Pilastri della Security

Obiettivi

- Presentare in dettaglio i concetti relative a quelli che vengono tipicamente considerati i *Pilastri della sicurezza*

Indice

- Pilastri basilari della Security:
  - Triade CIA
- Pilastri addizionali

Indice

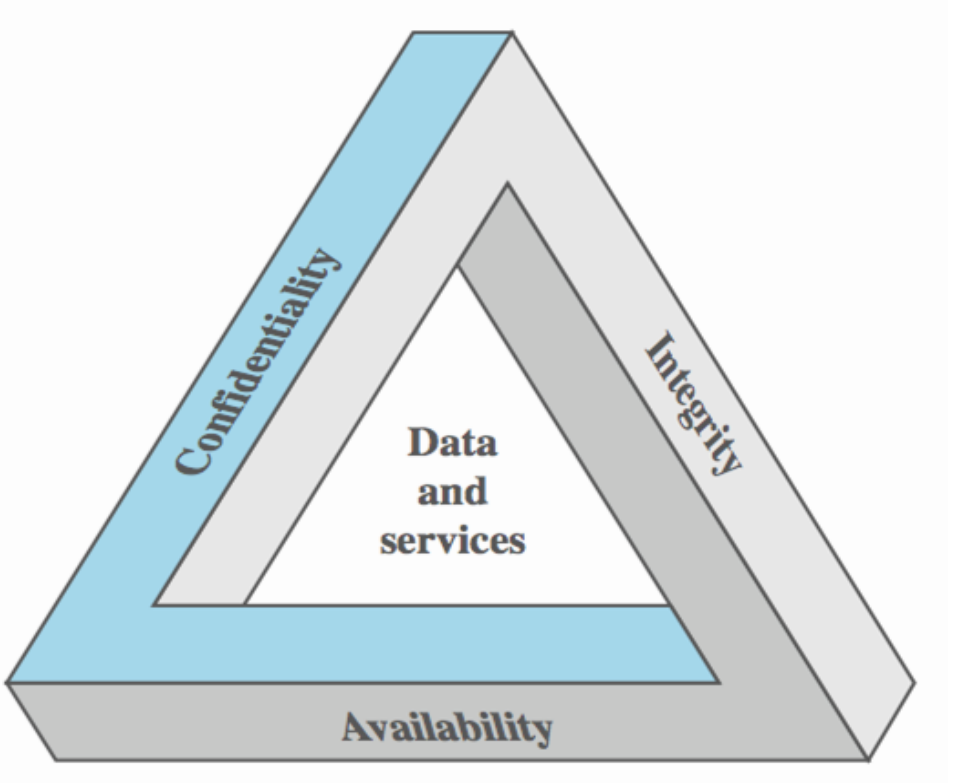
- Pilastri basilari della Security:
  - Triade CIA
- Pilastri addizionali

Pilastri basilari della Security

- *Confidenzialità*
  - La garanzia che le informazioni siano accessibili solo per i soggetti autorizzati
- *Integrità*
  - La garanzia che le informazioni non siano modificate da soggetti non autorizzati
- *Disponibilità*
  - La garanzia che l'accesso ai soggetti autorizzati sia sempre possibile

La triade CIA

- *Confidenzialità, Integrità, Disponibilità* formano quella che viene comunemente definita la *triade CIA* (the *CIA Triad*)



Pilastri basilari della Security

- *Confidenzialità*
  - La garanzia che le informazioni siano accessibili solo per i soggetti autorizzati
- *Integrità*
  - La garanzia che le informazioni non siano modificate da soggetti non autorizzati
- *Disponibilità*
  - La garanzia che l'accesso ai soggetti autorizzati sia sempre possibile

Confidenzialità

- *Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…*

[US Federal Information Security Management Act (FISMA) - United States Code, 2006 Edition, Supplement 5, Title 44]

Confidenzialità

Può essere declinata in due ambiti:

- *Gli individui (Privacy)*
- *Le organizzazioni (Segretezza)*

Confidenzialità

Può essere declinata in due ambiti:

- *Gli individui (Privacy)*
- *Le organizzazioni (Segretezza)*

- Assicura che le persone controllino o influenzino:
  - quali informazioni a loro correlate possano essere raccolte e archiviate e da chi
  - a chi tali informazioni possano essere divulgate

Confidenzialità

Può essere declinata in due ambiti:

- *Gli individui (Privacy)*
- *Le organizzazioni (Segretezza)*

- A volte viene utilizzato nel senso di *anonimato*, ossia mantenere la propria identità privata

https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali

Cosa intendiamo per dati personali?*

Sono **dati personali** le informazioni che identificano o rendono identificabile, **direttamente o indirettamente**, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

Particolarmente importanti sono:

- i **dati che permettono l'identificazione diretta** - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i **dati che permettono l'identificazione indiretta**, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

- i **dati rientranti in particolari categorie**: si tratta dei dati c.d. *"sensibili"*, cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i **dati genetici,** i **dati biometrici** e quelli relativi all'**orientamento sessuale**;

- i **dati relativi a condanne penali e reati**: si tratta dei dati c.d. *"giudiziari"*, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle nuove tecnologie, **altri dati personali** hanno assunto un ruolo significativo, come **quelli relativi alle comunicazioni elettroniche** (via Internet o telefono) e **quelli che consentono la geolocalizzazione**, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

Privacy

- Il tema della Privacy verrà approfondito nel
  - Modulo 4.2 - *GDPR, Codice dell'Amministrazione Digitale, NIS*

Confidenzialità

Può essere declinata in due ambiti:

- *Gli individui (Privacy)*
- *Le organizzazioni (Segretezza)*

- Riguarda la riservatezza per organizzazioni, come società commerciali o governi

Pilastri basilari della Security

- *Confidenzialità*
  - La garanzia che le informazioni siano accessibili solo per i soggetti autorizzati
- *Integrità*
  - La garanzia che le informazioni non siano modificate da soggetti non autorizzati
- *Disponibilità*
  - La garanzia che l'accesso ai soggetti autorizzati sia sempre possibile

Integrity

- Guarding against improper information modification or destruction, and includes ensuring information *non-repudiation* and *authenticity.*

[US Federal Information Security Management Act (FISMA) - United States Code, 2006 Edition, Supplement 5, Title 44]

Integrità

Copre due concetti collegati:

- *Integrità dei dati*
- *Integrità dei sistemi*

Integrità

Copre due concetti collegati:

- *Integrità dei dati*
- *Integrità dei sistemi*

- Assicura che le informazioni e i programmi vengano modificati solo in maniera specificata e autorizzata

Integrità

Copre due concetti collegati:

- *Integrità dei dati*
- *Integrità dei sistemi*

- Assicura che un sistema esegua le sue operazioni in maniera inalterata, libero da manipolazioni non autorizzate

Pilastri basilari della Security

- *Confidenzialità*
  - La garanzia che le informazioni siano accessibili solo per i soggetti autorizzati
- *Integrità*
  - La garanzia che le informazioni non siano modificate da soggetti non autorizzati
- *Disponibilità*
  - La garanzia che l'accesso ai soggetti autorizzati sia sempre possibile

Disponibilità

- Assicura che i sistemi funzionino tempestivamente e che il servizio non venga negato agli utenti autorizzati.

Availability

- Ensuring timely and reliable access to and use of information …

[US Federal Information Security Management Act (FISMA) - United States Code, 2006 Edition, Supplement 5, Title 44]

DAD vs CIA

- Gli attacchi alla CIA vengono tipicamente indicati come DAD:
  - **D**isclosure > **C**onfidentiality
  - **A**lteration > **I**ntegrity
  - **D**estruction > Availability

Approfondimenti

- Una analisi dettagliata degli attacchi alla CIA è riportata nel *Modulo 2.1 - Attacchi alla Confidenzialità, Integrità e Disponibilità*

Indice

- Pilastri basilari della Security:
  - Triade CIA
- Pilastri addizionali

Pilastri addizionali della Security

- *Resilienza*
- *Non ripudio*
- *Autenticità*
- *Controllo degli accessi*

[https://www.itgovernance.co.uk/cyber-resilience]

Pilastri addizionali della Security

- *Resilienza*
- *Non ripudio*
- *Autenticità*
- *Controllo degli accessi*

- È una misura di come un'organizzazione sia in grado di affrontare un attacco cibernetico (o una sottrazione dei propri dati), pur continuando a gestire la propria attività in modo efficace.

Pilastri addizionali della Security

- *Resilienza*
- *Non ripudio*
- *Autenticità*
- *Controllo degli accessi*

- Vedremo al riguardo 2 definizioni, mirate a evidenziare aspetti diversi

Pilastri addizionali della Security

- *Resilienza*
- *Non ripudio*
- *Autenticità*
- *Controllo degli accessi*

[NIST SP 800-53 Rev. 4 under Information System Resilience
NIST SP 800-39 under Information System Resilience]

- La capacità di un sistema di continuare a:
  - operare in condizioni avverse o di stress, anche se in uno stato degradato o debilitato, mantenendo le capacità operative essenziali;
  - recuperare una postura operativa efficace in un lasso di tempo coerente con le esigenze della mission.

Pilastri addizionali della Security

- *Resilienza*
- *Non ripudio*
- *Autenticità*
- *Controllo degli accessi*

- La capacità di un sistema di
  - continuare a funzionare mentre è sotto attacco, anche se in stato degradato o debilitato,
  - di recuperare rapidamente le capacità operative per le funzioni essenziali dopo un attacco riuscito

[NIST SP 800-30 Rev. 1 under Information System Resilience]

- Approfondimenti sulla resilienza in appendice

Ricadute della resilienza

- La resilienza aiuta una organizzazione a:
  - proteggersi dai *rischi cyber*
  - difendersi e a limitare la gravità degli attacchi
  - a garantire la propria sopravvivenza nonostante un attacco.

[https://www.itgovernance.co.uk/cyber-resilience]

Rischio

- *La possibilità che azioni o eventi portino a conseguenze che hanno un impatto su ciò che si ritiene possedere un valore*

[O. Renn, "*The role of risk perception for risk management*," Reliability Engineering & System Safety, vol. 59, no. 1, pp. 49 – 62, 1998, http://www.sciencedirect.com/science/article/pii/S0951832097001191]

Conseguenze

- I responsabili della sicurezza devono analizzare le possibili minacce per determinare quali si applichino al loro contesto; questi sono i *rischi* che possono essere presi in considerazione
- Questo favorisce la selezione di *contromisure*, le quali mirano a ridurre le *vulnerabilità*

“Gestione” dei rischi

- Una appropriate “gestione” dei rischi richiede diversi processi, tra i quali:
  - *Valutazione* dei rischi
  - *Gestione* dei rischi (sviluppo e valutazione delle opzioni per affrontare i rischi in modo accettabile)
  - *Governance* dei rischi

Governance dei rischi

- Un insieme globale di processi in corso e principi che mira a fornire la consapevolezza e la formazione sui rischi affrontati quando si verificano determinate condizioni, e a infondere un senso di responsabilità a tutti i soggetti coinvolti nella sua gestione.

[O. Renn, *Risk Governance: Coping With Uncertainty in a Complex World*. Springer, 2008]

Rischi residuali

- Alcune vulnerabilità possono permanere, lasciando, in questo modo, dei *rischi residuali*
- I responsabili della sicurezza devono cercare di minimizzare tali rischi, valutandone i margini di fattibilità e i relativi costi.

Pilastri addizionali della Security

- *Resilienza*
- *Non ripudio*
- *Autenticità*
- *Controllo degli accessi*

Pilastri addizionali della Security

- *Resilienza*
- *Non ripudio*
- *Autenticità*
- *Controllo degli accessi*

- Protezione contro un individuo che nega falsamente di aver compiuto una determinata azione.

[CNSSI 4009-2015 (NIST SP 800-53 Rev. 4)
NIST SP 800-53 Rev. 4 under Non-repudiation]

Pilastri addizionali della Security

- *Resilienza*
- *Non ripudio*
- *Autenticità*
- *Controllo degli accessi*

[CNSSI 4009-2015 (NIST SP 800-53 Rev. 4)
NIST SP 800-53 Rev. 4 under Non-repudiation]

- Fornisce la capacità di provare a terzi (ad es. a un giudice) se un determinato soggetto ha compiuto una particolare azione quale, ad esempio:
  - creazione di informazioni
  - invio di un messaggio
  - accesso a un documento
  - ricezione di un messaggio

Pilastri addizionali della Security

- *Resilienza*
- *Non ripudio*
- *Autenticità*
- *Controllo degli accessi*

Pilastri addizionali della Security

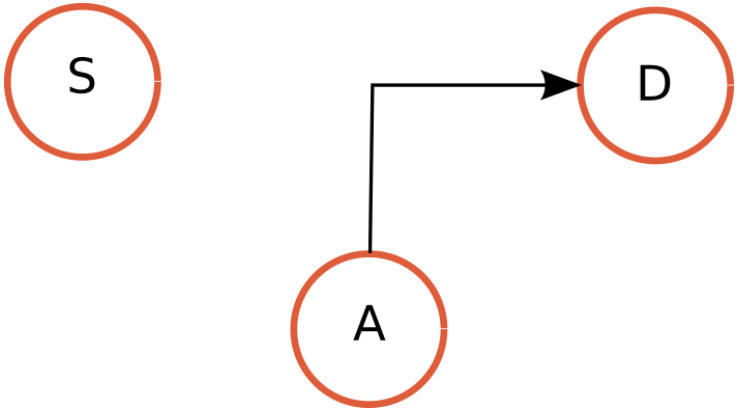
- *Resilienza*
- *Non ripudio*
- *Autenticità*
- *Controllo degli accessi*

[NIST SP 800-137 under Authenticity (CNSSI 4009)
NIST SP 800-30 Rev. 1 under Authenticity (CNSSI 4009)
NIST SP 800-39 under Authenticity
NIST SP 800-53 Rev. 4 under Authenticity
NIST SP 800-53A Rev. 4 under Authenticity]

- La proprietà di essere “genuini” e di poter essere verificati e credibili
- Fiducia nella validità di una trasmissione, di un messaggio o dell'autore del messaggio.

Esempio di attacco alla Autenticità

- L'aggressore crea un nuovo dato o messaggio
- In questo modo, rompe l'*autenticità*
- Esempi:
  - Falsificare una firma attraverso una vulnerabilità crittografica (e.g., le collisioni presenti in MD5)



Pilastri addizionali della Security

- *Resilienza*
- *Non ripudio*
- *Autenticità*
- *Controllo degli accessi*

Pilastri addizionali della Security

- *Resilienza*
- *Non ripudio*
- *Autenticità*
- *Controllo degli accessi*

- Il processo di autorizzare o negare delle specifiche richieste di accesso:
  - per ottenere e utilizzare informazioni e servizi per la loro elaborazione;
  - per accedere a specifiche strutture fisiche (ad esempio, edifici federali, stabilimenti militari e ingressi ai valichi di frontiera)

Indice

Best practice

- In letteratura si trovano numerose “buone pratiche” in materia di sicurezza, relative a diverse aree
- Nel loro insieme, aiutano a sviluppare un approccio *olistico* alla progettazione, allo sviluppo e alla implementazione di sistemi sicuri.

Esempio: I principi NIST

- Alcuni principi della progettazione di sistemi sicuri sono stati riassunti dal NIST nel testo:

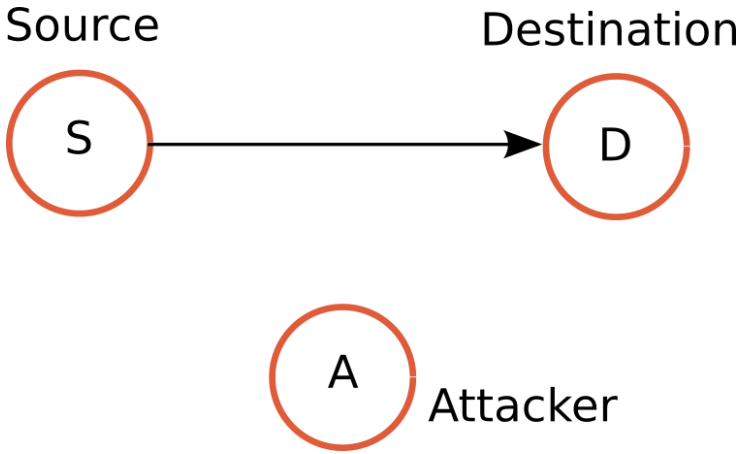
  R. Ross, M. McEvilley, and J. C. Oren, “Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems,” NIST, Tech. Rep. NIST.SP.800-160 Volume 1, Nov. 2016: https://doi.org/10.6028/NIST.SP.800-160v1

Esempio: I principi NIST

- Sono suddivisi in 3 grandi famiglie:
  - *Architetture di sicurezza e progettazione* (i.e., aspetti organizzativi, strutture e interfacce)
  - *Funzionalità di sicurezza e comportamenti intrinseci* (i.e., a cosa si riferiscono le protezioni)
  - *Sicurezza del ciclo di vita* (i.e., gli aspetti legati ai processi di produzione e manutenzione)

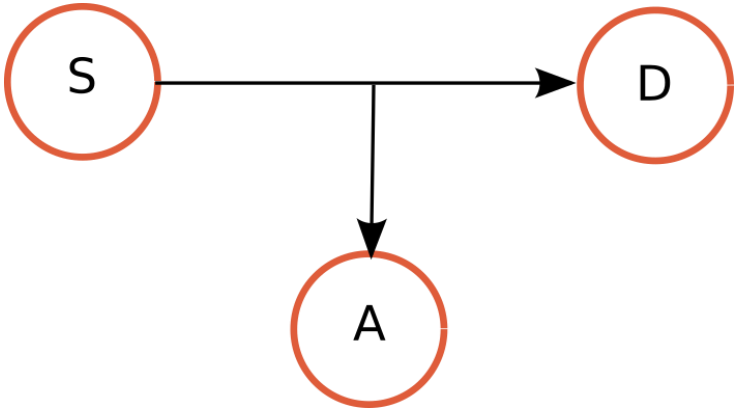
A practical example of CIA attack

- Let’s assume an information (or service) move from a source to a destination
- The attacker could subvert this pattern in several ways
- Let’s analyse some of them



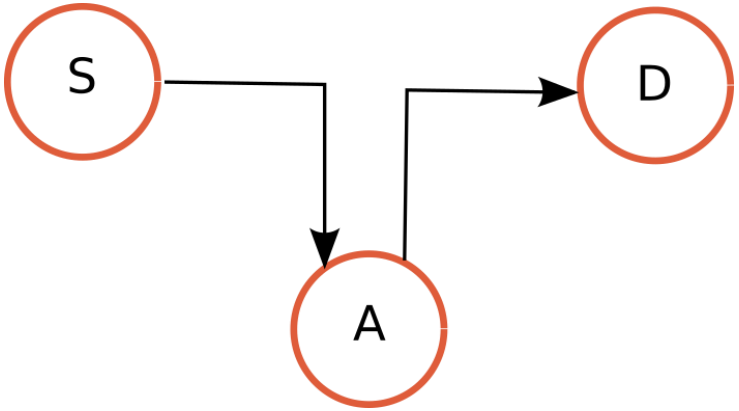
Stealing: attack to Confidentiality

- The attacker gets *unauthorized access* to information
- So, he breaks *confidentiality*
- Examples:
  - S is a vulnerable database
  - S sends a credit card number to D “in clear”



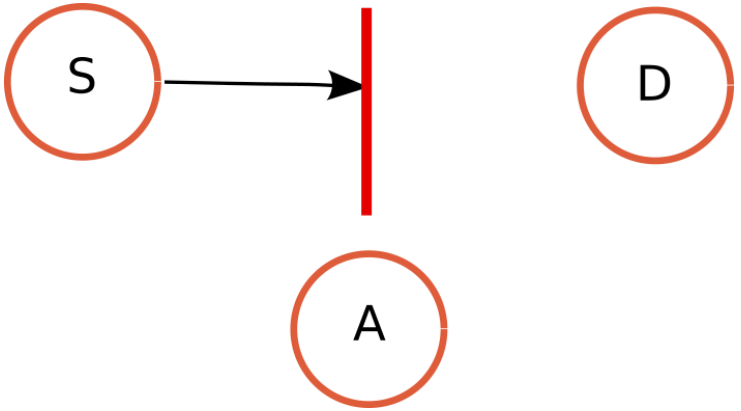
Corrupting: attack to Integrity

- The attacker *maliciously modifies* the transmitted information
- So, he breaks *integrity*
- Example:
  - A redirects S's bank transfer
  - NOTE: The attacker A can be either in the browser or on the network (*Man-in-the-middle*)



Inhibiting: attack to Availability

- The attacker *stops* the information flow
- So, he breaks *availability*
- Examples:
  - DoS on a server
  - Attack to the Ukrainian Power supply network



Countermeasures

- Attacks on the CIA can be taken to any level, from hardware to software to communications.
- To be effective, each application domain has developed and adopts its own specific countermeasures

Examples of possible countermeasures

- In the sequel we focus on just two examples of possible countermeasures in the field of protection of transmitted messages
  - *Hash functions*
  - *Encryption*

Hash Functions

- A Hash function:
  - gets in input a set of data M (of variable length)
  - returns a hash value h (of fixed length):

$$h = H(M)$$

Hash Functions usage

- Hash functions can be used to demonstrate the *integrity* of a message M.

Hash Functions usage

- Hash functions can be used to demonstrate the *integrity* of a message M.
- If M is sent together with h (i.e., the result of the hash function applied to it) and an attacker modifies M in M', the receiver, calculating the hash function on M', will get a value h' most likely different from the value h originally sent together with the message M.

Encryption

- Operation that, resorting to an *encryption algorithm* and a *key,* renders a message "blurred", so that it is not comprehensible/intelligible to persons not authorised to read it.

Encryption & Decryption

- Can be exploited to guarantee *confidentiality*.

The four elements of cyber resilience

- *Manage and protect*
- *Identify and detect*
- *Respond and recover*
- *Govern and assure*

- Being able to identify, assess and manage the risks associated with network and information systems, including those across the supply chain.
- It also requires the protection of information and systems from cyber attacks, system failures, and unauthorised access.

The four elements of cyber resilience

- *Manage and protect*
- *Identify and detect*
- *Respond and recover*
- *Govern and assure*

- Continual monitoring of network and information systems to detect anomalies and potential cyber security incidents before they can cause any significant damage.

The four elements of cyber resilience

- *Manage and protect*
- *Identify and detect*
- *Respond and recover*
- *Govern and assure*

- Implementing an incident response management programme and measures to ensure business continuity will help you continue to operate even if you have been hit by a cyber attack, and get back to business as usual as quickly and efficiently as possible.

The four elements of cyber resilience

- *Manage and protect*
- *Identify and detect*
- *Respond and recover*
- *Govern and assure*

- Ensure that your programme is overseen from the top of the organisation and built into business as usual.
- Over time, it should align more and more closely with your wider business objectives.