Network Security Games:
Combining Game Theory, Behavioral Economics, and Network Measurements

Nicolas Christin
Carnegie Mellon, INI/CyLab
nicolasc@cmu.edu

Collaborators (in alphabetical order)

- John Chuang (Berkeley)
- Serge Egelman (Berkeley)
- Jens Grossklags (Penn State)
- Benjamin Johnson (Berkeley)
- Keisuke Kamataki (CMU, graduated)
- Nektarios Leontiadis (CMU)
- Tyler Moore (Wellesley)
- Timothy Vidas (CMU)
- Sally Yanagihara (CMU, graduated)

Motivation: Security analysis

- Who/What is the target?
- What are the desired security properties?
- **Understand defenders resources**
  - **Economic, technological, behavioral**

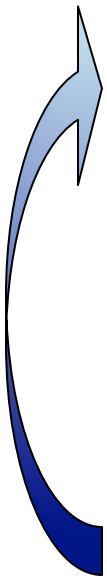
- Who are the adversaries?
  - Identify attackers
  - Probability of attack (risk assessment) and damages
- **Estimate attackers resources**
  - **Economic, technological, behavioral**

Research question

How can we better model attackers and defenders?

- Defenders *have been* assumed knowledgeable, interested in security, and altruistic
  - But in practice, generally self-interested
  - Rarely fully informed
  - Not even really rational: behavioral biases
- Attackers *have been* assumed omnipotent
  - But in practice very often financially motivated
  - Tend to be economically rational
  - May not lead us to devise effective defenses (see Anderson, 1993)
- Economics can tell us which intervention strategies most likely to succeed…
  - **… but for that we need sound economic models of all parties' behavior…**

The ten-year plan



1. Formal analysis
   - Game-theoretic predictions, selfishness vs. altruism
   - Impact of various parameters
2. Experimental research
   - Controlled lab experiments
   - Behavioral modeling
3. Field data measurement
   - Acquisition of attacker data
   - Acquisition of investment patterns
4. Testing intervention mechanisms
   - Incentives, legal…

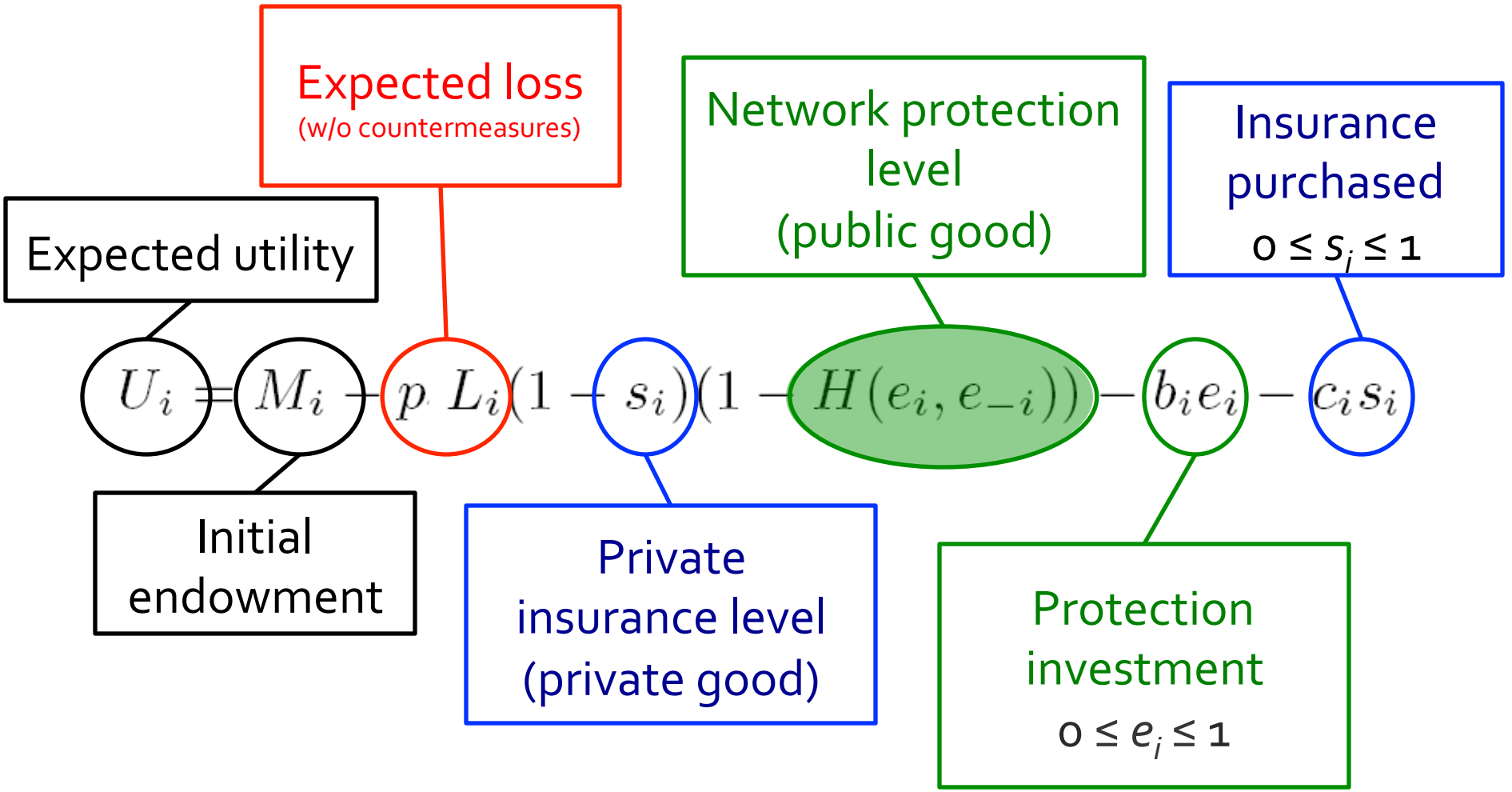
Part I: Modeling defenders

Formal analysis and Behavioral economics

Formal analysis of user behavior: Approach and contribution

- Variety of security threats and responses
  - Model most security interactions met in practice
  - Finite number of canonical security games
- Decouple security strategies
  - Self-protection investments (e.g., setting up a firewall)
  - Self-insurance coverage (e.g., archiving data as back up)
- Consider **network externalities**
  - Choice of strategy by a network participant affects other participants

General defender utility model
[GCC, WWW'08]



Contribution functions
(or: how is the network protected)

- Tightly coupled networks
  - Total/average effort $H(e_i, e_{-i}) = \frac{1}{N}\sum_i e_i$
    - Example: Distributed transfer of a file on a p2p network
  - Weakest-link $H(e_i, e_{-i}) = \min(e_i, e_{-i})$
    - Example: Corporate network penetration
  - Best shot $H(e_i, e_{-i}) = \max(e_i, e_{-i})$
    - Example: Censorship resilient networks
- Loosely coupled networks
  - Weakest target $H(e_i, e_{-i}) = \begin{cases} 0 & \text{if } e_i = \min(e_i, e_{-i}) \\ 1 & \text{otherwise} \end{cases}$
    - Example: Potential bots
  - Mitigated variant of the weakest link

Intuition behind Nash equilibrium outcome

- 3 types of pure Nash equilibria in our games
  - Protection only $(e_i, s_i) = (e^0, 0)$ (w/ $e^0=1$ fairly common)
  - Insurance only $(e_i, s_i) = (0, 1)$
  - Inactivity $(e_i, s_i) = (0, 0)$
- Increasing network size *N* affects Nash existence/nature

Summary of homogeneous results
($L_i = L$, $b_i = b$, $c_i = c$, $M_i = M$, pure Nash)

	Protection	Self-Insurance
Total Effort	$pL > \mathbf{bN}$ and $c > b + pL(N-1)/N$	*Other cases with* $pL > bN$ *or* $c < pL < bN$
Weakest Link	***Multiple*** symmetric protection equilibria	pL > c and too high protection cost
Best Shot	***No symmetric Nash***	Does exist if $b > c$ and $pL > c$
Weakest T w/o M	***No Nash***	*No Nash*
Weakest T with M	*Full protection if* b ≤ c	*No Nash*

Role of a social planner

- To achieve a social optimum
  - Sum of all players' utilities is maximized
  - Benevolent dictator
- Total effort:
  - More self-protection eq. ($pL > \boldsymbol{b}$ ~~$\boldsymbol{N}$~~$\boldsymbol{)}$)
- Weakest-link:
  - Planner would choose highest protection level
  - Pareto-optimal
- Best shot:
  - Planner now selects full protection for exactly **one** individual
  - In Nash eq. individuals frequently failed to protect
  - Insurance not needed
- Weakest target:
  - Sacrificial lamb
    - E.g., Honeypot
  - With or without insurance

Limited knowledge & information
[JGCC, ESORICS'10]

- Expert vs naive players
  - Expert players know the contribution function H and understand its effects.
  - Naive players are myopic; they behave as if $H(e_1, \ldots, e_n) = e_i$
- Complete vs incomplete information
  - An expert with complete information knows the expected losses for all players.
  - An expert with incomplete information knows her own expected loss L_i but does not know the expected losses of other players.
  - Experts assume that expected losses are independently and uniformly distributed in [0,1].

Best Shot and limited information

- In the Best Shot game, experts have a strong incentive to free-ride (Tragedy of the commons). Adding experts decreases the likelihood that the network is protected.

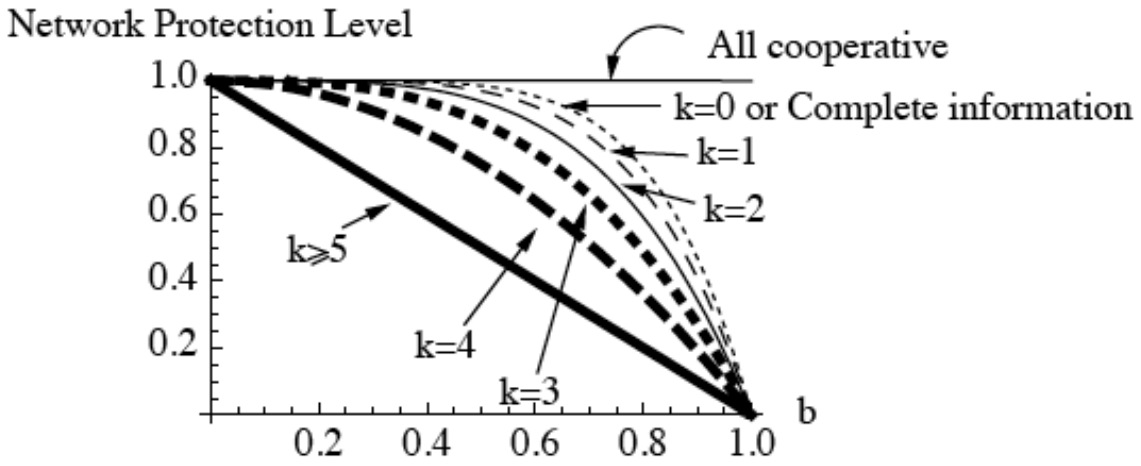
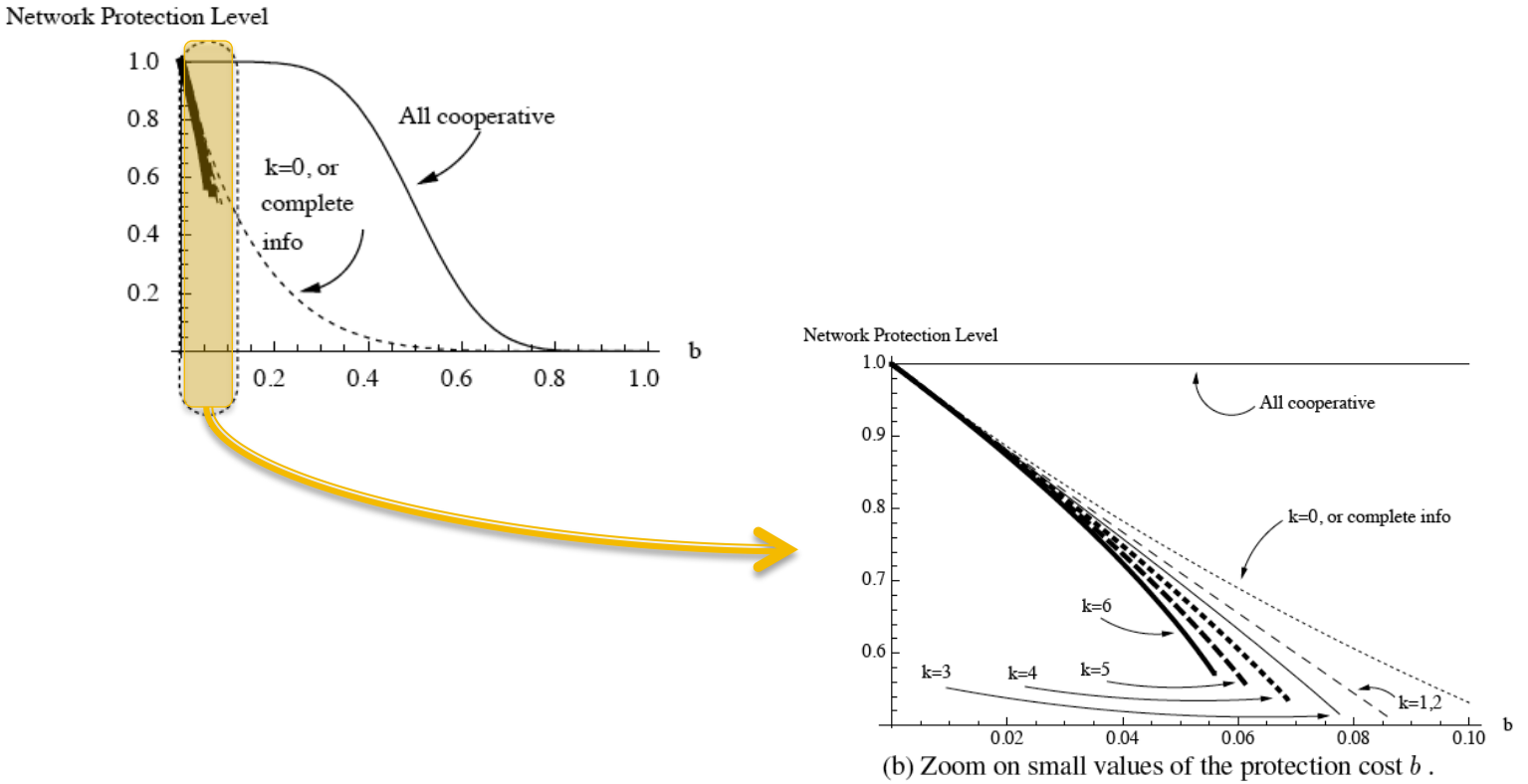


Fig. 2. Best shot. Evolution of the network protection level as a function of the protection cost b. The different plots vary the number of experts k in a network of $N = 6$ players. We observe that the fewer experts participating in the game, the higher the network protection level is, on average.

Weakest Link and limited information

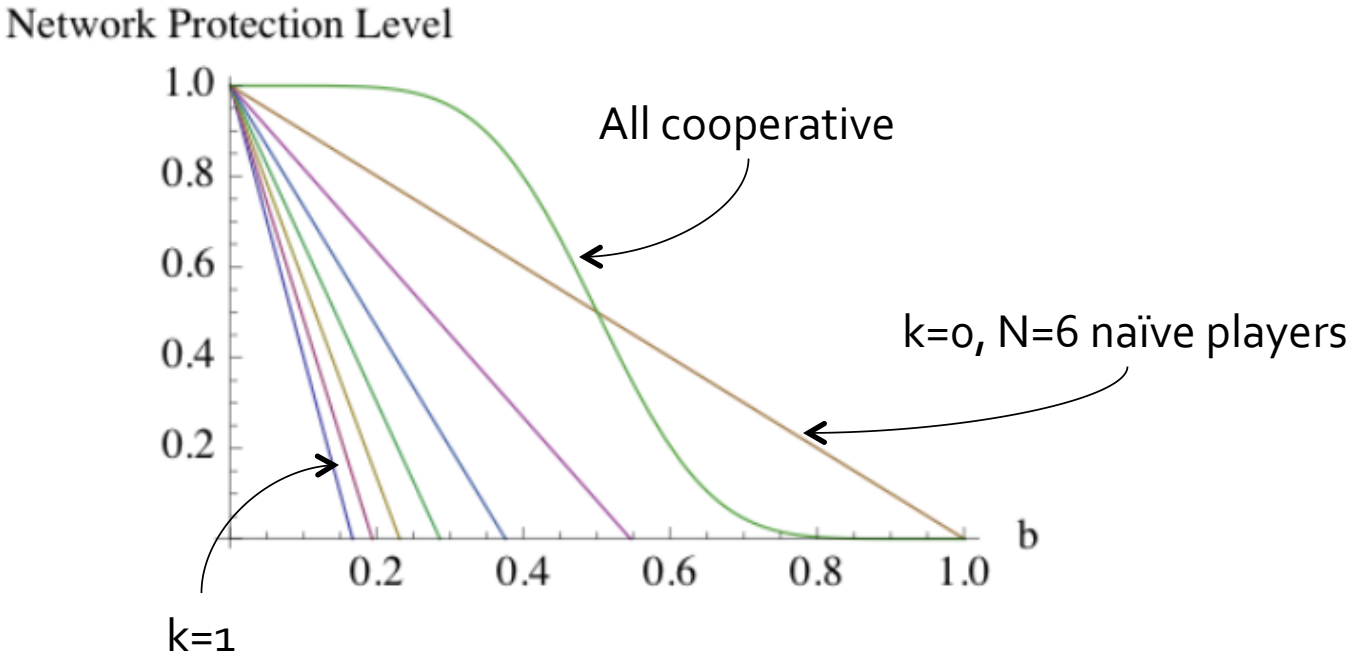
- Protection equilibria in the Weakest Link game only exist when protection costs are small; and the problem is exacerbated by the addition of expert players.



(b) Zoom on small values of the protection cost b .

Total Effort and limited information

- In the Total Effort game, the individual benefit of an investment is always proportional to a 1/N fraction of the investment's cost, regardless of the actions of other players. Experts understand this feature and do not protect very often.



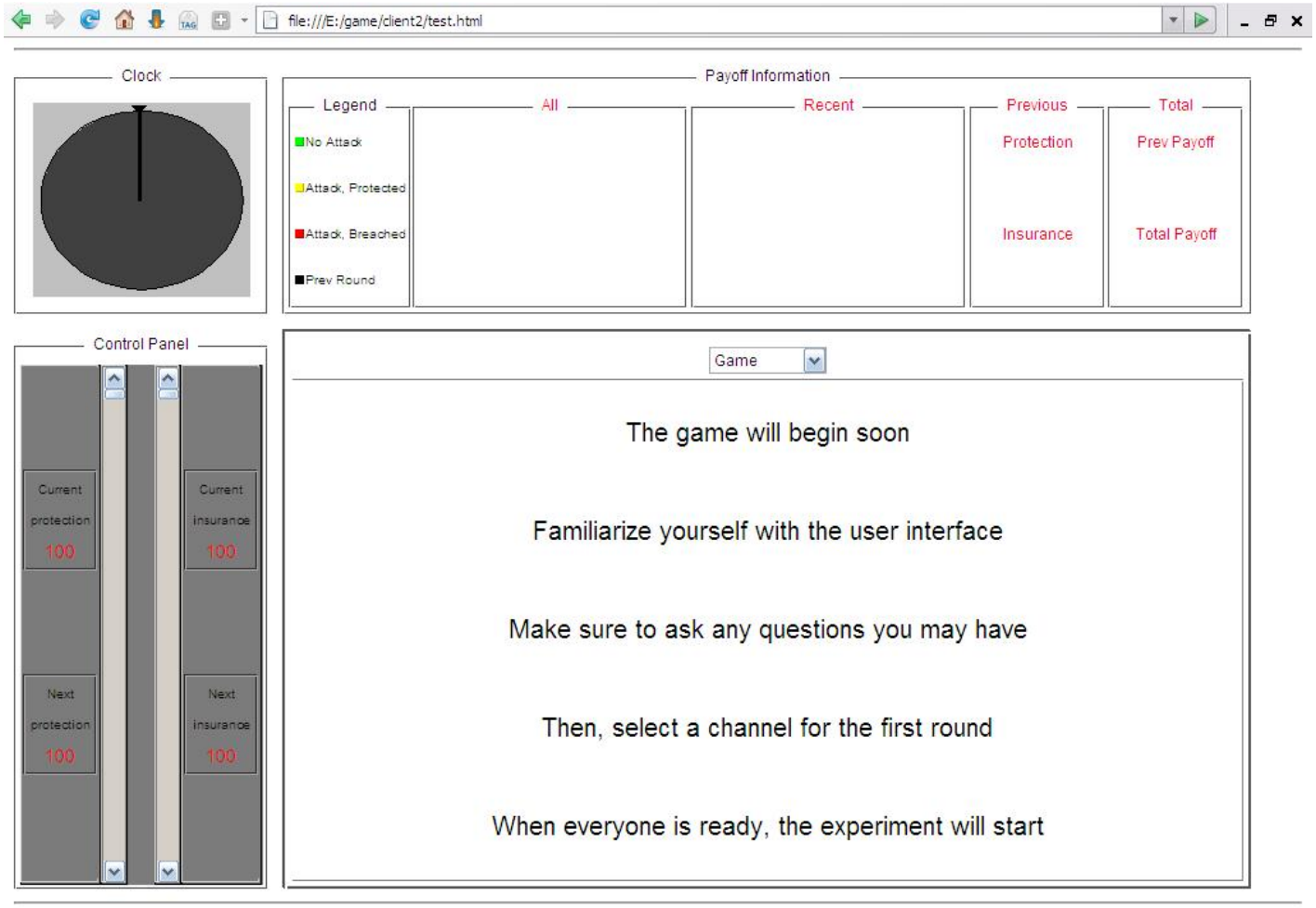
Implications

- (In some contexts), security experts are useful when (and only when) they collaborate.
- When security is divided among independent agencies, it is important to develop mechanisms for facilitating interagency collaboration.
- User education should focus on the collaborative nature of security

Outlook on experimental results [GCC, UPSEC'08]

- Will the game converge to a Nash equilibrium outcome?
  - How does strategy selection and convergence compare to traditional weakest-link experiments?
  - Does the insurance equilibrium dominate other outcomes?
  - Is experimentation a prominent part of players' strategies?

Experimental environment



Lab experiment outcome

- People are NOT good at optimizing two parameters at the same time
- Extremely slow convergence
  - Matters because economies and systems rarely start at equilibrium
  - Importance of experimentation highlighted for individual and group strategy choice

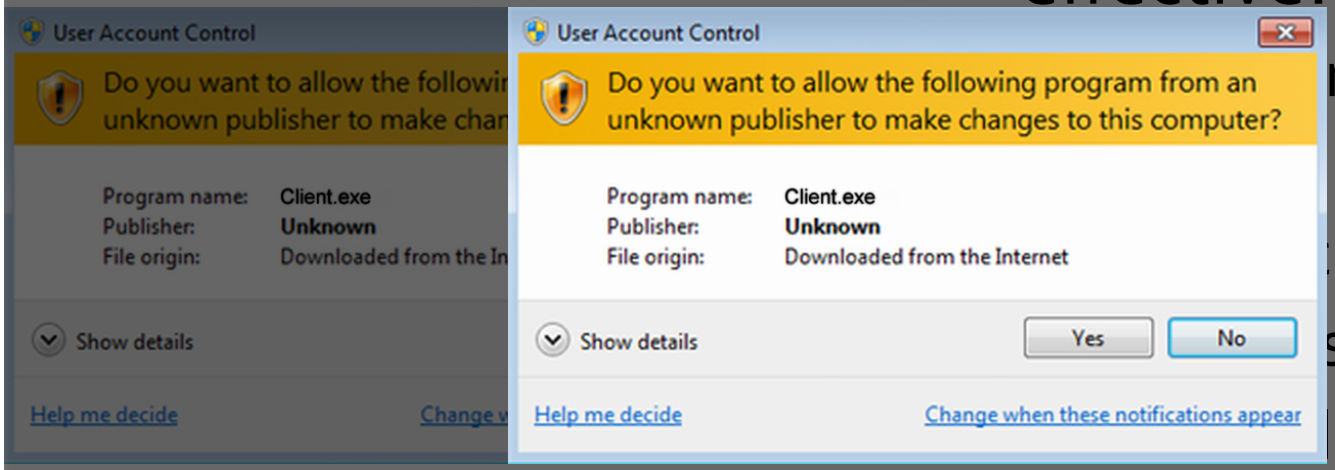
Behavioral bias case study
[CEVG, FC'11]

- People also show behavioral biases
  - Risk-aversion, risk-seeking behavior, hyperbolic discounting, instant gratification
  - Need to be integrated to formal modeling
- Case study: We paid people to download and run an unknown executable
  - Payment was increased every week
    - $0.01/$0.05/$0.10/$0.50/$1.00
  - Mechanical Turk as experimental platform
    - Measured views vs. downloads vs. runs

Experimental environment

- CMU Distributed Computing Project
  - No such project exists
  - All code was hosted on a third-party domain
  - No connection to us or our institutions

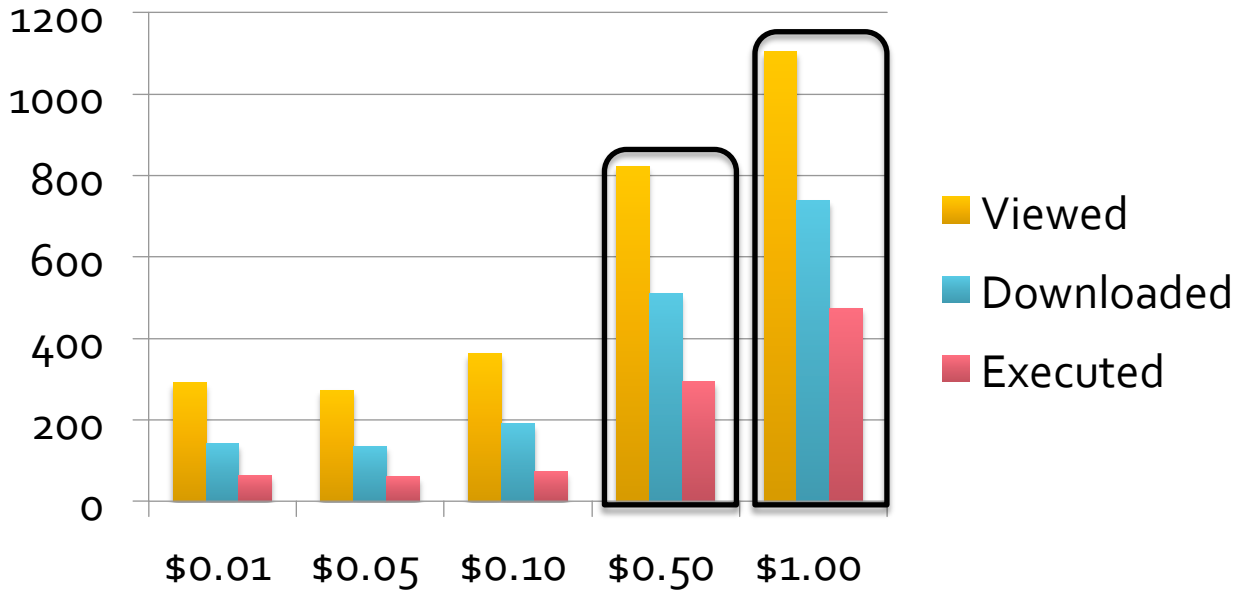
Experimental Environment



- Are current mitigations effective?
  - mpt for 50%
  - data:
  - ontrol
  - s version
  - ist
    - VM detection
- Displayed payment code
- Sent an exit survey

Results

	$0.01		$0.05		$0.10		$0.50		$1.00	
Viewed	291		272		363		823		1,105	
Downloaded	141	49%	135	50%	190	52%	**510**	**62%**	**738**	**67%**
Executed	64	22%	60	22%	73	20%	**294**	**36%**	**474**	**43%**



Results


The Daily W

Sunday, August 30, 2006

People Do Stuff for Money!

Peltzman effect in computer security

- Peltzman effect:
  - Availability of seatbelts leads to more risky driving
- Here:
  - Installation of security software correlates with risky behaviors
- Post-experimental survey revealed that users felt:
  - The experiment was dangerous
  - But that they were "safe" because they ran an AV!
  - … of course an AV won't help you much if you grant full access to your machine willingly…

Part II: Modeling attackers

Measurements, measurements, and more measurements

Understanding attackers

- Primary motivation: **financial**
  - Hacktivists (e.g., Anonymous), military-grade attacks (e.g., Stuxnet) make news b/c they are **rare**
  - Most attacks are motivated by monetary profits
    - Spam, botnets, malware distribution, MFA sites…

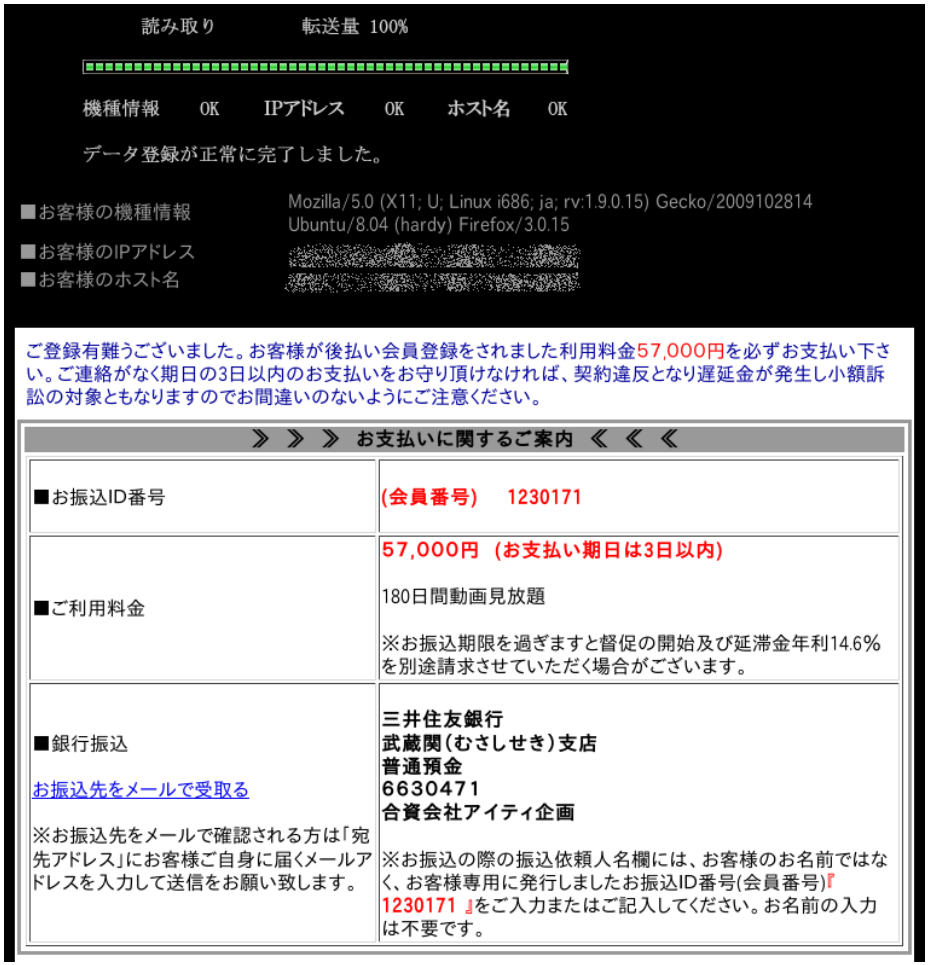
→ Attackers are (very) rational!

- Amenable to measurement (large amount of recent lit.)
- Attackers **often prey on behavioral biases**/flaws

Example: "One Click Fraud" [CYK, CSS'11]

- Pervasive online fraud found in Japan since 2004
  - "as seen on TV!"
- Japanese cousin of *scareware* scams

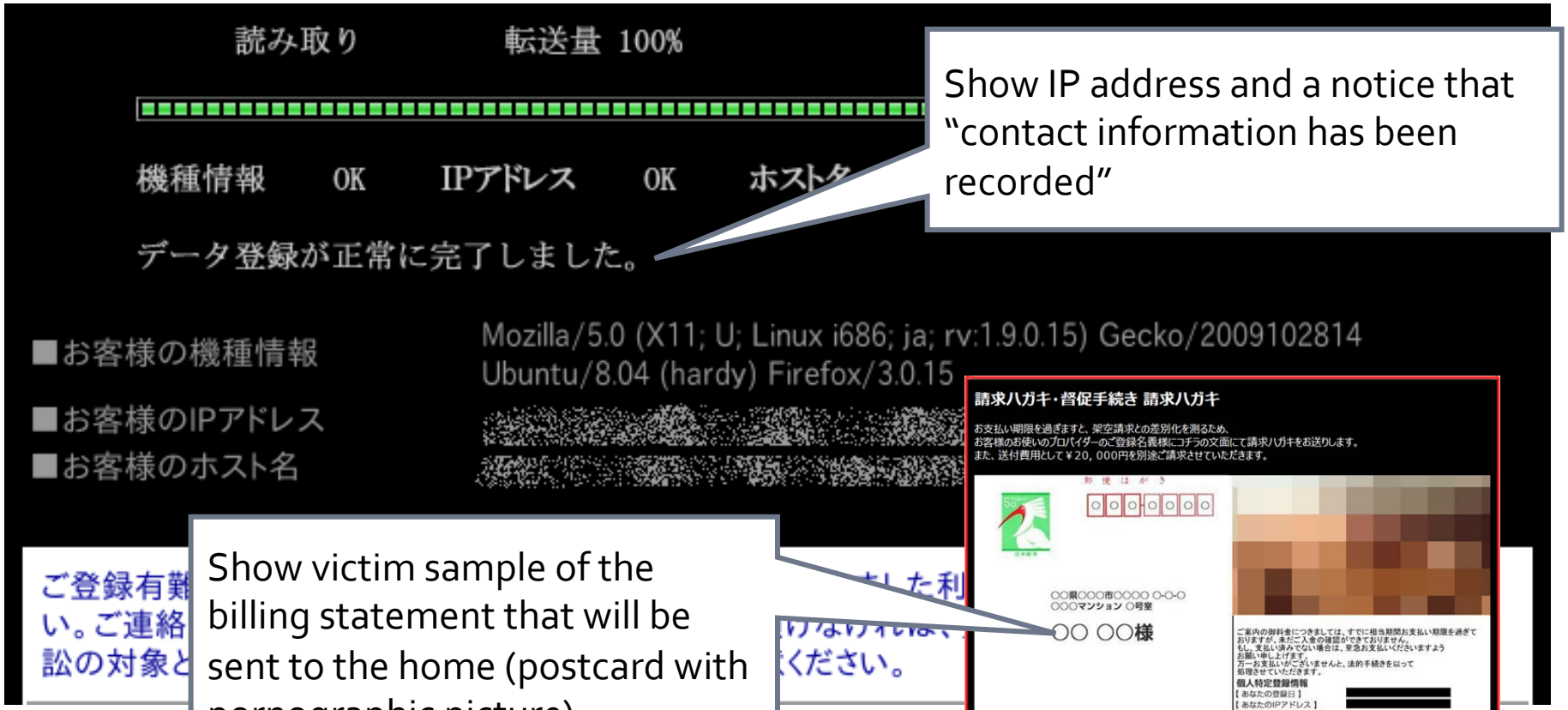
- Victim clicks on a (innocuous) HTML link
  - email, website, or SMS variants
- … only to be told they entered a binding contract…
- … and are required to pay a nominal fee or "legal action" will be taken



One Click Contracts/Frauds, Wikipedia http://ja.wikipedia.org/wiki/ワンクリック詐欺

Why do victims pay?

Fear of embarrassment, divorce, public shame, loss of job…

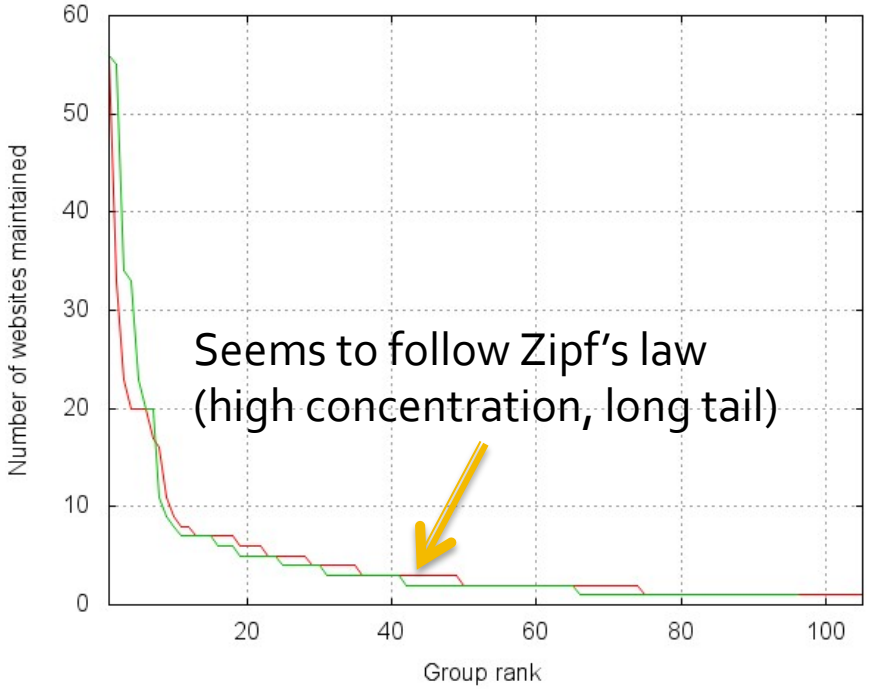


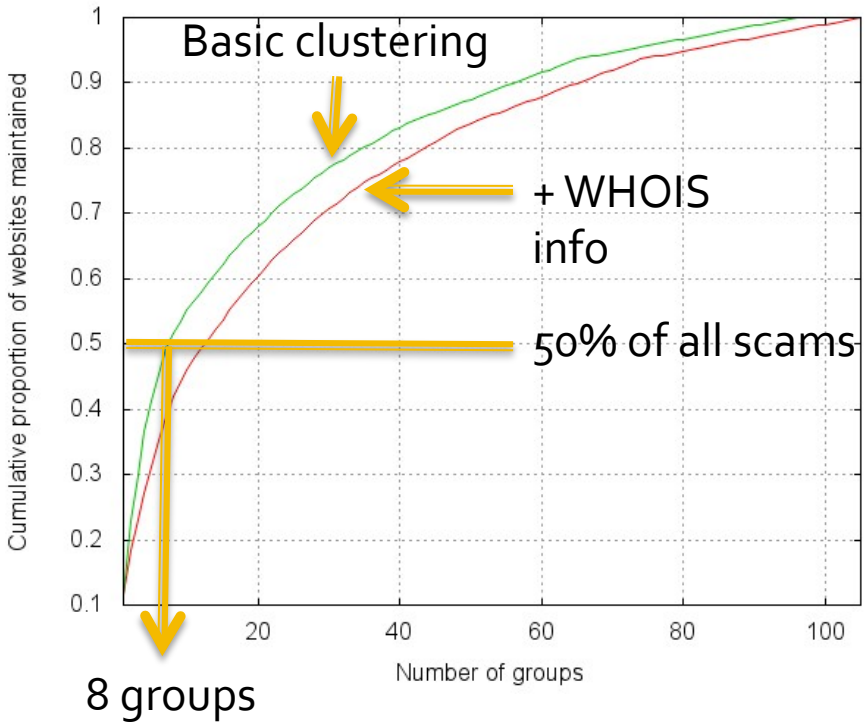
One Click Frauds, http://support.zaq.ne.jp/security/oneclick5.html

Collecting instances of One Click Frauds

- Source of data: "vigilante" websites posting information about frauds
- 2 Channel (２ちゃんねる　掲示板)
  http://society6.2ch.net/test/read.cgi/police/1215642976
  - Japan's largest BBS
  - We focus on the 'One Click Fraud' posts
  - Potential difficulty: posts made using natural language, lots of noise, potentially hard to parse automatically
- Koguma-neko Teikoku (こぐまねこ帝国) http://kogumaneko.tk/
  - Consumer-oriented website (helpdesks, information, …)
  - Structured reports, parsing easy
- Wan-Cli Zukan (ワンクリ図鑑) http://1zukan.269g.net/
  - Vigilante blog dedicated to exposing One Click Frauds
  - Structured reports, parsing easy
- Collected 2,140 incident reports, dated March 6,2006-October 26, 2009
  - No evidence of slander

Organized criminal groups





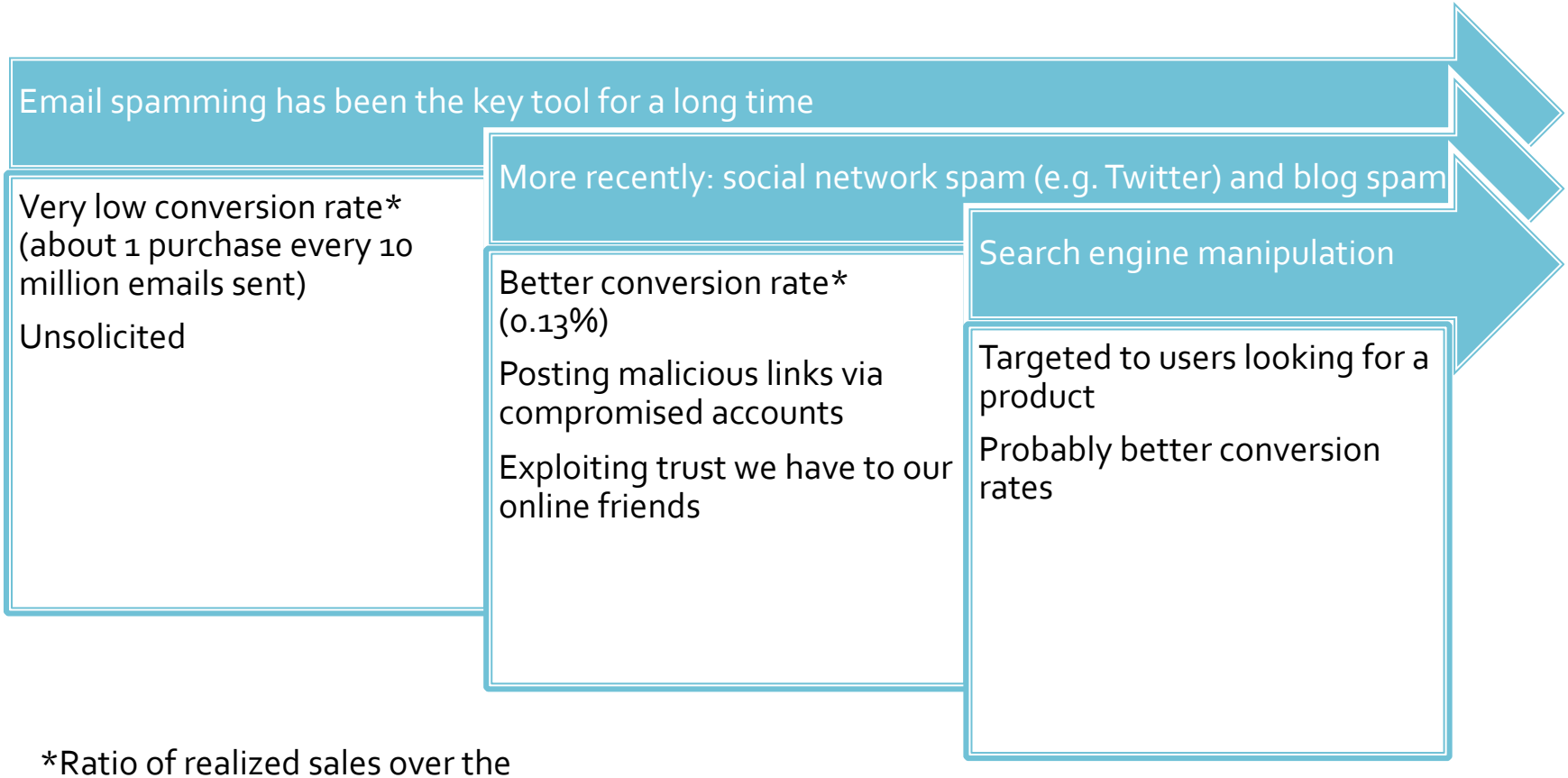
- Identified (at most) 105 organized criminal groups
- On average, each group
  - maintains 3.7 websites
  - 5.2 bank accounts
  - 1.3 phone numbers
- **A few "syndicates" seem responsible for most of the frauds**

Economic incentives of miscreants

- An average fraudster **breaks even as soon as approx. 4 users/site operated** (about 16 people total) **fall for the fraud within a year**

- … obviously some people make a lot more money
  - Up to USD 6 million in one case
- … while fines and penalties are low
  - 0-2.5 years in jail
  - Largest fine = USD 20K

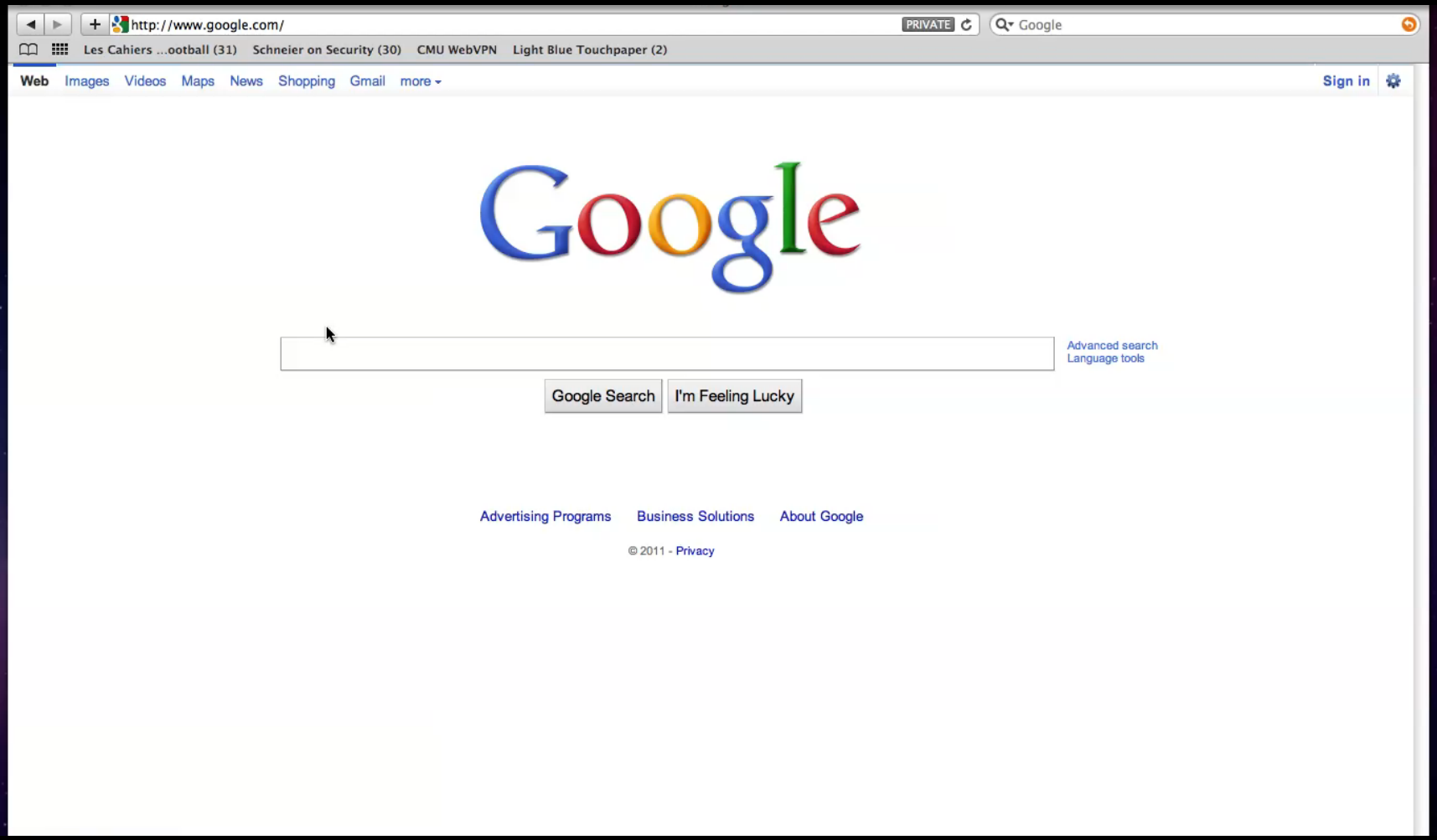
Make money fast(?): Illicit online advertising



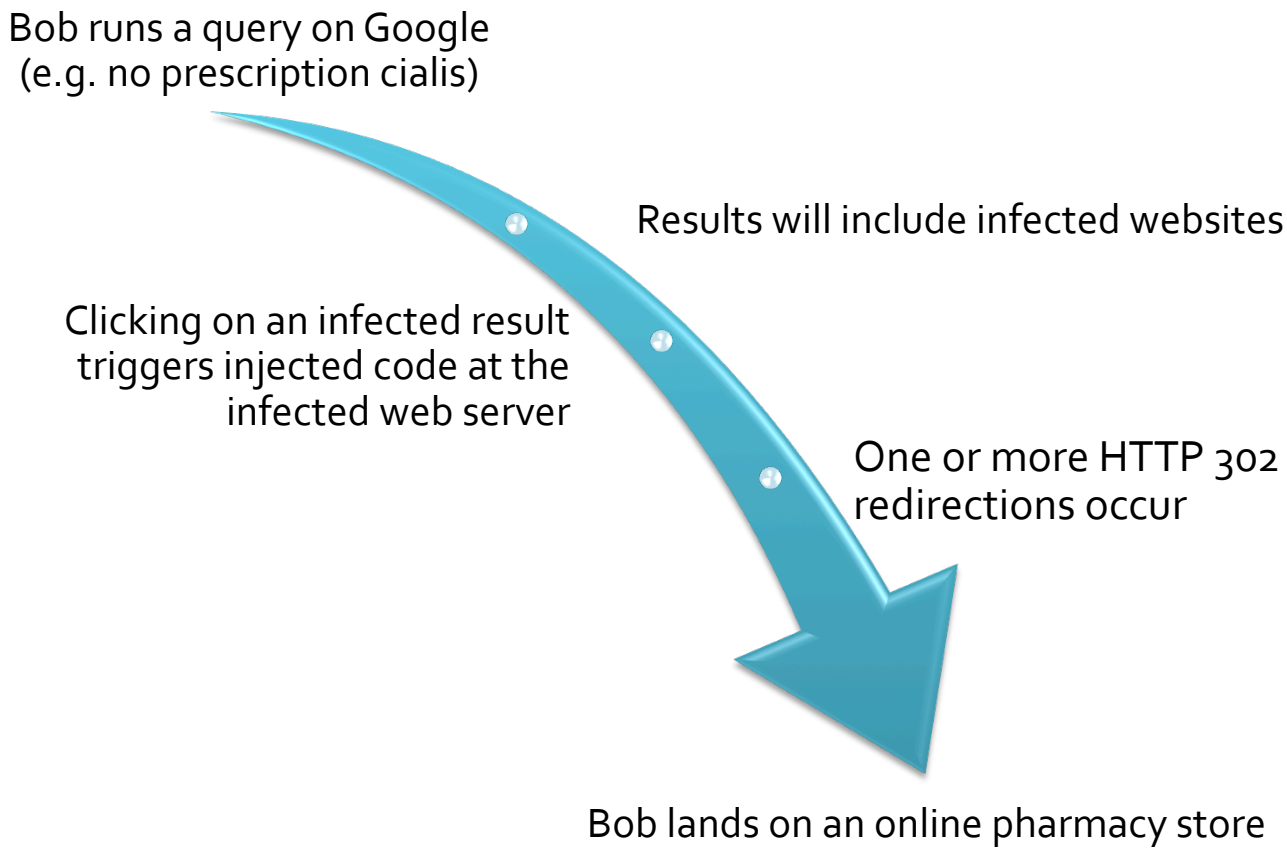
*Ratio of realized sales over the number of emails/clicks

Search-redirection attack

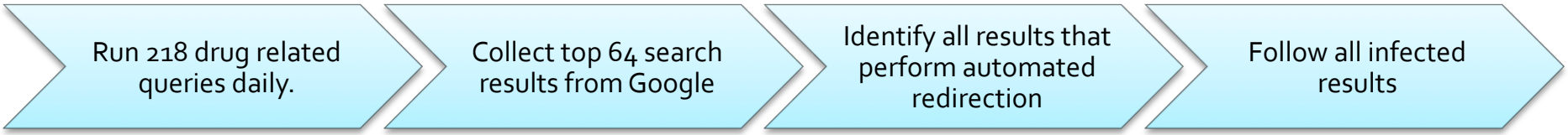
[LMC, USENIX Sec'11]



Attack modus operandi



Data collection process



- Daily collection from 4/12/2010.
- Using data until 10/21/2010.
- Complemented by a second 10-week dataset
- Collection process is still running.

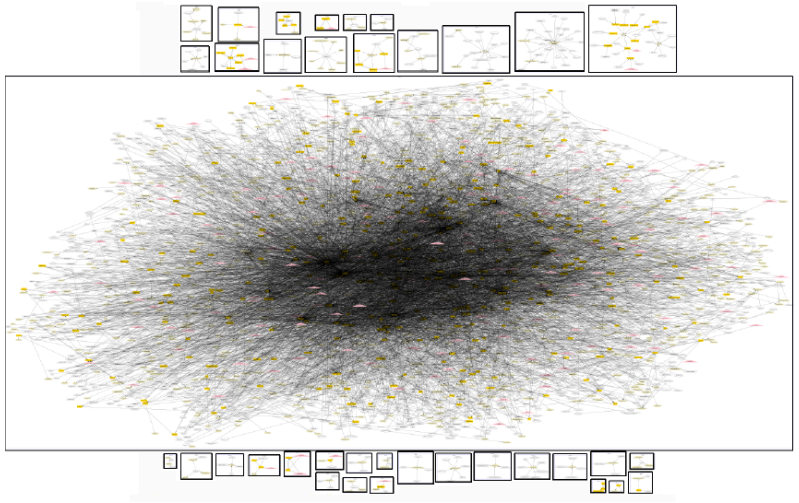
- The limit is defined by Google Search API
- Storing all results for later processing
- Will also examine position information

- A search result defines the website that a user will be redirected to when clicking on the link
- If the browser is redirected instead to a different website (domain), the result is infected.

- Follow each result identified as infected from previous step
- Follow all redirections that might occur
- Record all the redirection information

Connected components

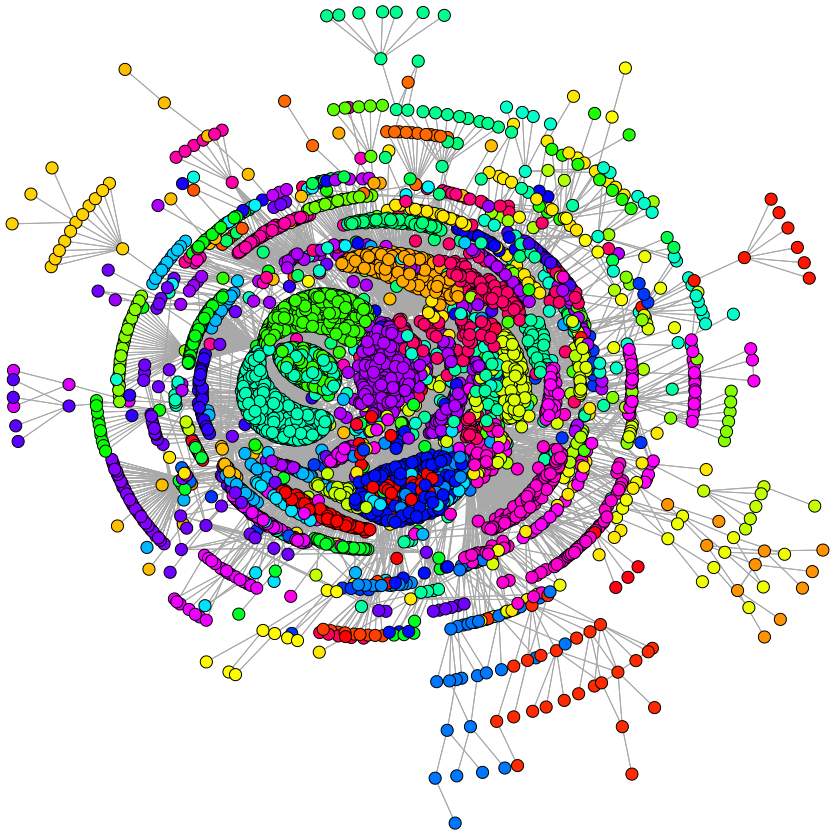
- 34 connected components
- One connected component contains
  - 96% of all infected domains
  - 90% of all redirection domains
  - 92% of all pharmacies



- Is one person responsible for all of this?!
  - Not necessarily, but evidence of partner relationships

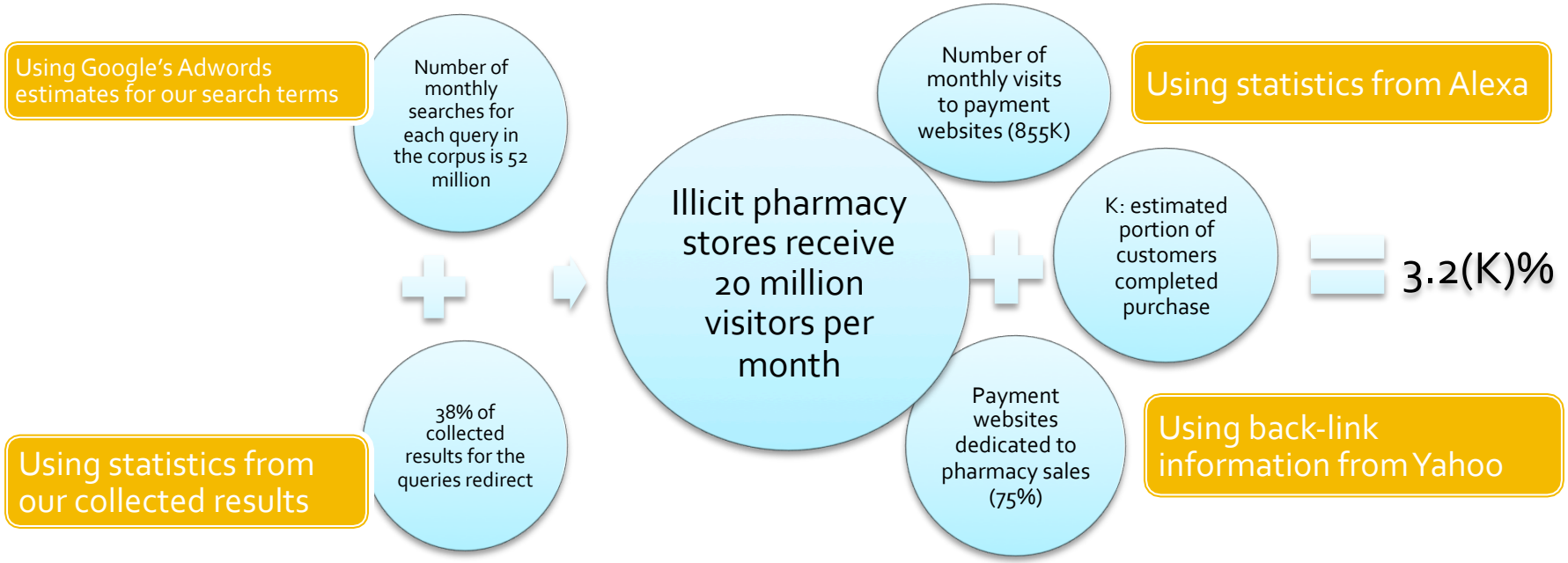
Identifying the main players

- Run (spinglass) clustering algorithm in big connected component
- Evidence of separate organized groups/ campaigns more loosely connected to each other
- Interesting AS/registrar patterns.
  - 11 ASes host most redirect servers
  - Some are over-represented



Conversion rate*

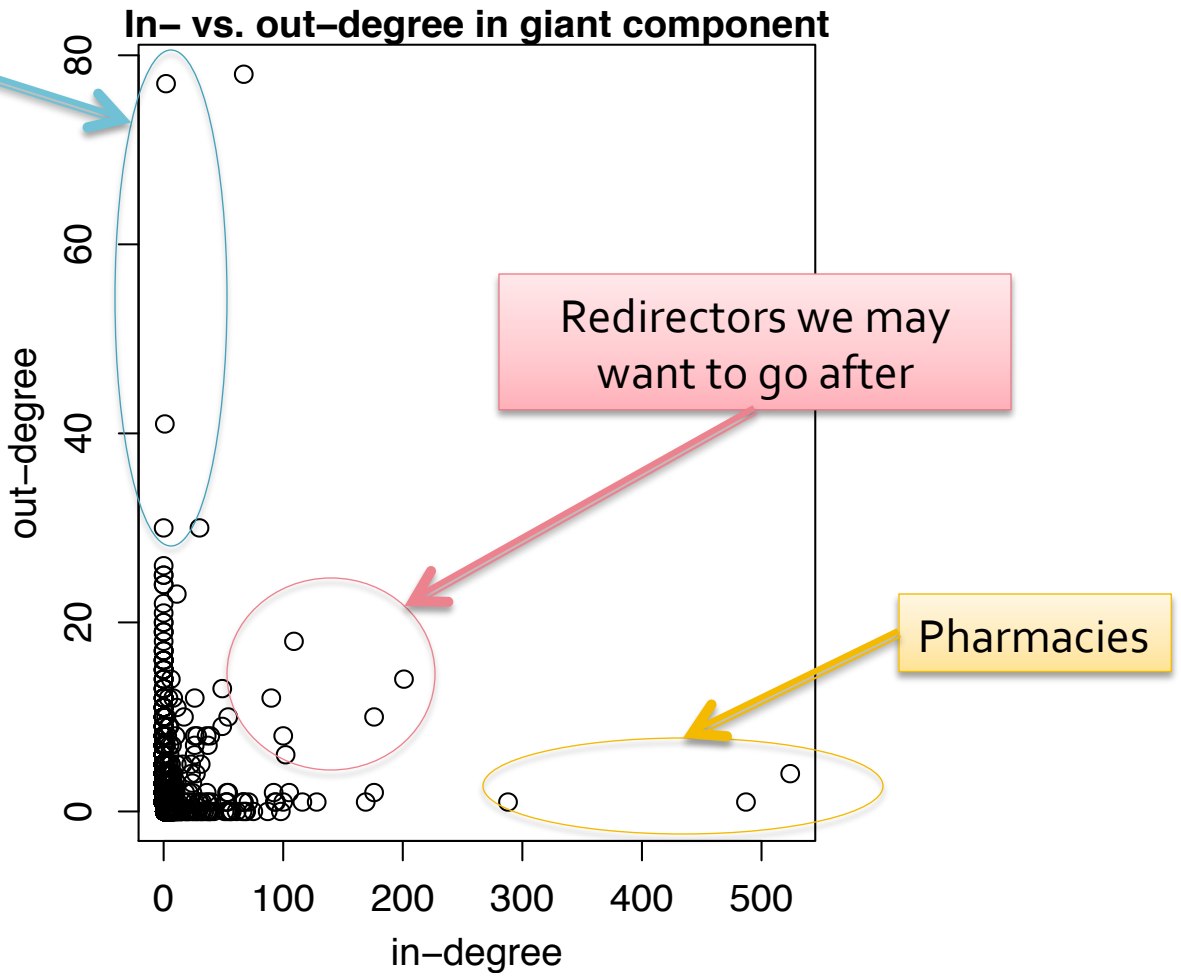
*Ratio of realized sales over the number of visitors



$$Conversion\_rate \geq 0.75K \frac{855{,}000}{20{,}000{,}000} \xrightarrow{K=0.1} 0.32\%$$

Possible intervention

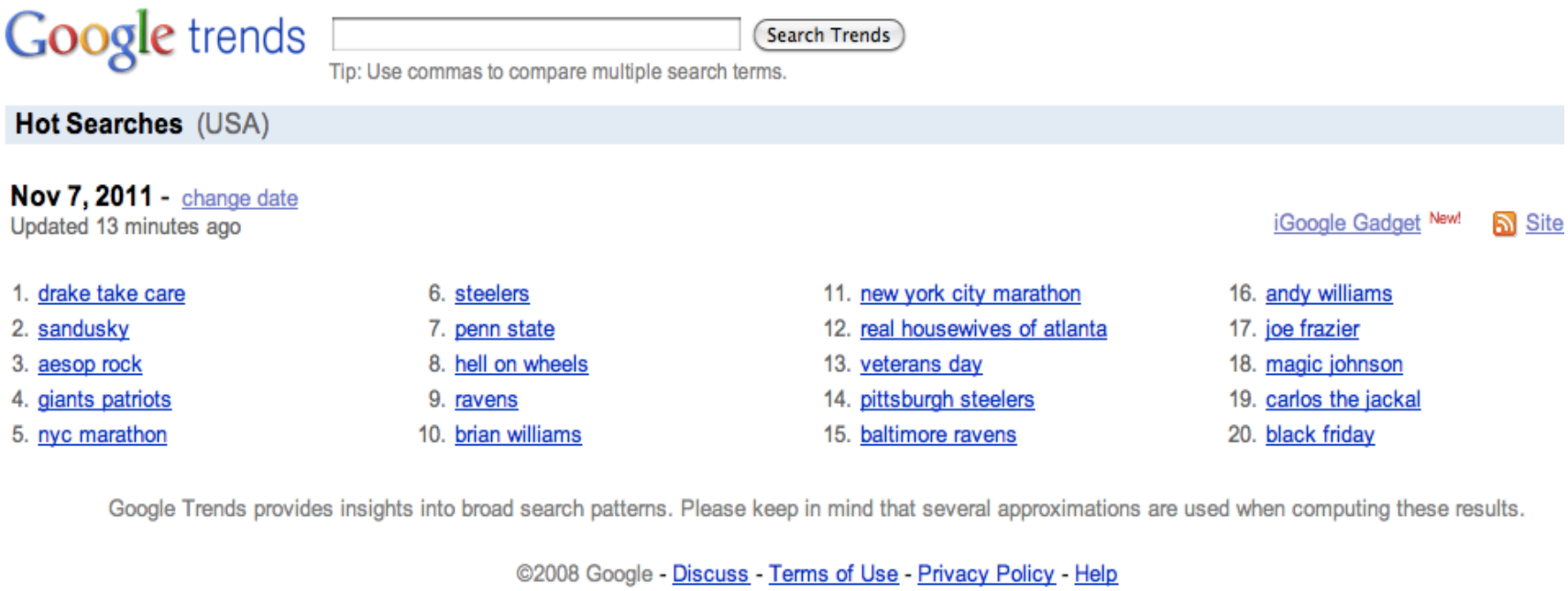
Valuable infected sites (e.g., mit.edu)



Redirectors we may want to go after

Pharmacies

Another target: Trending terms
[MLC, CCS'11]



Google trends

Search Trends

Tip: Use commas to compare multiple search terms.

Hot Searches (USA)

Nov 7, 2011 - change date
Updated 13 minutes ago

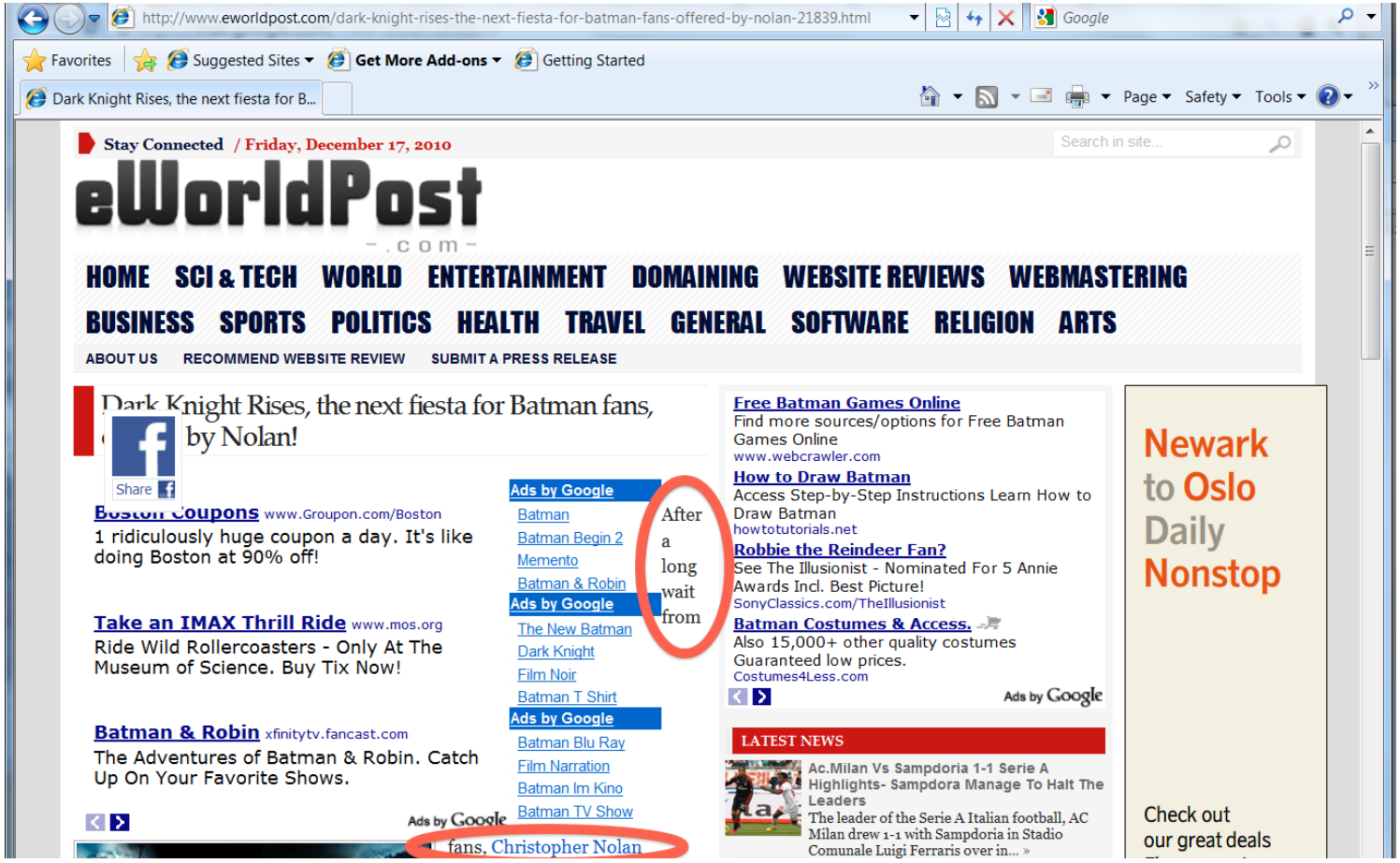
iGoogle Gadget New! Site

1. drake take care
2. sandusky
3. aesop rock
4. giants patriots
5. nyc marathon
6. steelers
7. penn state
8. hell on wheels
9. ravens
10. brian williams
11. new york city marathon
12. real housewives of atlanta
13. veterans day
14. pittsburgh steelers
15. baltimore ravens
16. andy williams
17. joe frazier
18. magic johnson
19. carlos the jackal
20. black friday

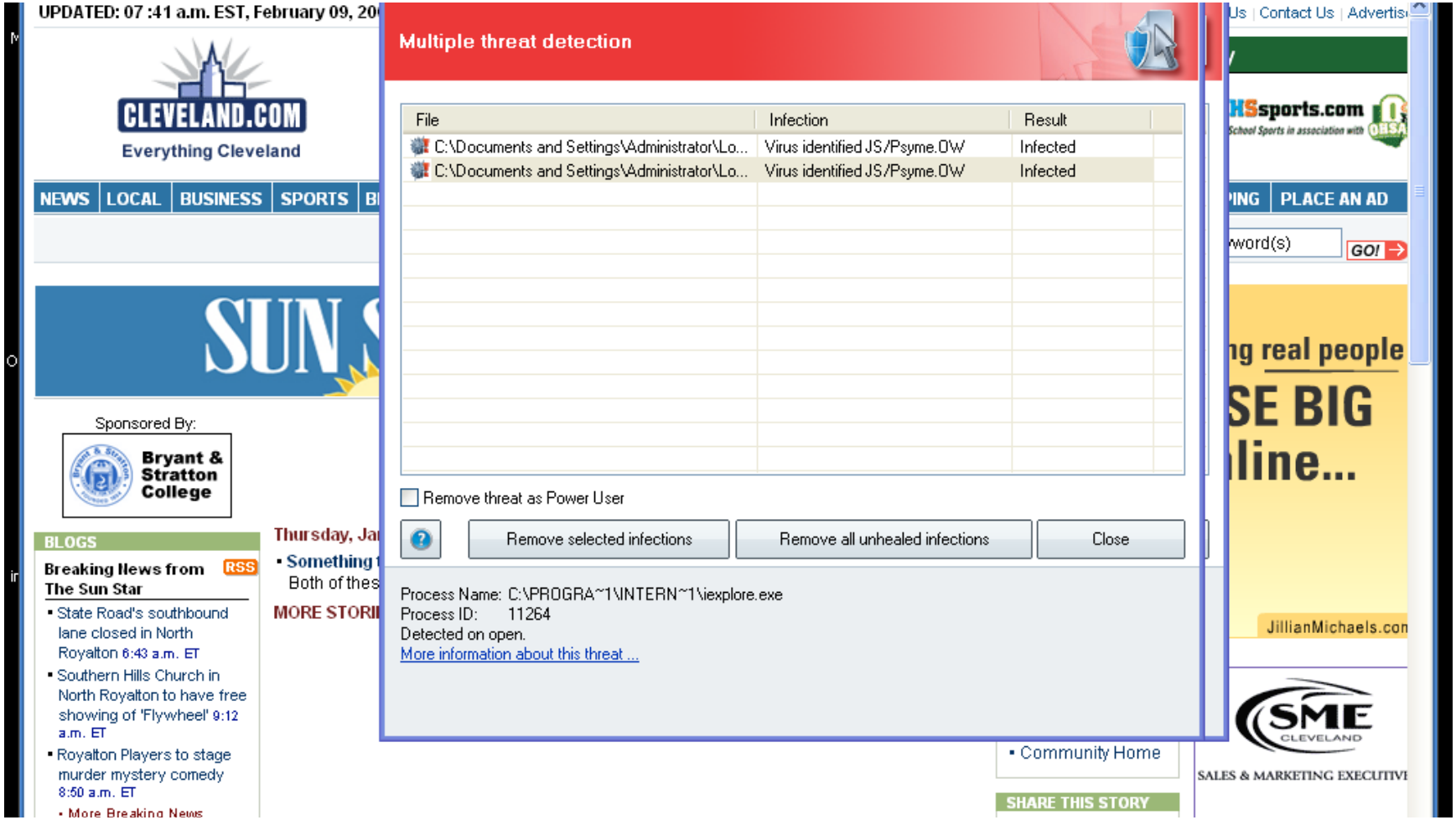
Google Trends provides insights into broad search patterns. Please keep in mind that several approximations are used when computing these results.

- News topics change fast
- Associated "trending terms" also change fast
  - "Haiti earthquake", "Fukushima", "Herman Cain", …

Trending-term exploitation: MFA



Trending term exploitation: Malware



Data collection

- Collected 9 months of trending queries
  - Trending set: collect 20 Google Hot Trends hourly, and
    - consider a term hot if it has appeared in last 72 hours
  - Control set: 495 persistently popular terms (most popular terms in 2010 for 27 categories according to Google)
- Checked Google, Bing, Twitter every 4 hours
  - Over 60,000,000 results gathered
- Classified sites as
  - Made for Adsense
    - (through supervised machine learning algorithm)
  - Malware distributor/Fake Anti-virus
    - (through blacklists, namely Google Safe Browsing API)
  - Benign

Economic results overview

- Regression analysis suggests that
  - Both MFAs and malware struggle to compromise more lucrative terms
  - MFAs and malware are *economic substitutes*
    - Malware thrives on relatively unpopular terms (lower ad prices)
    - MFAs thrives on more popular terms (higher ad prices)

Revenue analysis

- Can formalize the revenue made by websites with simple equations

$$R_{\text{MFA}}(t) = \sum_{w \in \text{MFA}(s)} \sum_{s} V(w,s,t) \cdot (p_{\text{PPC}} \cdot p_{\text{clk}} \cdot r_{\text{PPC}} + p_{\text{banner}} \cdot r_{\text{banner}} + p_{\text{aff}} \cdot p'_{\text{clk}} \cdot r_{\text{aff}})$$

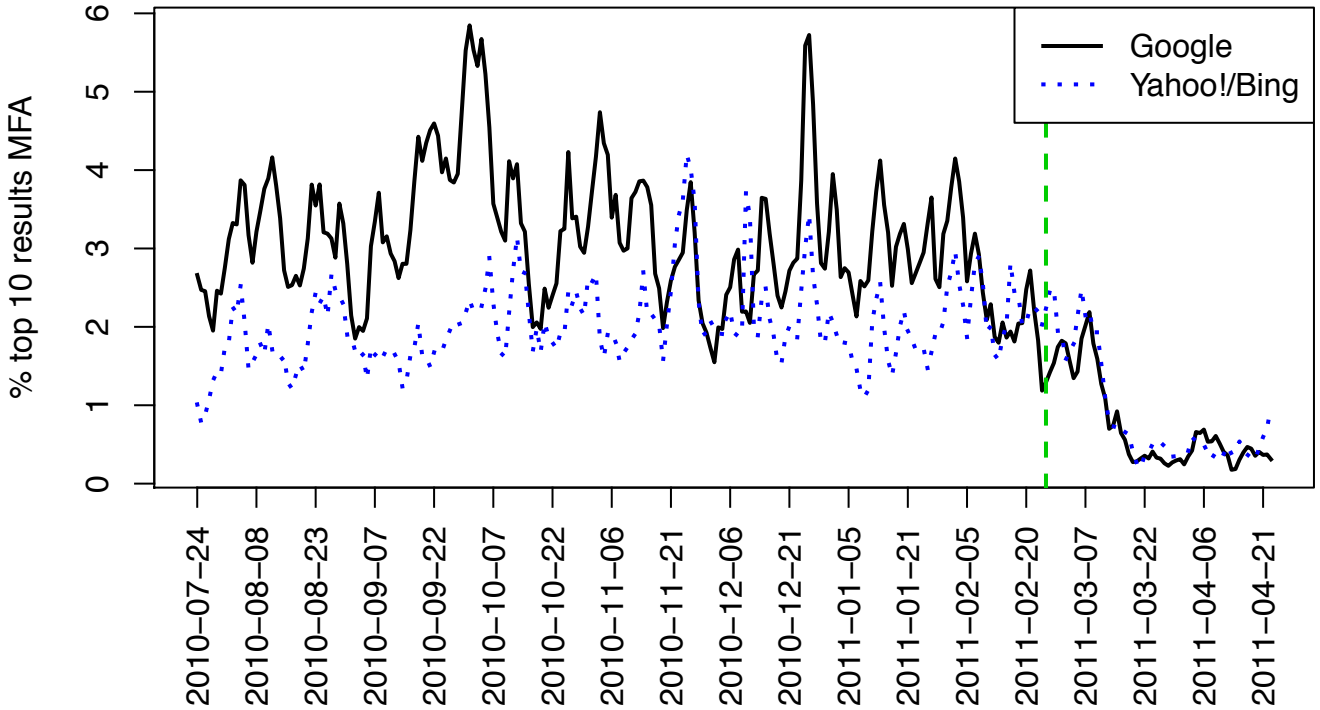
$$R_{\text{mal}}(t) = \sum_{\text{w} \in \text{mal(s)}} \sum_{s} V(w,s,t) \cdot p_{\text{exp}} \cdot p_{\text{pay}} * r_{\text{AV}}$$

Visits

Expected value generated per visit

- Using our measurements yields:
  - $R_{\text{MFA}}(1 \text{ month}) \approx \$97\,637$
  - $R_{\text{mal}}(1 \text{ month}) \approx \$61\,356$
- Very different revenue models, but very similar outcomes
  - Especially considering that there is about a 32% cut on MFA prices (Google's cut)
  - Consistent with the economic substitute theory

Effects of intervention

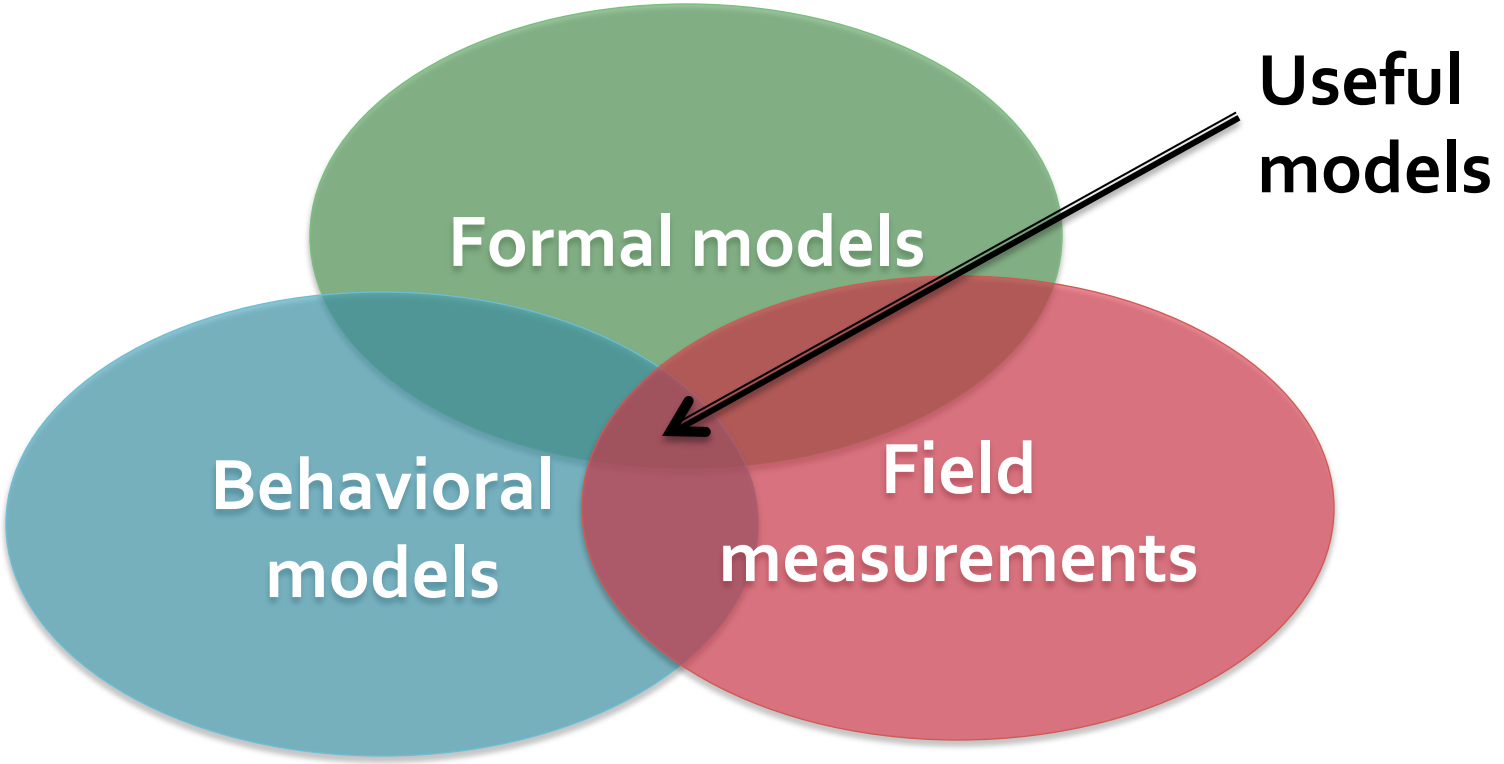


- Google changed algorithm in late Feb 2011
  - Noticeable drop in activity (-47%)
  - Yahoo!/Bing tracks Google more closely (+11%)!

Putting it together

- Users near-rational
  - Observed behaviors deviate from predicted models
  - … but not in a random fashion at all
  - Need to incorporate behavioral biases in our models
  - Conjecture: Distance to rationality increases with individual nature of player
    - I.e., institutional actors are likely to be much more rational than individuals
- Attackers much more rational
  - Attacks use incentive misalignment **and** behavioral biases
  - Observed quick reaction to intervention mechanisms
    - Responses are very rational!

Philosophical conclusion: Why I do what I do



(If you want to contribute to the ten-year plan, please contact on my behalf your nearest program manager…)

WEIS 2012

- If you enjoyed this talk, consider attending:
- Workshop on Economics of Information Security (WEIS)
  - A good place to see and engage in interdisciplinary research (Economics, Computer Science)
  - Berlin, Germany – June 25-27, 2012
  - http://weis2012.econinfosec.org/

(If you hated this talk, please don't mention I brought WEIS up to its organizers)

Questions?

Thank you!

Nicolas Christin
nicolasc@cmu.edu
Carnegie Mellon University INI/CyLab

With: John Chuang, Serge Egelman, Jens Grossklags, Benjamin Johnson, Keisuke Kamataki, Nektarios Leontiadis, Tyler Moore, Timothy Vidas, Sally Yanagihara