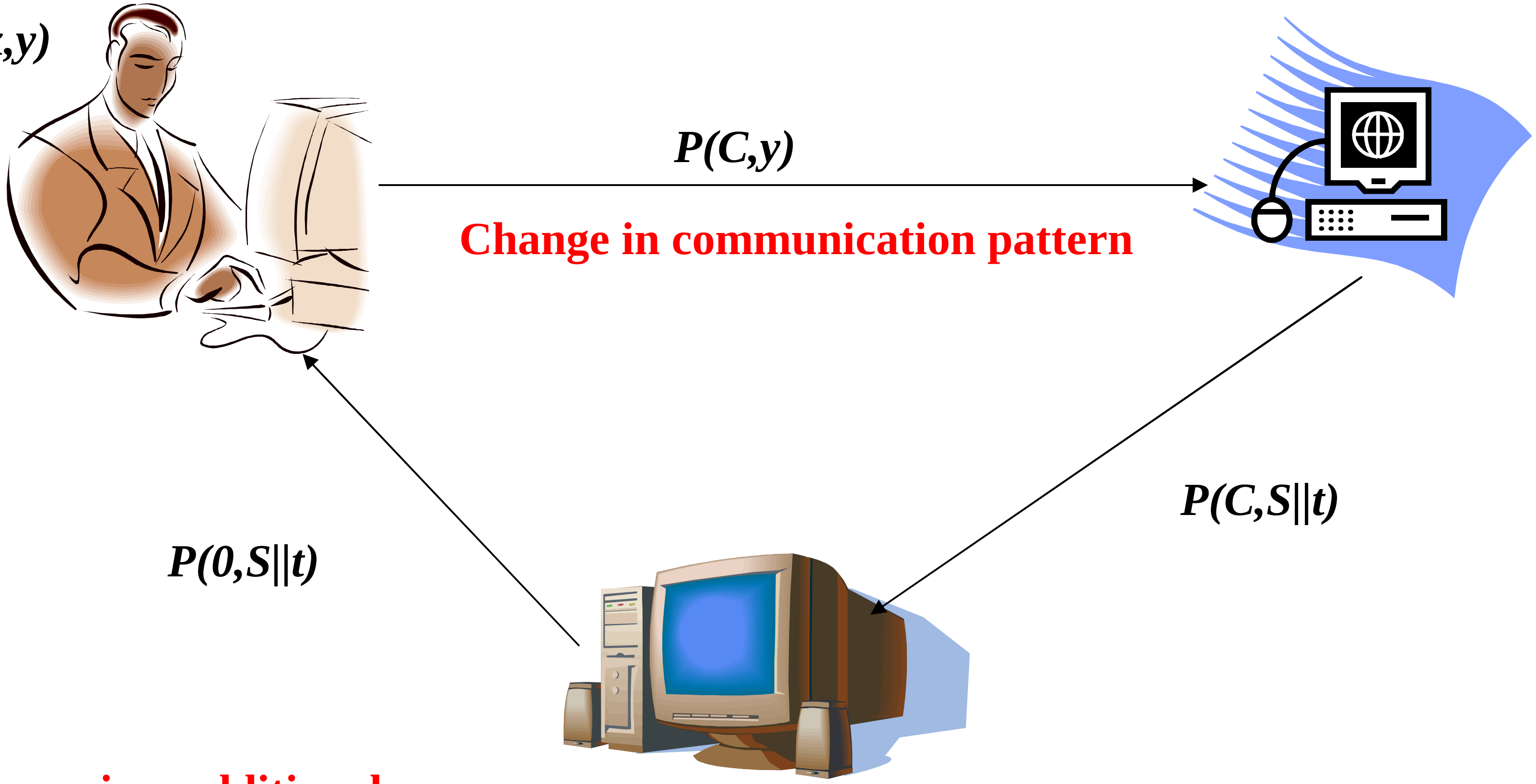
Secure and Efficient Metering

Discussion

Outline

- Clarifications
- Attack on Secure Metering
- Issues and Extensions
- Real World
- Other Directions
  - Metering for General Access Structures

Understanding the model



Audit Agency

$P(x,y)$

Client Machines C

$P(C,y)$

Change in communication pattern

$P(C,S\|t)$

$P(0,S\|t)$

Server *S*

Scheme requires additional computation

Recall Turnover

- Say you expect a particular client to visit again after c time frames

- Audit agency
  - Random challenge t from domain of size ck

- Hash function h, range ck

- Server should find $g^{r_i P(C)}$ such that $h(g^{r_i P(C)}) = t$

- g^{r_i} is a future challenge

Multiple Client Visits not counted?

- Same or different time frames?

- Turnover
  - Measures client loyalty across different time frames
  - Can trace client visits to different servers in same time frame

Turnover vs Privacy

- Turnover breaks privacy

- C is client that visits server S in time frame i
  - $t=h(g^{r_i P(C)})$

- S sends $g^{r_i P(C)}$ to audit agency

- Audit agency
  - Use same challenge t with other servers
  - Trace C’s visits in time frame i

One Fix ???(Footnote 7)

- Universal One Way Hash Function *h*
- Challenge *t* will be of form *h(x)*
- Send *x* and *t* to servers
- Server replies with $g^{r_i P(C)}$
  - $t=h(g^{r_i P(C)})$
  - $g^{r_i P(C)} \neq x$
- Essentially finding collisions?

Interpolation in exponent

- Sharing polynomial

$$s_i = f(i) = s + \sum_{j=1}^{k-1} f_j i^j$$

- Lagrange Interpolation

$$s = \sum_{i \epsilon A} b_i s_i$$

$$b_i = \prod_{m \in A, m \neq i} \frac{m}{m-i}$$

Interpolation in the exponent

$$s = \sum_{i \epsilon A} b_i s_i$$

$$g^s = g^{\sum b_i s_i}$$

$$g^s = \prod_{i \in A} g^{b_i s_i} = \prod_{i \in A} (g^{s_i})^{b_i}$$

Polynomial Security

- n corrupt clients
- m corrupt servers
- T time frames
- Corrupt clients information: nd evaluations
- Corrupt servers information: mkT evaluations
- nmT evaluations overlap
- $nd+mkT-nmT < kd$
- $T < \frac{kd-nd}{mk-nm}$

Attack

Robustness trick

- “I liked the robustness trick” ☺
- Is it really a secure trick??

Provably Secure Metering Scheme

[Ogata and Kurosawa, Asiacrypt, 2000]

- Attack – 2 colluding clients can prevent server from constructing a valid proof
- Present provably secure metering schemes

Security Goals

- Security for servers
  - Server should be able to compute a valid proof in presence of corrupt clients
- Security for audit agency
  - <k clients visit , server should not be able to compute proof
- Security for servers violated in Pinkas and Naor paper

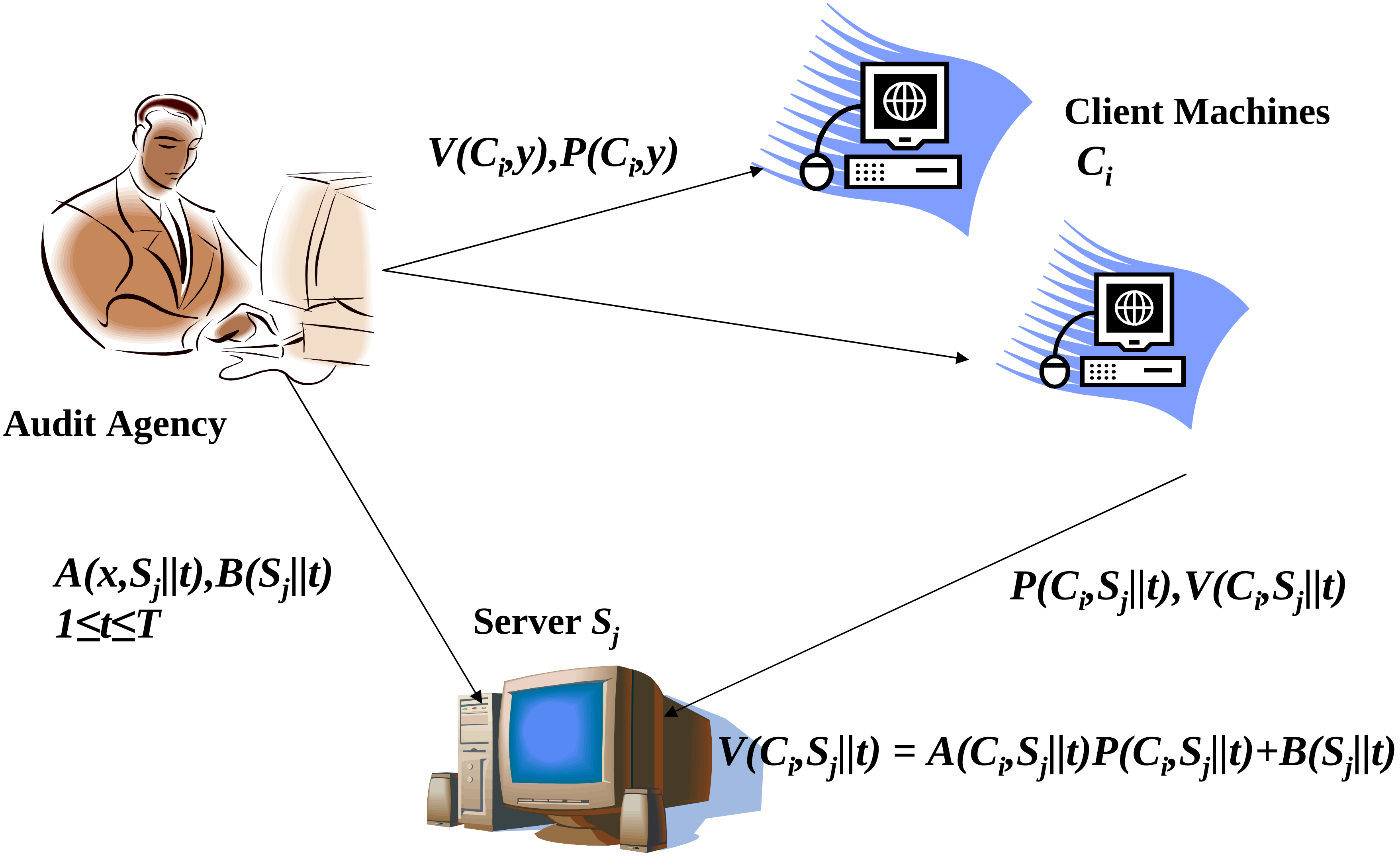
Quick Recap

- Audit Agency
  - $P(x,y)$
    - *degree k-1 in x, degree d-1 in y*
  - $A(x,y)$
    - *degree a in x , degree b in y*
  - $B(y)$
    - *degree b in y*
  - $V(x,y) = A(x,y)P(x,y)+B(y)$

***k* – Client visits**

***d* – Time frames**

Quick Recap ..



$V(C_i,y),P(C_i,y)$

Client Machines

C_i

Audit Agency

$A(x,S_j||t),B(S_j||t)$

$1 \leq t \leq T$

Server S_j

$P(C_i,S_j||t),V(C_i,S_j||t)$

$$V(C_i,S_j||t) = A(C_i,S_j||t)P(C_i,S_j||t)+B(S_j||t)$$

The Attack

- Say you are trying to trick server S_j in some time frame t

- Clients C_0, C_1
  - □ $P(C_0,S_j||t) = 0$
  - □ $P(C_1,S_j||t) \neq 0$

- Clients can collude and compute
  - □ $B(S_j||t)$, $A(C_1,S_j||t)$

Attack

For C_0:

$$V(C_0,S_j||t) = A(C_0,S_j||t)P(C_0,S_j||t)+B(S_j||t)$$

$$= A(C_0,S_j||t)\ (0) + B(S_j||t)$$

$$= B(S_j||t)$$

Attack

For C_1:

- $V(C_1,S_j||t) = A(C_1,S_j||t)P(C_1,S_j||t)+B(S_j||t)$
- $$A(C_1,S_j||t) = \frac{V(C_1,S_j||t)-B(S_j||t)}{P(C_1,S_j||t)}$$

  $$= \frac{V(C_1,S_j||t)-V(C_0,S_j||t)}{P(C_1,S_j||t)}$$

Use value from C_0

Attack …

- C_1 computes (P',V')
  - $\boldsymbol{P'} \neq P(C_1,S_j||t)$
  - $\boldsymbol{V'} = A(C_1,S_j||t)P' + B(S_j||t)$

- S_j will accept incorrect (P',V')

Issues and Extensions

Issues

- Fixed *k* can lead to a disaster!!!
- Doesn’t count accurately??
- Their scheme does not look like sampling
  - Audit agency to interact with each client before Is that the only aspect???

Right popularity metric?

- **Consider how many clients visited in a time frame**
- Multiple visits from same client to same server in given time frame
  - What happens to anonymity?
- Duration of client visit
  - Tied to Content

Issues and Extensions

- Model Broken
- Using metering for SPAM

Micro payment Schemes

- A micro-payment scheme encouraging collaboration in multi-hop cellular networks
  - [Jakobsson *et. al*. Financial Crypto 2003]

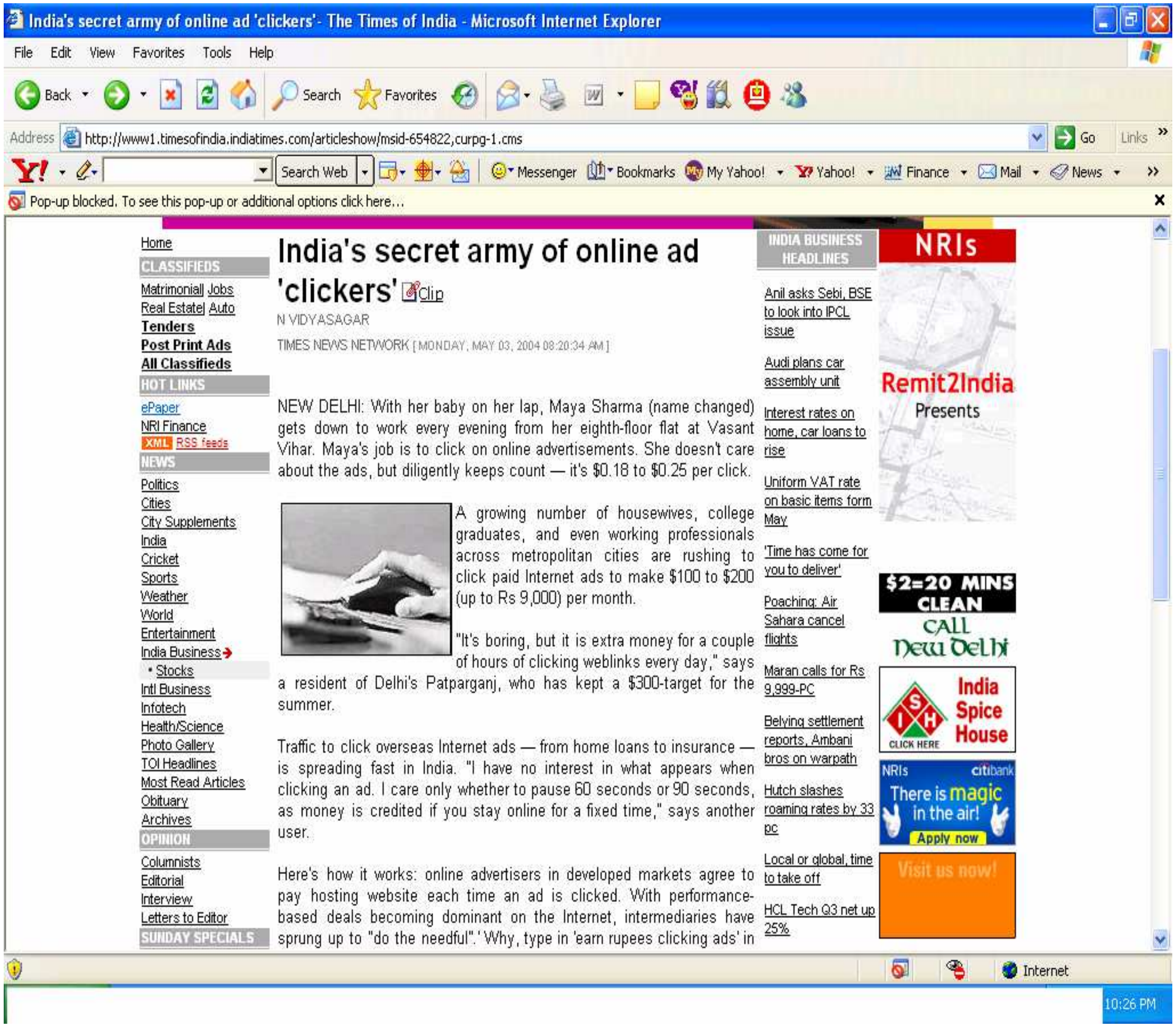
Distributed Metering

- Service is provided by multiple servers
- Collective popularity
- Audio/Video streaming

Metering an Outsourced service

- Would the model remain the same?
- How would it change?

Real World



India's secret army of online ad 'clickers' Clip

N VIDYASAGAR

TIMES NEWS NETWORK [MONDAY, MAY 03, 2004 08:20:34 AM]

NEW DELHI: With her baby on her lap, Maya Sharma (name changed) gets down to work every evening from her eighth-floor flat at Vasant Vihar. Maya's job is to click on online advertisements. She doesn't care about the ads, but diligently keeps count — it's $0.18 to $0.25 per click.

A growing number of housewives, college graduates, and even working professionals across metropolitan cities are rushing to click paid Internet ads to make $100 to $200 (up to Rs 9,000) per month.

"It's boring, but it is extra money for a couple of hours of clicking weblinks every day," says a resident of Delhi's Patparganj, who has kept a $300-target for the summer.

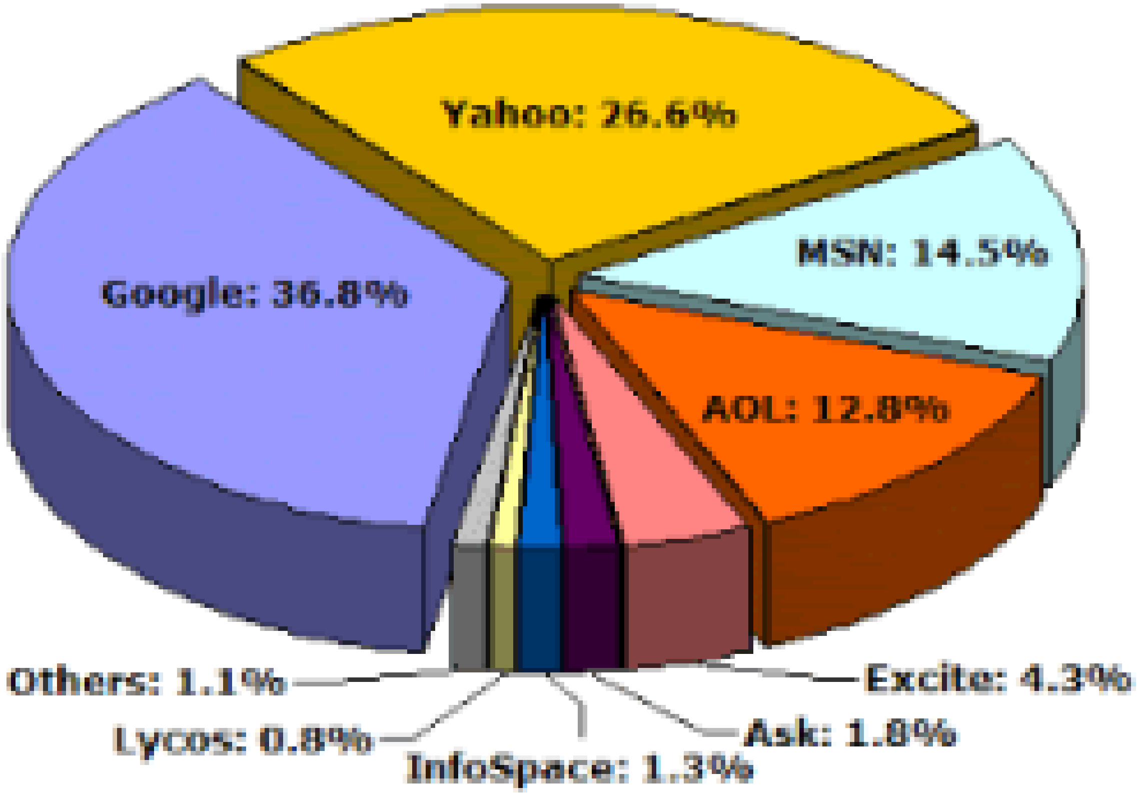
Traffic to click overseas Internet ads — from home loans to insurance — is spreading fast in India. "I have no interest in what appears when clicking an ad. I care only whether to pause 60 seconds or 90 seconds, as money is credited if you stay online for a fixed time," says another user.

Here's how it works: online advertisers in developed markets agree to pay hosting website each time an ad is clicked. With performance-based deals becoming dominant on the Internet, intermediaries have sprung up to "do the needful".' Why, type in 'earn rupees clicking ads' in

INDIA BUSINESS HEADLINES

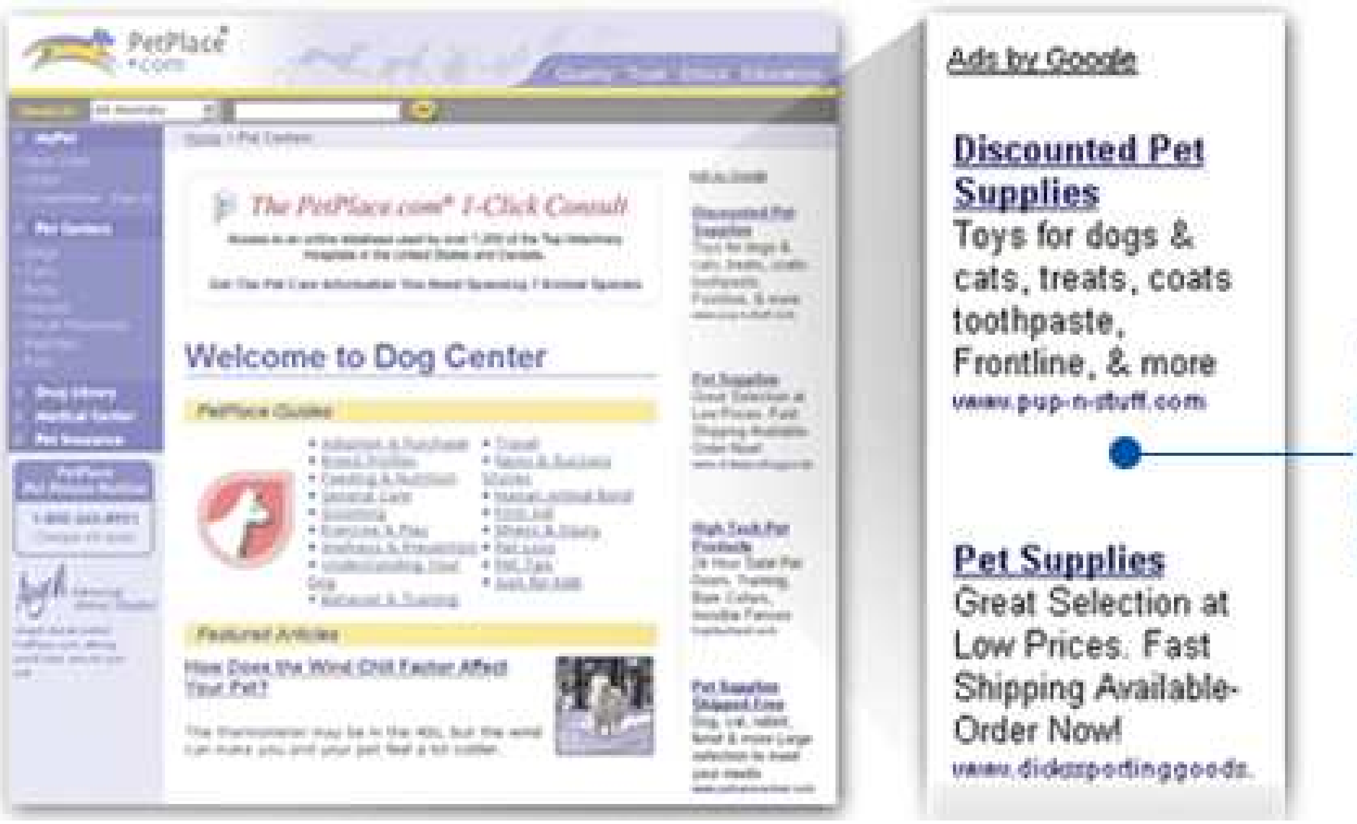
- Anil asks Sebi, BSE to look into IPCL issue
- Audi plans car assembly unit
- Interest rates on home, car loans to rise
- Uniform VAT rate on basic items form May
- 'Time has come for you to deliver'
- Poaching: Air Sahara cancel flights
- Maran calls for Rs 9,999-PC
- Belying settlement reports, Ambani bros on warpath
- Hutch slashes roaming rates by 33 pc
- Local or global, time to take off
- HCL Tech Q3 net up 25%

Search Engine Market



Source: http://www.completecents.com/public/marketing/free_traffic.htm

Google AdSense – Security?



Ads by Google

Discounted Pet Supplies
Toys for dogs & cats, treats, coats toothpaste, Frontline, & more
www.pup-n-stuff.com

Pet Supplies
Great Selection at Low Prices. Fast Shipping Available-Order Now!
www.didazsportinggoods.

You get ads that are relevant to your web pages. And when people click on these ads, Google pays you.

Google AdWords

- **Prohibited Uses.** You shall not, and shall not authorize any party to: (a) generate automated, fraudulent or otherwise invalid impressions or clicks; ….

- **Disclaimer and Limitation of Liability.** GOOGLE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION FOR NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR ANY PURPOSE. Google disclaims all guarantees regarding positioning or the levels or timing of: (i) costs per click, (ii) click through rates …

Other Directions

Applying General Access Structure to Metering Schemes [Nikov *et. al*. WCC’03, Cryptology Eprint 2002]

- Assumptions in threshold schemes
  - □ Uniformly distributed trust over players
  - □ Subset of players of certain cardinality is equally likely or unlikely to cheat
  - □ Audit agency deals with servers
  - □ In practice servers are owned by different companies

Basic Aspects

- General access structure on players
- Qualified and Forbidden client subsets
- Focus on general linear secret sharing
- Realize their access structures using monotone span programs

Thank you ☺