(경우에 따라 관련된 소스코드를 포함해 공격 대상 시스템에 대한 내부 지식을 갖고 있는 상태에서의 테스트)인가?
    - ...
- **사물 인터넷(IoT) 등 4차 산업혁명시대, 떠오르는 '화이트 해커'** (2018.07.24, 산업일보)
  - 중요성 더욱 높아진 사이버 보안에 일본 신직업군으로 등장
- **금융보안원, 모의해킹·악성코드분석 분야 등 2021년도 신입직원 채용** (2020.09.28 보안뉴스)
  - 모의해킹/악성코드분석은 **실기 전형** 실시

모의해킹/ 악성코드분석	○명	- 전자적 침해위협 탐지·대응 및 취약점 분석·평가 등
전산/ 정보보호	○○명	- 금융권 전산 및 보안 관련 기획·분석 - 전자적 침해위협 탐지·대응 및 취약점 분석·평가 - 핀테크 및 인공지능 등 보안 기술 연구·개발 - 금융분야 데이터 보안 및 개인정보보호 등

Whitehat Contest Korea

화이트햇 콘테스트

- 함께하는 강력한 사이버 국방, 최고의 화이트 해커를 찾아라, 정보통신신문, 2021.08.24
  - 문제는 리버싱(역공학) 기술, 포렌식 기술, 웹 해킹 기술 등 사이버 대응 역량을 평가하는 다양한 분야에서 출제된다.
  - 'CTF Jeopardy(Capture The Flag Jeopardy)' 형식
- 국방부, 해킹방어대회 '화이트햇 콘테스트'…현역장병 부문 신설, 연합뉴스, 2021-08-23
- "사이버 국방, 민·관·군 역량 통합해야"…2021 화이트햇 콘테스트 개최, 전자신문, 2021.11.03
  - 손기욱 국가보안기술연구소 본부장은 "사이버 분야에도 전술이 필요하다. 사이버 킬체인과 마이터 어택(MITRE ATT&CK) 프레임워크를 참고해 적합한 사이버 전술을 수립하자"고 제안했다.

Common Attack Pattern Enumerations and Classifications (CAPEC)

☞ An attack pattern is a description of the common attributes and approaches employed by adversaries to exploit known weaknesses in cyber-enable capabilities
- A cyber-enabled capability is any software enabled technology, irrespective of whether it be traditional IT, communications systems, industrial control systems, avionics, vehicle control systems, IoT, …

☞ Understanding how the adversary operates is essential to effective cybersecurity.

- CAPEC helps by providing a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities.
  - 사이버 공격 패턴 목록 및 분류
  - It can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses.
  - CAPEC View: Mechanisms of Attack

1000 - Mechanisms of Attack

- C Engage in Deceptive Interactions - *(156)*
- C Abuse Existing Functionality - *(210)*
- C Manipulate Data Structures - *(255)*
- C Manipulate System Resources - *(262)*
- C Inject Unexpected Items - *(152)*
- C Employ Probabilistic Techniques - *(223)*
- C Manipulate Timing and State - *(172)*
- C Collect and Analyze Information - *(118)*
- C Subvert Access Control - *(225)*

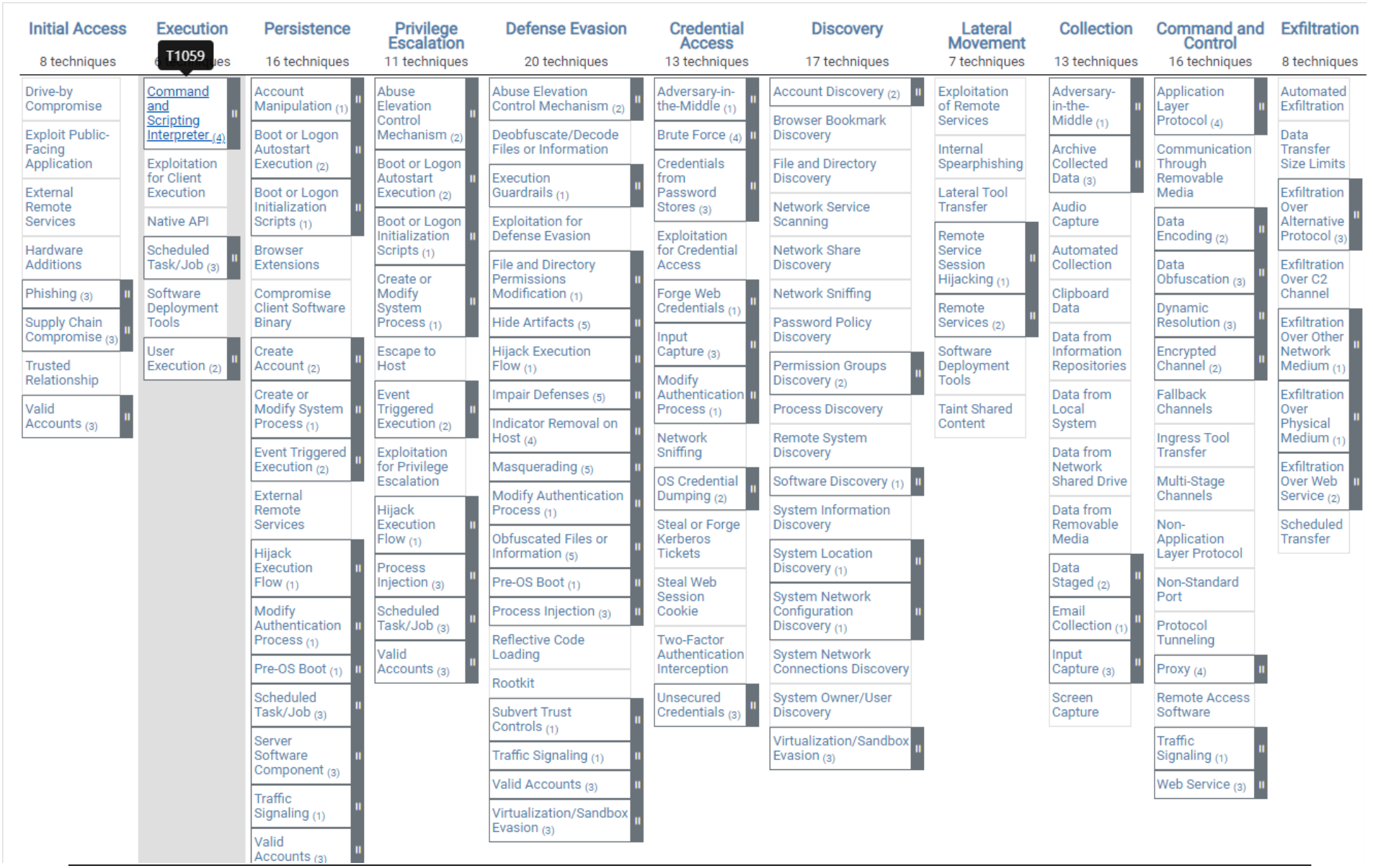
Source: https://capec.mitre.org/

MITRE ATT&CK Framework

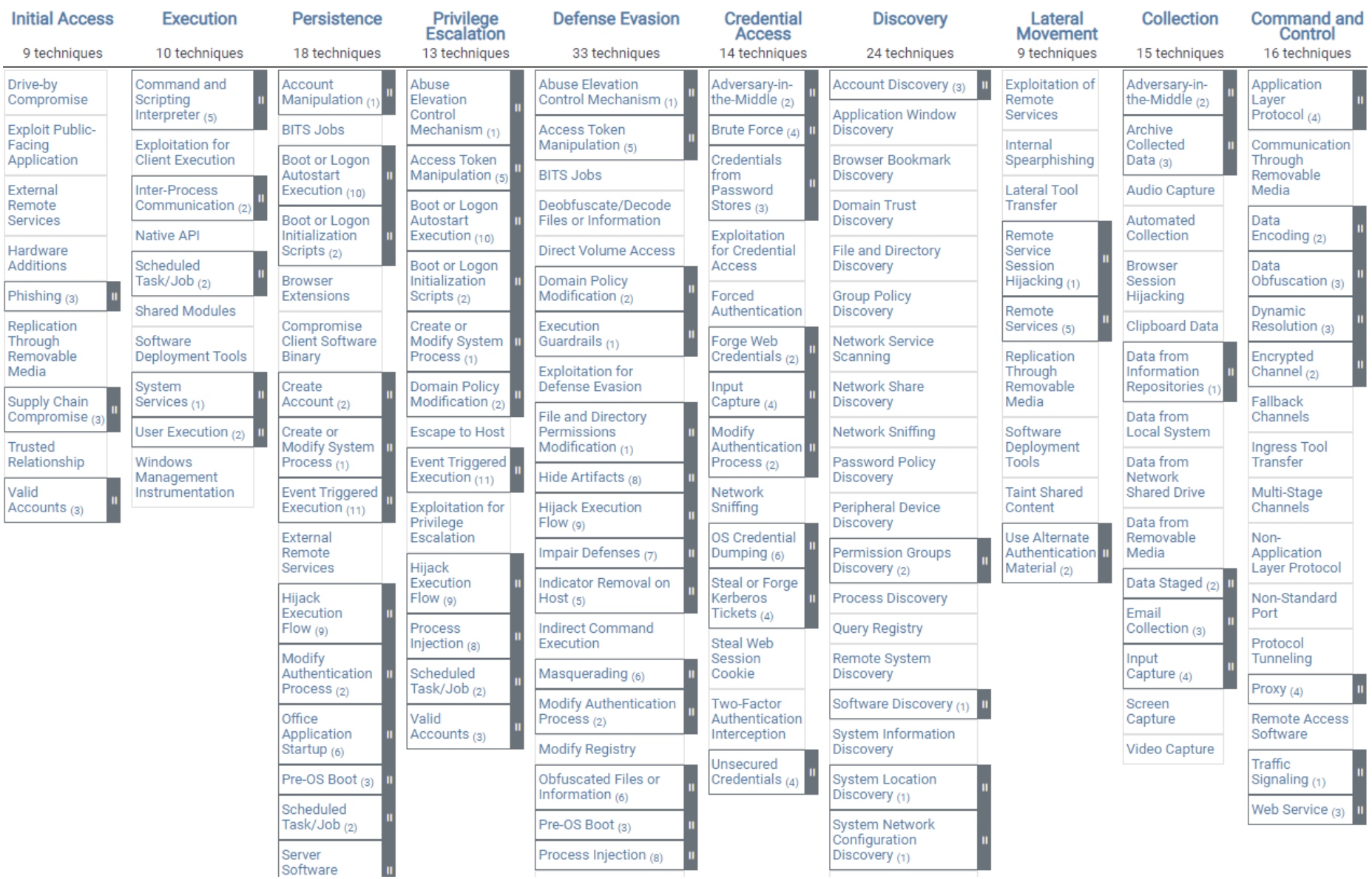
- Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)
  - A globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. (실제 공격 관찰을 통해 작성된 적대적 (위협) 전술과 기법 들의 지식 기반)
  - a knowledge base of cyber adversary behavior and taxonomy for adversarial actions across an adversary's attack lifecycle. (적대적 행위의 지식 기반이고, 공격(적대적 행동)들의 분류)
    - The tactics and techniques abstraction in the model provide a common taxonomy of individual adversary actions understood by both offensive and defensive sides of cybersecurity.
    - The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies
  - Source: https://attack.mitre.org/

  - "공격 방식과 도구를 분석해 방어한다" 마이터의 ATT&CK 프레임워크란 무엇인가
    - 목표는 일관되고 명확한 방식으로 공격을 분석하고 분류하는 것이다. 이는 대조와 비교를 통해 공격자가 네트워크와 엔드포인트를 어떻게 악용하면서 네트워크에 침입하는 지를 한층 수월하게 파악할 수 있게 해준다.
    - ATT&CK는 실제 악성코드 컴포넌트를 관찰하며 상세히 분해할 수 있는 한층 포괄적인 방법이다
    - 출처: ITWorld, 2021.09.10

MITRE ATT&CK Matrix for Enterprise : Linux



MITRE ATT&CK Matrix for Enterprise : Windows



MITRE ATT&CK Matrix for Mobile

Device Access

Initial Access (9 techniques)	Execution (4 techniques)	Persistence (9 techniques)	Privilege Escalation (4 techniques)	Defense Evasion (21 techniques)	Credential Access (11 techniques)	Discovery (9 techniques)	Lateral Movement (2 techniques)	Collection (18 techniques)	Command and Control (9 techniques)	Exfiltration (4 techniques)
Deliver Malicious App via Authorized App Store	Broadcast Receivers	Broadcast Receivers	Code Injection	Application Discovery	Access Notifications	Application Discovery	Attack PC via USB Connection	Access Calendar Entries	Alternate Network Mediums	Alternate Network Mediums
Deliver Malicious App via Other Means	Command-Line Interface	Code Injection	Device Administrator Permissions	Code Injection	Access Sensitive Data in Device Logs	Evade Analysis Environment	Exploit Enterprise Resources	Access Call Log	Call Control	Commonly Used Port
Drive-by Compromise	Native Code	Compromise Application Executable	Exploit OS Vulnerability	Delete Device Data	Access Stored Application Data	File and Directory Discovery		Access Contact List	Commonly Used Port	Data Encrypted
Exploit via Charging Station or PC	Scheduled Task/Job	Foreground Persistence	Exploit TEE Vulnerability	Device Lockout	Capture Clipboard Data	Location Tracking		Access Notifications	Domain Generation Algorithms	Standard Application Layer Protocol
Exploit via Radio Interfaces		Modify Cached Executable Code		Disguise Root/Jailbreak Indicators	Capture SMS Messages	Network Service Scanning		Access Sensitive Data in Device Logs	Remote File Copy	
Install Insecure or Malicious Configuration		Modify OS Kernel or Boot Partition		Download New Code at Runtime	Exploit TEE Vulnerability	Process Discovery		Access Stored Application Data	Standard Application Layer Protocol	
Lockscreen Bypass		Modify System Partition		Evade Analysis Environment	Input Capture	System Information Discovery		Call Control	Standard Cryptographic Protocol	
Masquerade as Legitimate Application		Modify Trusted Execution Environment		Geofencing	Input Prompt	System Network Configuration Discovery		Capture Audio	Uncommonly Used Port	
Supply Chain Compromise		Scheduled Task/Job		Hooking	Keychain	System Network Connections Discovery		Capture Camera	Web Service	
				Input Injection	Network Traffic Capture or Redirection			Capture Clipboard Data		
				Install Insecure or Malicious Configuration	URI Hijacking			Capture SMS Messages		
				Masquerade as Legitimate Application				Data from Local System		
				Modify OS Kernel or Boot Partition				Foreground Persistence		
				Modify System Partition				Input Capture		
				Modify Trusted Execution Environment				Location Tracking		
				Native Code				Network Information Discovery		
				Obfuscated Files or Information				Network Traffic Capture or Redirection		
				Proxy Through Victim				Screen Capture		
				Suppress						

In This Course…

- Always think like the bad guy
- Always look for weaknesses, vulnerabilities, …
- Strive to find a weak link
- Think like Trudy and a Threat Manager!

- But don’t do anything illegal…

Summary

Security Goals	Approaches / Mechanisms
Confidentiality (비밀성, 기밀성)	Cryptography (AES, RSA), Access control
Integrity (무결성)	Cryptographic hash functions (MAC, HMAC (Hash-based MAC), MD5, SHA-256, …)
Availability (가용성)	CDNs, Scrubbing center, Backup
Authentication (인증)	Password, Biometrics, Digital signature
Authorization (인가, 권한 부여)	Access control policies (ACL (DAC), MAC, RBAC, …)
Non-repudiation (부인 봉쇄)	Accountability, Auditing (Audit log), Digital signature

Security Goals = Security Properties

Appendix

SW 보안 이슈

- **[3.26 보안 이슈투데이] 앨런 튜링, 오픈SSL 취약점, 크롬의 HTTPS** (2021.03.26 보안뉴스)
  - 영국의 새 50파운드 지폐에 앨런 튜링 얼굴 새겨져…연합군 승리 이끈 주역
  - Open SSL이라는 암호화 소프트웨어 라이브러리에서 고위험군 취약점 발견돼
  - 크롬, 4월 중순부터 HTTPS 강제 적용…한 회사의 독단적 행위라는 비판 일기도 해

- **악성앱 이용한 스마트폰 해킹 공포… 실제 감염시 어떤 증상 나타날까** (2021.03.31 보안뉴스)
  - 전국민의 95%가 스마트폰 사용…스마트폰 노린 악성 앱과 악성코드 늘어나
  - 최근 국정원이 은행을 사칭한 가짜 앱으로 약 4만대의 스마트폰이 해킹 당했다고 밝히면서 …
  - 배터리 광탈, 데이터 사용량 급증, 화면 이동 및 변경 시 악성코드 감염 의심해봐야
  - 스마트폰에서 탈취한 개인정보 바탕으로 대부분 2차 피해 발생

정보보안은 법규/정책과 관련이 있음

● 정보보안기사

구분	시험과목	시험방법				
		문항수	배점	검정시간	문제유형	합격기준
필기시험	시스템보안	20	100	각 과목 30분	4지 택일형	각 과목 40점 이상, 5과목 평균 60점 이상
	네트워크 보안	20	100			
	어플리케이션 보안	20	100			
	정보보안 일반	20	100			
	정보보안관리 및 법규	20	100			
실기시험	정보보안 실무	15	100	총 180분	필답형	60점 이상

정보통신망 이용촉진 및 정보보호 등에 관한 법률 (약칭: 정보통신망법)

○ 정보보안산업기사

구분	시험과목	시험방법				
		문항수	배점	검정시간	문제유형	합격기준
필기시험	시스템보안	20	100	각 과목 30분	4지 택일형	각 과목 40점 이상, 4과목 평균 60점 이상
	네트워크 보안	20	100			
	어플리케이션 보안	20	100			
	정보보안 일반	20	100			
실기시험	정보보안 실무	15	100	총 150분	필답형	60점 이상