Introduzione alla *Sicurezza*

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.

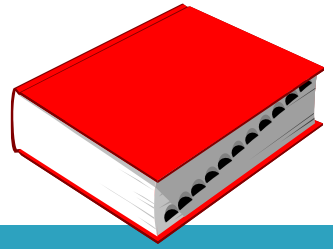
Obiettivo della presentazione

- Introdurre il concetto di sicurezza
- Fornire una tassonomia

Prerequisiti

- Nessuno

Nota editoriale



- Le slide nella quali in alto a destra è raffigurato un dizionario, come in questa, contengono delle definizioni.
- Un eventuale numero all'interno del dizionario indica definizioni diverse per uno stesso argomento

[In questo modo vengono invece riportati i riferimenti bibliografici]

Indice

- Il concetto di sicurezza
- Safety
- Security
- Dependability
- Cybersecurity

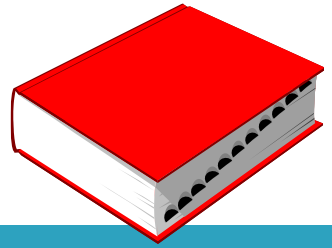
Il concetto di Sicurezza

- Nel seguito introdurremo il concetto di Sicurezza utilizzando definizioni diverse, che partono da diversi punti di vista.
- Come vedremo, al termine italiano *Sicurezza* corrispondono in inglese termini diversi.

Sicurezza

- Condizione oggettiva esente da *pericoli* o *minaccce* (*threats*)

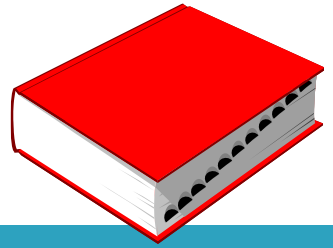
Pericolo



- Circostanza o complesso di circostanze da cui si teme che possa derivare grave danno

[http://www.treccani.it/vocabolario/pericolo/]

Minaccia



- Atteggiamento intimidatorio riguardante la sfera morale della vittima di cui risulta compromessa la capacità di autodeterminarsi e consistente nella prospettazione implicita o esplicita di un male ingiusto e futuro.

[https://www.brocardi.it/dizionario/4780.html]

Nota

- La natura e le peculiarità dei concetti di *pericolo* e *minaccia* dipendono fortemente dal contesto e dal dominio in considerazione

Sicurezza

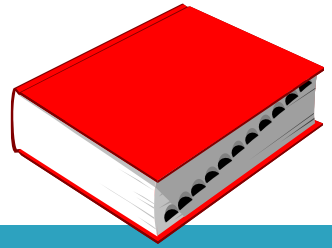
- L’assenza di quelle condizioni che possono causare la perdita di beni patrimoniali con conseguenze inaccettabili

[“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]

Implicazioni pratiche

- L'ambito specifico della sicurezza deve essere chiaramente definito dalle parti interessate in termini di:
  - *beni* (asset) a cui si applica la sicurezza
  - *conseguenze* rispetto alle quali viene valutata la sicurezza

Asset



- Qualsiasi bene o elemento di valore di proprietà di un ente che possa essere monetizzato

Asset - classificazioni

- Un asset può essere:
  - *tangibile* (e.g., un dispositivo fisico come hardware, piattaforma di calcolo, dispositivo di rete o qualsiasi altro componente tecnologico)
  - *intangibile* (e.g., dati, informazioni, software, marchi, copyright, brevetti, proprietà intellettuali, immagine o reputazione)

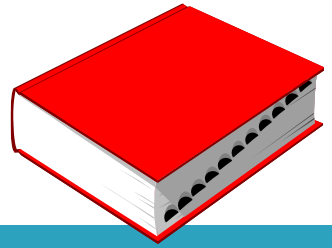
Impatto della perdita di un asset

- La perdita di un asset ha un *impatto*
- La valutazione dell'impatto deve essere fatta analizzando, per quell'asset:
  - valore
  - criticità
  - insostituibilità
  - suo ruolo nel raggiungere obiettivi, mission e business dello stakeholder

Conseguenze

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

Rischio



- La possibilità che azioni o eventi portino a conseguenze che hanno un impatto su uno degli asset dell'organizzazione

[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]

Cyber Risk

- Possibilità di danno (perdita finanziaria, interruzione di servizio o danno reputazionale) subito da una organizzazione a seguito di un malfunzionamento dei suoi sistemi informatici

Cyber Risk

- Il Keynote Speech del prof. Luciano FLORIDI alla conferenza ITASEC21 sulle implicazioni dell'analisi del rischio è scaricabile a questo indirizzo:
  - https://itasec.it/scientific-technical/keynote-speech-luciano-floridi/


ITASEC
KEYNOTE SPEECH
Luciano FLORIDI
University of Oxford

Cyber Risk Assurance

- Analogamente a quanto avviene per gli altri rischi, è oggi possible stipulare polizze assicurative per la copertura dei Cyber Risk residui

Protezione degli asset

- Alla luce di queste considerazioni, si devono progettare *protezioni* appropriate per garantire le prestazioni e l'efficacia del sistema di sicurezza contro la perdita di asset e le relative conseguenze.

Cosa proteggere

Cosa proteggere

- Persone
- Ambiente
- Oggetti
- Computer
- Informazioni
- Cyberspace

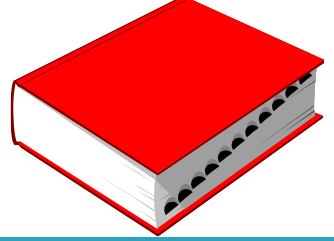
Cosa proteggere

- Persone
- Ambiente

SAFETY

- Oggetti
- Computer
- Informazioni
- Cyberspace

Safety



- Proprietà di un sistema che ne riflette la capacità di funzionare, normalmente o in modo anomalo, senza il rischio di causare lesioni o morte agli esseri umani e senza arrecare danni all'ambiente circostante.

Cosa proteggere

- Persone
- Ambiente

SAFETY

- Oggetti
- Computer
- Informazioni
- Cyberspace

SECURITY

Cosa proteggere

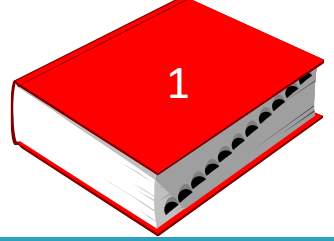
- Persone
- Ambiente

SAFETY

- Oggetti
- Computer
- Informazioni
- Cyberspace

SECURITY

Computer security

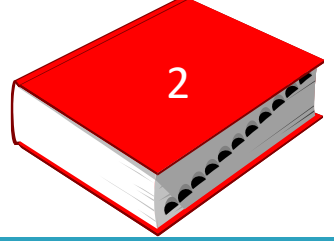


- Si occupa della prevenzione e del rilevamento di azioni *non autorizzate* da parte degli utenti di un sistema informatico

Computer security

- Si occupa della prevenzione e del rilevamento di azioni *non autorizzate* da parte degli utenti di un sistema informatico
- La definizione di *Autorizzazione* è cruciale
- È relativa esclusivamente a una *policy di sicurezza*, che dice chi (o che cosa) possa fare cosa quando

Computer security

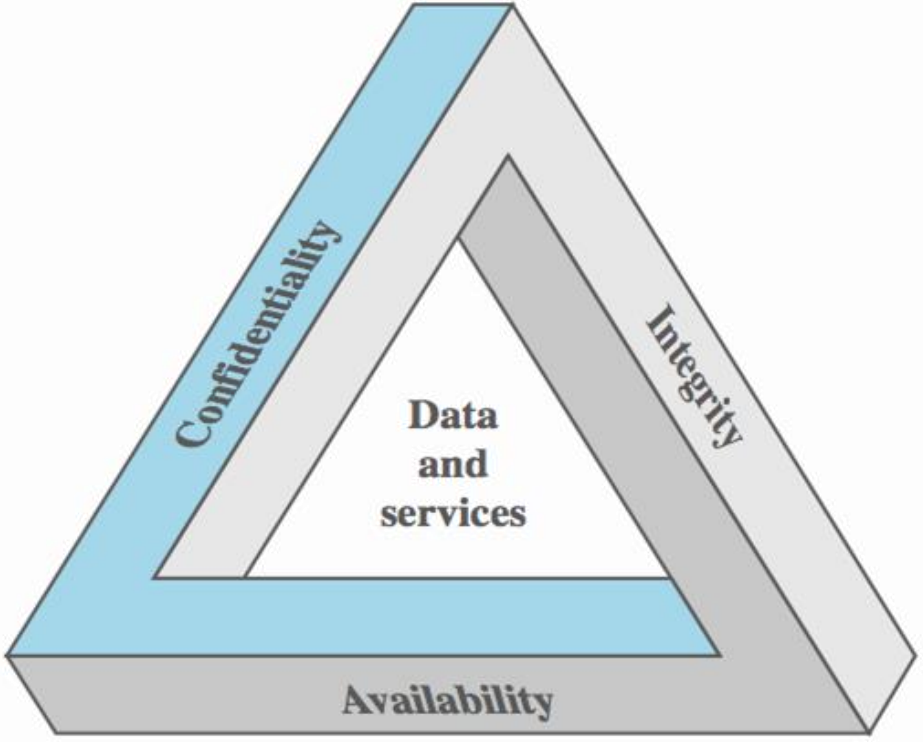


- Insieme di misure e controlli mirate a garantire la *confidenzialità*, *integrità* e *disponibilità* delle risorse di un sistema di elaborazione, incluse hardware, software, firmware e dati in elaborazione, archiviati o trasmessi.

[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

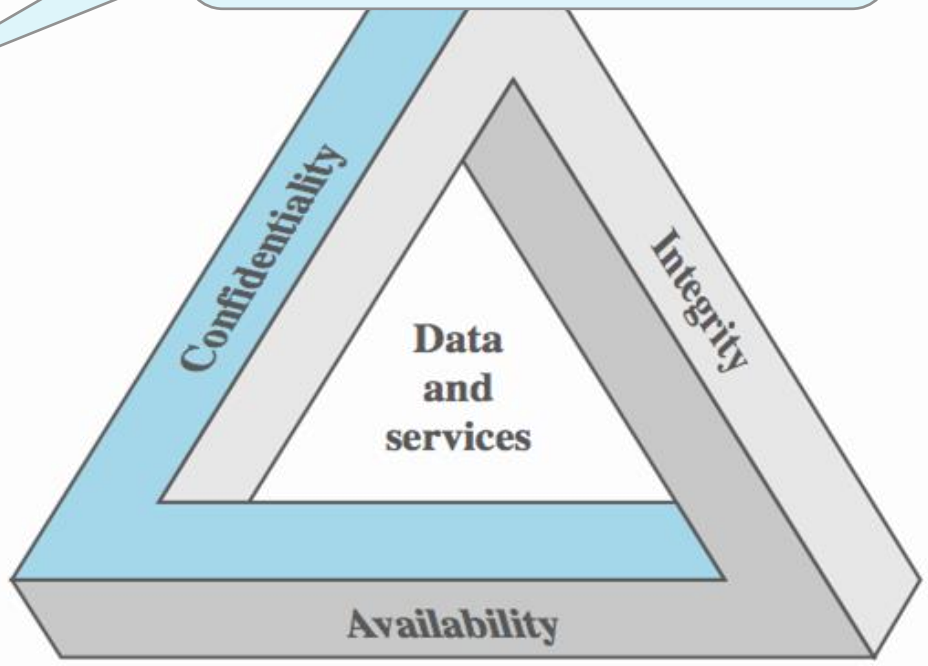
- *Confidenzialità, Integrità, Disponibilità* sono considerati i *pilastri della Security* e formano quella che viene comunemente definita la *triade CIA* (the *CIA Triad*)



La triade CIA

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

Saranno approfonditi nella lezione:
CS_1.03 - I Pilastri della Security



IT vs OT

- Nel seguito ci concentreremo, in particolare, su:
  - *IT - Information Technology*
  - *OT - Operational Technology*

IT vs OT

- Nel seguito ci concentreremo, in particolare, su:
  - *IT - Information Technology*
  - *OT - Operational Technology*

- Si riferisce a tutto ciò che riguarda la tecnologia informatica.
- Si concentra su memorizzazione, recupero, trasmissione, manipolazione e protezione dei dati.

IT vs OT

- Nel seguito ci concentreremo, in particolare, su:
  - *IT - Information Technology*
  - *OT - Operational Technology*

- Si riferisce a tutto ciò che, all'interno di una *azienda,* riguarda la gestione degli aspetti correlati al *monitoraggio* e al *controllo* di dispositivi, apparecchiature, processi ed eventi

Cosa proteggere

- Persone
- Ambiente

SAFETY

- Oggetti
- Computer
- Informazioni
- Cyberspace

SECURITY

Sicurezza delle informazioni

- Le informazioni sono più generali dei dati
- I dati veicolano informazioni
- Le informazioni possono anche essere rivelate senza rivelare dati (ad esempio, tramite riassunti statistici)
- Costituisce un diritto fondamentale: protezione di sé (possesso, ...)

Sicurezza delle informazioni

- Le informazioni vanno protette, indipendentemente dai sistemi informativi dai quali vengono trattate

Cosa proteggere

- Persone
- Ambiente

SAFETY

- Oggetti
- Computer
- Informazioni

SECURITY

- Cyberspace

CYBERSECURITY

Cybersecurity

- Pratica che consente a una entità (organizzazione, cittadino, nazione, …) la protezione dei propri asset fisici e la *confidenzialità*, *integrità* e *disponibilità* delle proprie informazioni dalle minacce che provengono dal *cyberspace.*

[standard ISO/IEC 27000:2014 e ISO/IEC 27032:2012]

Cosa proteggere

- Persone
- Ambiente

SAFETY

- Oggetti
- Computer
- Informazioni
- Cyberspace

SECURITY

Cosa proteggere

- Persone
- Ambiente

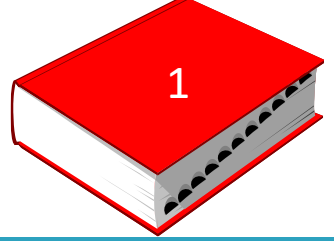
SAFETY

- Oggetti
- Computer
- Informazioni
- Cyberspace

SECURITY

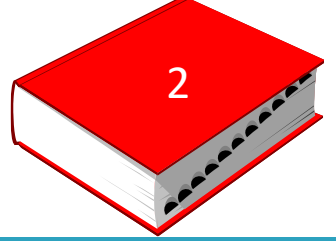
} *DEPENDABILITY*

Dependability



- Proprietà di un sistema che consente di fare affidamento in modo giustificato sul servizio che esso fornisce

Dependability



- La misura in cui si può fare affidamento sul fatto che un determinato sistema esegua esclusivamente e correttamente i compiti definiti, in condizioni operative e ambientali definite, in un determinato periodo o istante di tempo.

["Industrial-Process Measurement and Control - Evaluation of System Properties for the Purpose of System Assessment", Part 5: Assessment of System Dependability, Publication 1069-5, Int'l Electrotechnical Commission (IEC) Secretariat, Feb. 1992]

L’albero della *Dependability*

- Un’esposizione sistematica dei concetti di dependability consiste in tre parti:
  - le *minacce*
  - gli *attributi*
  - i *mezzi* con cui ottenerla

L’albero della *Dependability*

- Un’esposizione sistematica dei concetti di dependability consiste in tre parti:
  - le *minacce*
  - gli *attributi*
  - i *mezzi* con cui ottenerla
- Circostanze *indesiderate* (non *impreviste*) che causano o derivano dalla *undependability* (non si può o non si vuole più fare affidamento sul servizio)

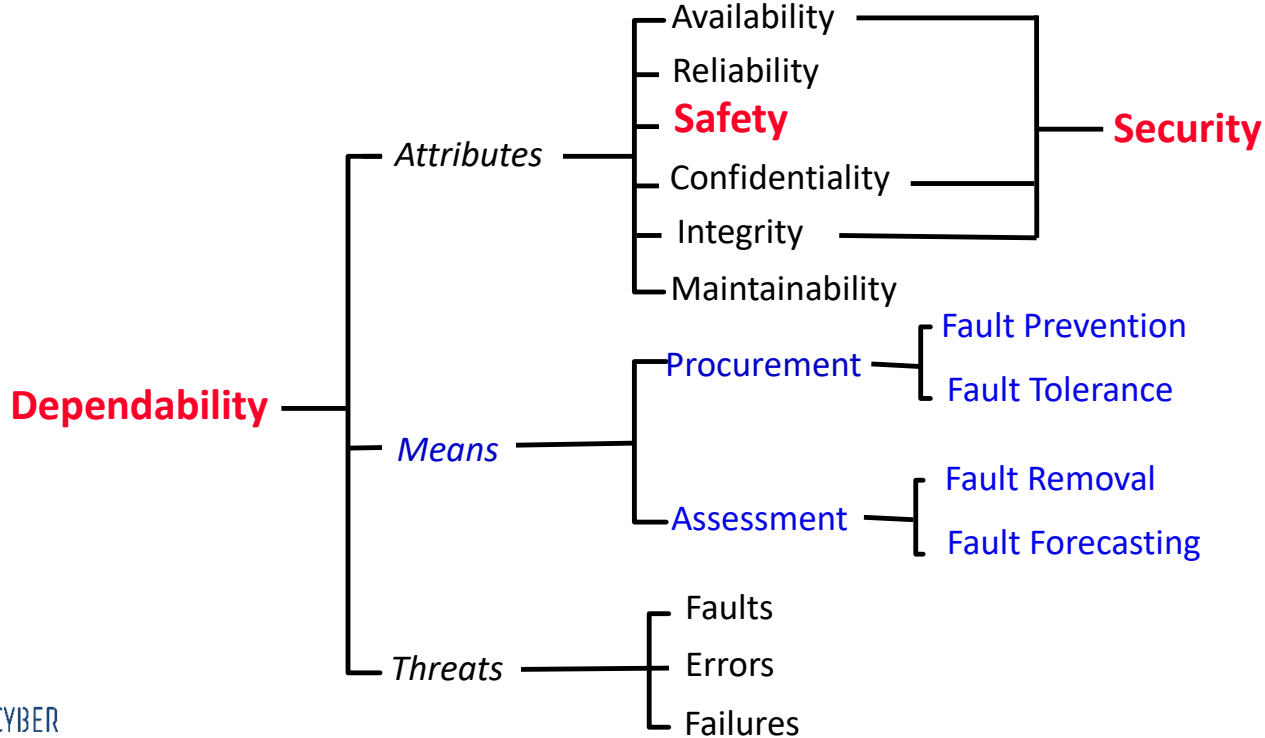
L’albero della *Dependability*

- Un’esposizione sistematica dei concetti di dependability consiste in tre parti:
  - le *minacce*
  - gli *attributi*
  - i *mezzi* con cui ottenerla
- Insieme di proprietà che ci si aspetta dal sistema e in base alle quali se ne valuta la qualità del servizio

L’albero della *Dependability*

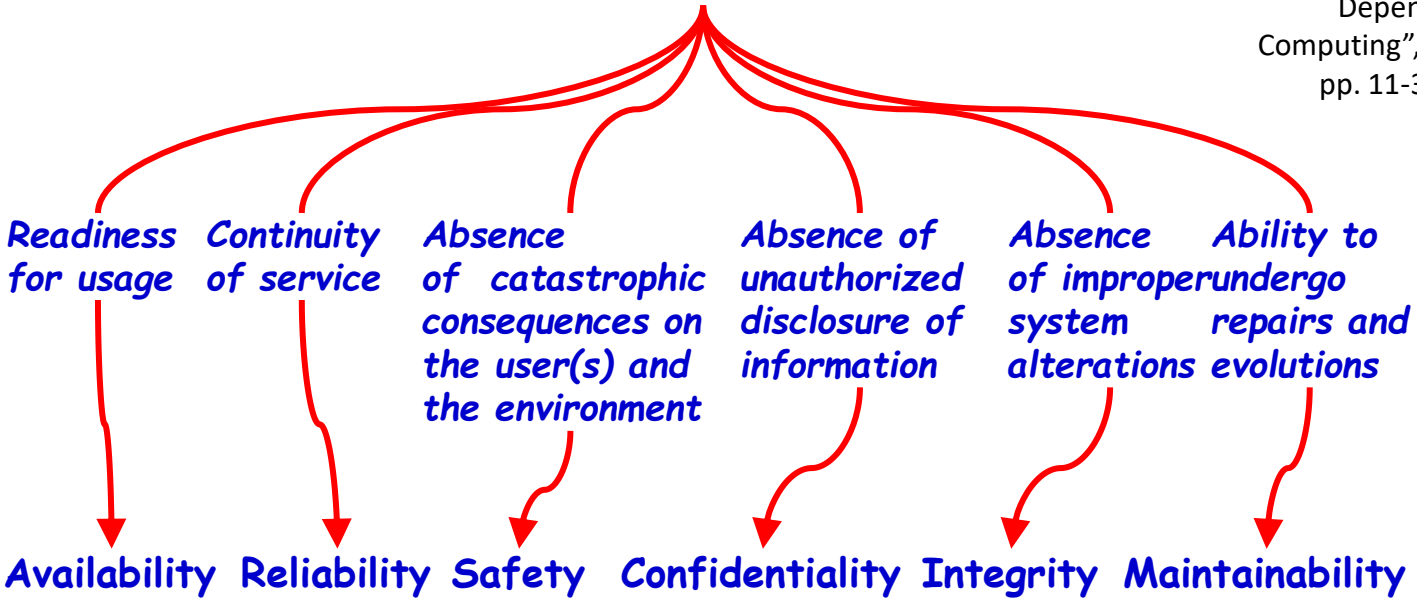
- Un’esposizione sistematica dei concetti di dependability consiste in tre parti:
  - le *minacce*
  - gli *attributi*
  - i *mezzi* con cui ottenerla
- Metodi e tecniche che permettono di:
  - fornire un servizio su cui si può fare affidamento
  - avere fiducia nella sua capacità di fornitura del servizio

L’albero della *Dependability*



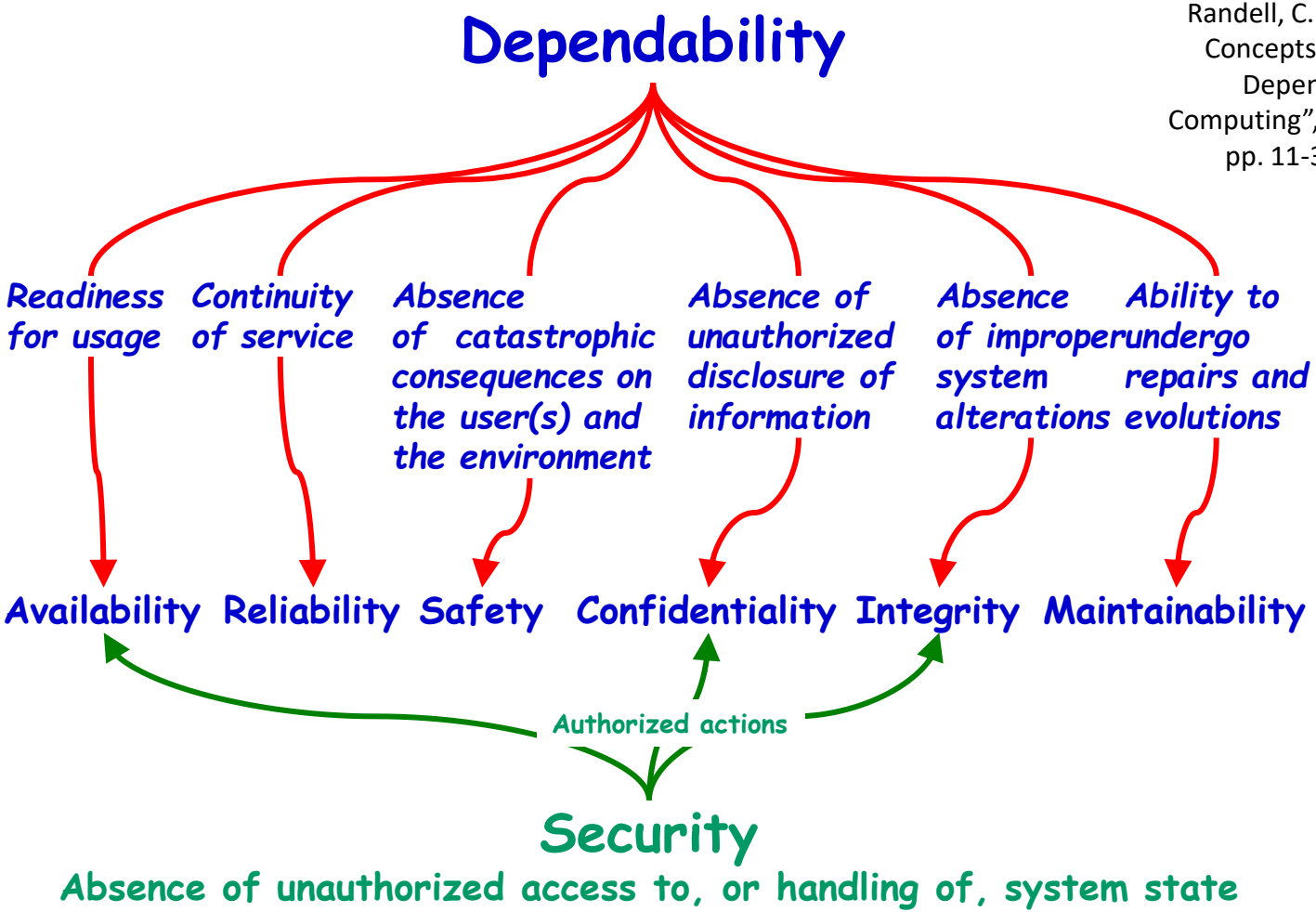
[A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr: “Basic Concepts and Taxonomy of Dependable and Secure Computing”, IEEE TDSC, 1 (1), pp. 11-33, Jan-Mar 2004]

Dependability



[A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr: "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE TDSC, 1 (1), pp. 11-33, Jan-Mar 2004]

[A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr: "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE TDSC, 1 (1), pp. 11-33, Jan-Mar 2004]



Introduzione alla *Sicurezza*

Paolo PRINETTO

Direttore
CINI Cybersecurity
National Laboratory

https://cybersecnatlab.it