

Raffronto tra il passato e
l'era di Internet,

Controllo dell'informazione e
libertà degli utenti.

vecna - <http://www.delirandom.net>
Lugano, 02/10/2009

Sicurezza, controllo, privacy

Punti cardine del racconto:

Sicurezza e Privacy sono una "percezione".

Quanto è sincera questa percezione ?

Con Internet, come e perché cambia la fruizione delle informazioni.

E quali equilibri son stati scossi ?

La bassa cultura in termini di sicurezza, porta a chiedere soluzioni liberticide.

*Ma hanno, **almeno un**, vantaggio ?*

Come percepiamo i valori di sicurezza-privacy ?

Utilizzare un termine nella discussione significa rievocare nel soggetto al quale si parla una serie di ricordi, ai quali associa il significato.

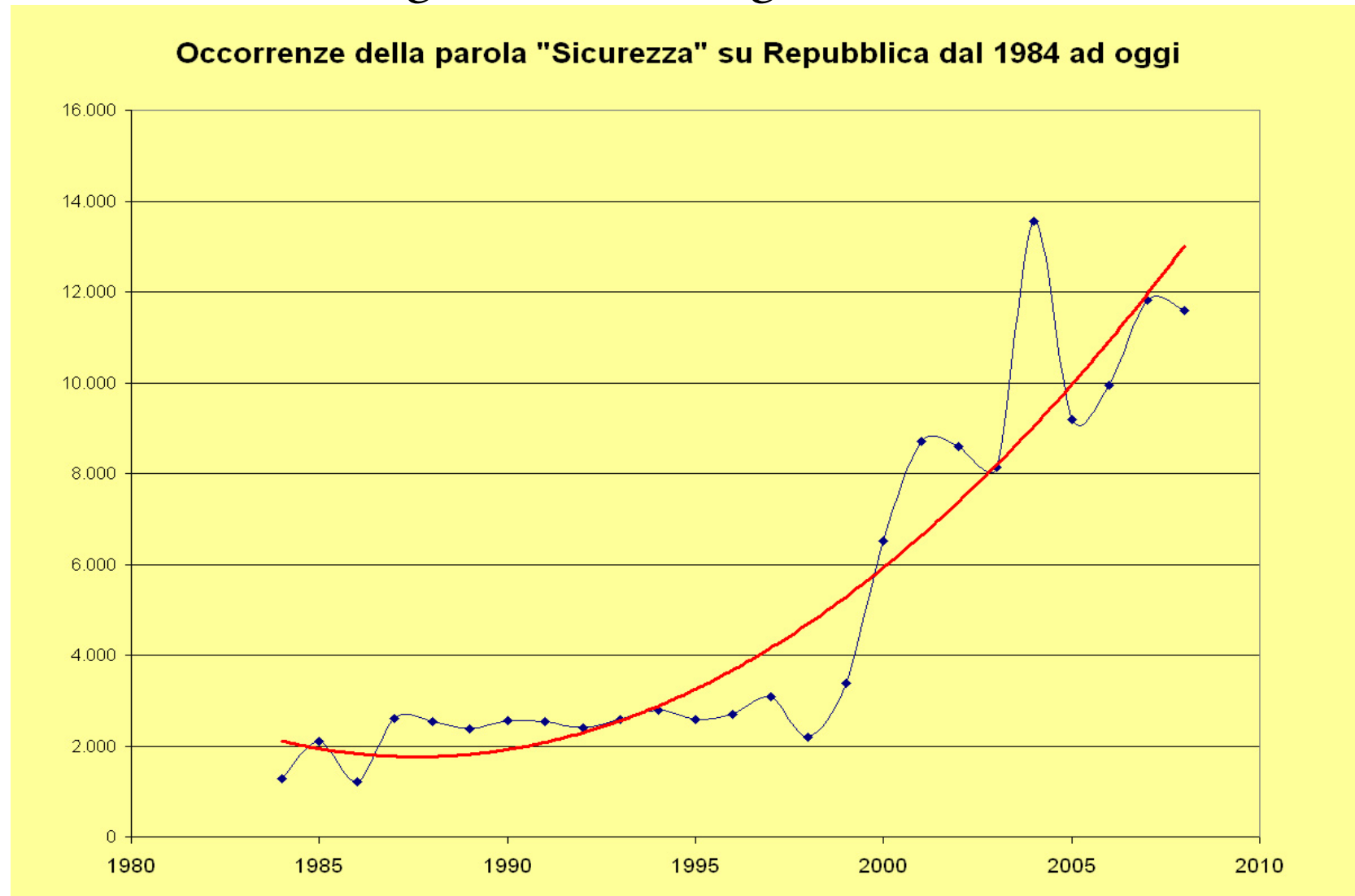
Parlare di sicurezza e privacy può diventare estremamente complesso perché, l'influenza dei mass media, ha gradualmente distorto il significato che entrambe queste parole avevano fino agli anni '90.

Sicurezza: sine-cura, non curarsi di un elemento perché è affidabile e garantito

Privacy: “*right to be alone*”, racchiude tutto ciò che è considerato privato (intimità, pudore) e tutto ciò che arbitrariamente vorremmo tenere privato. (quando si parla di **Riservatezza**, si allude alla proprietà che si vuol dare ad un dato che riteniamo privato)

Come fa un problema sociale a far carriera ?

L'influenza mediatica è qualcosa che in modo delicato, subdolo, costante e crescente, è in grado di rendere un qualunque aspetto organizzativo alla stregua di un "emergenza" (almeno, in italia! :)



un'idea si vende come un'automobile...

By **Clotaire Rapaille**, CHAIRMAN OF ARCHETYPE DISCOVERIES WORLDWIDE AND AUTHOR OF *THE CULTURE CODE*, PUBLISHED THIS MONTH BY BROADWAY BOOKS

Marketing to the Reptilian Brain

Pry away the slick answers of a focus group and get to the instincts buried beneath.

WHAT'S THE BIGGEST PROBLEM with traditional market research? You can't believe what people say.

It's not that people intentionally lie during surveys and focus groups; it's that they try too hard to please. When asked about their interests and preferences, they tend to give answers they believe the questioner wants to hear. This is because people respond with their cerebral cortexes, the part of the brain that controls intelligence, rather than emotion or instinct. Their answers are the product of deliberation. In most cases, however, they aren't saying what they feel. One of the great-
est focus group flops of all time



when an interviewer takes the role of a "visitor from another planet," asking participants to help the visitor understand the product in question. In the second hour participants use their limbic systems to tell stories about the products. In the third hour they tap their reptilian inner selves. Lying on pillows with the lights dimmed, they first go through a relaxation exercise. Then they write about their first experiences with the product, expressing what was imprinted into their subconscious.

For Chrysler, this process demonstrated that cookie-cutter sedans are "off-Code." This information led to the creation of the pr

Quali sono gli effetti di questa richiesta ?

Con la crescita dell'esigenza a sentirsi sicuri, si sono visti svariati effetti, stimola nella popolazione, nel politico e nel giornalista, l'(assurdo) assioma per cui si ha bisogno di **maggior controllo**:

Credendo che sia un semplice sacrificio di privacy, a fronte di una maggior sicurezza percepita.

“se io non ho nulla da nascondere, non ho nulla da temere”

<http://www.digitalrights.ie/2009/07/13/if-youve-nothing-to-hide-youve-nothing-to-fear/>

Per l'intelligence e la prevenzione, non è il controllo la soluzione funzionale ne parziale.

“Londra, risolto un crimine all'anno ogni 1000 telecamere”

http://www.schneier.com/bbg/archives/2009/08/on_londons_surv.html

Perdere la propria riservatezza significa rendersi attaccabili da chi ha in mano le tue informazioni.

“Ma chi vuoi che si interessi a me ?”

targeted/untargeted attacks

Come si colloca Internet in questa situazione ?

Sconvolge il panorama giornalistico, rendendo evidente che la distinzione qualitativa tra professionisti e amatoriali (blogger, ricercatori, fotografi) esiste solo marginalmente.

Rompendosi la “barriera all'ingresso” della comunicazione il pluralismo ne ha goduto. Elemento in comune con il giornalismo d'assalto di dissidenti iraniani/birmani/cinesi.

Rompe gli standard statali per uno standard globale, incrinando ogni formalismo fiscale/di quota. addirittura crea valute proprie :)

Tra gli sfruttatori dei diritti d'autore: è diventato evidente che la presenza di “un mezzo di comunicazione non controllato” rappresenta una spina nel fianco per quella lobby.

Perdono gradualmente utilità alcuni ruoli intermediari.

Davanti a questo sconvolgimento dello status-quo, una buona fetta di conservatori vede Internet come una minaccia.

Quanto è vulnerabile Internet ?

“Teoricamente” è inattaccabile!

E' stata studiata dai laboratori ARPANET per fornire comunicazione in caso di guerra atomica

Gli elementi di resistenza, indipendenza e decentralizzazione sono le sue fondamenta.

Eppure il discorso pubblico vede le innovazioni portate da Internet come problemi da arginare.

Si tenta di arrabattare soluzioni che possano, al più possibile, uniformare Internet al vecchio modello legislativo/economico... Ma questo è impossibile, se non a causare evidenti limitazioni a quello che gli utenti stanno dimostrando di voler e di poter fare.

Alla rete, non è ancora stata riconosciuta la sua importanza.

Entità dello sconvolgimento derivato da Internet

Un interessante studio del RAND, per l'US-Navy (1993), cercava di razionalizzare che tipo di problematiche avrebbe causato l'avvento di Internet nel mondo. Titolo: “the advent of netwar”.

<http://www.tsa.gov/assets/pdf/NetWar.pdf>

La loro visione era due passi più avanti, già 16 anni fa!

Partiva da un'analisi antropologica, domandandosi:

“Quale tipo di cambiamento preannunciava la nascita di una nuova forma di organizzazione sociale ?”

E questo cambiamento è il numero di contatti, comunicazioni, scambi, che un individuo nella sua vita può avere con altri.

La loro analisi tratta di **storia** e di **storia degli attacchi** (il loro è un punto di vista militaristico, che soppesava le forme organizzative di stati/NGO/chiese/gruppi/ideologie/cosche...). Analizzando le proprietà che attribuiscono alle reti distribuite rispetto alle organizzazioni gerarchiche, **molte atipicità di Internet trovano risposta.**

attacchi - difese - contromisure

Per capire il livello di solidità della rete, seguirà una panoramica delle diverse tipologie d'attacco che vengono portate **ad** e **tramite** essa.

Saranno presi degli esempi di riferimento, ma ciò che va trattato non sono i soggetti nello specifico, quanto le tecnologie ed i meccanismi che sono entrati nel merito.

Target dell'attacco:

La comunità di utenti che faceva file sharing, poiché la tecnologia di trasmissione veniva utilizzata per la condivisione di materiale protetto dal diritto d'autore

Cosa c'è di nuovo ?:

Chiunque già prima poteva copiarsi la propria cassetta/cd, ma la disponibilità rimaneva limitata alla sua rete sociale. Napster espande questa rete sociale a “tutti i suoi utenti” e le possibilità di scambio aumentano esponenzialmente

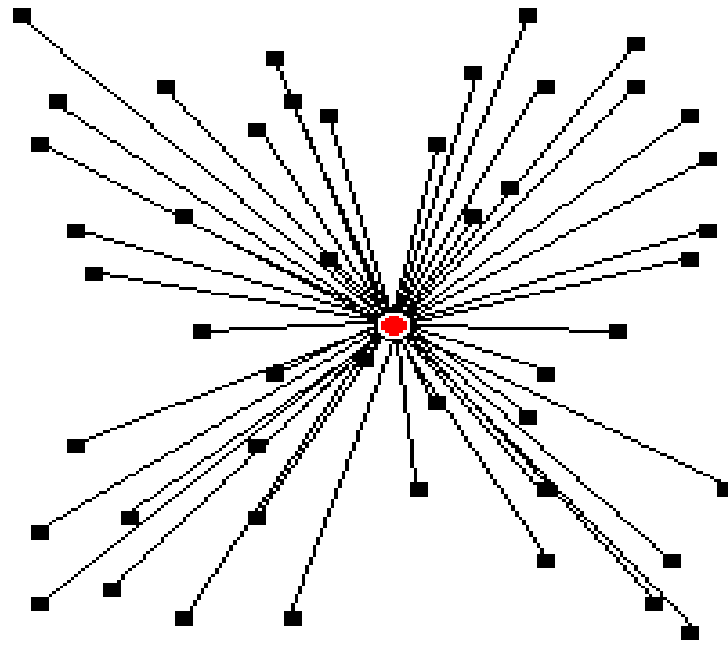
Modalità di attacco:

Pressioni legali all'“anello debole” della catena

Contromisura:

Non prevedere anelli deboli.

Napster 2/3



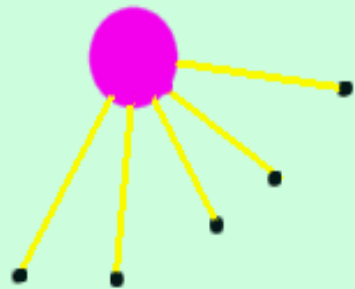
**Centralized
Network**

Gli utenti per trovare il file ricercato devono chiederlo ad un server centrale.

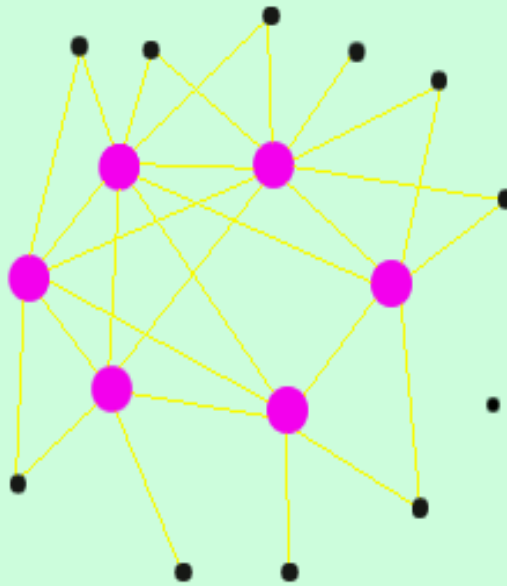
Se il server viene compromesso, può non segnalare ciò che l'attaccante non vuole più che appaia.

Una sola entità (quindi un solo attacco, sia esso legale/digitale/sociale/personale) per ottenere il massimo risultato.

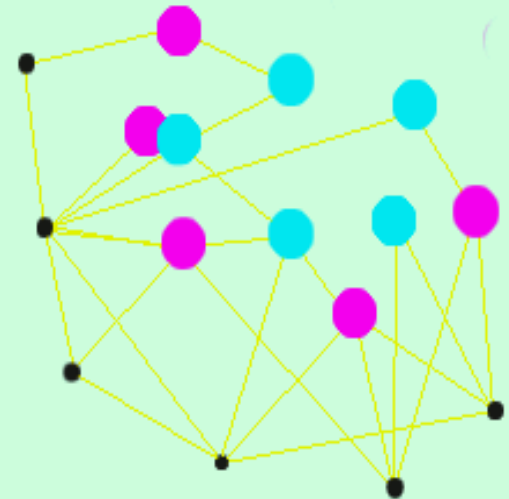
Il peer to peer, è nella sua accezione pubblica nato da questa esperienza, le tecnologie che sono seguite hanno evitato di riproporre lo stesso errore. Fino ad arrivare a commetterlo consapevolmente, forti della propria solidità.



Napster



Emule



BitTorrent

i link indicati non son di dati ma di management

Target dell'attacco:

Le comunicazioni internet (equiparate alle telefonate)

Cosa c'è di nuovo?:

Lo stato non è più l'esecutore, ma sono i privati.

Tutti i privati che svolgono un servizio di accesso alla rete, possono effettuare un'intercettazione

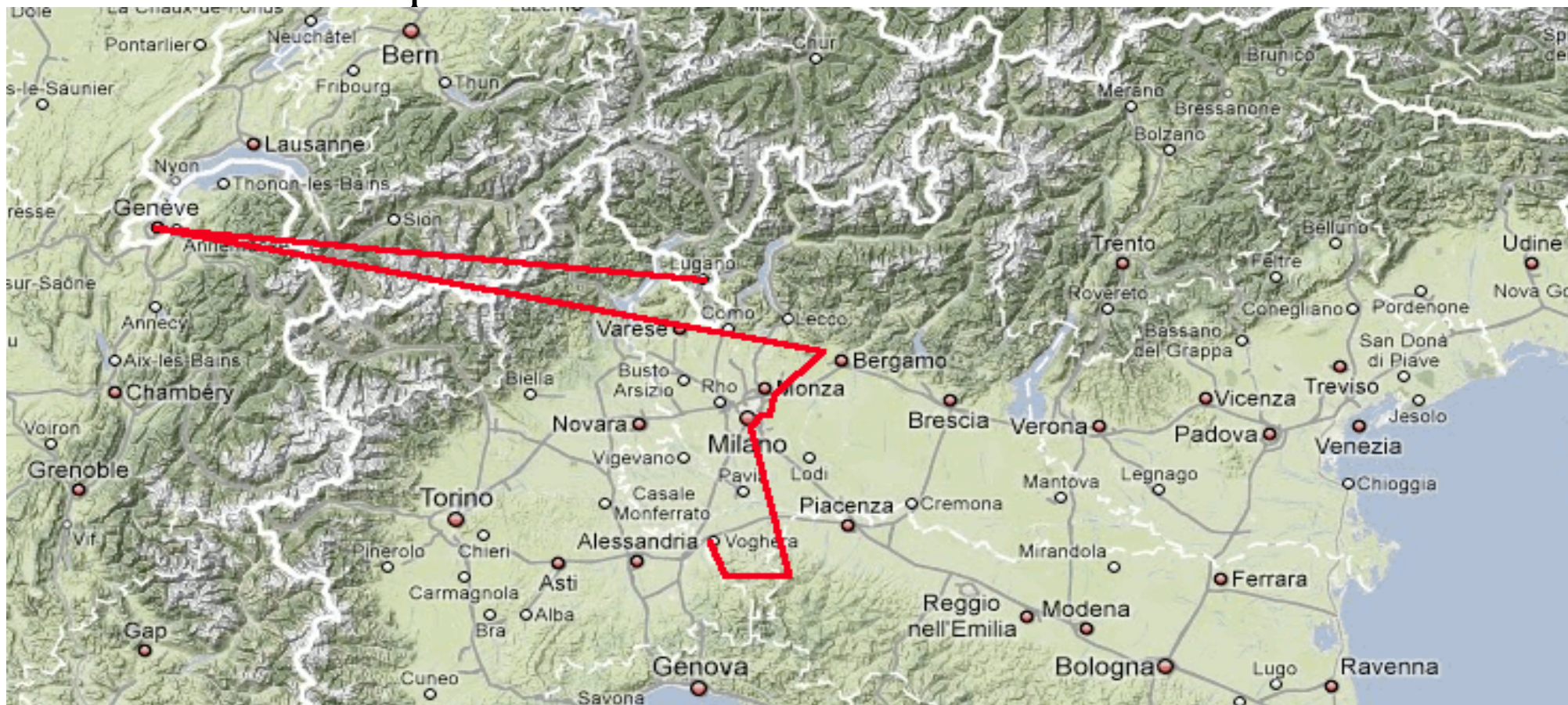
Modalità di attacco:

A seconda del punto di rete a cui si ha accesso, più o meno dati verranno intercettati, ed in seguito analizzati/raccolti

Contromisura:

Comunicare in modo che i dati trasmessi non siano comprensibili a nessuno ad eccezione del destinatario.

In un rete che non è statalmente posseduta, ne statalmente vincolata a leggi. **I dati possono essere facilmente registrati da ogni intermediario.** Io considero dovere morale di un utente proteggere i suoi dati, per se stesso e per i suoi destinatari, un po' come usare una busta chiusa per inviare una lettera, o parlarsi in modo riservato quando si sta in un ambiente affollato.



Crittografia e intercettazioni 3/8

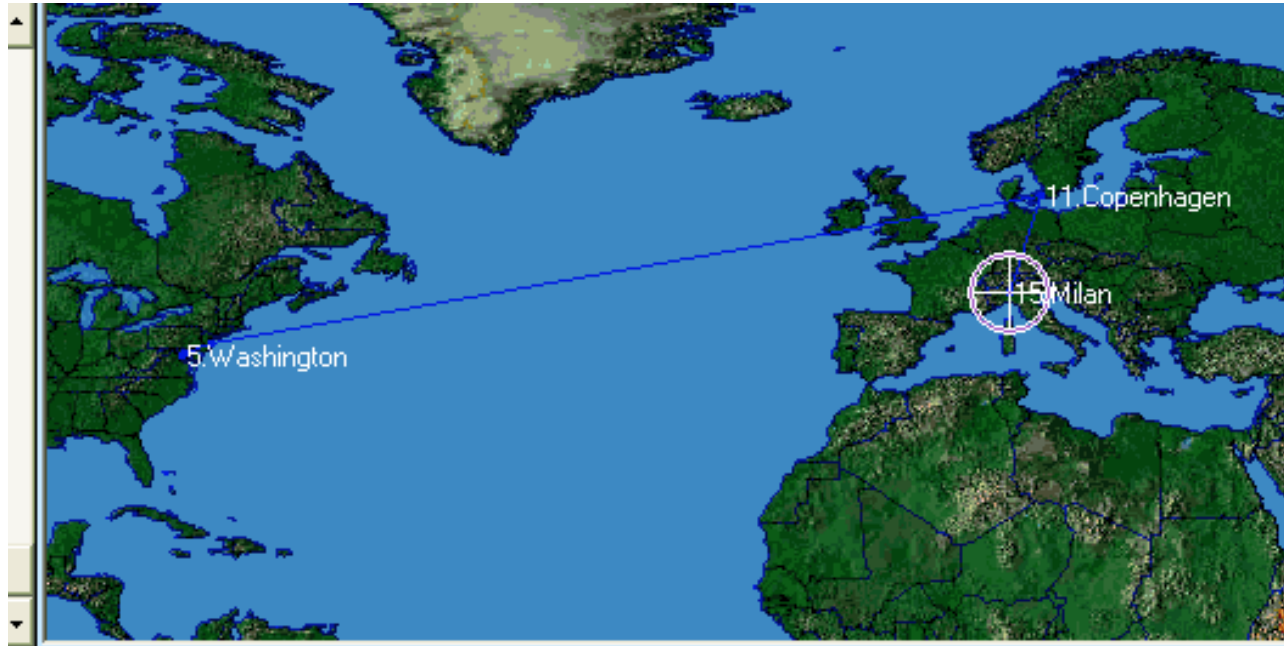
Software: visualroute

su Linux/MacOSX:

traceroute www.google.com

su Windows:

tracert www.delirandom.net



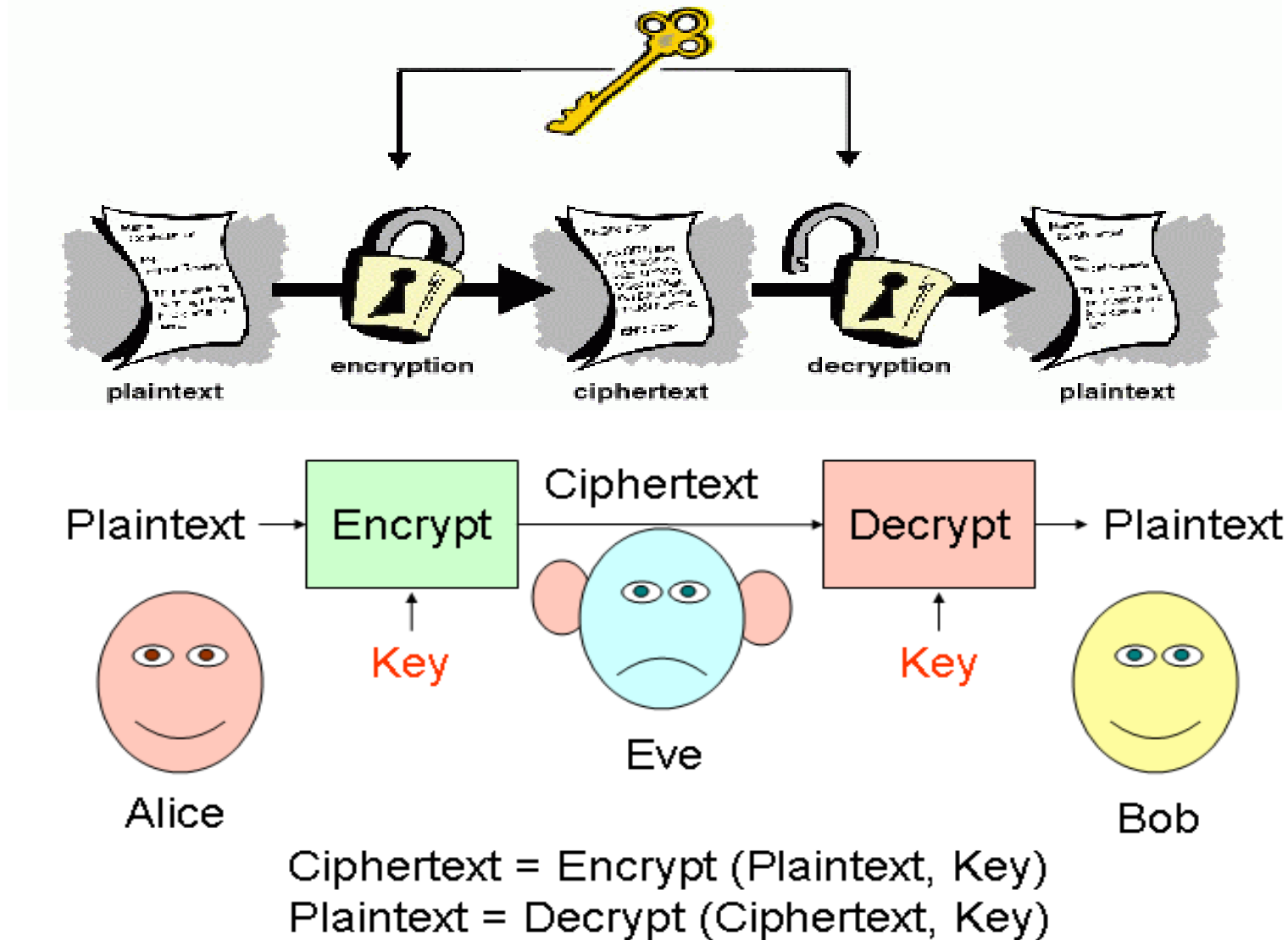
Hop	%Loss	IP Address	Node Name	Location	Tz	ms	Graph	Network
8		209.244.11.	so-6-0-0.edge	Washington, D	-05:	10		Level 3 Communi
9		209.244.219	sl-st20-ash.spi	-		16		Level 3 Communi
10		144.232.20.	sl-bb22-ry-14-	Elkridge, MD, U	-05:	18		Sprint SPRINT-INI
11		144.232.19.	sl-bb21-msq-1	Manasquan, N.	-05:	16		Sprint SPRINT-INI
12		144.232.19.	sl-bb20-cop-14	Copenhagen, [+01	99		Sprint SPRINT-INI
13		80.77.64.34	sl-bb21-cop-15	Copenhagen, [+01	112		Sprintlink DK
14		213.206.129	sl-bb21-ham-1	-		119		Sprintlink UK
15		213.206.129	sl-bb20-fra-13-	-		105		Sprintlink UK
16		213.206.129	sl-bb21-mil-13	Milan, Italy	+01	113		Sprintlink UK
17		217.147.128	sl-gw10-mil-15	Milan, Italy	+01	113		Sprintlink IT
18		217.147.129	sle-ediso-2-0.s	-		193		Sprintlink IT
19		62.94.0.129	f8-1-0.rm1.ee.e	Milan, Italy	+01	130		Edisontel S.p.A.
20	10	62.94.46.38	inet.cp.edisont	Milan, Italy	+01	143		Edisontel S.p.A.
21		194.185.46.	srp4-0.milano1	Milan, Italy	+01	164		I.NET S.p.A
22		194.185.46.	fe0-0.milano1-	Milan, Italy	+01	194		I.NET S.p.A

Crittografia e intercettazioni 4/8

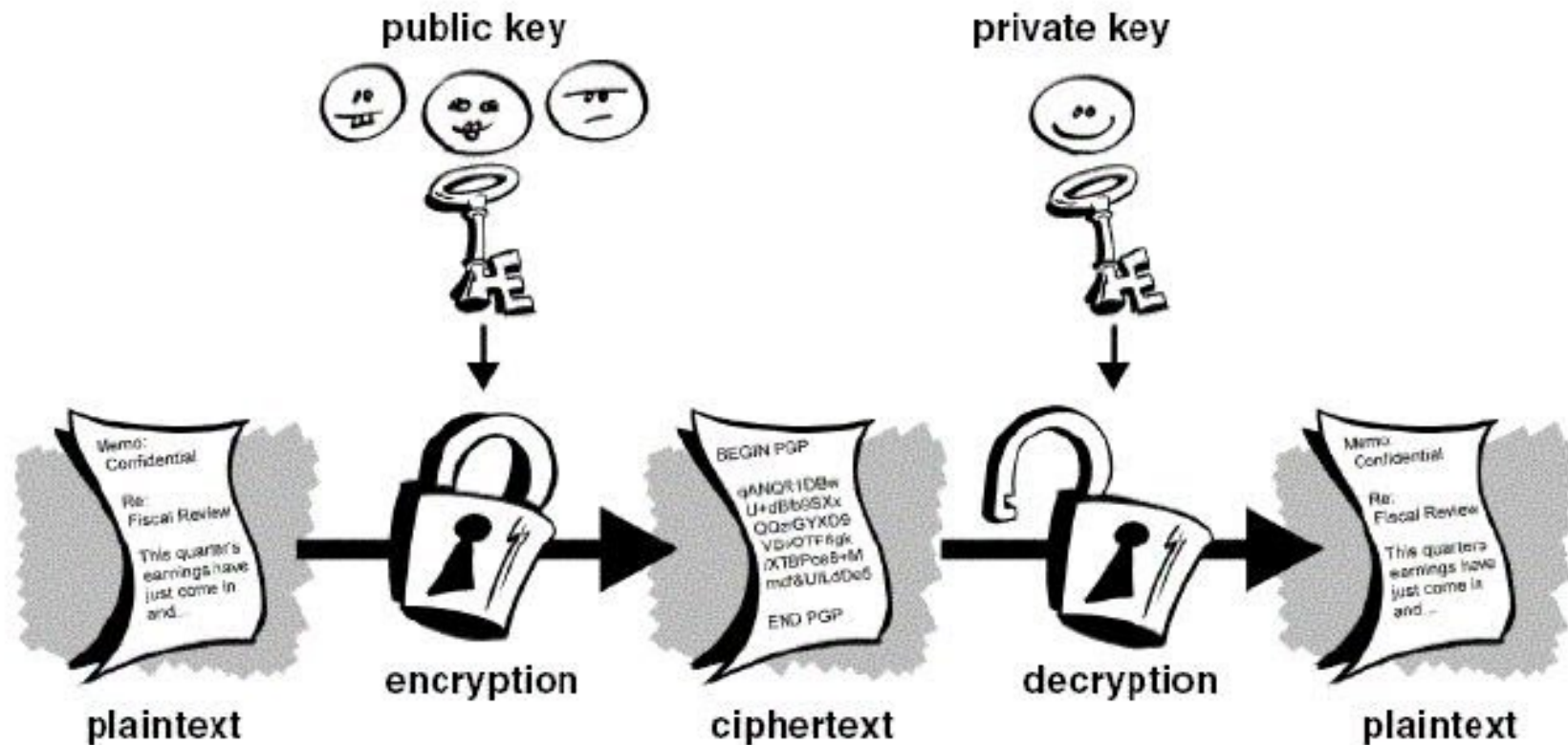
Non c'è un'indipendenza statale, e il traffico che transita è soggetto alle leggi presenti nello stato di transito. (Patriot Act ? ;)



Cifratura dei dati (e quindi, del traffico online, sia esso web, posta, chat, ...), nelle sue prima modalità: **Crittografia simmetrica**:



Cifratura dei dati (e quindi, del traffico online, sia esso web, posta, chat, ...), nelle sue seconda modalità: **Crittografia asimmetrica:**



<http://www.mozillamessaging.com/en-US/thunderbird/>

<http://enigmail.mozdev.org/home/index.php>

<http://www.gnupg.org/>

La crittografia è la tecnica che assicura la riservatezza dei dati.

A patto che l'altro comunicante la supporti

<http://vanish.cs.washington.edu/>

A patto che abbiate considerato correttamente il
“modello di minaccia”

http://e-privacy.winstonsmith.info/2003/atti/Ep2003_E-privacy_e_Infosmog.pdf

A patto che l'implementazione non sia una trappola

<http://punto-informatico.it/2558593/PI/Commenti/forza-del-voip-p2p.aspx>

A patto d'aver badato alla sicurezza locale della macchina

<http://punto-informatico.it/2700193/PI/News/skype-intercettare-si-puo.aspx>

Internet è una rete basata su **protocolli aperti**, chiunque effettui un'intercettazione, potrà acquisire i dati solo se ha i mezzi per interpretare i dati che transitano...

Solitamente, vengono utilizzati software e protocolli di default. La crittografia si usa senza difficoltà.

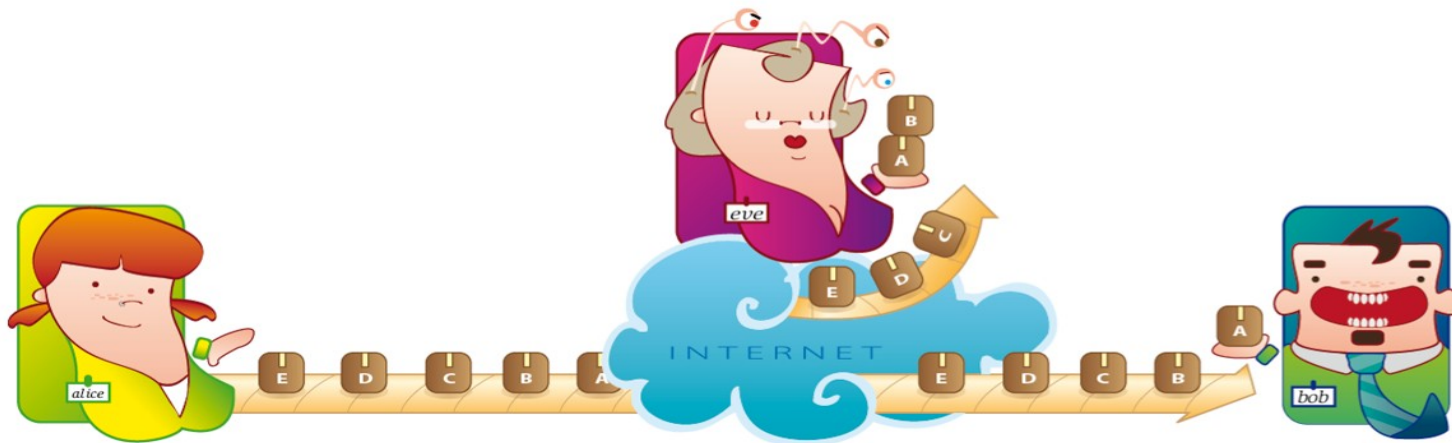
Potenzialmente chiunque può sviluppare un proprio software che comunichi in un modo nuovo/imprevisto/sconosciuto.

Questo significa che soggetti alle intercettazioni sono solo i cittadini di serie B, quelli che non se ne curano, che pensano di non aver nulla da nascondere, e chi non sa che rischi corre.

Quelli di serie A, ovvero chi teme di essere intercettato, perché è semplicemente paranoico, perché tiene alla sua privacy, perché svolge un ruolo potenzialmente attaccabile o perché vuole proteggersi dalle indagini... può farlo. E non c'è nulla che possa impedire questo fatto...

... Perché è l'elemento di forza di Internet!

Intercettazioni: attacco finale!



Without Sniff Joke

SniffJoke è un software **trasparente, libero, monodirezionale**, che rende le proprie connessioni non ricostruibili da sniffer massivi.

<http://www.delirandomnet/sniffjoke/>



With Sniff Joke

Target dell'attacco:

I dati che un cittadino ha deciso di proteggere

Cosa c'è di nuovo?:

Viene criminalizzato, generalizzato l'uso di un sistema di protezione, che se è stato scelto dall'utente è perché evidentemente ha necessità di garantire la riservatezza di alcuni suoi dati

Modalità di attacco:

Se non rivela la password, fa 2 anni di carcere.

Contromisura:

“Ogni legge che fa assunzioni, stimola la nascita di infiniti software che non la rispettano”

The only laws on the Internet are assembly and RFCs

<http://www.phrack.org/issues.html?issue=65&id=6#article>

software di plausible deniability: **Elettra**

<http://pws.winstonsmith.info/julia/elettra/>

Deniable Encryption per filesystem: **TrueCrypt**

<http://www.truecrypt.org/>

Steganografia, “l'arte della scrittura nascosta”

<http://home.comcast.net/~ebm.md/stego.html>

Triste nota: una legge da “usare contro il terrorismo”...

http://www.schneier.com/blogarchives/2008/04/more_ripa_creep.html

Non dissimile il paio di leggi US che abilitano al sequestro di PC:

http://www.schneier.com/blogarchives/2008/08/us_government_p.html

Censura “per il bene dei cittadini” 1/4

Target dell'attacco:

I dati che vengono considerati “illeciti” alla pubblicazione

Cosa c'è di nuovo?:

La censura idealmente è una pratica fascista e dittatoriale; La visione che le è stata data è come “necessario intervento” in caso di reati gravi (cioè, shockanti per l'opinione pubblica) come la diffusione di materiale pedopornografico. Una volta consolidata la tecnologia, se ne fa l'uso che si vuole.

Modalità di attacco:

Quando una scappatoia legale consente la censura, la si usa.

Contromisura:

Non usare il DNS di un ISP, usare un proxy, usare TOR.

La censura in Italia è stata diffusa per due motivazioni:

Il monopolio sul gioco d'azzardo,
La diffusione di materiale pedopornografico.

In linea “teorica” questi strumenti di blocco devono essere utilizzati quando un reato di questi due tipi viene appurato e un sito viene reso inaccessibile.

Fino a che non è stato iniziato ad usare come strumento di “oscurazione preventiva”.

Ad esempio, su ThePirateBay...

<http://thepiratebay.org/blog/123>

<http://punto-informatico.it/2718088/PI/News/cassazione-dissequestro-della-baia-va-rivisto.aspx>

La legge dice: “Ogni ISP deve premunirsi di un sistema in grado di rigirare la risoluzione di uno specifico DNS nel caso fosse richiesto dall'entità preposta”.

La risoluzione DNS è l'operazione che converte un nome di dominio: (www.google.com) in un indirizzo IP (20985.129.103) lo rigira ad un altro indirizzo IP (quello deciso dalla procura).

Ma un server DNS puo' non essere di un ISP,
Puo' non essere italiano,
Puo' essere il proprio computer.

Iniziativa "libera": <http://it.peacereporter.net/libera>

Tratta il fenomeno della censura effettuato da stati dittatoriali (ma anche no, la censura come semplice limitazione della propria espressione e libertà di parola).

Contiene spunti su:

Censura e democrazia, necessità dei cittadini di essere informati

Anonimato come diritto (per/del) le minoranze

Oni: <http://opennet.net/>

PsyOp in ambienti di conflitto e non.

Soluzioni non comuni (telefoni satellitari)

Soluzioni diffondibili, TOR e reti collaborative

Progetto Winston Smith

<http://punto-informatico.it/2594786/PI/Commenti/informazione-libera-online.aspx>

Target dell'attacco:

Gli utenti che rivelano notizie non conformi all'immagine che un regime dittatoriale vuole dare di se, all'estero e all'interno.

Cosa c'è di nuovo?:

Chiunque puo' avere un cellulare in grado di riprendere, chiunque puo' in tempo zero diffondere questi media online, superando quindi ogni forma di censura.

Modalità di attacco:

Controllare la rete nazionale, censurare l'accesso ai maggiori hub internazionali.

Contromisura:

bypassare censura ed al controllo, usare hub atipici.

Birmania 10/2007

Per la prima volta si vede l'utilizzo massiccio dei cellulari per finalità di comunicazione giornalistica. Dopo 3 giorni di leaks, l'unico link Internet verso l'estero viene interrotto.

<http://punto-informatico.it/2077266/PI/News/rete-rosso-vestita.aspx>

<http://punto-informatico.it/2074778/PI/News/myanmarweb-oltre-crisi.aspx>

Cina/Tibet 02/2008

a Lasha si scatenano rivolte dei tibetani, c'è lo zampino dei media occidentali che per una volta utilizzano la disinformazione per un motivo politico (*una mezza verità è una menzogna*, ma vabbè) che stranamente ha anche una certa importanza sociale. Su youtube e sui blog piovono notizie da parte di improvvisati giornalisti, la censura cinese ha effetto per lo più all'interno, ma il resto del mondo ha ciò che gli era stato preparato.

Iran 2009

facebook, per questioni di quantità d'uso, diventa il punto di riferimento temporaneo dove scambiarsi informazioni. Giornalisti e blogger iniziano la ripresa degli eventi, e questo stimola inizialmente la sensazione che la rete aiuti, effettivamente, la fuoriuscita di informazioni altrimenti censurate. (twitter segue)

<http://thelede.blogs.nytimes.com/> E' il primo giornalista a fare un'azione di giornalismo atipico. Egli sa di non poter essere in loco, ne di potersi affidare a risorse informative dirette. Ma anche che non è etico ne efficiente copiare informazioni tratte da altre fonti non autorevoli. Il suo lavoro è quello di scremare le informazioni reperite in rete e valutare al meglio la loro attendibilità.

Si rischia al massimo la parzialità della selezione
Ha dimostrato il funzionamento della teoria dei 6 HOP per puro caso, nel tentativo di far chiarezza sulla morte di Neda.

Target dell'attacco:

Le persone e la loro facile seduzione dal gratuito,
Le persone in quanto cacciatori di informazioni.

Cosa c'è di nuovo ?:

Prima era il regime ufficiale

Poi il regime de-facto

Ora un bel predefinito disegno mascherato come “tua scelta”

Modalità di attacco:

Google Search, Google News; iniziative encomiabili come Digg

Contromisura:

troppe o nessuna ? :) trattate alla slide

Certezza consolidata:

La presenza di portali, servizi e programmi, totalmente gratuiti agli utenti, rende gli utenti felici.

E pensano forse che società milionarie quotate in borsa, con spese di ricerca, tecnologia e personale enormi, facciano i **benefattori della rete** ?

Sapendo soprattutto, che gli introiti derivati dall'ADV online sono ben ristretti (finché si parla di banner e testi ?)

La profilazione:

E' la tecnica con la quale viene stilato un "profilo" di un utente. Analogamente al profilo di un volto, serve a riconoscere i tratti generali, non i tratti di dettaglio.

Quanto è possibile arbitrare l'opinione degli utenti ?



Digg & Google, la democrazia conformista della “votazione”.

The Imagined International Community: Dominant American Priorities and Agendas in Google News

<http://lass.calumet.purdue.edu/cca/gmj/fao8/graduate/gmj-fao8-grad-segev.htm>

YouTube, censura, muto, featured video: La possibilità di GoogleTube di sapere con quale percentuale, con quali meccanismi, un utente sceglie un link piuttosto che un altro si basa su una quantità di dati unica al mondo.

La profilazione all'interno di una rete sociale consente di eliminare il falso positivo, di soppesare l'importanza delle informazioni raccolte proporzionalmente a quanto la persona sia “viva” online.

googleapis.com, google-analytics.com, ads, search, youtube embedded... la visione che puo' avere un'entità simile è unica, enorme, terribile.

La percezione della disinformazione cessa di essere obiettiva.

Esistono soluzioni ?

Esperimenti come DIGG sono funzionali, ma hanno vulnerabilità legate all'organizzazione di gruppi di utenti.
(filtro collaborativo)

<http://punto-informatico.it/2298862/PI/Commenti/contrappunti-google-non-trova-orienta.aspx>

L'utilizzo del web of trust puo' essere una soluzione, ma mancano ancora implementazioni pratiche.

Offuscare il proprio profilo inondando i servizi di dati falsi

<http://mrl.nyu.edu/~dhowe/trackmenot/>

Ok il web, ma non cambiando il modello di informazione ...?

http://mediablog.corriere.it/2009/10/il_web_prima_fonte_per_le_news.html

<http://punto-informatico.it/2427926/PI/Commenti/contrappunti-una-mela-lava-altra.aspx>

<http://punto-informatico.it/2576412/PI/Commenti/contrappunti-italia-vista-conto-terzi.aspx>

Lo stesso “pluralismo” delle fonti sia tale per i fornitori di news:

<http://yacy.net/>

EOF

Grazie dell'attenzione!

```
pub 1024D/C6765430 2009-08-25 [expires: 2011-08-25]
Key fingerprint = 341F 1A8C E2B4 F4F4 174D 7C21 B842 093D C676 5430
uid          vecna <vecna@s0ftpj.org>
uid          vecna <vecna@delirandom.net>
sub 3072g/E8157737 2009-08-25 [expires: 2011-08-25]
```