UNIVERSITA' DEGLI STUDI
DI TORINO

DIPARTIMENTO
DI INFORMATICA

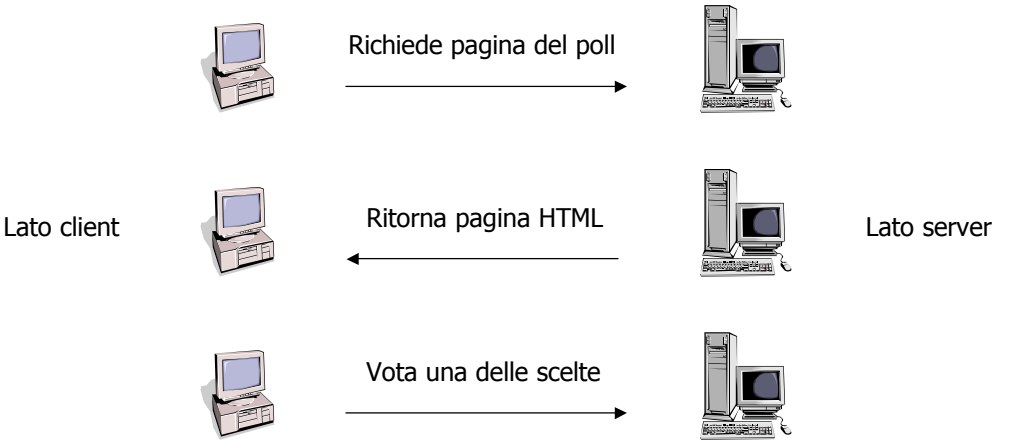
Internet Polls Sicuri

Un approccio innovativo alla sicurezza degli Internet polls

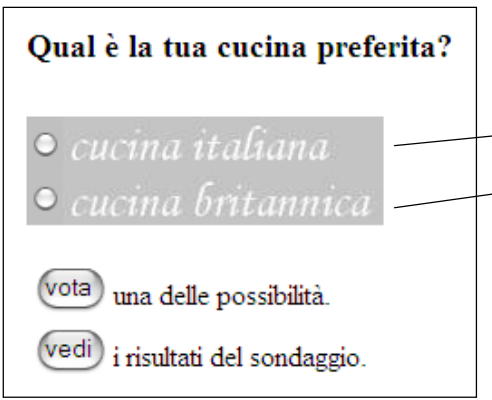
Internet Poll

- Internet Poll = sondaggio in Internet
- Fenomeno recente e in costante diffusione
- Importanza dell'attendibilità dei risultati di un sondaggio
- Difficile garantire l'affidabilità di un sondaggio in Internet

Struttura di un sondaggio



Struttura di un sondaggio (2)



- Ad ogni scelta viene associato un id:
  - cucina italiana -> id1
  - cucina britannica -> id2
- L'id consente al server di identificare univocamente la scelta

Sicurezza degli Internet polls

- Vincoli:
  - il browser non può essere modificato
  - impossibile distribuire password ai votanti
  - NAT, Proxy, IP dinamico (ISP)
  - gli utenti si possono connettere da postazioni differenti

Stato dell'arte

- Situazione di scarsa sicurezza che attualmente caratterizza i polls
- I risultati possono essere facilmente alterati attraverso meccanismi di voto automatico
- Non viene garantita la possibilità di voto ad ogni utente della rete

Meccanismi di protezione

- Due tecniche utilizzate per prevenire alterazioni dei risultati di un poll:
  - *IP locking*
  - *Cookie method*

IP locking

- Effettua il controllo sull'indirizzo IP del client
- Se IP è gia presente nel DB -> il client ha già votato
- Sicurezza elevata: l'utente non può effettuare votazioni multiple

IP locking (2)

- Problema con alcune categorie di utenti:
  - utenti connessi da LAN che usano il NAT
  - utenti connessi attraverso un Proxy
  - utenti connessi attraverso indirizzi IP dinamici
  - utenti connessi da postazioni multi-utente

IP locking (3)

- Queste categorie di utenti non possono votare correttamente dal momento che condividono lo stesso indirizzo IP
- Tentativi di miglioramento:
  - *Browser header*
  - *Time interval*

I risultati comunque non soddisfacenti

Cookie method

- Il server utilizza il cookie per tenere traccia delle votazioni dei clients
- Problema: i cookie risiedono sul client quindi possono essere cancellati -> possibili votazioni multiple
- Livello di sicurezza molto basso

Una soluzione innovativa

- Obiettivi:
  - ottenere un livello di sicurezza più elevato
  - garantire la possibilità di votare anche in presenza di NAT, Proxy, indirizzi IP dinamici e postazioni multiutente
  - mantenere la semplicità e l'immediatezza nell'interfaccia di voto che caratterizza gli attuali Internet polls

CAPCHA

- CAPCHA = "*Completely Automatic Public Turing Test to tell Computers and Humans Apart*" (Blum, Ahn, Langford)
- Insieme di tests che un essere umano può passare ma che un computer fallisce

L'idea

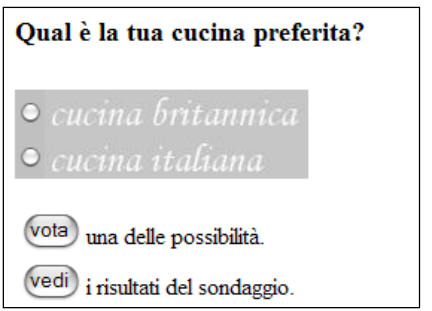
Come si può impedire la votazione da parte di software automatici?

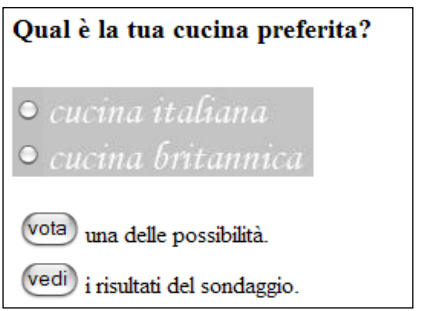
Evitare che i parametri di voto vengano memorizzati sul client in forma comprensibile da un computer

CAPTCHA che sfrutta il gap nell'abilità di visione tra computer ed esseri umani applicato all'ambito dei polls = *sistema order-based*

Il sistema order-based

- Le scelte del sondaggio sono contenute in un'unica immagine creata a runtime in maniera sempre differente





Il metodo in dettaglio

- L'immagine viene ricreata ad ogni richiesta della pagina del poll
- L'ordine delle scelte è variabile in modo casuale, quindi non determinabile
- L'ordine delle scelte viene deciso mediante una rotazione della lista delle scelte intorno ad un elemento perno
- Lo *schema di mapping* (scelta <--> id) scelto dal server è memorizzato in forma cifrata in un cookie, sul client

Il metodo in dettaglio (2)

- Quando un client vota, il cookie viene inviato al server insieme all'id scelto
- Il server ricostruisce l'associazione tra id e scelta mediante lo schema di mapping contenuto nel cookie
- Un software di voto automatico non può determinare i legami tra scelte e id --> non è in grado di decidere la scelta da votare
- Solo un essere umano può effettuare la scelta di voto corretta, osservando l'immagine

Ulteriore sicurezza

- Sistema order-based + Cookie method
- Il flag di voto è memorizzato nel cookie insieme allo schema di mapping, in forma cifrata
- Impedite le votazioni multiple da un singolo client
- Cancellare il cookie non consente di votare in maniera automatica poichè non si conosce lo schema di mapping

Impossibile determinare l'id della scelta da votare

Proprietà dell'immagine

- Difficile da analizzare per un OCR
- Carattere opportunamente scelto (stile italico, grazie...)
- Qualità povera ma sufficientemente elevata da risultare facilmente comprensibile
- Prevenire identificazioni attraverso l'uso di funzioni hash --> tonalità di alcuni pixels variabile

Vantaggi del nuovo sistema

- Determina un costo significativo nella realizzazione di software per il voto multiplo e automatico
- È possibile effettuare votazioni multiple, ma solo manualmente

irrealizzabile nel caso di ingenti alterazioni dei risultati di un poll

Open Challenge

- Open Challenge = sondaggio pubblico in cui i partecipanti cercano di "forzare" lo schema di protezione proposto
- Mettere alla prova l'efficacia della soluzione sviluppata
- Due scelte inizializzate con un numero di voti elevato in proporzioni uguali (50%)
- Scopo = portare la percentuale di una scelta al 90% entro un tempo massimo
- Impossibile la falsificazione manuale dei risultati

Poll management

- Sistema di gestione dei polls che sfrutta la tecnica di protezione da noi sviluppata
- Permette di:
  - creare un proprio utente
  - realizzare e configurare sondaggi riguardo ad un generico argomento
  - elencare tutti i sondaggi attivi
  - avviare, sospendere o eliminare un sondaggio
  - ottenere i links dei sondaggi da inserire nelle proprie pagine web

Web e Contatti

- Dettagli relativi al challenge ed al sito di poll management:

  http://security.di.unito.it/research/ipoll.html

- Si ringrazia la Regione Piemonte e Sinapsi per il contributo alla realizzazione del progetto