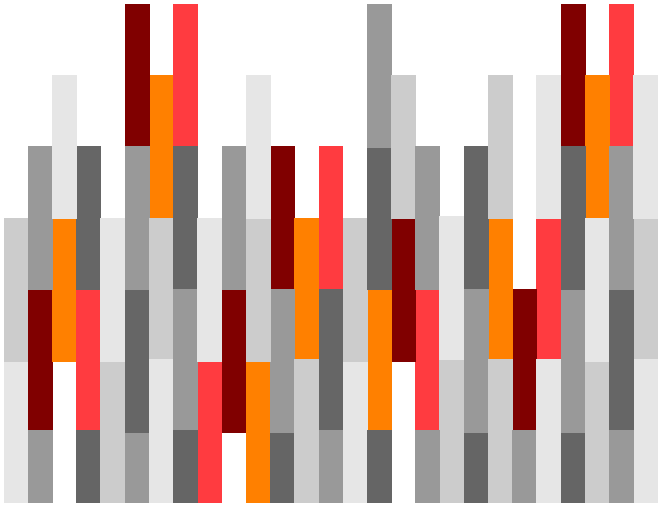
Fluency



Implicazioni sociali dell'informatica

Capitolo 10

Privacy

- I nostri **corpi**
- I nostri **luoghi**
- Le **informazioni**
- Le **comunicazioni** personali

La privacy

- Con i moderni dispositivi è possibile violare la privacy delle persone **senza che se ne accorgano**
  - Nel 1890, Brandeis scrisse che gli individui meritano "protezione sufficiente contro la **circolazione impropria**" delle loro immagini

Una definizione di privacy

- Il diritto di una persona di scegliere **liberamente** in quali circostanze e fino a che punto **rivelare agli altri**
  - **se stessa**
  - il proprio **atteggiamento** e
  - il proprio **comportamento**

Social network

- Riduzione **volontaria** della propria privacy
- *La rete non dimentica mai*
- Utilizzati regolarmente anche per le assunzioni

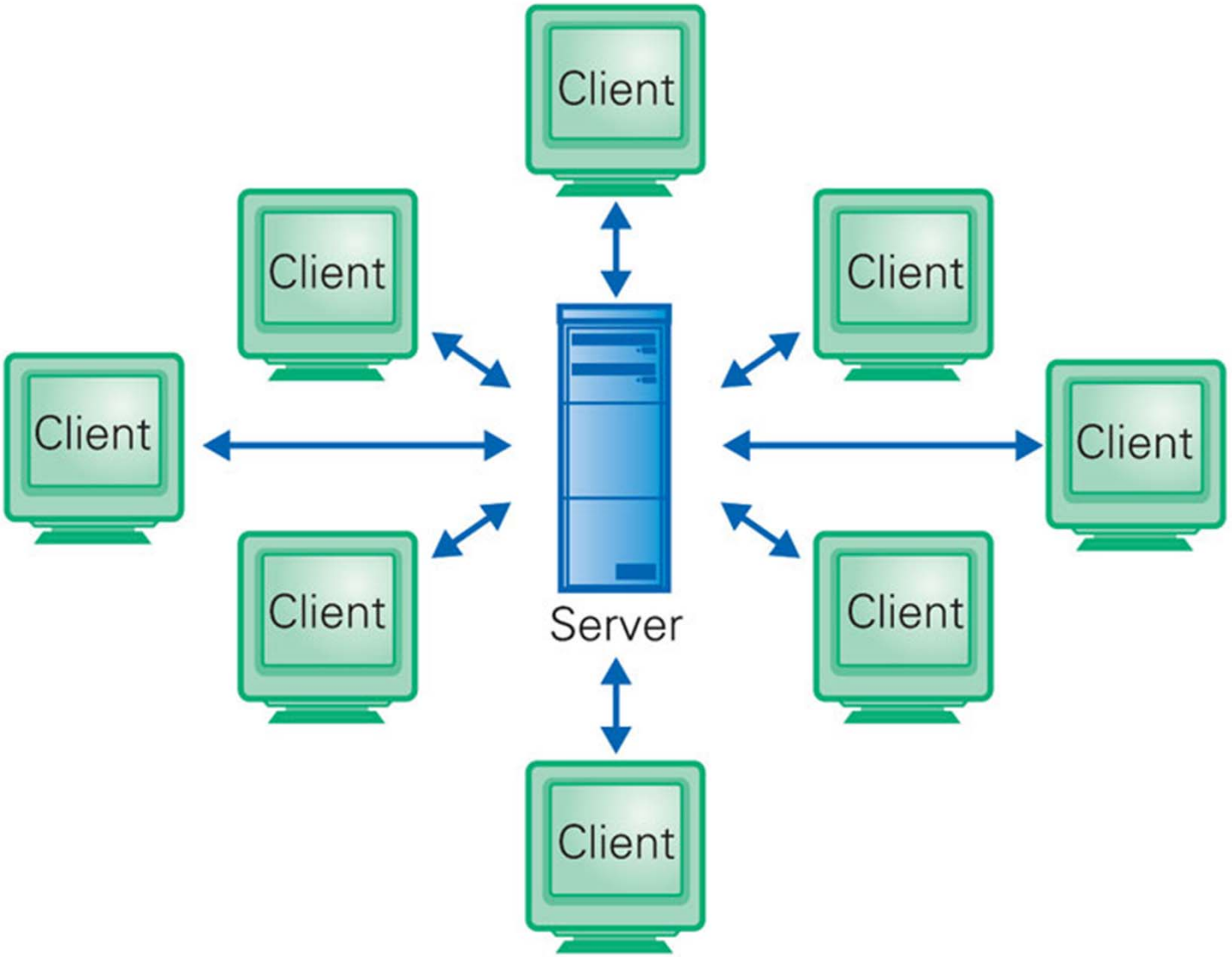
Chi minaccia la privacy?

- Gli organi governativi
- Aziende commerciali
- Spionaggio
- Malavita

Cookie

- Un piccolo file che contiene sette campi di informazione
  - **identificare univocamente una sessione**.
- Il cookie è memorizzato sul computer client
  - lettura e scrittura **solo dal sito** che si sta visitando

Server stateless



Third party cookie

- Venditori di pubblicità presenti come “esterni” (*third party*) su un sito web
  - connessione con il computer del cliente durante il caricamento della pagina
- Se l’utente raggiunge **un’altra pagina su un altro sito con lo stesso third party**
  - il cookie può essere **riconosciuto e utilizzato** per dedurre informazioni

Proteggere la privacy

- **Aggiornare** il software antivirus
- **Configurare** la gestione dei cookie
- Fare sempre attenzione ai messaggi di possibili "**phishing**"

Proteggere la privacy

- Scaricare file solo da **siti affidabili**
- Mantenere sempre un **sano scetticismo**
- **Mantenersi aggiornati** sulle tecniche di attacco alla privacy

Accesso

- Coppia **login-password**
  - identificazione **univoca** dell'utente
  - **firma elettronica**
- Il ruolo delle password
  - **limitare l'accesso** a un computer
  - **identificare** chi accede
    - identificarne anche le *azioni*

Login & password

- Provare ad accedere a un computer *senza password*
  - si possono **provare tutte le combinazioni** possibili
  - fino a trovare la password corretta,
  - il software in genere limita il numero di tentativi

Login & password

- Dimenticare la password
  - le password sono **criptate e registrate**,
  - l'amministratore del sistema *non può* ricostruire una password dimenticata
    - può solo **cancellarla** o **sostituirla**

Una buona password

- **NO**: qualcosa che si può facilmente indovinare
  - data di nascita, nome proprio, nome figli, …
- **SI**: essere *almeno* di sei caratteri
  - la lunghezza dipende dal sistema

Una buona password

- **SI**: un mix *vero*
  - lettere maiuscole,
  - minuscole,
  - numeri,
  - punteggiatura (se permessa)

Una buona password

- **SI**: una parola che non è nei dizionari
  - resiste all'*attacco del dizionario*
- **NO**: ha un collegamento ovvio con la vostra persona
  - indirizzo, matricola, nomignolo, …

Generare una password

- Scegliete un **argomento** che vi interessa
- Partite da una **frase** anziché da una singola parola

Generare una password

- Codificate la frase in modo personale
  - **abbreviandola**,
    - acronimo
  - **sostituendo** lettere o sillabe con caratteri alternativi
  - **scegliendo** lettere particolari

Cambiare password

- Una password dovrebbe essere cambiata **periodicamente**
  - molti sistemi impongono un cambiamento periodico

Sicurezza

- Malware
- Protezione

Virus

- È un programma che ne "**infetta**" un altro **attaccandogli una copia** di sé stesso.
- Quando il programma infettato viene eseguito,
  - il virus crea ulteriori copie di sé
  - infetta altri programmi ancora

Worm

- È un programma indipendente che copia se stesso e viaggia sulla rete

Trojan

- è un programma che si nasconde all'interno di un altro programma utile
- esegue operazioni all'insaputa dell'utente
  - i trojan possono registrare le battute dei tasti o altri dati dell'utente o
    - *keylogger*
  - mandare in esecuzione programmi dannosi

Exploit

- È un programma che sfrutta la vulnerabilità del software
  - il backdoor permette l'accesso al computer e ne *riconfigura* il comportamento da remoto

Virus per e-mail

- **Non aprite quell'*allegato***:
- Conosco il *mittente* di questo messaggio?
- Il contenuto è *coerente* con la nostra ultima conversazione?
- È *plausibile* che il mittente voglia dirmi delle cose?
- C'è una buona ragione per *includere* un allegato?

Virus per altre vie

- Copia di file da un computer infettato
- Scambio *peer-to-peer* di file (fonti *insicure*)
- Installazione di programmi
  - ogni software è una *fonte potenziale* di infezione
  - la *maggior parte* dei distributori di software prende tutte le precauzioni

Software antivirus

- *McAfee*, *Norton* e *Sophos*
  - sono tre delle più importanti *softwarehouse* che producono antivirus
- Questi programmi possono identificare virus, worm, ecc.
  - ogni giorno nascono nuovi virus,
  - è necessario *aggiornare spesso* l'antivirus

Phishing

- Gli utenti ricevono una e-mail
  - che *chiede* di fornire numeri di carta di credito o informazioni bancarie

Phishing

- Il messaggio è “camuffato”
  - *appare* inviato da una azienda vera
  - spesso finge di essere motivato proprio da *esigenze di sicurezza*
  - quando l’utente ci clicca sopra,
    - viene trasportato in un *sito falso* per rubare informazioni

Esempio di phishing

Posteitaliane

Gentile Cliente di **Poste Italiane**,

Il Servizio Tecnico di *Poste Italiane* sta eseguendo un aggiornamento programmato del software al fine di migliorare la qualità dei servizi bancari.

Le chiediamo di avviare la procedura di conferma dei dati del Cliente.
A questo scopo, La preghiamo di cliccare sul link che Lei troverà alla fine di questo messaggio.

http://bancopostaonline.poste.it/bpol/bancoposta/iormconfirm.asp

Ci scusiamo per ogni eventuale disturbo, e La ringraziamo per la collaborazione.

Figura 10.1 Un tipico esempio di phishing.

Virus Melissa

Table 12.2. Variations of the Melissa virus email

Subject Line	Email Body
Question for you ...	It's fairly complicated so I've attached it.
Check this!!	This is some wicked stuff!
Cool Web Sites	Check out the Attached Document for a list of some of the best Sites on the Web.
80mb Free Web Space	Check out the Attached Document for details on how to obtain the free space. It's cool, I've now got heaps of room.
Cheap Software	The attached document contains a list of web sites where you can obtain Cheap Software.
Cheap Hardware	I've attached a list of web sites where you can obtain Cheap Hardware.
Free Music	Here is a list of places where you can obtain Free Music.
* Free Downloads	Here is a list of sites where you can obtain Free Downloads.

* A randomly selected digit

Combattere il *phishing*

- **Non rispondere**
  - **alle richieste** da e-mail di informazioni personali
    - come le *password*;
  - le aziende non richiedono mai informazioni in **questo modo**

Combattere il *phishing*

- **Non cliccare**
  - sui **collegamenti** proposti o accettate campi già compilati,
    - perché possono essere **dirottati** su altri siti;
  - digitate l'URL nella finestra del browser

Combattere il *phishing*

- Assicuratevi che il sito faccia **uso della crittografia**
- Tenete sempre d'occhio
  - il vostro *estratto conto* bancario e quello della carta di credito,
  - per accorgervi tempestivamente di ogni movimento illecito

Combattere il *phishing*

- Se sospettate di essere vittima di un abuso,
  - contattate immediatamente le autorità responsabili

Crittografia: terminologia

- Cifratura
  - rende la rappresentazione incomprensibile
- Sistema di crittografia
  - per la *cifratura* e la *decifratura*
- Testo in chiaro
  - l'informazione prima di essere cifrata

Crittografia: terminologia

- Testo cifrato
  - l'informazione cifrata
- Crittografia monodirezionale
  - non può essere facilmente decodificato
- Decifratura
  - operazione inversa della cifratura

usata per le password

Crittografia Simmetrica

- **Stessa chiave** segreta
  - cifrare
  - decifrare
- Esempio
  - singolo lucchetto con due chiavi

XOR - OR esclusivo

- Operatore binario, $\oplus$
  - $0 \oplus 0 \Rightarrow 0$
  - $1 \oplus 0 \Rightarrow 1$
  - $0 \oplus 1 \Rightarrow 1$
  - $1 \oplus 1 \Rightarrow 0$

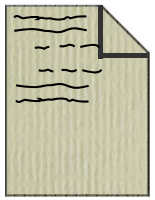
XOR e crittografia

- Facilita **l'applicazione di una chiave** a un testo in chiaro
- Per ottenere di nuovo il testo in chiaro basta **riapplicare la stessa chiave**
- Il risultato dello XOR
  - **non cambia** se la chiave è a destra o sinistra dell'operatore

Es.: cifrare con XOR

- La chiave, 16 bit, è: *00010111 00101101*
- Usiamo rappresentazione ASCII del messaggio
- XOR, bit per bit, tra il messaggio e la chiave
  - ripetendo la chiave per la lunghezza necessaria

Es.: cifrare con XOR



Meet@12:15@Joe's

00010111 00101101

ZHrYW$^{F}_{S}$%$^{E}_{\Sigma}$&$^{C}_{N}$WgxH0_

Es.: cifrare con XOR

testo in chiaro

valore ASCII testo

chiave

testo XOR chiave

testo cifrato

M	e	e				2	:
01001101	01100101	01100101				00110010	0111010
00010111	00101101	00010111				00010111	00101101
01011010	01001000	01110010				00100101	00010111
Z	H	r				%	E_{Σ}

Es.: cifrare con XOR

1	5	@	J	o	e	’	s
00110001	00110101	01000000	01001010	01101111	01100101	00100111	01110011
00010111	00101101	00010111	00101101	00010111	00101101	00010111	00101101
00100110	00011000	01010111	01100111	01111000	01001000	00110000	01011111
&	$^{C}_{N}$	W	g	x	H	0	_

Es.: decifrare con XOR

- Il testo cifrato è posto in XOR dal ricevente con la **stessa chiave**
- Si ottiene nuovamente la sequenza di bit originale

Es.: decifrare con XOR

testo in chiaro

testo XOR chiave

chiave

valore ASCII testo cifrato

testo cifrato

M	e	e					:
01001101	01100101	01100101				10010	0111010
00010111	00101101	00010111				00010111	00101101
01011010	01001000	01110010				00100101	00010111
Z	H	r					E_{Σ}

Proprietà cifratura simmetrica

- Canale di comunicazione “pubblico”
- Scambio chiave tramite **canali sicuri**
- Una chiave per **ogni coppia** di utenti
  - 100 utenti 4’950 chiavi => ognuno 99 chiavi
  - problema “rimozione”
- **Ripudiabile**

Infrangere il codice

- Più è lungo il testo più è facile decodificarlo
  - si notano quali sequenze di bit compaiono più frequentemente
  - ci si basa sulla conoscenza delle lettere più comuni nel linguaggio in cui è stato scritto il messaggio

Sistemi a chiave pubblica

- Le persone **pubblicano** una chiave che i mittenti devono usare per cifrare i testi
- La chiave è tale che **solo il destinatario** legittimo possa decifrare il testo

Proprietà firma digitale

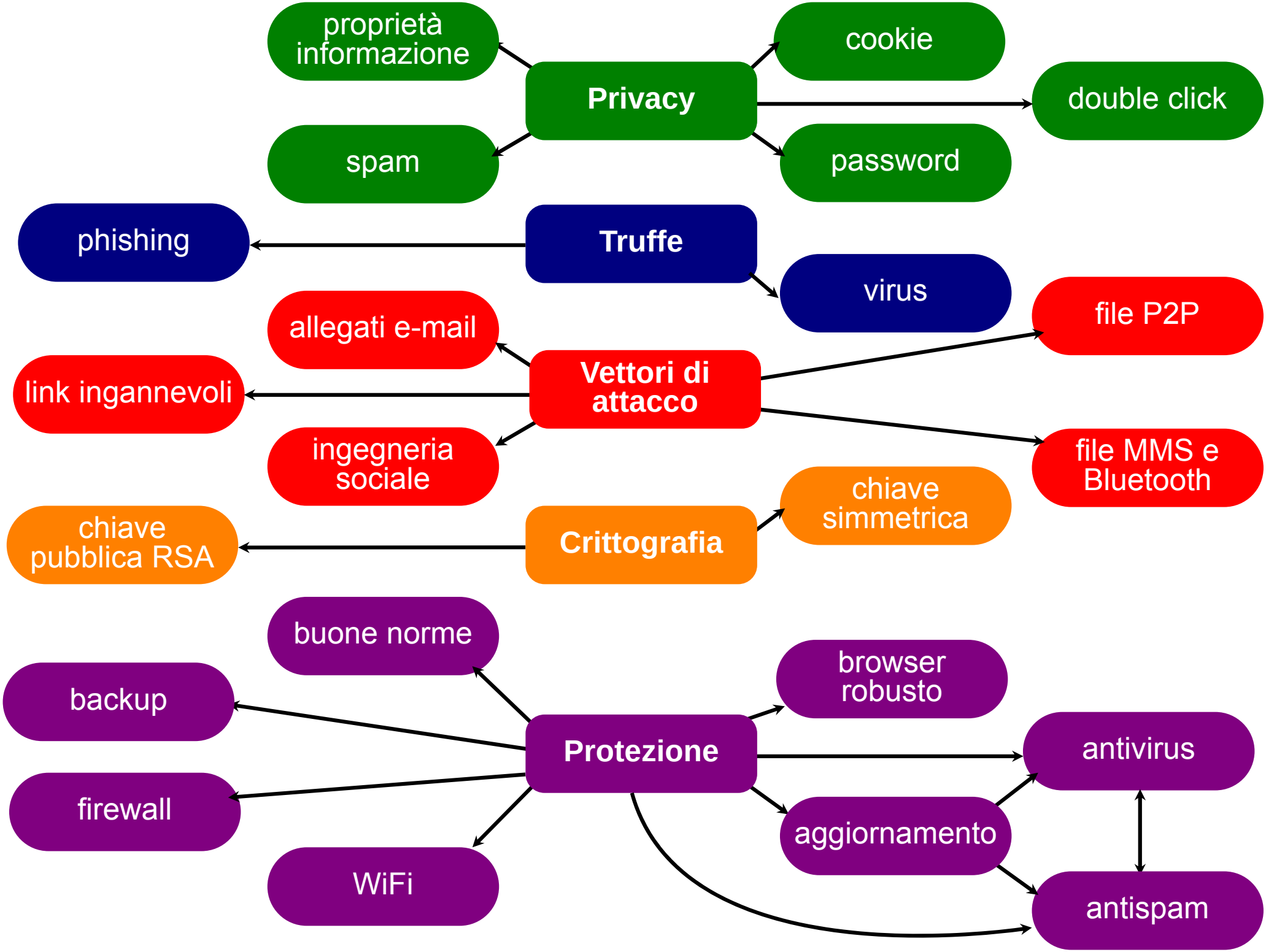
- Segretezza
- Autenticità
- Non ripudiabilità

Attacchi di “forza bruta”

- Efficaci contro qualsiasi algoritmo
- Chiave di n bit $\Rightarrow 2^n$ possibili chiavi

Lunghezza della chiave

- Chiave corta: facilmente individuabile
  - 40 bit $\Rightarrow 10^{12}$ possibilità
  - PC con 10^9 operazioni al secondo
- Chiave lunga: non significa automaticamente più sicurezza
  - misura il **massimo** sforzo non il **minimo** sforzo


proprietà informazione
Privacy
cookie
double click
spam
password
phishing
Truffe
virus
allegati e-mail
file P2P
link ingannevoli
Vettori di attacco
ingegneria sociale
file MMS e Bluetooth
chiave pubblica RSA
Crittografia
chiave simmetrica
buone norme
backup
browser robusto
Protezione
antivirus
firewall
aggiornamento
WiFi
antispam