

tesi di laurea

Rilevamento dell'analisi della censura di Internet su reti mobili

Anno Accademico 2014/2015

relatore

Ch.mo prof. Antonio Pescapé

correlatore

Ing. Giuseppe Aceto

candidato

Giovanni Gentile

Matr. M63/000338

Contesto e contributo

Contesto

- Con l'espressione "**censura di Internet**" si intende il controllo o il blocco della pubblicazione di contenuti , o dell'accesso ad essi, nella rete Internet.
- Tale censura può essere effettuata dal governo o da società private su richiesta del governo, da un'autorità di controllo, o di propria iniziativa.

Progetto UBICA

UBICA (*User-Based Censorship Internet Analysis*) è una piattaforma per la rilevazione e l'analisi di dati di censura tramite un approccio **user-based**

Basato sulla piattaforma HoBBIT per la valutazione delle prestazioni delle connessioni ad Internet

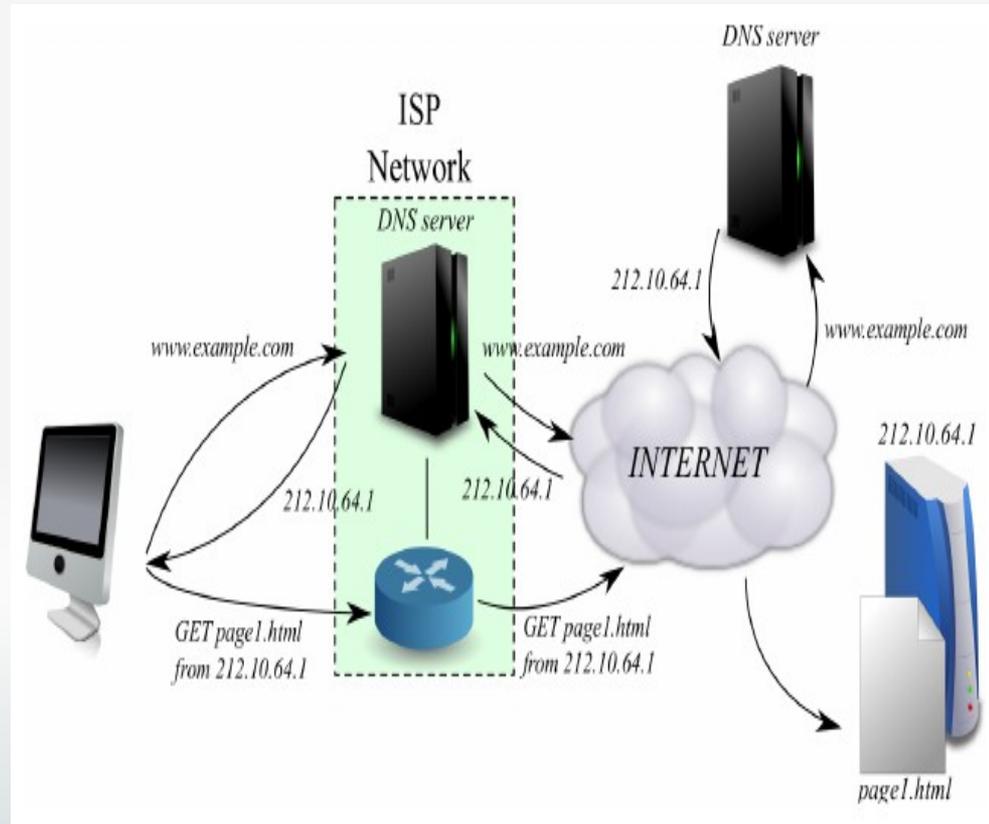
Contributo

Progettazione e sviluppo di un algoritmo per la raccolta e l'analisi di dati di monitoraggio della censura su reti mobili

Motivazioni ed obiettivi

Motivazioni

- Nessuno studio antecedente questo, in ambito mobile in Italia...
- ...in Turchia :
- Utilizzo di una metodologia dedicata emulando il comportamento dell'utente
- Censura applicata tramite un uso non standard dei protocolli di comunicazione
- Distinguere tra applicazione di censura e problema temporaneo o permanente di uno dei nodi



• Obiettivo

- Studiare il fenomeno al fine di rispondere alle domande presentate in seguito

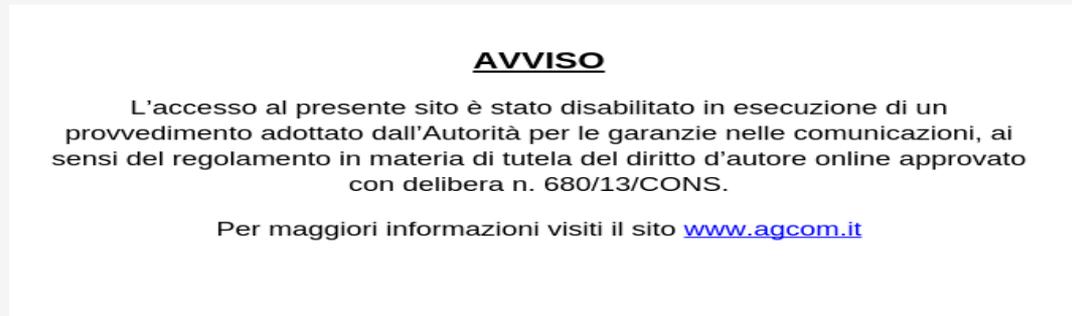
Dove e come agisce la censura e quali sono gli effetti sull'utente

DNS

- Poisoning
- Injection
- Redirect
- Errors

1)

Cosa potrà visualizzare l'utente:



TCP

- Reset
- Timeout
- Filtering

2)



HTTP

- Blocking
- Filtering
- Redirect

3)

Ottenimento, a sua insaputa, di una pagina diversa da quella richiesta

Variabili in gioco

nell'applicazione della censura

WISP (Wireless Internet Service Provider)

- Responsabile di fornire la connettività all' utente
- Applica la censura del paese in cui opera
- Esistono WISP reali e virtuali (es. Poste Mobile)

Quelli analizzati coprono il 96,5% delle quote di mercato[2]



Server DNS

- Traduce i nomi di dominio in indirizzi IP
- Ogni WISP offre la risoluzione tramite un proprio server DNS (default)
- E' possibile effettuare una risoluzione tramite un server non appartenente alla rete del WISP (open)



Finger-printing

- Insieme delle informazioni che servono ad identificare un utente
- La maggior parte di esse è inclusa nella stringa User-Agent
- User-Agent utilizzati : 2 Mobile (Android e IOS),
1 Desktop (Google Chrome), 1 Web-Crawler (Googlebot)

[2] Osservatorio MVNO, www.mvnonews.com/osservatorio-mvno/

Progettazione di un algoritmo di rilevazione della censura

Approccio User-based

Target : URL della pagina Web

```
target=www.example.com/
```

```
FOR EACH SERVER DNS
```

```
  FOR EACH USER-AGENT{
```

```
    While ( target != 'vuoto' )    {
```

```
      lista ← APPEND_LIST (target)
```

```
      proto,host,path ← DIVIDE (target)
```

```
      hostip ← DNS_RESOLVE (serverDNS, host)
```

```
      header,content ← CURL_REQ (target, hostip, useragent)
```

```
      target ← EXTRACT_LOCATION (header)
```

```
    }
```

Consumo dati medio calcolato:

- Per un WISP : 40 MB
- Per singolo target : 5 KB

Per ogni richiesta di una pagina:

- Salva header e content
- Segue eventuali redirect e ne salva le informazioni → analizzare cambi di schema URL

Test effettuati su una lista di 200 target, fornita dal sito censura.bofh.it, relativi a sentenze emesse negli ultimi anni

Presentazione degli obiettivi 1

Gli obiettivi sono stati posti sotto forma di 8 domande, le risposte più interessanti...

1) Quante e quali esperienze di navigazione diverse sperimenteranno gli utenti, nel richiedere una risorsa?

Le principali:

- Risoluzione DNS diversa, Default: Restituzione Ind. Not routable, Open: Contenuto 26,1%*
- Risoluzione DNS diversa, Default: Pagina di blocco, Open: Contenuto 15,1%*
- Risoluzione DNS diversa, Default: Restituzione Ind. vuoto, Open: Contenuto 14,7%*

2) Ci saranno differenze tra un WISP virtuale e il relativo WISP reale che noleggia l'architettura?

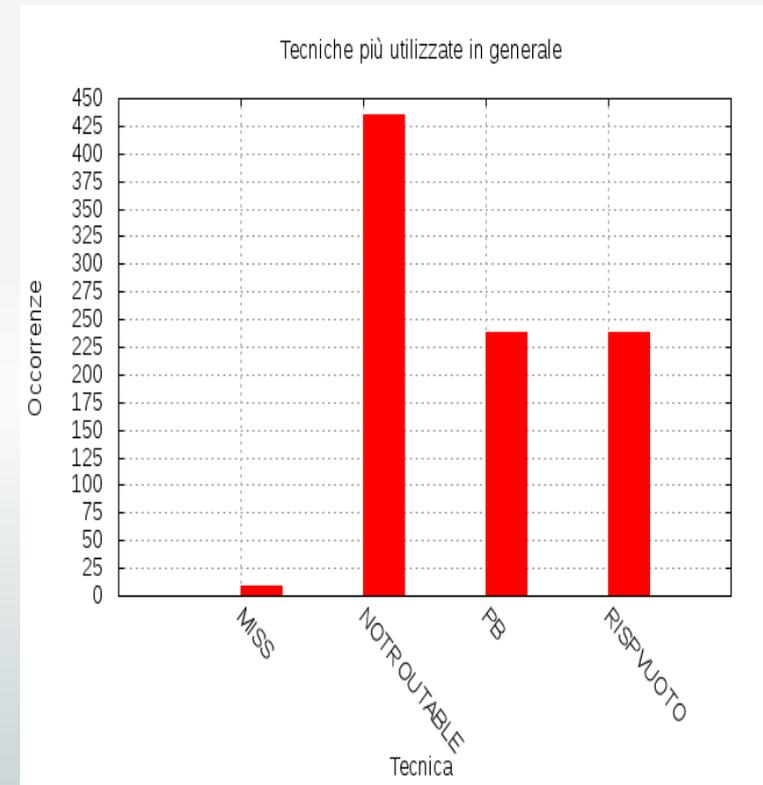
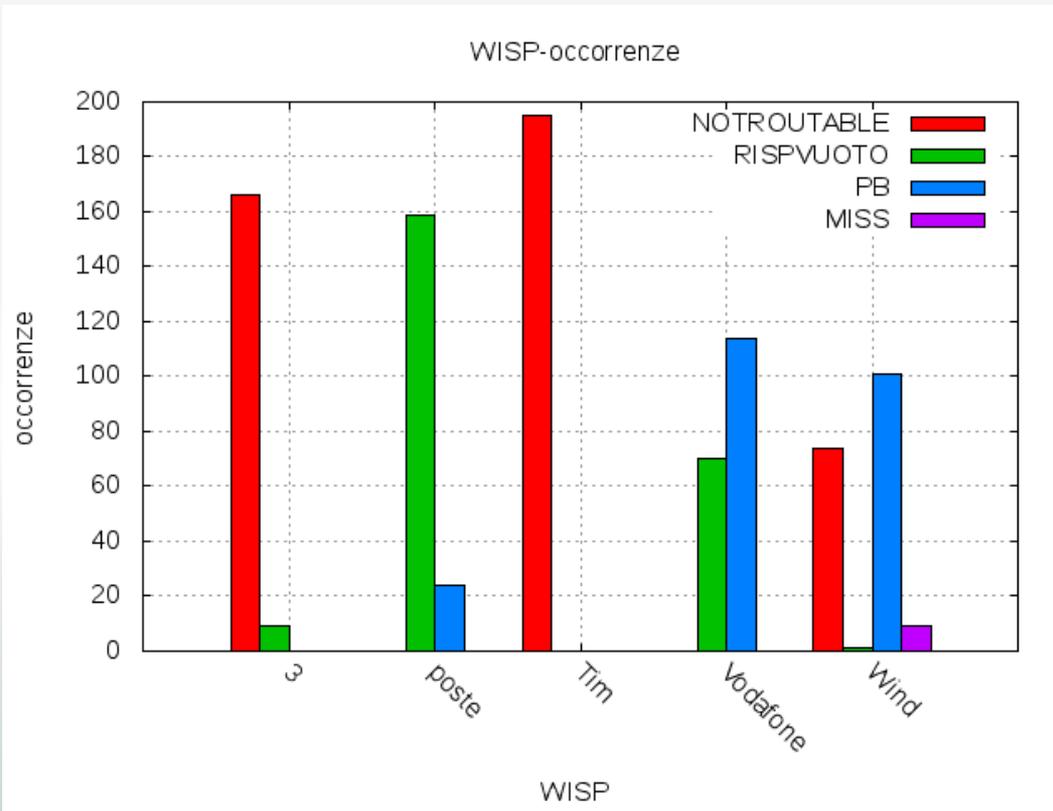
Stessa architettura? Stessa censura?



Il WISP virtuale non ha applicato lo stesso tipo di censura dell'operatore dal quale noleggia l'architettura nel 95% dei casi

Presentazione degli obiettivi 3

3) Quali sono le tecniche più usate da ogni WISP? Quali sono le tecniche più usate in generale?



Presentazione degli obiettivi 4

4) *Sono stati rilevati casi di target non bloccati con una tecnica non DNS?*

Caso 1 ispezionato manualmente : mp3limone.net

Vodafone, l' header della risposta:

```
HTTP/1.1 503 Service Unavailable
Server: WebProxy/1.0 Pre-Alpha
Date: Mon, 08 Feb 2016 10:56:13 GMT
Content-Length: 0
Connection: keep-alive
```

Per tutti gli altri WISP:

- Richiesta Indirizzo IP
- Ottenimento Indirizzo IP **Fase DNS OK**
- Invio SYN
- Ottenimento di un RST **Impossibile stabilire connessione TCP**

Non è possibile fare ulteriori ipotesi, la risorsa non è mai stata raggiunta

Presentazione degli obiettivi 5

Caso 2 ispezionato manualmente : steroid4u.org

Vodafone, ispezionando l' header della risposta:

```
HTTP/1.1 504 Gateway Time-out
Server: WebProxy/1.0 Pre-Alpha
Date: Mon, 08 Feb 2016 11:30:37 GMT
Content-Length: 0
Connection: keep-alive
```

Tim e Poste, ispezionando la cattura:

- Richiesta Indirizzo IP
- Ottenimento Indirizzo IP
- Invio SYN
- Nessuna risposta

Fase DNS OK

Impossibile stabilire connessione TCP

Per Wind e 3 invece...

- Richiesta Indirizzo IP, Ottenimento Indirizzo IP
- Invio SYN, Ottenimento SYN+ACK , Invio ACK
- Richiesta Pagina
- Ottenimento Pagina, response_code = 200

Fase DNS OK

Fase TCP OK

Fase HTTP OK

Un solo caso rilevato di Tcp filtering

Due casi di blocco tramite proxy server, entrambe per lo stesso WISP.

Conclusioni

- I risultati ottenuti nel rilevamento della censura in ambito mobile sono stati verificati attraverso 3 campagne di test
- Utilizzare una risoluzione DNS open è risultato efficace nella quasi totalità dei casi
- 2 casi su 200 hanno mostrato blocchi tramite tecniche non DNS, per un WISP, nei quali anche un utente più esperto, non avrebbe comunque raggiunto il contenuto
- Un monitoraggio continuo delle tecniche utilizzate e lo studio di nuove, è quindi utile a garantire l'affidabilità alle informazioni che la rete ci fornisce.

Sviluppi futuri

- E' possibile utilizzare un criterio di scelta dei target, al fine di realizzare un test parziale, riducendo i consumi della connessione dati del WISP
- Aumentare la durata delle osservazioni e la frequenza degli esperimenti
- Uso del crowdsourcing, cioè la segnalazione da parte degli utenti di una possibile censura, tramite un APP mobile

Grazie!