I “Pilastri” della *Security*

Paolo PRINETTO

Direttore
CINI Cybersecurity
National Laboratory

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Obiettivo della presentazione

- Presentare in dettaglio i concetti comunemente considerati come *pilastri della security*

Prerequisiti

- Lezioni:
  - *CS 1.01 - Introduzione alla Sicurezza*
  - *CS 1.02 - Cybersecurity -- Definizione e Rilevanza*

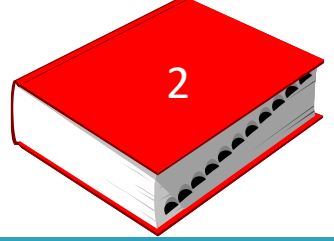
Indice

- Pilastri basilari:
  - Triade CIA
- Pilastri addizionali

Indice

- Pilastri basilari:
  - Triade CIA
- Pilastri addizionali

Computer security

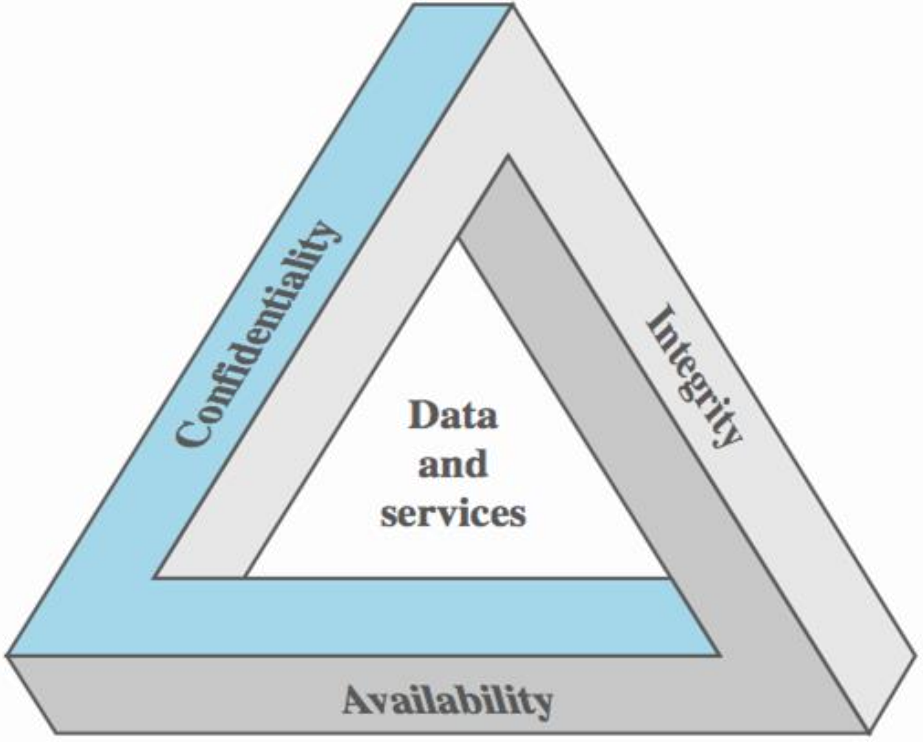


- Insieme di misure e controlli mirate a garantire la *confidenzialità*, *integrità* e *disponibilità* delle risorse di un sistema di elaborazione, incluse hardware, software, firmware e dati in elaborazione, archiviati o trasmessi.

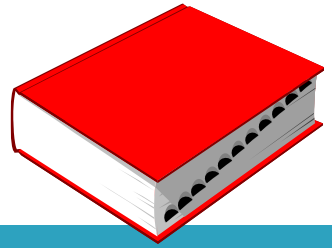
[The NIST Internal/Interagency Report NISTIR 7298
- Glossary of Key Information Security Terms, May 2013
(**NIST** = U.S. National Institute of Standards and Technology)]

La triade CIA

- *Confidenzialità, Integrità, Disponibilità* sono considerati i *pilastri della Security* e formano quella che viene comunemente definita la *triade CIA* (the *CIA Triad*)



Confidenzialità (o Riservatezza)



- La capacità di garantire che le informazioni siano accessibili solo ai soggetti autorizzati ad accedervi

Confidenzialità

Copre 3 sfere collegate:

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

Confidenzialità

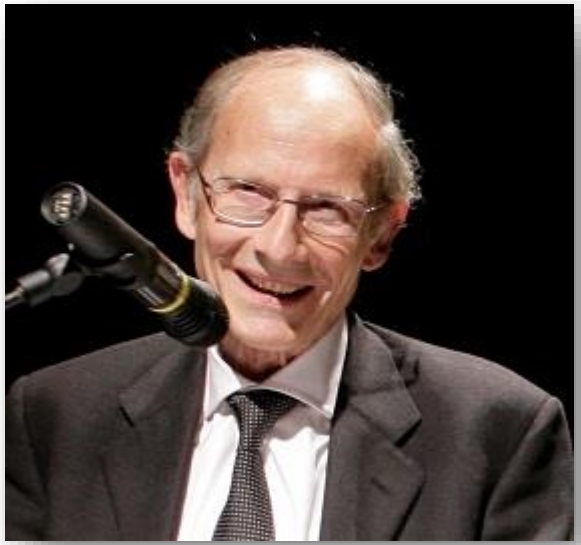
Copre 3 sfere collegate:

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

- Assicura che le informazioni riservate non vengano divulgate a persone non autorizzate

Datacrazia

"C'è una rivoluzione digitale in corso che coinvolge tutti. La quantità di dati che produciamo raddoppia ogni anno: nel 2018 abbiamo prodotto tanti dati quanto l'intera umanità fino al 2017" e "con l'Internet of Things entro cinque-sette anni avremo 150 miliardi di sensori connessi in rete, pari a 20 volte il numero di persone sulla terra. Allora la quantità di dati raddoppierà ogni 12 ore. Tutto diventerà intelligente, presto avremo non solo gli smartphone ma anche smart home, smart cars, smart factories e smart cities. La domanda è se avremo anche 'smarter people'".



[Mario RASETTI – ISI Foundation]

Confidenzialità

Copre 3 sfere collegate:

- *I dati*
- *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

Copre 3 sfere collegate:

- *I dati*
- *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

GARANTE
PER LA PROTEZIONE
DEI 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.

Quotazioni dei dati nel Dark Web

- data di nascita, social security number
- informazioni su carte di credito
- social media account
- cartelle sanitarie

Quotazioni dei dati nel Dark Web

- data di nascita, social security number 3 $
- informazioni su carte di credito 75 ¢ - 40 $
- social media account 16 $ - 325 $
- cartelle sanitarie 500 $ - 1200 $

Confidenzialità

Copre 3 sfere collegate:

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

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

Normativa italiana

- A titolo di esempio, l'ordinamento italiano prevede quattro classifiche di segretezza, definite come Nazionali, cui corrispondono crescenti livelli di protezione delle informazioni:
  - *RISERVATO* (R), danno lieve agli interessi della Repubblica;
  - *RISERVATISSIMO* (RR), danno agli interessi della Repubblica;
  - *SEGRETO* (S), danno grave agli interessi della Repubblica;
  - *SEGRETISSIMO* (SS), danno eccezionalmente grave agli interessi della Repubblica.

[Legge 3 agosto 2007, n. 124

Decreto del Presidente del Consiglio dei Ministri 12 giugno 2009, n. 7]

Normativa Internazionale

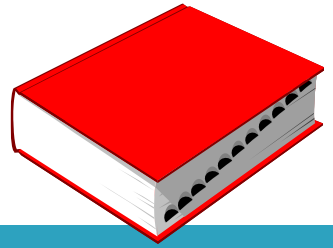
Italia	USA	UK	Francia
SEGRETISSIMO	TOP SECRET	TOP SECRET	TRÈS SECRET DÉFENSE
SEGRETO	SECRET	SECRET	SECRET DÉFENSE
RISERVATISSIMO	CONFIDENTIAL	NO NATIONAL EQUIVALENT [1]	CONFIDENTIAL DÉFENSE
RISERVATO	NO NATIONAL EQUIVALENT	OFFICIAL SENSITIVE [2]	NO NATIONAL EQUIVALENT

Normativa Internazionale

NATO	UE
COSMIC TOP SECRET	TRÈS SECRET EU / EU TOP SECRET
NATO SECRET	SECRET UE / EU SECRET
NATO CONFIDENTIAL	CONFIDENTIAL UE / EU CONFIDENTIAL
NATO RESTRICTED	RESTREINT UE / EU RESTRICTED

NB: la dicitura NATO UNCLASSIFIED apposta sui documenti NATO non classificati NON è una classifica di segretezza, ma garantisce comunque un regime minimo di protezione (non divulgabilità).

Integrità



- La capacità di garantire che le informazioni non siano modificate o distrutte da soggetti non autorizzati ad accedervi

Integrità

- Include:
  - la garanzia di non ripudio
  - autenticità delle informazioni

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

Integrità

Copre due concetti collegati:

Integrità

Copre due concetti collegati:

- *Integrità dei dati*

Integrità

Copre due concetti collegati:

- *Integrità dei dati*
  - 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*

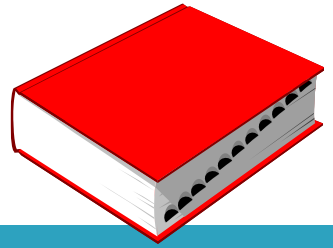
Integrità

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

Disponibilità

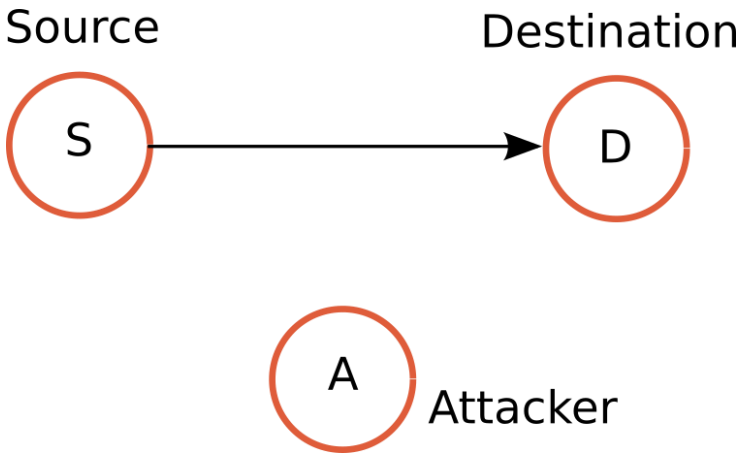


- La capacità di garantire un accesso tempestivo e affidabile alle informazioni da parte dei soggetti autorizzati ad accedervi

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

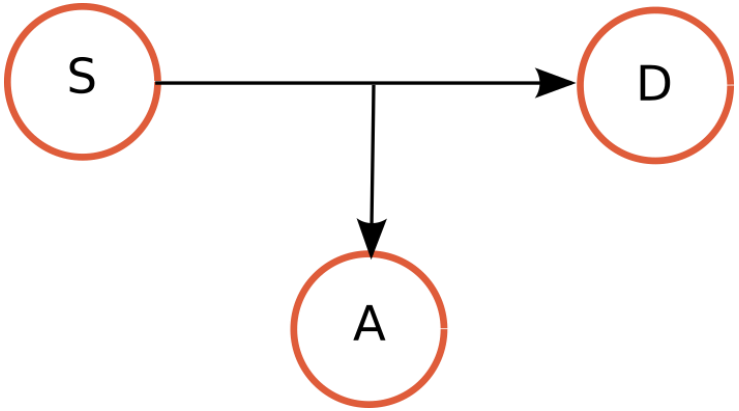
Un esempio pratico di attacco a CIA

- Supponiamo che una informazione (o un servizio) si sposti da una sorgente a una destinazione
- Un aggressore potrebbe sovvertire questo schema in diversi modi
- Analizziamone alcuni



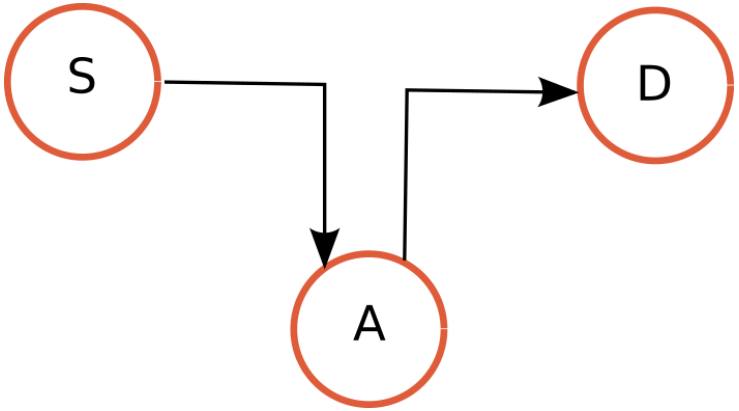
Rubare: attacco alla Confidenzialità

- L'aggressore ottiene un *accesso non autorizzato* alle informazioni
- Quindi, infrange la *Confidenzialità*
- Esempi:
  - S è un database vulnerabile
  - S invia un numero di carta di credito a D "in chiaro".



Corruzione: attacco alla Integrità

- L'aggressore *modifica in modo malevolo* le informazioni trasmesse
- Quindi, infrange la *Integrità*
- Esempio:
  - A reindirizza un bonifico bancario inviato da S
  - NOTA: L'aggressore A può essere sia nel browser sia nella rete (*Man-in-the-middle*)



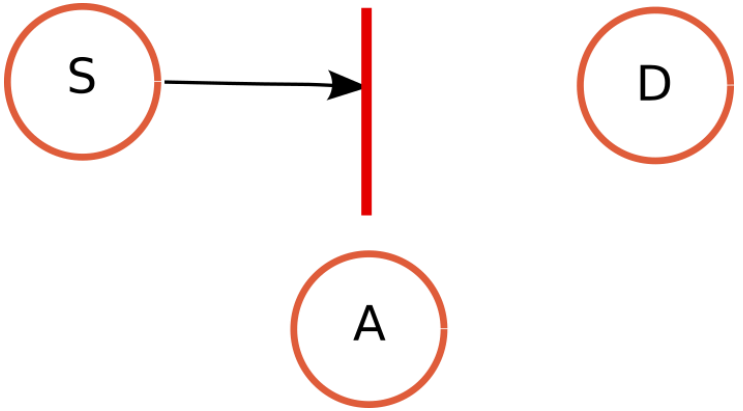
Caveat

- Non tutti gli attaccanti e non tutti i *Trojan* (hardware o software che siano) sono necessariamente malevoli!!

Publio Virgilio Marone - Eneide (Libro II, 49)

Inibizione: attacco alla Disponibilità

- L'aggressore *interrompe* il flusso di informazioni
- Quindi, rompe la Disponibilità
- Esempi:
  - DoS su un server
  - Attacco alla rete elettrica ucraina



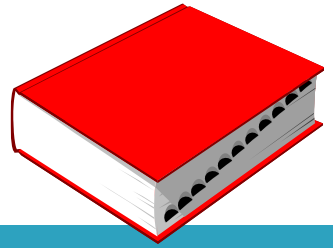
Contromisure

- Gli attacchi alla CIA possono essere portati a qualsiasi livello, dall'hardware al software alle comunicazioni.
- Per essere efficace, ogni dominio applicativo deve sviluppare e adottare le proprie contromisure specifiche.

Esempi di possibili contromisure

- Nel seguito ci concentriamo su due esempi di possibili contromisure nel campo della protezione dei messaggi trasmessi:
  - *Cifratura*
  - *Funzioni Hash crittografiche*

Cifratura



- Operazione che, ricorrendo a un *algoritmo di cifratura* e a una *chiave*, rende un messaggio "offuscato", in modo che non sia comprensibile/intelligibile a persone non autorizzate a leggerlo.

Cifratura & Decifratura

- Possono essere sfruttate per garantire la *Confidenzialità*:

Principi della crittografia *asimmetrica*

- Ciascun soggetto possiede 2 chiavi:
  - *chiave pubblica*: divulgata pubblicamente dal soggetto
  - *chiave privata*: tenuta segreta dal soggetto.
- Le due chiavi possono essere utilizzate (in modo complementare) per la cifratura/decifratura:
  - La cifratura con la chiave pubblica garantisce la *Confidenzialità*
  - La cifratura con la chiave privata garantisce la *Autenticità*
  - Con un mix appropriato è possible garantire anche la *Integrità*

Funzioni Hash crittografiche

- Una funzione Hash:
  - riceve in ingresso un insieme di dati M (di lunghezza variabile)
  - restituisce un valore di hash h (di lunghezza fissa), spesso chiamato *digest*:

$$h = H(M)$$

Uso delle funzioni Hash

- Le funzioni Hash possono essere utilizzate per provare la *Integrità* di un messaggio M, rilevando le eventuali modifiche al testo introdotte da un attaccante malevolo

Uso delle funzioni Hash

- Le funzioni Hash possono essere utilizzate per provare la *Integrità* di un messaggio M, rilevando le eventuali modifiche al testo introdotte da un attaccante malevolo
- Se M viene spedito unitamente al suo digest h e un aggressore modifica M in M', il ricevitore, calcolando la funzione hash su M', otterrà un valore h' diverso dal valore h originariamente inviato insieme a M.

Nota

1. Le chiavi e gli algoritmi di cifratura
2. Le funzioni hash e la lunghezza del *digest*
3. Il loro uso congiunto

sono via via selezionati in base a criteri specifici, finalizzati a massimizzare la sicurezza

Indice

- Pilastri basilari:
  - Triade CIA
- Pilastri addizionali

Pilastri addizionali della Security

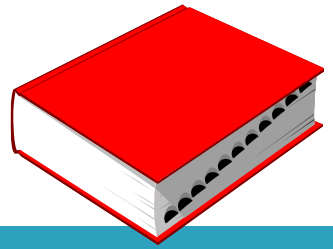
- *Resilienza*
- *Non ripudio*
- *Autenticità*
- *Controllo degli accessi*

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

Pilastri addizionali della Security

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

Resilienza

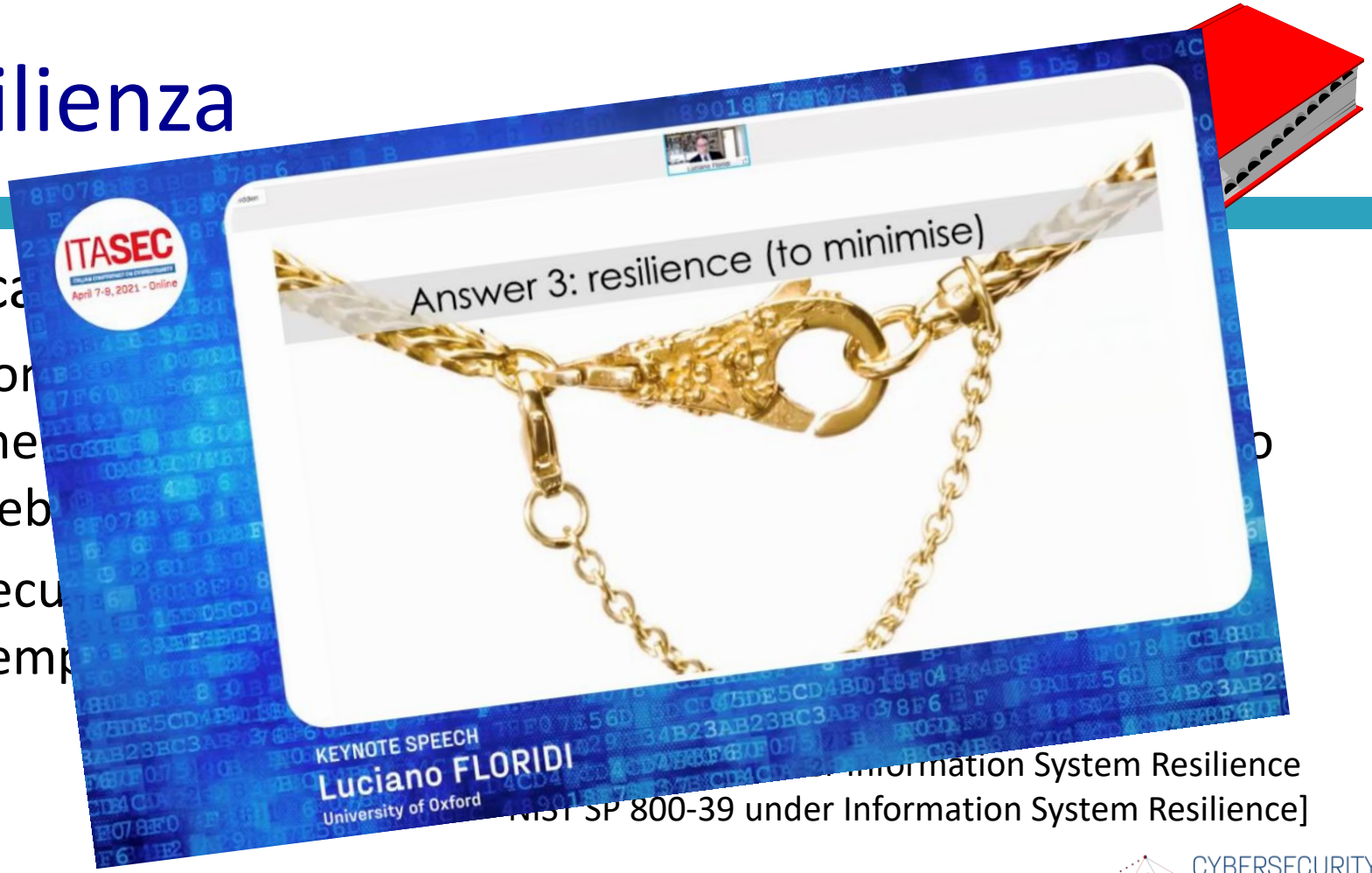


- La capacità di un sistema di:
  - continuare a operare in condizioni avverse o di stress o mentre è sotto attacco, anche se in uno stato degradato o debilitato, mantenendo le capacità operative essenziali;
  - recuperare una postura operativa efficace in un lasso di tempo coerente con le esigenze della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

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

Resilienza

- La ca
  - cor
    me
    deb
  - recu
    temp

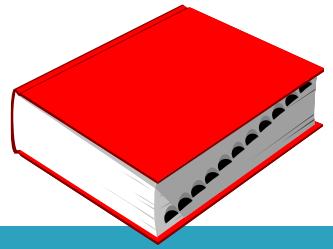


Information System Resilience
NIST SP 800-39 under Information System Resilience]

Pilastri addizionali della Security

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

Non ripudio



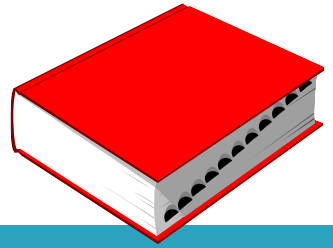
- La capacità di stabilire se un determinato soggetto abbia compiuto una particolare azione quale, ad esempio:
  - creazione di informazioni
  - invio di un messaggio
  - approvazione di informazioni
  - ricezione di un messaggio
  - ...

[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*

Autenticità



- 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.

[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]

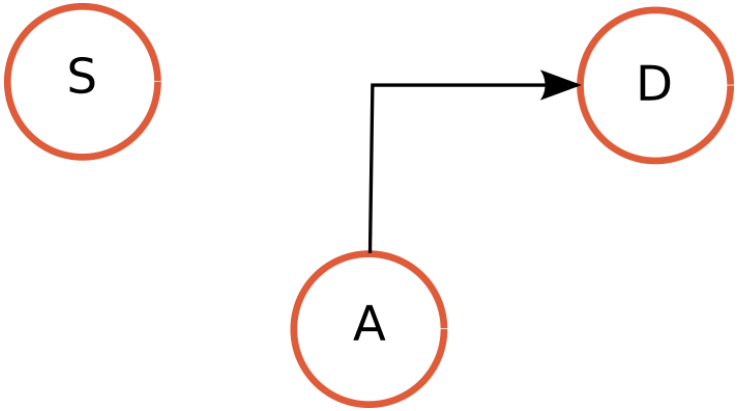
Autenticità e Fiducia

- “Ci si può fidare di un’entità se questa si comporta sempre nel modo previsto per lo scopo previsto.”

[D. Grawrock, Dynamics of a Trusted Platform: A building block approach. Intel Press, 2008]

Esempio di attacco alla Autenticità: *Fucina*

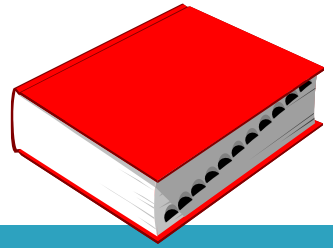
- L'aggressore crea un nuovo dato o messaggio
- In questo modo, rompe l'*autenticità*
- Esempi:
  - Falsificare una firma attraverso una vulnerabilità crittografica (e.g., le collisioni presenti nel protocollo MD5)



Pilastri addizionali della Security

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

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).

I “Pilastri” della *Security*

Paolo PRINETTO

Direttore
CINI Cybersecurity
National Laboratory

https://cybersecnatlab.it