Sicurezza dei sistemi e delle reti[1]

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2014/15

Lezione XX: Censura e controllo in rete

Censura e controllo in rete

Le reti telematiche risultano essere uno strumento di libertà, ma sono esposte al rischio di controllo di massa da parte dei *carrier* e dei governi.

- Censura
- Content filtering
- Tracking delle abitudini

Anche quando ci possono essere buone ragioni, i filtri possono essere imprecisi.

Diritti fondamentali

Dichiarazione universale dei diritti dell'uomo, art. 12

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.

Costituzione italiana, art. 15

La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.

Tutela

Gli utenti delle reti hanno quindi diritto di

- veder tutelati i loro diritti dalla legge
- usare la tecnologia in modo da difendersi all'interno di una rete (quindi in potenziale conflitto con l'amministratore della rete stessa)

Privacy-Enhancing Technologies (PET)

PET: tecnologia progettata allo scopo di tutelare la privacy (privatezza, riservatezza)

- Non solo reti: le porte dei bagni sono PET...
- In campo informatico:
  - tecniche per minimizzare o eliminare i *dati personali*
  - tecniche per evitare il controllo delle attività

Privacy e sicurezza

La privacy è importante anche per la sicurezza

- identity theft
- controllo e repressione del dissenso (piú efficace della tortura, vedi *The Man in the Snow White Cell*, CIA `http://ur1.ca/6lef8`)
- le persone cambiano, ma i dati restano (diritto all'oblio)

Minimizzazione dei dati

- Ogni servizio dovrebbe richiedere e raccogliere solo l'insieme minimo di dati necessario a fornirlo
- I dati personali (o addirittura *sensibili*) dovrebbero essere raccolti solo quando strettamente necessari (e conservati in maniera adeguatamente protetta)

Sanitization

La sanitization consiste nel eliminare dai dati le caratteristiche che li rendono personali o sensibili.

- Molto difficile: anche le aggregazioni statistiche dovrebbero risultare anonime
- L'anonimato richiede spesso grandi quantità di dati (es. un nero di 30-40 abitante a Dalvík, Islanda).

Protezione

Ogni volta che dati personali/sensibili sono conservati, processati o trasmessi dovrebbero essere protetti

- Controllo degli accessi
- Crittografia e *shredding*

In Italia norme di legge piuttosto precise: vedi Decreto legislativo 30 giugno 2003, n. 196 *Codice in materia di protezione dei dati personali*.

Riassumendo

La Rete è senz'altro uno strumento di libertà d'espressione, ma si presta a un controllo sistematico e potenzialmente oppressivo.

- Censura
- Content filtering
- Privacy

Anonimato

La difesa rispetto ai pericoli di controllo è l'anonimato (non a caso tutti i tentativi di controllo politico di Internet cercano, in un modo o nell'altro, di limitare l'accesso anonimo)
Tema assai controverso, perché l'anonimato perfetto permette azioni non perseguibili (e in effetti in alcuni casi la legalità *locale* potrebbe essere in contrasto con i diritti fondamentali).

Inosservabilità

Un utente usa una risorsa senza che terze parti siano in grado di osservare l'uso
Per un evento E, Se O_A è l'insieme di eventi osservabili dall'attaccante A

Unobservability

$\forall \omega \in O_A : 0 < P(E|\omega) < 1$

Perché sia efficace $0 \ll P(E|\omega) \ll 1$

Inosservabilità perfetta

Se nessuna osservazione è in grado di cambiare la probabilità a posteriori di un evento, si parla di inosservabilità perfetta.

Perfect Unobservability

$\forall \omega \in O_A : P(E) = P(E|\omega)$

Incollegabilità

Un utente usa diverse risorse o servizi senza che sia possibile collegare i diversi usi.
Per due eventi E, F, con una caratteristica comune (link) $L_{E,F}$

Unlinkability

$\forall \omega \in O_A : 0 < P(L_{E,F}|\omega) < 1$

Perché sia efficace $0 \ll P(L_{E,F}|\omega) \ll 1$
Perfect Unlinkability: $\forall \omega \in O_A : P(L_{E,F}) = P(L_{E,F}|\omega)$

Incollegabilità di mittente e destinatario

Un caso particolare è l'unlinkability fra mittente e destinatario in una comunicazione.

- A, B comunicano
- A *comunicante* è osservabile, B *comunicante* è osservabile...
- ... ma non è osservabile il fatto che A comunica con B

Anonimato

Un utente usa una risorsa senza rendere nota la propria identità. Si definisce rispetto al ruolo $R_{U,E}$ dell'utente U nell'evento e un insieme W di identità

Anonymity

$\forall \omega \in O_A,\ \kappa \in W : 0 < P(R_{\kappa,E}|\omega) < 1$

In pratica deve essere $0 \ll P(R_{\kappa,E}|\omega) \ll 1$
Anonimato perfetto: $\forall \omega \in O_A,\ \kappa \in W : P(R_{\kappa,E}) = P(R_{\kappa,E}|\omega)$

Pseudonymity

Un utente usa una risorsa identificandosi con uno pseudonimo.

- Lo pseudonimo rimane costante
- ma non è possibile (o solo alcuni sono in grado di farlo) collegarlo all'identità reale
- può essere legato ad un ruolo

Riassumendo

La principale difesa rispetto ai pericoli di controllo è l'anonimato:

- Inosservabilità, unlinkability
- Anonimato e pseudonimi