Personalized Search Under Attacks

Wenke Lee

College of Computing
Georgia Institute of Technology

What Your Search Does Not Tell You

Park West Gallery | Fine Art Auctions
www.parkwestgallery.com/
Collect fine art including original paintings, drawings, sculpture, jewelry, sports memorabilia and animation through our **gallery** or art auctions at sea.
You've visited this page 2 times. Last visit: 3/7/12

Park West Art Collections
Park West Gallery and Park West art auctions at sea offer a vast ...

About Park West
Visit Park West's fine art gallery – home to the largest collection ...

Park West Gallery | Artist ...
Park West Gallery artists both living and legacy. Discover the ...

Albert Scaglione
Albert Scaglione is the founder and CEO of Park West Gallery ...

More results from parkwestgallery.com »

Park West Gallery® | Philanthropy
www.parkwestgallery.org/
Park West Gallery, The Park West Foundation and the Scaglione family are committed to serving the community and reaching out to those in need.

The Official Blog of **Park West Gallery**
parkwestgallery.wordpress.com/
6 days ago – **Park West Gallery** was also excited to introduce our newest artist, Dualv, an internationally known painter and cellist. Deeply inspired by ...
+ Show map of 29469 Northwestern Highway, Southfield, MI 48034

Park West Gallery - Art Gallery - Southfield, MI | Facebook
www.facebook.com/ParkWestGallery
To connect with **Park West Gallery**, sign up for Facebook today. ... **Park West Gallery** offers works of art through its galleries in Michigan and Florida, at art auction ...
+ Show map of 29469 Northwestern Highway, Southfield, MI 48034

Park West Gallery (@ParkWestGal) on Twitter
twitter.com/#!/parkwestgal
Sign up for Twitter to follow **Park West Gallery** (@ParkWestGal). Founded in 1969, **Park West Gallery** connects people to fine art and the artists who create it -- on ...

Park West Gallery | Park West Galleries | Anatole Krasnyansky
www.parkwest-krasnyansky.com/
Park West Gallery collection of Anatole Krasnyansky art.

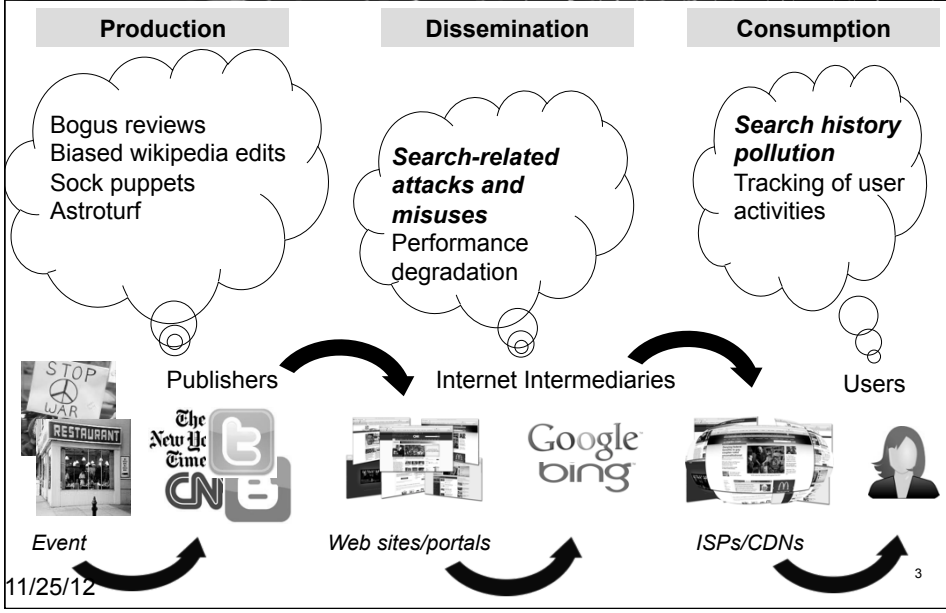
Park West Gallery - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Park_West_Gallery

Search "park west gallery" on Google
Negative comments: Victims of a Park West at Sea …
Some in Asia, Europe, Canada but not at US at all… …

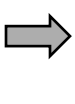
A Cyber Security Frontier: Information Manipulation

- **A New Class of Attacks:** Manipulate contents and human mind instead of machines or code
  - Affect users' decision-making process, (e.g., for financial gains and other interests)
  - Spam and phishing are well-known examples
  - New, more subtle ones are emerging
- **Why Now:** The Web makes information manipulation more scalable and targeted
  - The explosion of unvetted producers
  - The rise of intermediaries
  - Complex inter-dependencies of data

Manipulation At Every Stage



Attacking the Core: Personalized Search


Internet

- *Web pages*

Search Engine

User history/profile

- *User behaviors*
- *User web history*
- *User search history*
- *User location*
- …


Overview

- *Threats from Internet mercenary, blackhat SEO and location-based search personalization*
- Attacks on navigation based search personalization

Internet Mercenary and Blackhat SEO

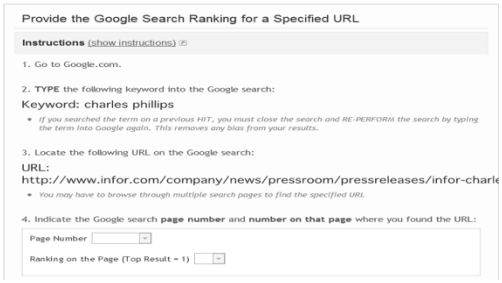
- Threats:
  - Online reputation management companies use blackhat SEO, Internet mercenary to manipulate search rankings
- Target:
  - Search Engine users, e.g., Google users
- Goal:
  - Hide online scams and complaints (to achieve or maintain financial gains)

Hiding "Negative" Pages

- Blackhat SEO
  - Register domain names containing the search term
    - e.g. registering www.parkwestgallery.org, www.parkwest-krasnyansky.com, www.parkwest-kinkade.com for search term "park west gallery"
  - Create web pages that contain the search term on high-page-rank websites
    - e.g. creating www.facebook.com/ParkWestGallery, www.parkwestgallery.wordpress.com, etc.
- Internet Mercenary
  - Hire Internet mercenary to search the term, and click positive messages or these web pages/domains
    - e.g. using Mechanical Turk

It's a Real Business

Many reputation management companies use blackhat SEO techniques to demote negative comments.



Reputation management companies hire authentic users to click positive comments on Google and attempt to affect Google ranking. We find that this also applies to Bing.

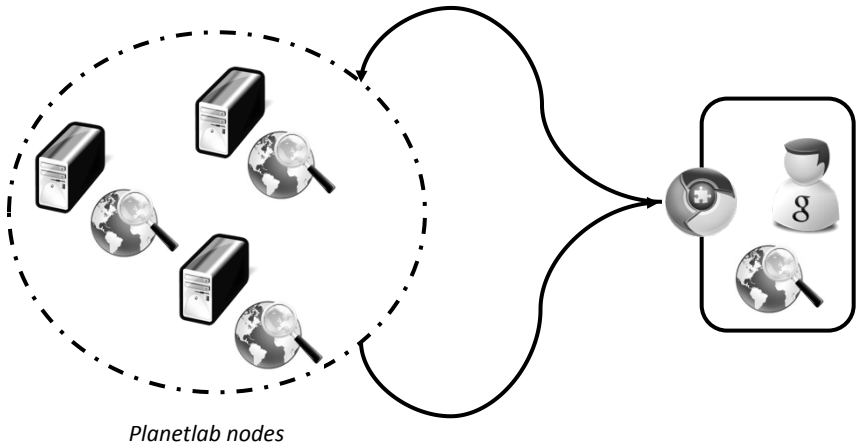
Increase the Cost of Blackhats

- Hypothesis:
  - Blackhat techniques and mercenary promote positive pages over negative ones
    - Works well or economically because search localization/ regionalization, e.g., North America only
- Solution: obtain multiple perspectives of the same information from multiple network points/personas
  - Expose manipulation
    - E.g., comparing different results
  - Mitigate negative effects
    - E.g., using aggregated results, synthesized new view
  - Blackhats have to cover the whole Internet with higher cost
  - Crowdsurfing: using the power of people to help individuals

Bobble

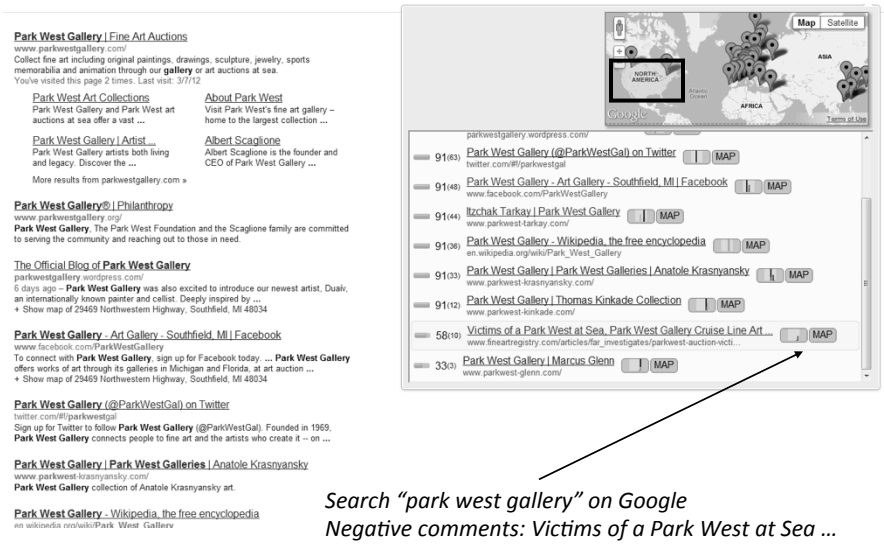
- Browser agents (a chrome extension running on Google clients)
- Search agents (automatic search bots running on ~300 Planetlab nodes)
  - Deployed since November 2011
  - Installed by 117 Google users
  - Logged 120,000+ Google queries and corresponding Google returns from both 117 Bobble users and planetlab's search agents
  - Downloadable from http://bobble.gtisc.gatech.edu/

Bobble Workflow



Chrome extension Google search

Bobble Shows Missing Information

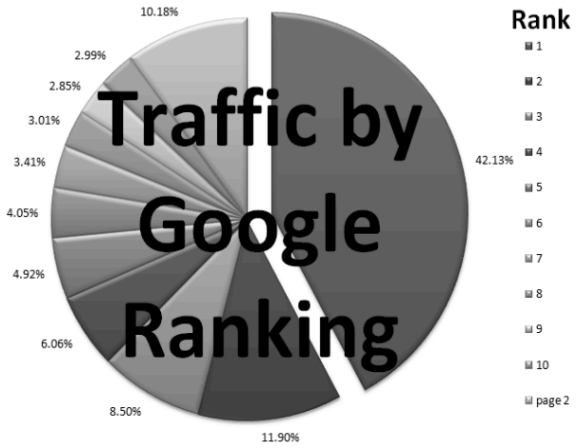


Search "park west gallery" on Google
Negative comments: Victims of a Park West at Sea …
Some in Asia, Europe, Canada but not at US at all… …

Overview

- Threats from Internet mercenary, blackhat SEO and location-based search personalization
- *Attacks on navigation based search personalization*

It Is All in the Rankings



- It is very worthwhile to promote the ranking of a page!

Navigational Pollution

- Harness session hijacking to inject clicking behaviors to Google or Bing user's history
  - Cookie theft
    - Eavesdrop Bing users' search traffic (no https protection)
    - Utilize pay-per-install services to distribute malicious browser plugin
  - New business for underground markets
    - Traditionally, stolen cookies are used for accessing victims' email accounts, abusing victims' email accounts to spam and thus obtaining clickthrough
      - email spam at 0.002% – 0.006% of clickthrough rates
    - Navigational pollution attacks can promote attackers' websites to the top and receive higher clickthrough rates
      - 62.53% clickthrough rates for the top three Google search returns

Navigational Pollution (cont'd)

- Serious security implications
  - The attack lifetime is 2-year long for Google users and 25 years long for Bing users if they check a "keep me signed in" box
  - It is difficult for Google users to notice navigational pollution attacks
  - Google cannot revoke stolen cookies even if the cookies are deleted by browser plugins unless the users change their passwords
  - Traditional attack: clean the machine and malware is gone
  - Search history attack: your history sticks with you!

Effectiveness of Pollution

Search engine rank	Top 1–10	Top 11–20	Top 21–30	Top 31–50	Top 51–100
Non-personalized URL # (Bing)	201	82	47	45	N/A
Non-personalized URL # (Google)	1,520	611	155	106	57
Personalized URL # in top 10 (Google)	1,364	506	51	2	0
Personalized URL # in top 3 (Google)	1,151	293	41	1	0

The non-personalized ranks vs. personalized ranks of promotable URLs for Bing and Google.

Conclusions

- Attackers have moved up the layer: manipulate the information received by users
- Personalized search is under attack: data used by search algorithms can be manipulated or compromised
  - Blackhat techniques to create “noise”
  - Pollution of search history
- We need to develop new tools to counter these attacks
  - E.g., crowdsurfing

Credits

- Xinyu Xing
- Dan Doozan
- Alex Snoeren
- Nick Feamster

- Hans Klein
- Robert Rosenberger

- Generous support from Google