SICUREZZA E DIRITTO INFORMATICO

Introduzione

INTRODUZIONE

Inizia qui un percorso didattico
che mira a chiarire aspetti che probabilmente crediamo di conoscere
ma che hanno molti aspetti nascosti.

- Sicurezza di un sistema
- Privacy
- Diritto d'autore
- Reati informatici

ALESSANDRO URSOMANDO

SICUREZZA E DIRITTO INFORMATICO

Sicurezza di un sistema informatico

SICUREZZA DI UN SISTEMA INFORMATICO

Cosa si intende per sicurezza di un sistema informatico?

Chiariamo innanzitutto cosa intendiamo per **sicurezza** e per **sistema informatico**.

ALESSANDRO URSOMANDO

SICUREZZA

IL CONCETTO DI SICUREZZA

TRECCANI

Il fatto di essere sicuro, come condizione che rende e che fa sentire di essere esente da pericoli, o che dà la possibilità di prevenire, eliminare o rendere meno gravi danni, rischi, difficoltà, evenienze spiacevoli e simili.

SICUREZZA

SISTEMA INFORMATICO

IL CONCETTO DI SISTEMA INFORMATICO

TRECCANI

Il fatto di essere sicuro, come condizione che rende e che fa sentire di essere esente da pericoli, o che dà la possibilità di prevenire, eliminare o rendere meno gravi danni, rischi, difficoltà, evenienze spiacevoli e simili.

SICUREZZA

Complesso di hardware e software che gestendo dei dati offre dei servizi agli utenti

SISTEMA INFORMATICO

DIFFERENZA TRA INFORMAZIONE E DATO

Un'**informazione** archiviata in un computer prende il nome di **dato**.

UNA PRIMA DEFINIZIONE

TRECCANI

Il fatto di essere sicuro, come condizione che rende e che fa sentire di essere esente da pericoli, o che dà la possibilità di prevenire, eliminare o rendere meno gravi danni, rischi, difficoltà, evenienze spiacevoli e simili.

SICUREZZA

Complesso di hardware e software che gestendo dei dati offre dei servizi agli utenti

SISTEMA INFORMATICO

Quindi per **sicurezza di un sistema informatico** si intende la **salvaguardia** dei dati che gestisce.

DEFINIZIONE

LA SALVAGUARDIA DEI DATI

Salvaguardare i dati vuol dire occuparsi di **ogni aspetto** della sicurezza:

- ❑ riservatezza
- ❑ integrità
- ❑ disponibilità

A livello internazionale per fare riferimento alla sicurezza in questi termini si usa l'acronimo **CIA:**

Confidentiality (riservatezza)
Integrity (integrità)
Availability (disponibilità).

CIA

La sicurezza che nessuna persona non autorizzata possa arrivare a leggere i dati.

RISERVATEZZA

La sicurezza che i dati non siano stati ne' cancellati, ne' modificati, ne' alterati.

INTEGRITÀ

La sicurezza di poter accedere ai dati 24 ore su 24 e 7 giorni su 7

DISPONIBILITÀ

LA SALVAGUARDIA DEI DATI IN TRASMISSIONE

Salvaguardare i dati vuol dire occuparsi di **ogni aspetto** della sicurezza:

- ❑ riservatezza
- ❑ integrità
- ❑ disponibilità

Una gestione **completa** della sicurezza dei **dati in trasmissione** aggiunge a quanto detto i seguenti aspetti:

- ❑ autenticità
- ❑ non ripudio

La sicurezza che il mittente ed il destinatario siano chi dicono di essere

AUTENTICITÀ

La sicurezza che il mittente ed il destinatario non possano negare di avere rispettivamente spedito e ricevuto il messaggio.

NON RIPUDIO

ALESSANDRO URSOMANDO

PERCHÉ SALVAGUARDARE I DATI?

ALESSANDRO URSOMANDO

PERCHÉ SALVAGUARDARE I DATI?

Perché qualcuno (o qualcosa) potrebbe causare dei danni al sistema .

PERCHÉ SALVAGUARDARE I DATI?

Perché qualcuno (o qualcosa) potrebbe **causare dei danni al sistema** .

compromettere
un aspetto della sicurezza

- ❑ riservatezza
- ❑ integrità
- ❑ disponibilità
- ❑ autenticità
- ❑ non ripudio

PERCHÉ SALVAGUARDARE I DATI?

Perché **qualcuno (o qualcosa)** potrebbe **causare dei danni al sistema** .

- minaccia
  - umana
  - ambientale
- compromettere un aspetto della sicurezza
  - ❑ riservatezza
  - ❑ integrità
  - ❑ disponibilità
  - ❑ autenticità
  - ❑ non ripudio

ALESSANDRO URSOMANDO

PERCHÉ SALVAGUARDARE I DATI?

Perché **qualcuno (o qualcosa)** potrebbe **causare dei danni al sistema** .

- minaccia
  - umana
    - accidentale
    - consapevole
  - ambientale
- compromettere un aspetto della sicurezza
  - ❑ riservatezza
  - ❑ integrità
  - ❑ disponibilità
  - ❑ autenticità
  - ❑ non ripudio

ALESSANDRO URSOMANDO

PERCHÉ SALVAGUARDARE I DATI?

Perché **qualcuno (o qualcosa)** potrebbe **causare dei danni al sistema** .

minaccia

- umana
  - accidentale
  - consapevole
- ambientale

comprometterе un aspetto della sicurezza

- riservatezza
- integrità
- disponibilità
- autenticità
- non ripudio

Una minaccia (umana accidentale, umana consapevole o ambientale) potrebbe compromettere un aspetto della sicurezza.

ALESSANDRO URSOMANDO

DEFINIZIONE DI MINACCIA

Azione umana (accidentale o consapevole) o evento ambientale che **potrebbe** compromettere un aspetto della sicurezza.

MINACCIA

Una minaccia (umana accidentale, umana consapevole o ambientale) potrebbe compromettere un aspetto della sicurezza.

ALESSANDRO URSOMANDO

ESEMPI DI MINACCIA

Azione umana (accidentale o consapevole) o evento ambientale che **potrebbe** compromettere un aspetto della sicurezza.

MINACCIA

- un errore di battitura
- un'omissione in inserimento
- una cancellazione accidentale
- un errore di configurazione
- inciampare in un cavo
- ...

UMANE ACCIDENTALI

- un **attacco** (sniffing, spoofing, virus..)
- una modifica o una cancellazione intenzionale
- ...

UMANE DELIBERATE

- terremoto
- fulmine
- alluvione
- incendio
- black out
- ...

AMBIENTALI

RISCHI DERIVANTI DA MINACCE

Azione umana (accidentale o consapevole) o evento ambientale che **potrebbe** compromettere un aspetto della sicurezza.

MINACCIA

È il danno (potenziale) che si potrebbe avere al verificarsi di una minaccia.

RISCHIO

L'analisi del rischio
è la valutazione
di tutte le possibili minacce
in termini di probabilità di occorrenza
e relativo danno potenziale.

- nessun effetto
- rischio trascurabile
- rischio significativo
- rischio elevato
- rischio catastrofico

CATEGORIE DI RISCHIO

MINACCE E VULNERABILITÀ

Azione umana (accidentale o consapevole) o evento ambientale che **potrebbe** compromettere un aspetto della sicurezza.

MINACCIA

È il danno (potenziale) che si potrebbe avere al verificarsi di una minaccia.

RISCHIO

Per vulnerabilità si intende una **debolezza** di una **risorsa** (un file, un db, una macchina, una connessione, un cavo, ecc.) che può essere sfruttata da una **minaccia**.

VULNERABILITÀ

- ❑ carenza di formazione
- ❑ assenza di un sistema firewall
- ❑ mancanza di un sistema di backup
- ❑ ...

ESEMPI DI VULNERABILITÀ

ALESSANDRO URSOMANDO

SICUREZZA DI UN SISTEMA INFORMATICO

Azione umana (accidentale o consapevole) o evento ambientale che **potrebbe** compromettere un aspetto della sicurezza.

MINACCIA

È il danno (potenziale) che si potrebbe avere al verificarsi di una minaccia.

RISCHIO

Per vulnerabilità si intende una **debolezza** di una **risorsa** (un file, un db, una macchina, una connessione, un cavo, ecc.) che può essere sfruttata da una **minaccia**.

VULNERABILITÀ

Quindi per **sicurezza di un sistema informatico** si intende l'insieme di accorgimenti tecnici e organizzativi (**policy**) volti a ridurre le **vulnerabilità**.

DEFINIZIONE

ALESSANDRO URSOMANDO

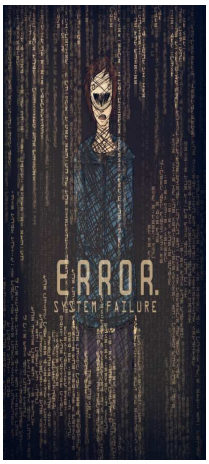
SICUREZZA E DIRITTO INFORMATICO

Attacco ad un sistema informatico

COS'È UN ATTACCO A UN SISTEMA INFORMATICO?

ALESSANDRO URSOMANDO

COS'È UN ATTACCO A UN SISTEMA INFORMATICO?



Un attacco a un sistema informatico
è un'azione umana (consapevole)
volta a compromettere un aspetto della sicurezza.

CHI VIOLA IL SISTEMA ?

CHI VIOLA IL SISTEMA ?

Un attacco a un sistema informatico è un'azione umana (consapevole) volta a compromettere un aspetto della sicurezza.

Se chi effettua l'attacco ha lo scopo di creare un **danno** al sistema, magari con l'obiettivo finale di trarre **profitto**, allora questi è un **criminale informatico**.

Se chi viola il sistema lo fa per **testare** le proprie capacità o le misure di sicurezza allora questi è un **hacker**.

ALESSANDRO URSOMANDO

HACKER

Se da un punto di vista **morale**, la **differenza** tra hacker e criminale informatico è **enorme** da un punto di vista **legale** in molti casi **non c'è** differenza.

Se l'hacker viola il sistema su **richiesta** dell'azienda proprietaria del sistema o se **informa** i responsabili della sicurezza della stessa azienda allora egli potrebbe anche ricevere una **proposta di lavoro**, in caso contrario l'hacker agli occhi della legge è un **criminale informatico**.

ALESSANDRO URSOMANDO

TECNICHE DI ATTACCO

- Sniffing
- Spoofing
- Denial of Service
- Spamming
- Phishing
- Nuking
- Malware

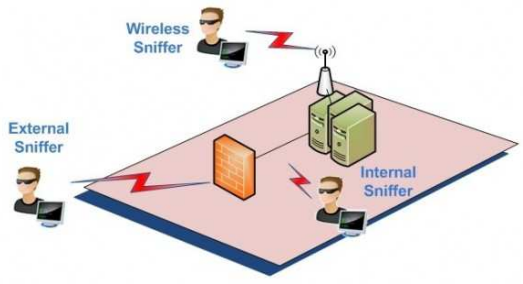
Un attacco a un sistema informatico
è un'azione umana (consapevole)
volta a compromettere un aspetto della sicurezza.

Ma quali sono le tecniche di attacco ?

SNIFFING

- Sniffing
- Spoofing
- Denial of Service
- Spamming
- Phishing
- Nuking
- Malware

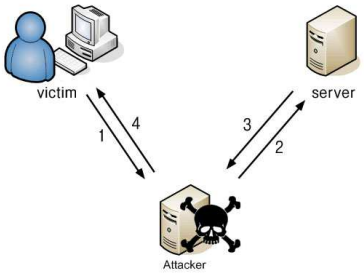
Il criminale informatico **ascolta** il canale
con lo scopo di leggere i dati che passano (riservatezza).



SPOOFING

- Sniffing
- **Spoofing**
- Denial of Service
- Spamming
- Phishing
- Nuking
- Malware

Il criminale informatico
si **intromette** in una comunicazione tra due **host**
sostituendosi ad uno dei due
(autenticità, riservatezza e integrità).

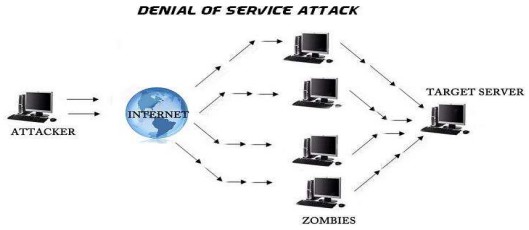


DENIAL OF SERVICE

- Sniffing
- Spoofing
- **Denial of Service**
- Spamming
- Phishing
- Nuking
- Malware

Il criminale informatico
è capace di indurre alcuni host (detti **zombie**)
ad eseguire dei normalissimi **accessi** WEB.

Facendo eseguire a tutti gli zombie sotto il suo controllo
la richiesta di una certa pagina WEB,
mette il server in condizione di **non soddisfare** più le richieste
dei suoi utenti normali (disponibilità).



SPAMMING

- Sniffing
- Spoofing
- Denial of Service
- Spamming
- Phishing
- Nuking
- Malware

Consiste nell'invio di messaggi **indesiderati**.
Tali messaggi possono arrivare via **email**,
via chat, via sms o possono anche trovarsi nei forum.
L'uso più pericoloso (e più frequente) che si fa dello spam
è per pubblicizzare materiale **pornografico** o **illegale**
e per veicolare tentativi di **truffa** (riservatezza).

PHISHING

- Sniffing
- Spoofing
- Denial of Service
- Spamming
- Phishing
- Nuking
- Malware

È una tecnica con la quale si cerca di
ingannare la vittima
convincendola a fornire i **dati** per accedere
al **conto corrente** o alla **carta di credito**.
(riservatezza).


Security & Safety | Posteitaliane
Sicurezza Logica

Egregio Cliente,

La preghiamo di esaminare con la massima serietà e immediatamente questo messaggio di posta elettronica che mostra le nuove misure di sicurezza.

Il reparto sicurezzo della nostra bance le notifica che sono state prese misure per accrescere il livello di sicurezza dell'online banking, in relazione ai frequenti tentativi di accedere illegalmente ai conti bancari.

Per ottenere l'accesso alla versione piu sicura dell'area clienti preghiamo di dare la sua autorizzazione.

Accedi ai servizi online »

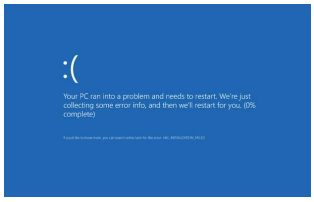
Se scegliete di ignorare la nostra richiesta, purtroppo non avremo altra scelta che bloccare temporaneamente il suo account.

Distinti saluti,
BancoPostaonline

NUKING

- Sniffing
- Spoofing
- Denial of Service
- Spamming
- Phishing
- Nuking
- Malware

Un nuke è un **attacco generico** che sfrutta un **bug** del **sistema** in uso sulla macchina della vittima. Per portare a segno un nuke, il criminale informatico deve conoscere **l'indirizzo IP** della macchina della vittima (riservatezza e integrità).



MALWARE

- Sniffing
- Spoofing
- Denial of Service
- Spamming
- Phishing
- Nuking
- Malware

Con il termine malware si intende un qualsiasi **mal**icious soft**ware**.

MALWARE

- Virus
- Worm
- Trojan Horse
- Rouge antispyware
- Backdoor
- Adware
- Spyware
- Hijack
- Keylogger

Con il termine malware si intende un qualsiasi **mal**icious soft**ware**.

VIRUS

- Virus
- Worm
- Trojan Horse
- Rouge antispyware
- Backdoor
- Adware
- Spyware
- Hijack
- Keylogger

I virus si possono nascondere **ovunque**.
I virus **di file** sono codici malware che si agganciano (o sostituiscono) a file eseguibili.

I virus **di boot** si installano nel settore zero di un disco sostituendosi al software che il computer lancia all'avvio del sistema.

I virus che si installano nella **RAM** infettano tutti i processi in esecuzione.

WORM

- Virus
- **Worm**
- Trojan Horse
- Rouge antispyware
- Backdoor
- Adware
- Spyware
- Hijack
- Keylogger

I worm (più o meno come i **rabbit**)
hanno l'obiettivo di **saturare il sistema**.

Possono essere sia dei **processi**
(con l'intenzione di occupare tutta la **RAM**)
sia dei **file** (con l'obiettivo di esaurire lo spazio su **disco**).

Inoltre possono avere lo scopo di attaccare le comunicazioni
inviando **pacchetti** fasulli o **e-mail** fasulle
fino a saturare il rispettivo **server**.

TROJAN HORSE

- Virus
- Worm
- **Trojan Horse**
- Rouge antispyware
- Backdoor
- Adware
- Spyware
- Hijack
- Keylogger

Un **trojan horse** (o cavallo di troia)
è un malware che entra nella macchina
spacciandosi per software benevolo
e una volta avviato
– sebbene **apparentemente** pare non faccia nulla –
mette la macchina **completamente** nelle mani dell'attaccante
(zombie, backdoor, adware, spyware, hijack, keylogger,…)

ROUGE ANTISPYWARE

- Virus
- Worm
- Trojan Horse
- **Rouge antispyware**
- Backdoor
- Adware
- Spyware
- Hijack
- Keylogger

Un esempio di trojan è il rouge antispyware.

Questa tecnica induce l'utente a scaricare ed installare un software che poi si rivelerà un malware.

La tecnica consiste nell'offrire una **scansione** (fasulla) via web del sistema, nell'allarmare l'utente palesando una **situazione di pericolo** e nell'induzione a scaricare il programma per "**pulire**" il sistema.

BACKDOOR

- Virus
- Worm
- Trojan Horse
- Rouge antispyware
- **Backdoor**
- Adware
- Spyware
- Hijack
- Keylogger

Una **backdoor** è una porta di servizio, ovvero un **accesso riservato** ad una certa macchina.

Il proprietario della macchina **non è a conoscenza** di tale ingresso nascosto a qualsiasi funzionalità del suo sistema.

Tipicamente viene attivata in modo **inconsapevole** dall'utente stesso, ma si può anche attivare di persona.

ADWARE

- Virus
- Worm
- Trojan Horse
- Rouge antispyware
- Backdoor
- **Adware**
- Spyware
- Hijack
- Keylogger

Un **Adware** (advertisement software) è per definizione un software che contiene delle **pubblicità**: l'utente non paga il software perché guarda le pubblicità.

Le attività di un tale tipo di software però possono diventare invadenti ed eccessive fino a rendere impossibile la navigazione o compromettere le prestazioni del sistema: in questo caso si parla di malware.

SPYWARE

- Virus
- Worm
- Trojan Horse
- Rouge antispyware
- Backdoor
- Adware
- **Spyware**
- Hijack
- Keylogger

Uno spyware è un altro malware che entra nel sistema spacciandosi per software **benevolo**.
L'obiettivo di uno spyware è quello di ottenere **informazioni** dalla macchina attaccata.

L'utilizzatore di uno spyware sa bene che i dati più interessanti si trovano nei **cookie** (file che contengono le informazioni inserite in un browser).

HIJACK

- Virus
- Worm
- Trojan Horse
- Rouge antispyware
- Backdoor
- Adware
- Spyware
- **Hijack**
- Keylogger

L'hijacking è un malware
che si aggancia ad un browser
dirottando la navigazione dell'utente
su alcune **pagine prestabilite**
in modo tale da incrementare in modo artificioso
le visite ed aumentare di conseguenza i guadagni
dovuti alle inserzioni pubblicitarie.

KEYLOGGER

- Virus
- Worm
- Trojan Horse
- Rouge antispyware
- Backdoor
- Adware
- Spyware
- Hijack
- **Keylogger**

Un **keylogger** è uno strumento
(sia software che hardware) in grado di intercettare
(e quindi salvare e spedire via internet)
tutto quanto digitato sulla **tastiera**.

Evidentemente un tale malware è interessato alle **password**.

SICUREZZA E DIRITTO INFORMATICO

Sistema di difesa

COSA SI INTENDE PER SISTEMA DI DIFESA?

COSA SI INTENDE PER SISTEMA DI DIFESA?

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

Un **sistema di difesa** di un sistema informatico
è quel complesso di accorgimenti tecnici e organizzativi (**policy**)
da mettere in atto
per ridurre le **vulnerabilità** di un sistema.

ALESSANDRO URSOMANDO

RIDONDANZA DEGLI APPARATI

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

Duplicare qualsiasi parte del sistema
(alimentazione, hard disk, ecc.)
riduce le vulnerabilità relative a minacce ambientali
tutelando integrità e affidabilità.

ALESSANDRO URSOMANDO

RIDONDANZA DEGLI APPARATI E BACKUP

- **Ridondanza degli apparati**
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

Duplicare qualsiasi parte del sistema (alimentazione, hard disk, ecc.) riduce le vulnerabilità relative a minacce ambientali tutelando integrità e affidabilità.

Duplicando una risorsa che contiene **dati**, implicitamente duplichiamo anche i dati.

La gestione organizzata della duplicazione dei dati si chiama **backup** e rappresenta la policy più diffusa.

La copia dei dati può avvenire in **locale** (mirroring) o in **remoto** (NAS, cloud o altre soluzioni).

ALESSANDRO URSOMANDO

ANTIVIRUS

- Ridondanza degli apparati
- **Antivirus**
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

L'antivirus è un **software** che gira **sempre** su un sistema per evitare che lo stesso possa essere infettato da **malware**. In questo modo si tentano di arginare le minacce di malintenzionati che potrebbero attaccare il sistema con lo scopo di acquisire informazioni (**riservatezza**) o compromettere l'utilizzo (**integrità** e **affidabilità**).

ALESSANDRO URSOMANDO

FIREWALL

- Ridondanza degli apparati
- Antivirus
- **Firewall**
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

Il **firewall** è un filtro
che osserva tutto ciò che **entra** in un sistema
provvedendo a intercettare possibili minacce (tipo **malware**).

Un firewall può anche governare il traffico **in uscita** dal sistema
qualora ci siano delle **policy** che lo richiedano.

Un **personal firewall** agisce su un singolo calcolatore
ed è ovviamente un software;
un **firewall di rete** invece sovrintende alla gestione di una LAN
e spesso coincide con un dispositivo apposito.

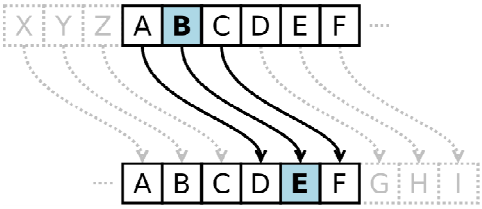
CRITTOGRAFIA

- Ridondanza degli apparati
- Antivirus
- Firewall
- **Crittografia**
- Firma digitale
- Sistema di autenticazione
- Proxy

La crittografia entra in gioco quando
siamo interessati alla sicurezza nell'ambito delle **trasmissioni**.

Quando vogliamo garantire **autenticità** e/o **non ripudio**
(di mittente e destinatario) o la **riservatezza** e **l'integrità** di dati
che vengono veicolati su un **mezzo non sicuro**.

Il Cifrario di Cesare è il più antico
(e il più semplice)
sistema di crittografia mai esistito.

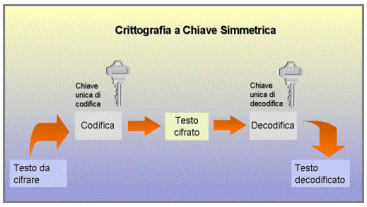


CRITTOGRAFIA SIMMETRICA

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

La **crittografia simmetrica** è detta anche a **chiave privata** o a chiave segreta.

Mittente e destinatario conoscono la **chiave** e la usano per **cifrare** e **decifrare**.



Il suo problema è la necessità di **scambiarsi** la chiave

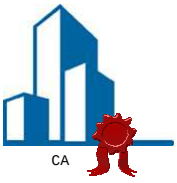
ALESSANDRO URSOMANDO

CRITTOGRAFIA ASIMMETRICA

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

La **crittografia asimmetrica** è detta anche a **chiave pubblica**.

La crittografia asimmetrica si basa sulla presenza di una **Certification Authority** che garantisce il funzionamento del meccanismo.

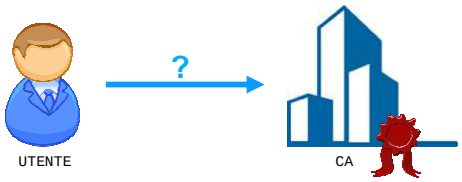


ALESSANDRO URSOMANDO

CRITTOGRAFIA ASIMMETRICA

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

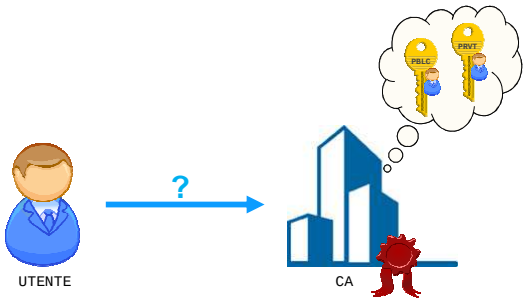
Un **utente**
interessato a proteggere i dati che invia/riceve
(una banca, un'istituzione pubblica, un servizio online, ..)
si rivolge alla **Certification Authority**



CRITTOGRAFIA ASIMMETRICA

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

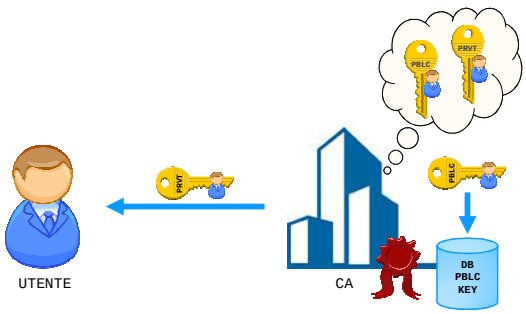
Tale **CA** produce una **coppia di chiavi**,
una **pubblica** (o **diretta**) e l'altra **privata** (o **inversa**)



CRITTOGRAFIA ASIMMETRICA

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

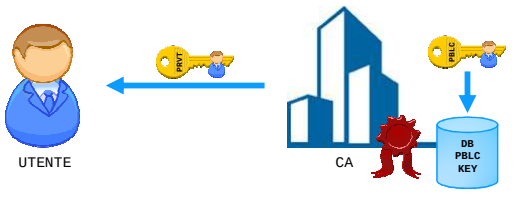
Tale **CA** produce una **coppia di chiavi**, una **pubblica** (o **diretta**) e l'altra **privata** (o **inversa**): poi fornisce quella privata all'utente e rende disponibile a tutti quella pubblica.



CRITTOGRAFIA ASIMMETRICA

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

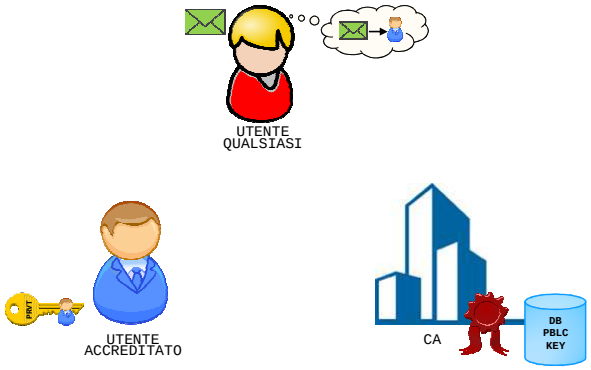
Tutto ciò che viene **cifrato** con una delle due chiavi può essere **decifrato** solo usando l'altra chiave.



CRITTOGRAFIA ASIMMETRICA: UN ESEMPIO D'USO

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

Tutto ciò che viene **cifrato** con una delle due chiavi può essere **decifrato** solo usando l'altra chiave.



CRITTOGRAFIA ASIMMETRICA: UN ESEMPIO D'USO

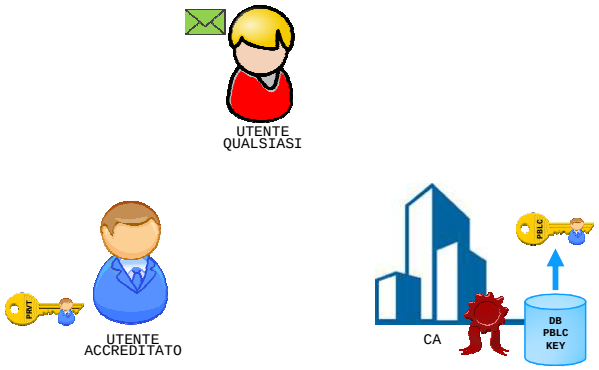
- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

Tutto ciò che viene **cifrato** con una delle due chiavi può essere **decifrato** solo usando l'altra chiave.

CRITTOGRAFIA ASIMMETRICA: UN ESEMPIO D'USO

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

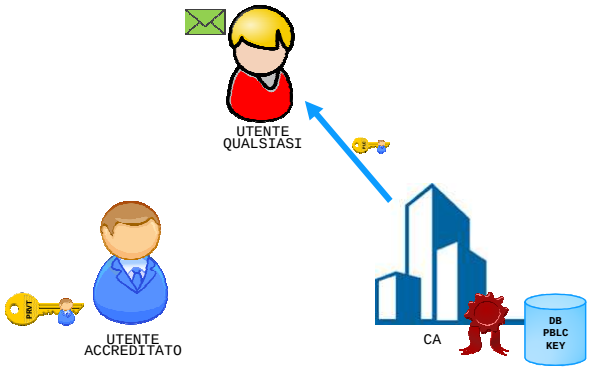
Tutto ciò che viene **cifrato** con una delle due chiavi può essere **decifrato** solo usando l'altra chiave.



CRITTOGRAFIA ASIMMETRICA: UN ESEMPIO D'USO

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

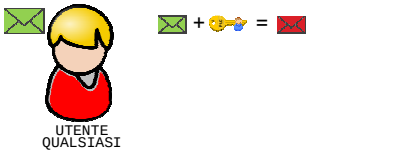
Tutto ciò che viene **cifrato** con una delle due chiavi può essere **decifrato** solo usando l'altra chiave.

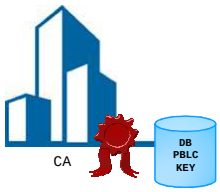


CRITTOGRAFIA ASIMMETRICA: UN ESEMPIO D'USO

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

Tutto ciò che viene **cifrato** con una delle due chiavi può essere **decifrato** solo usando l'altra chiave.

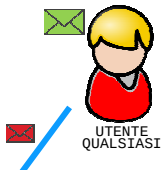


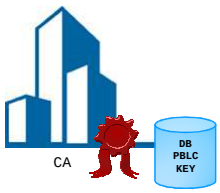


CRITTOGRAFIA ASIMMETRICA: UN ESEMPIO D'USO

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

Tutto ciò che viene **cifrato** con una delle due chiavi può essere **decifrato** solo usando l'altra chiave.

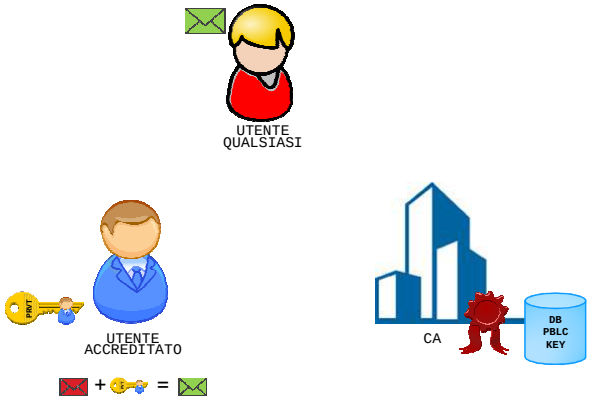




CRITTOGRAFIA ASIMMETRICA: UN ESEMPIO D'USO

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

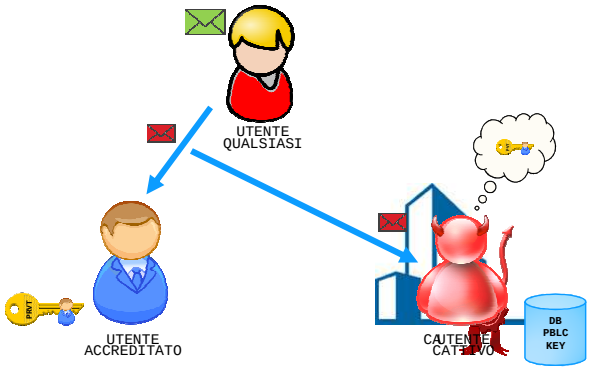
Tutto ciò che viene **cifrato** con una delle due chiavi può essere **decifrato** solo usando l'altra chiave.



CRITTOGRAFIA ASIMMETRICA: UN ESEMPIO D'USO

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

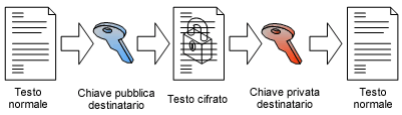
Tutto ciò che viene **cifrato** con una delle due chiavi può essere **decifrato** solo usando l'altra chiave.



CRITTOGRAFIA ASIMMETRICA

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

Tale **CA** produce una **coppia di chiavi**, una **pubblica** (o **diretta**) e l'altra **privata** (o **inversa**): poi fornisce quella privata all'utente e rende disponibile a tutti quella pubblica.



FIRMA DIGITALE

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

La **firma digitale**, per la legge italiana, è un particolare tipo di **firma elettronica** basata su un sistema di **crittografia asimmetrica**.

Il **mittente** spedisce il messaggio (in chiaro) e il **fingerprint** codificato con la sua **chiave privata**.

Il **fingerprint** è un riassunto del messaggio da spedire prodotto con una funzione **one-way hash.**

Il **destinatario** decodifica la firma con la chiave pubblica e confronta con il fingerprint per verificare **l'autenticità del mittente**.

SISTEMA DI AUTENTICAZIONE

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- **Sistema di autenticazione**
- Proxy

L'obiettivo di un **sistema di autenticazione** è quello di stabilire **l'identità digitale** dell'utente.

Il processo di autenticazione prevede la specifica di:
un nome utente
e uno o più fattori di questo tipo:
qualcosa che si conosce (password, PIN, ecc.)
qualcosa che si ha (card, ..)
qualcosa che si è (impronta digitale, impronta vocale,..)

ALESSANDRO URSOMANDO

SISTEMA DI AUTENTICAZIONE: PASSWORD

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- **Sistema di autenticazione**
- Proxy

Nel 99% dei casi il processo di autenticazione avviene mediante l'inserimento nel sistema di:
nome utente + **password**.

Come si sceglie una buona password?

Come si usa la password?

ALESSANDRO URSOMANDO

SISTEMA DI AUTENTICAZIONE: PASSWORD

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- **Sistema di autenticazione**
- Proxy

Come si sceglie una buona password?

Ecco un elenco di buone regole:

1) non usare '123456' ne' tantomeno 'password'
2) lunghezza di almeno 8 caratteri
3) coinvolgere maiuscole, minuscole, simboli e numeri
4) parole senza senso (in qualsiasi lingua)
5) non partire da date di nascita (tue o di altri)
6) non partire da nomi o soprannomi (tuoi o di altri)

ALESSANDRO URSOMANDO

SISTEMA DI AUTENTICAZIONE: PASSWORD

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- **Sistema di autenticazione**
- Proxy

Come si usa la password?

Ecco un elenco di buone regole:

1) cambiare la password ogni 3 o 6 mesi
2) non usare la stessa password per account diversi
3) non salvare la password nel browser
4) inserire la password solo in siti con protocollo **https**

ALESSANDRO URSOMANDO

SISTEMA DI AUTENTICAZIONE: PASSWORD

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

SISTEMA DI AUTENTICAZIONE: PASSWORD

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

Il prof. **Ursomando** suggerisce di:

Inventare un **algoritmo** che sia facile da eseguire
ogni volta a mente
e che produca una password che rispetti tutte le regole viste.

Facciamo un **esempio**.

SISTEMA DI AUTENTICAZIONE: PASSWORD

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- **Sistema di autenticazione**
- Proxy

Cominciamo con le prime lettere delle parole di una frase di una canzone che mi piace:

"E nell'aria ancora il tuo profumo dolce splendido.."

E	N	A	A	I	T	P	D	S

Codifico le doppie (o triple) con i numeri.

E	N	2	A	I	T	P	D	S

Cambio le A in 4, le E in 3, le I in 1

3	N	2	4	1	T	P	D	S

ALESSANDRO URSOMANDO

SISTEMA DI AUTENTICAZIONE: PASSWORD

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- **Sistema di autenticazione**
- Proxy

3	N	2	4	1	T	P	D	S

Sostituisco al primo numero la prima lettera del sito o servizio ed al secondo numero l'ultima lettera.

Se sto codificando la password per paypal:

P	N	A	4	1	T	P	D	S

Tra sei mesi potrei invertire le ultime due lettere e tra altri sei mesi rimetterle a posto.

ALESSANDRO URSOMANDO

PROXY

- Ridondanza degli apparati
- Antivirus
- Firewall
- Crittografia
- Firma digitale
- Sistema di autenticazione
- Proxy

Un **proxy server** è una macchina che intercetta
tutte le richieste **TCP/IP**
da una macchina della rete verso l'esterno
si assicura che tali richieste
rispettino le **policy** di sicurezza in essere sulla rete
ed eventualmente **inoltra** la richiesta all'esterno a suo nome
consegnando poi a chi ne aveva fatto richiesta
le **risorse** ottenute opportunamente **verificate**.

ALESSANDRO URSOMANDO

SICUREZZA E DIRITTO INFORMATICO

Privacy

COSA SI INTENDE PER IDENTITÀ

COSA SI INTENDE PER IDENTITÀ

L'identità è **l'insieme delle caratteristiche** che rendono qualcuno ciò che è **distinguendolo** da tutti gli altri.

COSA SI INTENDE PER IDENTITÀ DIGITALE?

COSA SI INTENDE PER IDENTITÀ DIGITALE?

L'identità è **l'insieme delle caratteristiche** che rendono qualcuno ciò che è **distinguendolo** da tutti gli altri.

L'identità digitale è **l'insieme delle informazioni** presenti **online** relative ad un **soggetto**.

- persona fisica
- ente
- azienda
- software
- sistema informatico

http://www.youtube.com/watch?v=F7pYHN9iC9I

IDENTITÀ DIGITALE E WEB-REPUTATION

- persona fisica
- ente
- azienda
- software
- sistema informatico

L'identità è **l'insieme delle caratteristiche** che rendono qualcuno ciò che è **distinguendolo** da tutti gli altri.

L'identità digitale è **l'insieme delle informazioni** presenti **online** relative ad un **soggetto**.

La **web-reputation** è **l'immagine** che un utente si può fare di un **soggetto** a partire dalle **informazioni** su di esso presenti **online**.

Internet ricorda tutto e già oggi esistono in rete **sistemi per il monitoraggio** e per la **modifica** della web-reputation.

ALESSANDRO URSOMANDO

DATI PERSONALI

Dati identificativi

Dati sensibili

Dati giudiziari

- nome
- cognome
- immagini
- filmati
- ...

- religione
- voto
- malattie
- geo-localizz.
- ...

- divieti
- obblighi
- ...

I **dati identificativi** sono quelli che permettono **l'indicazione diretta**.

I **dati sensibili** sono quelli che possono rilevare:
l'origine razziale ed etnica;
le convinzioni religiose, filosofiche o di altro genere;
l'adesione a partiti, sindacati o altre organizzazioni,
lo stato di salute;
la vita sessuale;
i luoghi frequentati; ecc.

I **dati giudiziari** sono quelli che riguardano l'esistenza di determinati provvedimenti giudiziari o la qualità di indagato o di imputato.

ALESSANDRO URSOMANDO

TRATTAMENTO DEI DATI PERSONALI

"Chiunque cagiona danno ad altri per effetto del **trattamento** dei **dati personali** è tenuto al risarcimento." (art. 2050 – codice civile)

Ecco perché
passiamo parte della nostra vita
a cliccare su "**accetto**"
o firmando il **consenso**
al trattamento dei nostri dati.

Ed ecco perché è nato il
Garante per la Privacy.

- dati identificativi
- dati sensibili
- dati giudiziari

- raccolta
- conservazione
- elaborazione
- modifica
- collegamento
- confronto
- diffusione
- ...

ALESSANDRO URSOMANDO

IL GARANTE PER LA PRIVACY

Il **garante per la privacy** tutela il **cittadino**
mettendolo in guardia da **comportamenti pericolosi**.

http://www.garanteprivacy.it

http://www.youtube.com/watch?v=BqtnYcfgLbM

ALESSANDRO URSOMANDO

IL GARANTE PER LA PRIVACY

Il **garante per la privacy** tutela il **cittadino** mettendolo in guardia da **comportamenti pericolosi**.

Il garante per la privacy
(vero nome: **garante per la tutela dei dati personali**)
è un organo **collegiale** di 5 persone elette dal Parlamento
che restano in carica per 7 anni (carica non rinnovabile).

La **privacy** è un insieme di norme create per **garantire** che il trattamento dei dati si svolga secondo il pieno **rispetto** dei **diritti** e delle **libertà** fondamentali di ogni individuo.

Il diritto che i propri dati vengano trattati secondo specifiche misure di protezione e sicurezza

Il diritto di accedere, aggiornare, rettificare, cancellare i dati che ci riguardano

Il diritto di opposizione per motivi legittimi o per finalità commerciali

ALESSANDRO URSOMANDO

SICUREZZA E DIRITTO INFORMATICO

Diritto d'autore

DIRITTO D'AUTORE

DIRITTO D'AUTORE

Con la locuzione
diritto d'autore
si intende
fare riferimento al complesso di
ordinamenti nazionali e
convezioni internazionali
che governano
la posizione giuridica
di un **autore**
di **un'opera dell'ingegno**.

DIRITTO D'AUTORE

1700

Mecenatismo

1980

2001

DIRITTO D'AUTORE

1700

Mecenatismo

Copyright e droit d'auter

1980

2001

DIRITTO D'AUTORE

1700 Mecenatismo

1980 Copyright e droit d'auter

Copyleft

2001

DIRITTO D'AUTORE

1700 Mecenatismo

1980 Copyright e droit d'auter

Copyleft

2001 Creative Commons

MECENATISMO

MECENATISMO

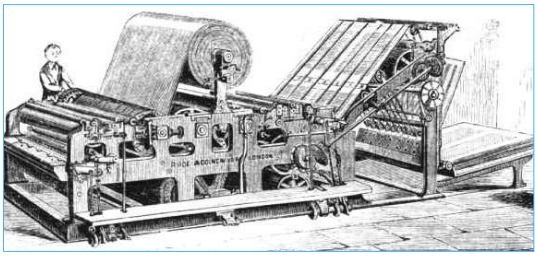
Mecenate (68 A.C.) era un uomo ricco e potente che finanziava l'attività artistica di Orazio, Virgilio e tanti altri.

Da qui il nome dell'attività dei vari sovrani che nel tempo si sono circondati di **artisti** di ogni genere.

L'artista quindi non ricavava proventi dalla sua **opera**, ma solo **prestigio**.
Quel prestigio che gli garantiva incarichi ben retribuiti.

COPYRIGHT E DROIT D'AUTER

Con l'avvento della **stampa** la copia di un opera non era più destinata a rimanere appannaggio di pochi eletti ma si apprestava all'uso di **massa**.



Nacque la figura dell'**editore** che era colui il quale traeva beneficio **economico** dalla **distribuzione** dell'opera.

ALESSANDRO URSOMANDO

COPYRIGHT E DROIT D'AUTER

Al verificarsi delle prime **controversie** si verificò l'esigenza di una **regolamentazione** del rapporto tra **autore** ed **editore**.

Il primo intervento (1500) fu del governo **inglese** che produsse una legge per il "**copyright**".
Molto successivamente (1600) in **Francia** si legiferò in merito al "**droit d'auter**"

ALESSANDRO URSOMANDO

ABBIAMO GIÀ DETTO CHE OGGI..

Con la locuzione
diritto d'autore
si intende
fare riferimento al complesso di
ordinamenti nazionali e
convezioni internazionali
che governano
la posizione giuridica
di un **autore**
di **un'opera dell'ingegno**.

OGGETTO DELLA REGOLAMENTAZIONE

Oggi i diritti connessi alla produzione di un'opera
di ingegno sono il **diritto morale**
ed il **diritto di utilizzazione economica**.

- paternità
- integrità

La giurisprudenza **mondiale** riconosce questi diritti
all'autore, il quale ha facoltà di **trattenerli, cederli** a qualcuno
(dietro compenso o meno) o **rinunciarvi**.

- riproduzione
- esecuzione
- diffusione
- distribuzione
- elaborazione

ENTI PREPOSTI

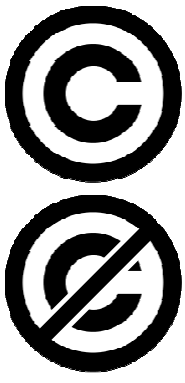
In Italia la **SIAE**
(Società Italiana Autori ed Editori)
è l'ente che gestisce i rapporti tra **autori**, **editori** e **fruitori** delle opere dell'ingegno.

COPYRIGHT E PUBBLICO DOMINIO

Oggi, con copyright
si intende che **tutti** i diritti relativi all'opera
in questione sono riservati.

La legge vigente oggi in Italia
prevede che i diritti su un opera dell'ingegno
continuino a restare riservati
fino a **70 anni** dopo la morte dell'autore.

Trascorso tale periodo l'opera
è da considerarsi di **dominio pubblico.**



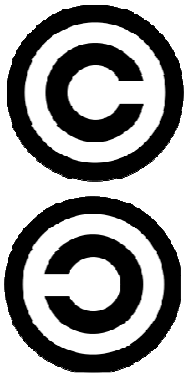
COPYLEFT

COPYLEFT

Il concetto di **copyleft** nasce in contrapposizione a quello di **copyright**.

right: diritto
right: destra

left: sinistra
left: lasciato



COPYLEFT

L'opera può essere **utilizzata**, **modificata** e **diffusa** liberamente ma sempre in regime di **copyleft**

Nasce nell'ambito dello **sviluppo software**.

Spesso, all'inizio, il movimento del copyleft veniva confuso con la **pirateria**.

ALESSANDRO URSOMANDO

COPYLEFT

Il personaggio simbolo del movimento copyleft è **Richard Stallman** che ha inaugurato il filone del **software libero** e del software **open source**, che ha guidato lo sviluppo del progetto **GNU** e che ha ideato la licenza **GPL**.

Vediamo cosa ho detto.

ALESSANDRO URSOMANDO

FREE SOFTWARE

Il personaggio simbolo del movimento copyleft è **Richard Stallman** che ha inaugurato il filone del **software libero** e del software **open source**, che ha guidato lo sviluppo del progetto **GNU** e che ha ideato la licenza **GPL**.

- libertà di eseguire il software a qualsiasi scopo
- libertà di accedere al codice sorgente, studiarlo ed adattarlo alle proprie esigenze
- libertà di copiare il software e ridistribuirlo
- libertà di migliorarlo e di rendere pubblici i miglioramenti

OPEN SOURCE

Il personaggio simbolo del movimento copyleft è **Richard Stallman** che ha inaugurato il filone del **software libero** e del software **open source**, che ha guidato lo sviluppo del progetto **GNU** e che ha ideato la licenza **GPL**.

Il software open source è semplicemente a sorgente aperto e cioè disponibile.

GNU IS NOT UNIX

Il personaggio simbolo del movimento copyleft è **Richard Stallman** che ha inaugurato il filone del **software libero** e del software **open source**, che ha guidato lo sviluppo del progetto **GNU** e che ha ideato la licenza **GPL**.

Il progetto GNU ha lo scopo di realizzare un sistema operativo composto esclusivamente da software libero

GENERAL PUBLIC LICENSE

Il personaggio simbolo del movimento copyleft è **Richard Stallman** che ha inaugurato il filone del **software libero** e del software **open source**, che ha guidato lo sviluppo del progetto **GNU** e che ha ideato la licenza **GPL**.

Questa licenza prevede che le opere derivate possono essere distribuite solo sotto gli stessi termini di licenza.

COPYLEFT

FREE SOFTWARE - OPEN SOURCE

CREATIVE COMMONS

CREATIVE COMMONS

Tra **copyright** (tutti i diritti riservati) e **dominio pubblico** (nessun diritto riservato) vi è il concetto di "**alcuni diritti riservati**".

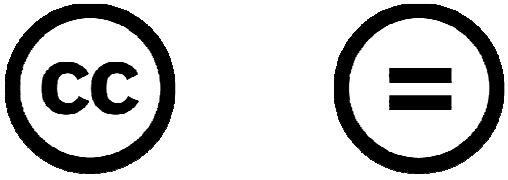
Vengono individuate alcune **attività** che l'utilizzatore di un'opera potrebbe voler fare (**copiarla**, **modificarla** , ecc.) e l'autore sceglie quali **riservarsi** e a quali **rinunciare**.

ATTRIBUTION (BY)

Indicare adeguatamente la **paternità** del materiale oggetto di licenza ed indicare se sono state effettuate **modifiche**

NO DERIVATES (ND)

Se modifichi il materiale oggetto di licenza poi **non** puoi condividerlo

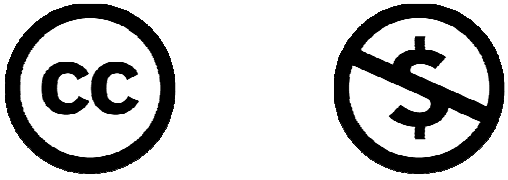


SHARE ALIKE (SA)

Se vuoi condividere il materiale oggetto di licenza da te modificato, devi ridistribuirlo con la **stessa** licenza.

NON COMMERCIAL (NC)

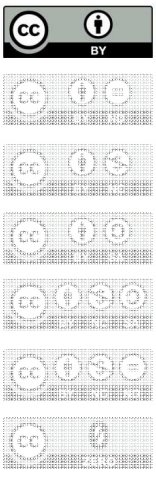
Puoi condividere il materiale oggetto di licenza (eventualmente da te modificato), ma **senza scopo di lucro**.



PUBLIC DOMAIN (ZERO)

Tutti gli utilizzi sono possibili.

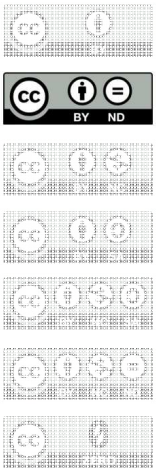
LICENZE CREATIVE COMMONS



Questa licenza consente qualsiasi utilizzo
a patto che venga riconosciuta
la paternità della creazione originale.

CC BY ND

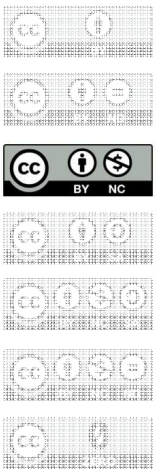
LICENZE CREATIVE COMMONS



Questa licenza permette la ridistribuzione, commerciale e non, dell'opera intera ed invariata e riportante il nome dell'autore.

CC BY ND

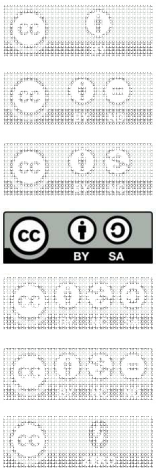
LICENZE CREATIVE COMMONS



Questa licenza permette di usare l'opera come base per altri prodotti, purché essi non siano messi in commercio e riportino l'autore originale. Non è richiesto però di licenziare i prodotti derivati allo stesso modo.

CC BY NC

LICENZE CREATIVE COMMONS

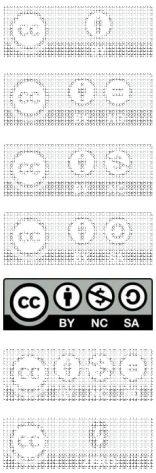


Questa licenza permette di usare l'opera come base per altri prodotti, commerciali e non, purché questi riportino l'autore orginiale e vengano licenziate allo stesso modo.

CC BY SA

Questa licenza è usata per la produzione di **Wikipedia**.
Questa licenza è assimilabile a quelle dei software **opensource**.

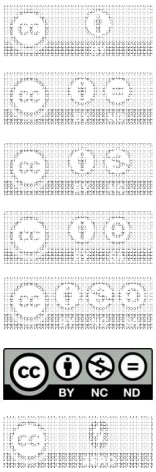
LICENZE CREATIVE COMMONS



Questa licenza consente la modifica e la redistribuzione (gratuita) dell'opera, purché essa avvenga con la stessa licenza e riconoscendo l'autore originale.

CC BY NC SA

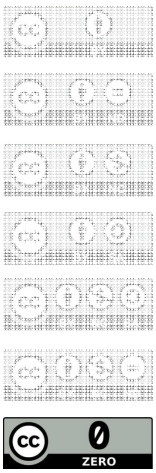
LICENZE CREATIVE COMMONS



Questa licenza è la licenza più restrittiva,
l'opera può essere ridistribuita
ma senza scopo di lucro, nella sua integrità
e riconoscendone l'autore originale.

CC BY NC ND

LICENZE CREATIVE COMMONS



Questa licenza esprime che
l'autore originale cede tutti i diritti sull'opera
e pertanto tutti gli usi sono possibili.

CC ZERO

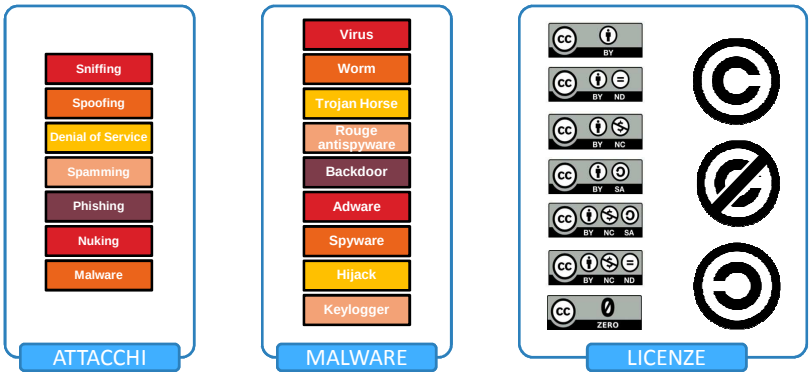
CREATIVE COMMONS

SICUREZZA E DIRITTO INFORMATICO

Reati Informatici

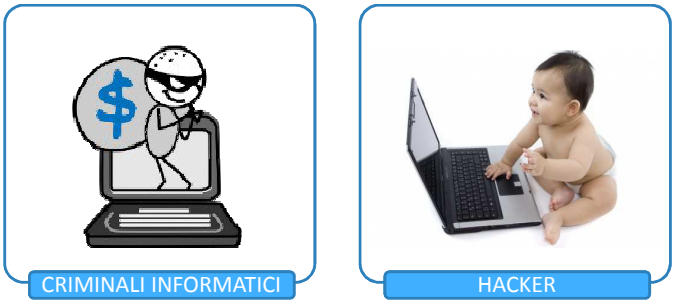
ABBIAMO GIÀ PARLATO DI..

..ed è chiaro che si commette un **reato** informatico effettuando un **attacco**, diffondendo un **malware**, contravvenendo ad una **licenza**.



ABBIAMO GIÀ CONTRAPPOSTO..

..ed abbiamo già detto che per la legge chi commette un **reato** è un **criminale**, **indipendentemente** dai suoi **obiettivi**.



MA C'È MOLTO MOLTO DI PIÙ

Un intricato mondo fatto di
DL, leggi, modifiche ai codici civile e penale, recepimento di direttive UE
regolamenta tutto quanto di irregolare
accade intorno alle nuove tecnologie.

Una interpretazione di tutto ciò potrebbe essere la seguente:

- ❑ vecchi reati perpetrati sfruttando le nuove tecnologie
- ❑ vecchi reati che assumono una nuova forma
- ❑ nuovi reati

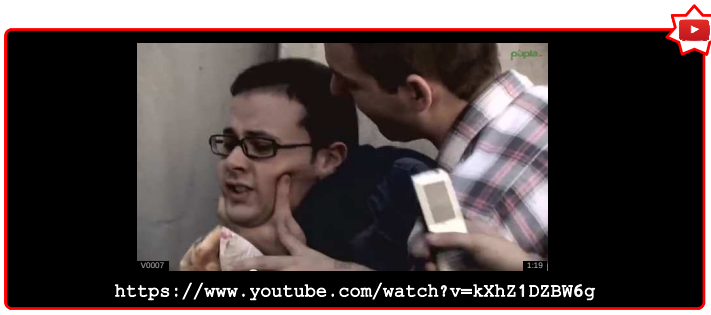
VECCHI REATI PERPETATI SFRUTTANDO LE NUOVE TECNOLOGIE

VECCHI REATI PERPETATI SFRUTTANDO LE NUOVE TECNOLOGIE

- bullismo
- diffamazione
- spionaggio industriale
- sfruttamento della prostituzione
- adescamento
- pedofilia
- stalking

VECCHI REATI PERPETATI SFRUTTANDO LE NUOVE TECNOLOGIE

- bullismo
- diffamazione
- spionaggio industriale
- sfruttamento della prostituzione
- adescamento
- pedofilia
- stalking



https://www.youtube.com/watch?v=kXhZ1DZBW6g

VECCHI REATI PERPRETATI SFRUTTANDO LE NUOVE TECNOLOGIE

- bullismo
- diffamazione
- spionaggio industriale
- sfruttamento della prostituzione
- adescamento
- pedofilia
- stalking

http://www.video.mediaset.it/video/iene/puntata/367366/toffa-cyber-bullismo.html

ALESSANDRO URSOMANDO

VECCHI REATI CHE ASSUMONO UNA NUOVA FORMA

ALESSANDRO URSOMANDO

VECCHI REATI CHE ASSUMONO UNA NUOVA FORMA

- effrazione
- intrusione
- furto e ricettazione
- atti vandalici
- truffa

VECCHI REATI CHE ASSUMONO UNA NUOVA FORMA

- **effrazione**
- intrusione
- furto e ricettazione
- atti vandalici
- truffa

VECCHI REATI CHE ASSUMONO UNA NUOVA FORMA

- **effrazione**
- intrusione
- furto e ricettazione
- atti vandalici
- truffa

Violazione delle misure di sicurezza di un sistema

VECCHI REATI CHE ASSUMONO UNA NUOVA FORMA

- effrazione
- **intrusione**
- furto e ricettazione
- atti vandalici
- truffa

VECCHI REATI CHE ASSUMONO UNA NUOVA FORMA

- ❑ effrazione
- ❑ **intrusione**
- ❑ furto e ricettazione
- ❑ atti vandalici
- ❑ truffa

Utilizzo non autorizzato di un sistema

VECCHI REATI CHE ASSUMONO UNA NUOVA FORMA

- ❑ effrazione
- ❑ intrusione
- ❑ **furto e ricettazione**
- ❑ atti vandalici
- ❑ truffa

VECCHI REATI CHE ASSUMONO UNA NUOVA FORMA

- effrazione
- intrusione
- **furto e ricettazione**
- atti vandalici
- truffa

Usare e diffondere materiale protetto da licenza (craccato o meno)

ALESSANDRO URSOMANDO

VECCHI REATI CHE ASSUMONO UNA NUOVA FORMA

- effrazione
- intrusione
- furto e ricettazione
- **atti vandalici**
- truffa

ALESSANDRO URSOMANDO

VECCHI REATI CHE ASSUMONO UNA NUOVA FORMA

- effrazione
- intrusione
- furto e ricettazione
- **atti vandalici**
- truffa

Danneggiamento di dispositivi e/o manomissione di software e/o dati

VECCHI REATI CHE ASSUMONO UNA NUOVA FORMA

- effrazione
- intrusione
- furto e ricettazione
- atti vandalici
- **truffa**

VECCHI REATI CHE ASSUMONO UNA NUOVA FORMA

- ❑ effrazione
- ❑ intrusione
- ❑ furto e ricettazione
- ❑ atti vandalici
- ❑ **truffa**

Phishing

NUOVI REATI

- Sviluppo e/o utilizzo di strumenti per intercettare, registrare, impedire o modificare comunicazioni.
- Sviluppo e/o utilizzo di strumenti per alterare un sistema.
- Trattamento dei dati personali non a norma.
- Furto dell'identità digitale.

FURTO D'IDENTITÀ

DEEP WEB