Privacy in rete:
una panoramica della situazione internazionale

Alessio Frusciante
algol@firenze.linux.it

Convegno “E-Privacy: riservatezza e diritti individuali in rete”

Firenze, Palazzo Vecchio - 27 Aprile 2002

Sommario

- Stati Uniti
  - USA PATRIOT act
  - Carnivore/DCS-1000
  - Anonimato - CyberSLAPP
  - ITAR
  - Clipper Chip
- Comunità Europea
  - Echelon
  - RIP act (UK)
- Cina

USA PATRIOT act

Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism.

- Proposta il 19 settembre 2001, votata il 26 ottobre 2001.
- Riguarda molti campi, ben oltre la privacy elettronica.
- Articoli a validità limitata nel tempo (31 dicembre 2005)
- Articoli a validità illimitata.

USA PATRIOT act

- Meccanismi di sorveglianza
  - Intercettazioni
  - Perquisizioni
  - Dispositivi “pen-register” e “trap and trace”

USA PATRIOT act

- I dati inviati sulla rete possono essere monitorati, su ordine di un giudice, indipendentemente dal fatto che la persona sia indagata, se si reputa che ciò sia rilevante per un'indagine.
- Si estende la sorveglianza per atti non terroristici (Computer Fraud and Abuse Act).
- Si estende la definizione di terrorismo.
- Estensione dei dispositivi pen/trap and trace alle comunicazioni via internet.
  - Problema: i dati e le informazioni di instradamento sono mescolate tra loro.
  - Questa norma non scade.
  - In questo articolo si fa esplicita menzione di Carnivore/DCS-1000 come dispositivo da adottare per la sorveglianza.

Carnivore/DCS-1000

- Dispositivo sviluppato per FBI dalla NSA (National Security Agency).
- Analogo agli sniffer utilizzati comunemente.
- Necessita dell'ordine di un giudice per essere installato.
  - Il giudice deve specificare la persona da tracciare e quali dati vanno tracciati.
- I dettagli di funzionamento non sono noti, anche se una richiesta di EPIC ha permesso di rendere pubblico almeno il funzionamento a grandi linee.

CyberSLAPP

Strategic Lawsuits Against Public Participation

- Cause intentate strategicamente contro chi protesta.
- Hanno il cosiddetto “chilling effect”, ossia intimidatorio contro chi si mobilita.
- Chi perde deve anche pagare i danni di immagine subiti dall’azienda.
- Tipico esempio: ambientalisti.

CyberSLAPP

- Anonimato tutelato dalla costituzione statunitense.
- Possibilita‘ di attacco
  - Diffamazione.
  - Leggi di copyright o dei marchi.
  - Rivelazione di segreti industriali da parte di dipendenti di un’azienda.

CyberSLAPP

- Gli ISP hanno i mezzi per risalire all'autore di un messaggio.
- Gli ISP non possono rivelare informazioni confidenziali su un cliente.
- Di fronte ad una citazione sono pochi gli ISP che non rivelano tali informazioni, anche perché potrebbero essere citati a loro volta.
- Possibile tutela: anonimato "forte".

Crittografia negli USA

- ITAR International Traffic in Arms Regulations
- L'esportazione di crittografia era regolata dalla stessa legge che regolava l'esportazione di armi.
- Permessa solo l'esportazione di crittografia debole.
- Mettere un programma accessibile su internet era considerato esportazione.
- Grossi problemi per l'hardware.

Crittografia negli USA

- Problemi aggirabili per il software usando patch o interi archivi che si trovano fuori dagli Stati Uniti.
- Fino al 2000 alcuni noti browser prodotti negli Stati Uniti usavano solo crittografia debole.
- Le leggi sono gradualmente cambiate negli anni, allentando i controlli.
- Attualmente i programmi di cui viene fornito il sorgente sono esenti da restrizioni.
- Rimangono sempre fuori i “paesi terroristi” Cuba, Corea del Nord Iran, Iraq, Libia, Sudan e Siria.

Crittografia negli USA

Il caso Bernstein

- Nel 1995 insieme alla EFF ha fatto causa all'agenzia per il controllo delle armi, sostenendo che l'ITAR e le successive EAR erano incostituzionali.
  - ⋆ Code as speech.
- Questo caso è stato importantissimo, in quanto ha dichiarato incostituzionali le norme che impedivano l'esportazione di codice sorgente. È stato un motivo fondamentale per il cambio delle leggi.
- Bernstein sta tuttora facendo causa in quanto è comunque necessaria un'autorizzazione governativa prima dell'esportazione.

Il Clipper Chip

Dispositivo crittografico, per cifrare le comunicazioni vocali, in modo che non fossero intellegibili a terze parti

- Algoritmo segreto, skipjack, scritto dalla NSA.
- Vantaggio per FBI: NSA poteva decifrare qualsiasi messaggio in quanto aveva una sorta di passepartout.
- Key escrow (o key recovery).
- Critiche all'approccio
  - Gli algoritmi segreti non sono sottoposti a peer reviewing.
  - Difficilmente sarebbe stato usato da criminali che volevano nascondere i loro messaggi.
  - Il key escrow è intrinsecamente una cattiva idea, perché dà un percorso alternativo di accesso ai dati cifrati, che costituisce un punto debole del sistema.

Echelon

- Sistema di sorveglianza molto ramificato a cui partecipano
  - Stati Uniti
  - Regno Unito
  - Canada
  - Australia
  - Nuova Zelanda
- Il progetto originario sembra essere del 1971.
- Intercetta comunicazioni di molti tipi diversi, dalle telefonate satellitari ai messaggi email.

Echelon

- Il parlamento europeo ha formato una comissione di inchiesta.
- I responsabili della NSA e della CIA si sono rifiutati di incontrare la commissione.
- Nel 2001 la commissione di inchiesta ha pubblicato un documento in cui si afferma che Echelon esiste nonostante gli Stati Uniti lo neghino, e si consiglia agli stati membri di diffondere l'uso della crittografia per proteggere i propri cittadini.
- La commissione non aveva abbastanza dati per decidere quali comunicazioni erano state spiate.
- Contemporaneamente negli Stati Uniti EPIC ha richiesto uno studio sulla NSA a proposito delle attività di sorveglianza dei cittadini statunitensi.

RIP

Regulation of Investigatory Powers

- Entrato in vigore nel 2000 nel Regno Unito.
  - Nel caso che un sospetto utilizzi comunicazione cifrata dovrà fornire le chiavi per decifrarla, pena 2 anni di detenzione.
  - Chi abbia fornito le chiavi agli investigatori non può dirlo ad una terza parte.
  - È ammesso dimenticarsi una chiave.
- Installazione di ”black boxes” negli ISP, simili a Carnivore.
- È quantomeno improbabile che un terrorista tema due anni di prigione.
- Possibile tutela: steganografia.

RIP

Le libertà preesistenti a queste leggi hanno in qualche modo impedito di rintracciare efficacemente i terroristi?

Repubblica popolare cinese

- Si stimano 60 milioni di utenti internet in Cina.
- Firewall e router controllati a livello nazionale.
- Filtrati siti considerati non adatti per il contenuto.
- I motori di ricerca cinesi non riportano i siti scomodi.
- Chiusura di moltissimi internet cafè e installazione di software di sorveglianza sui rimanenti.

Organizzazioni per i diritti nel ciberspazio

- Electronic Privacy Information Center http://www.epic.org
- Electronic Frontier Foundation http://www.eff.org
- Center for Democracy and Technology http://www.cdt.org
- Computer Professionals for Social Responsibility http://www.cpsr.org