

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

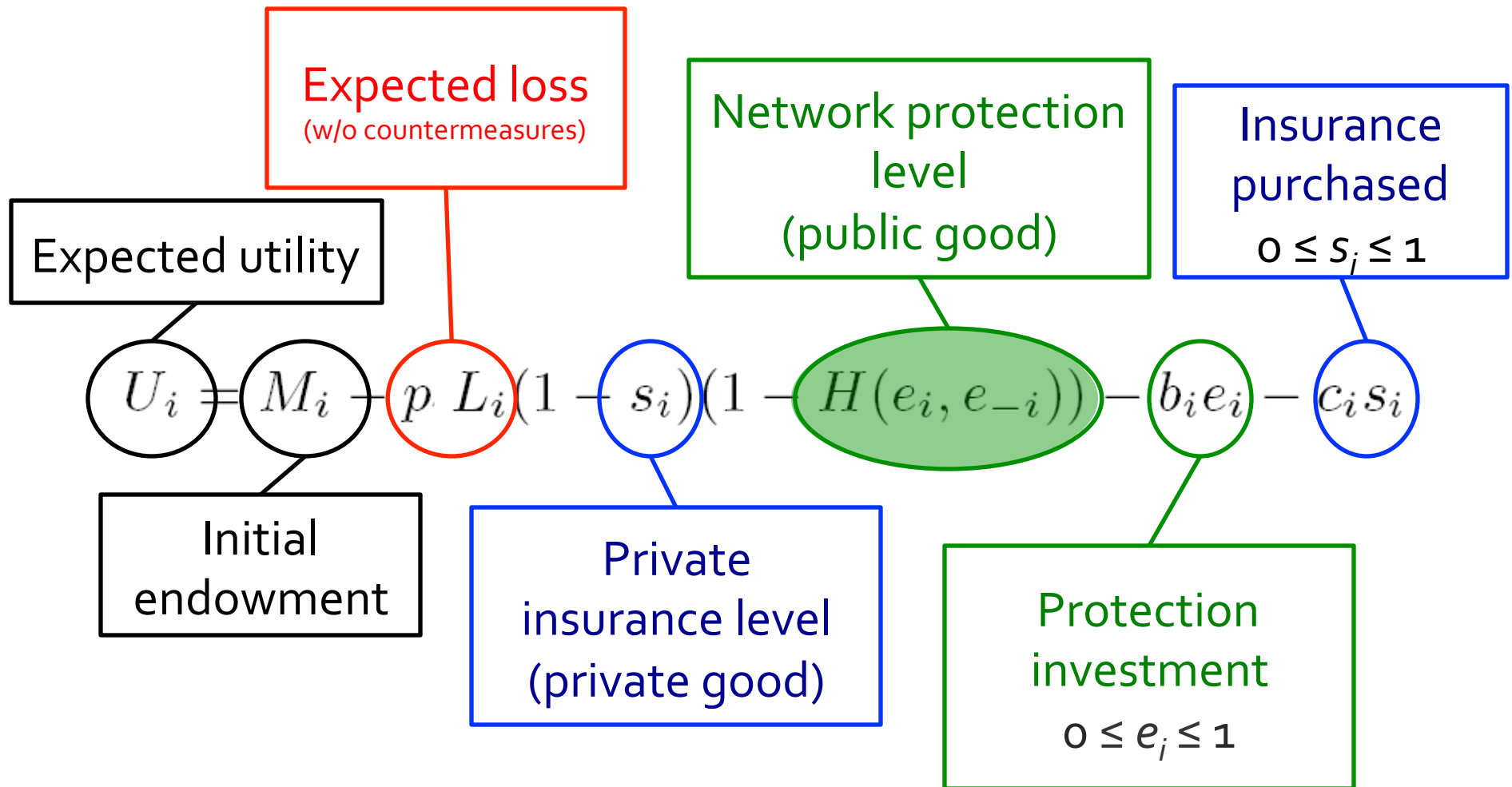
Formal analysis and Behavioral economics

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

$(L_i = L, b_i = b, c_i = c, M_i = M, \text{ pure Nash})$

	Protection	Self-Insurance
Total Effort	$pL > bN$ 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	<i>No Nash</i>
Weakest T with M	<i>Full protection if $b \leq c$</i>	<i>No Nash</i>

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. ($pL > b$)
- 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 $H(e_1, \dots, e_n) = e_i$

■ 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.

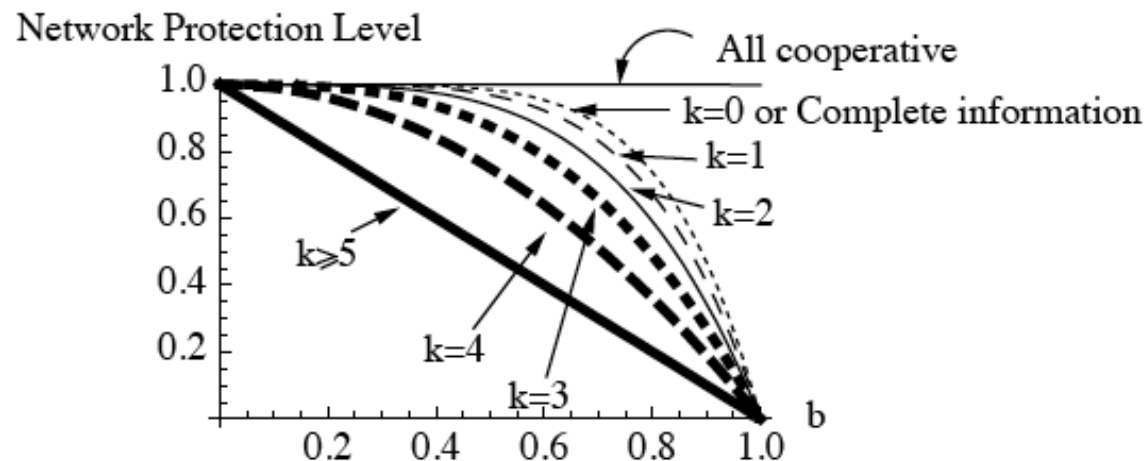
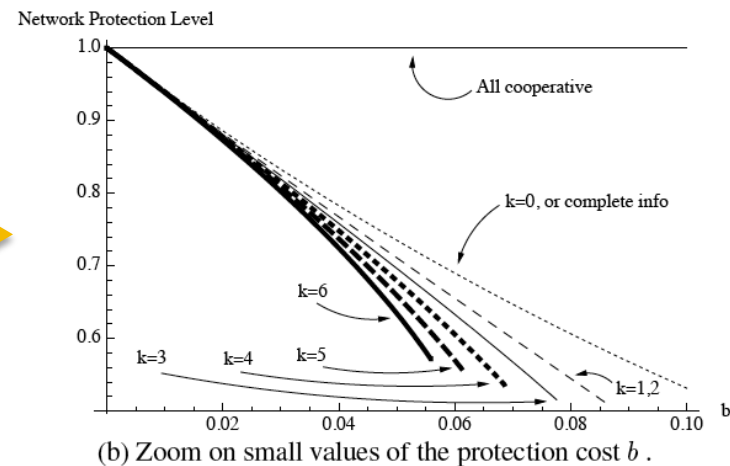
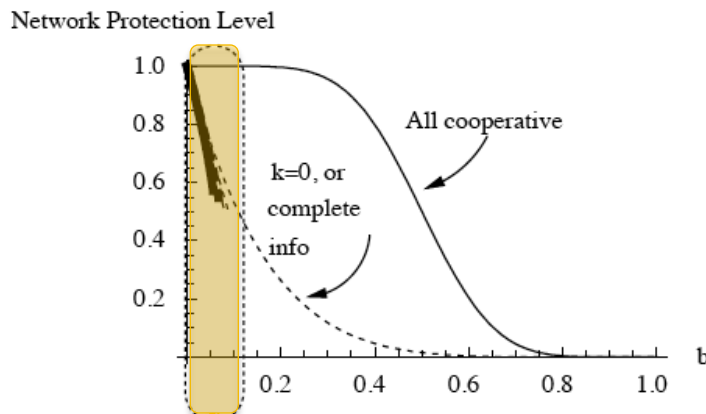


Fig. 2. Best shot. Evolution of the network protection level as a function of the protection cost b . The different plots vary the number of experts k in a network of $N = 6$ players. We observe that the fewer experts participating in the game, the higher the network protection level is, on average.

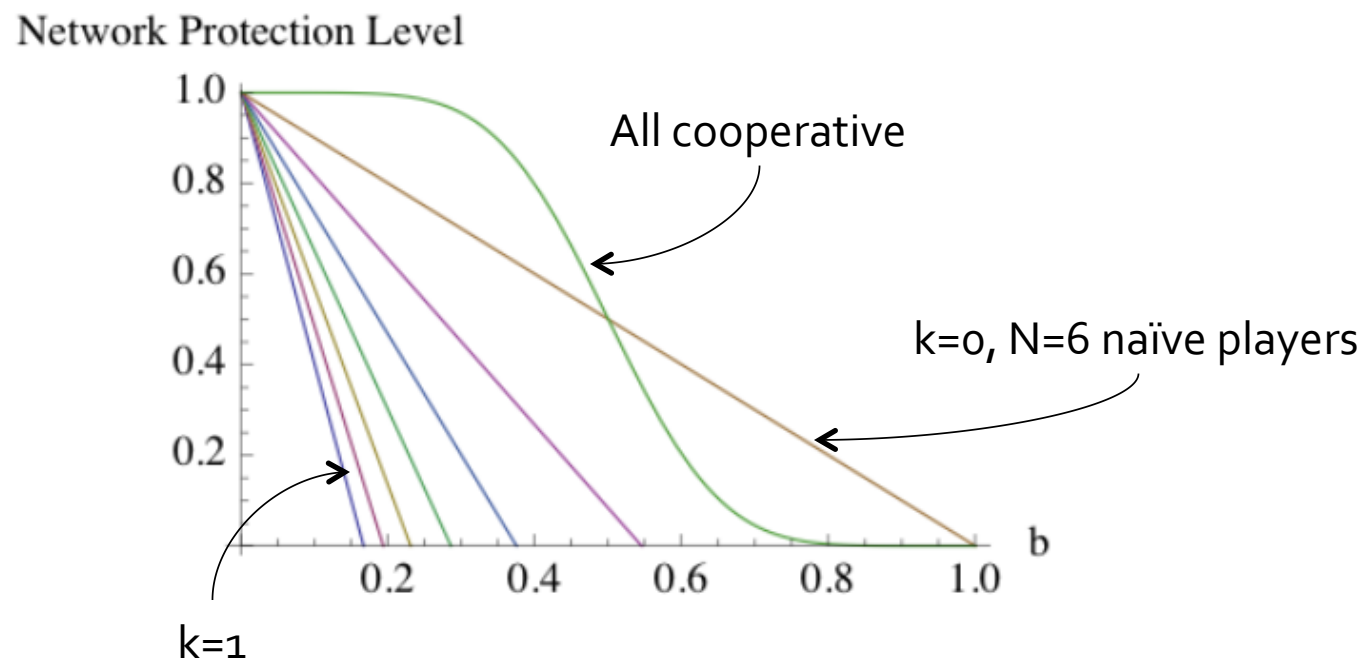
Weakest Link and limited information

- 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.



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

file:///E:/game/client2/test.html

Clock

Payoff Information

Legend	All	Recent	Previous	Total
■ No Attack			Protection	Prev Payoff
■ Attack, Protected			Insurance	Total Payoff
■ Attack, Breached				
■ Prev Round				

Control Panel

Current protection	100	Current insurance	100
Next protection	100	Next insurance	100

Game

The game will begin soon

Familiarize yourself with the user interface

Make sure to ask any questions you may have

Then, select a channel for the first round

When everyone is ready, the experiment will start

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

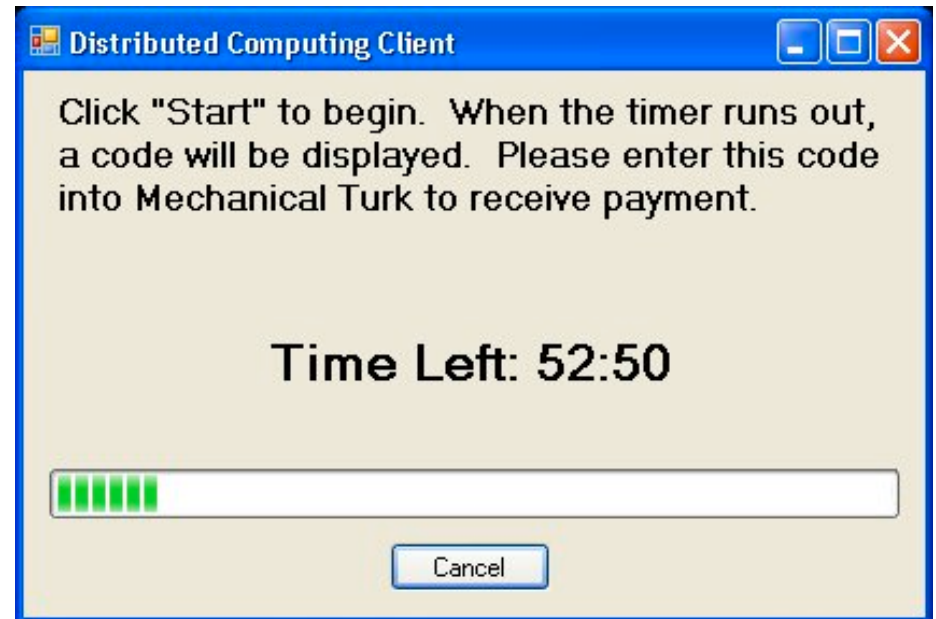
Behavioral bias case study

[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

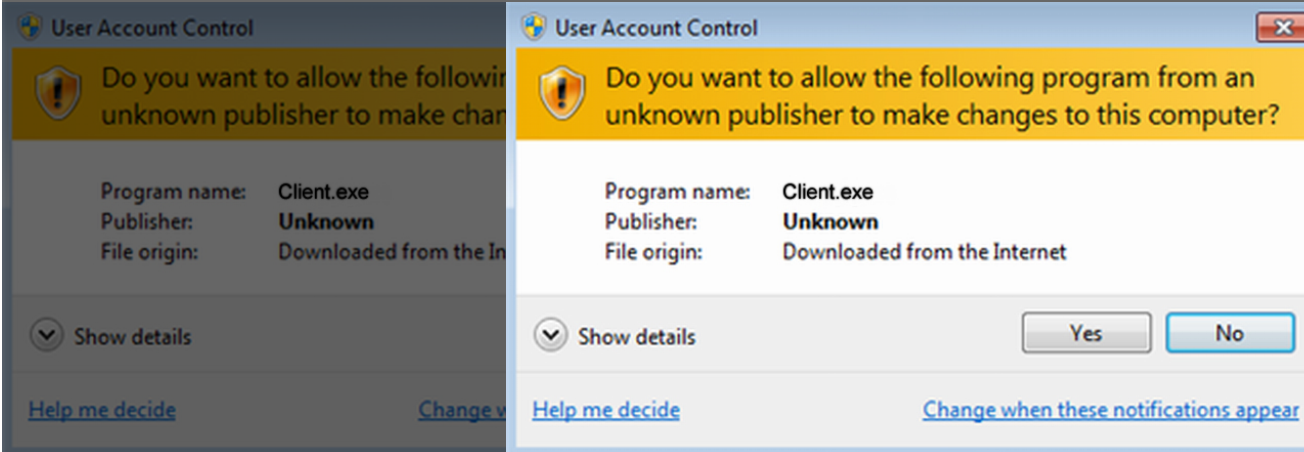
Experimental environment

- 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?

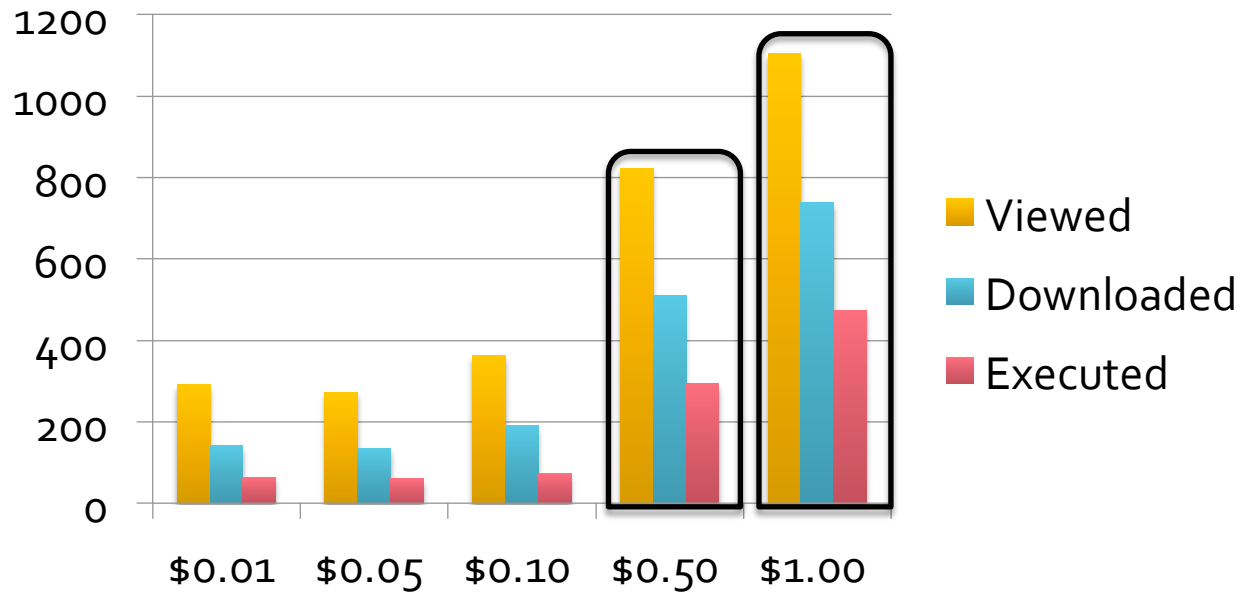


prompt for 50%
data:
control
s version
list

- 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



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

読み取り 転送量 100%

機種情報 OK IPアドレス OK ホスト名 OK

データ登録が正常に完了しました。

■お客様の機種情報 Mozilla/5.0 (X11; U; Linux i686; ja; rv:1.9.0.15) Gecko/2009102814 Ubuntu/8.04 (hardy) Firefox/3.0.15

■お客様のIPアドレス [REDACTED]

■お客様のホスト名 [REDACTED]

ご登録有難うございました。お客様が後払い会員登録をされました利用料金**57,000円**を必ずお支払い下さい。ご連絡がなく期日の3日以内のお支払いをお守り頂けなければ、契約違反となり遅延金が発生し小額訴訟の対象ともなりますのでお間違いのないようにご注意ください。

お支払いに関するご案内

■お振込ID番号	(会員番号) 1230171
■ご利用料金	57,000円 (お支払い期日は3日以内) 180日間動画見放題 ※お振込期限を過ぎますと督促の開始及び延滞金年利14.6%を別途請求させていただく場合がございます。
■銀行振込 お振込先をメールで受取る	三井住友銀行 武蔵関(むさしせき)支店 普通預金 6630471 合資会社アイティ企画 ※お振込先をメールで確認される方は「宛先アドレス」にお客様ご自身に届くメールアドレスを入力して送信をお願い致します。 ※お振込の際の振込依頼人名欄には、お客様のお名前ではなく、お客様専用に行行しましたお振込ID番号(会員番号)『1230171』をご入力またはご記入してください。お名前の入力 は不要です。

Why do victims pay?

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

読み取り 転送量 100%

機種情報 OK IPアドレス OK ホスト名

データ登録が正常に完了しました。

■お客様の機種情報 Mozilla/5.0 (X11; U; Linux i686; ja; rv:1.9.0.15) Gecko/2009102814
Ubuntu/8.04 (hardy) Firefox/3.0.15

■お客様のIPアドレス

■お客様のホスト名

ご登録有難い。ご連絡の対

請求ハガキ・督促手続き 請求ハガキ

お支払い期限を過ぎますと、架空請求との差別化を測るため、お客様のお使いのプロバイダーのご登録名義様にコチラの文面にて請求ハガキをお送りします。また、送付費用として¥20,000円を別途ご請求させていただきます。

郵便はがき

〇〇県〇〇市〇〇〇〇 〇-〇〇
〇〇マンション 〇号室

〇〇〇〇様

ご案内の御料金につきましては、すでに相当期間お支払い期限を過ぎておりますが、まだご入金の確認ができておりません。もし、支払い済みでない場合は、早急にお支払いいただきますようお願い申し上げます。万が一お支払いがございませんと、法的手続きを以って処理させていただきます。

個人特定登録情報

【あなたの登録日】

【あなたのIPアドレス】

【あなたのOS】

【あなたのブラウザ】

【最終アクセス日】

【ポート番号】

【あなたの利用履歴】

【あなたの個人認識ID番号】

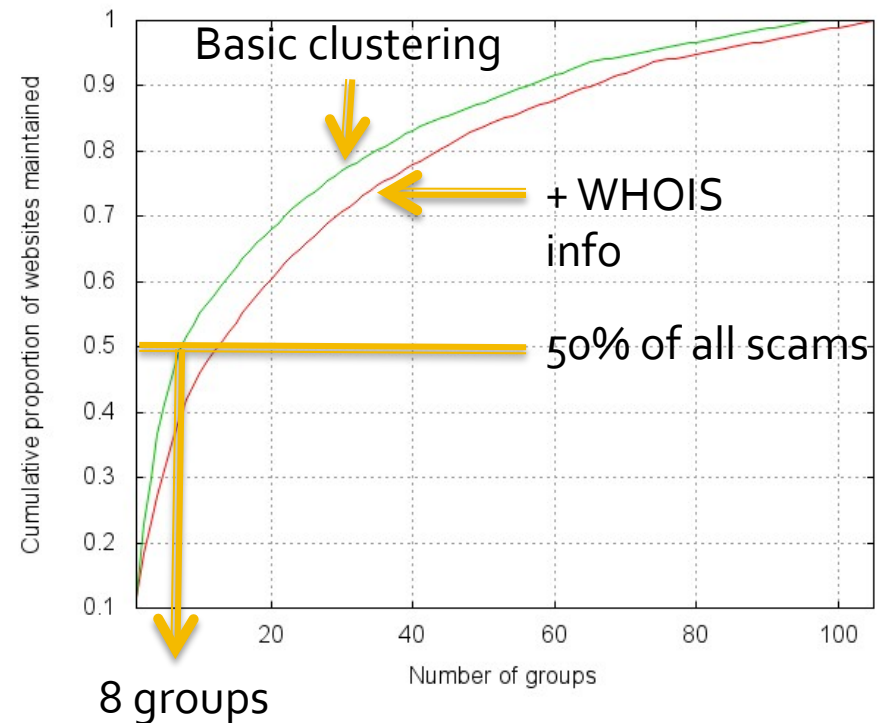
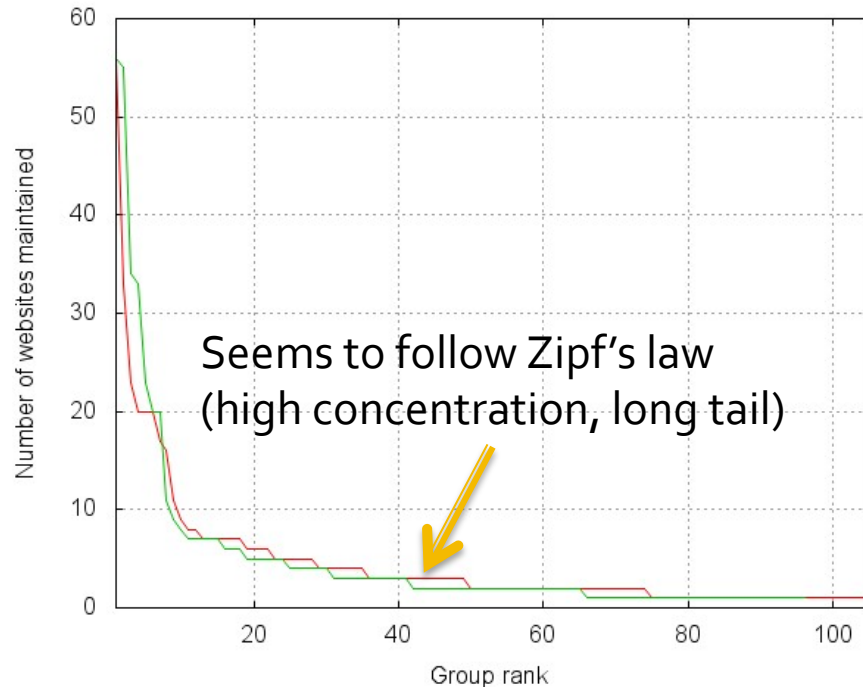
支払期限を過ぎています。早急に90,000円をお支払ください。

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 (ワンクリ凶鑑) <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

Email spamming has been the key tool for a long time

Very low conversion rate*
(about 1 purchase every 10
million emails sent)

Unsolicited

More recently: social network spam (e.g. Twitter) and blog spam

Better conversion rate*
(0.13%)

Posting malicious links via
compromised accounts

Exploiting trust we have to our
online friends

Search engine manipulation

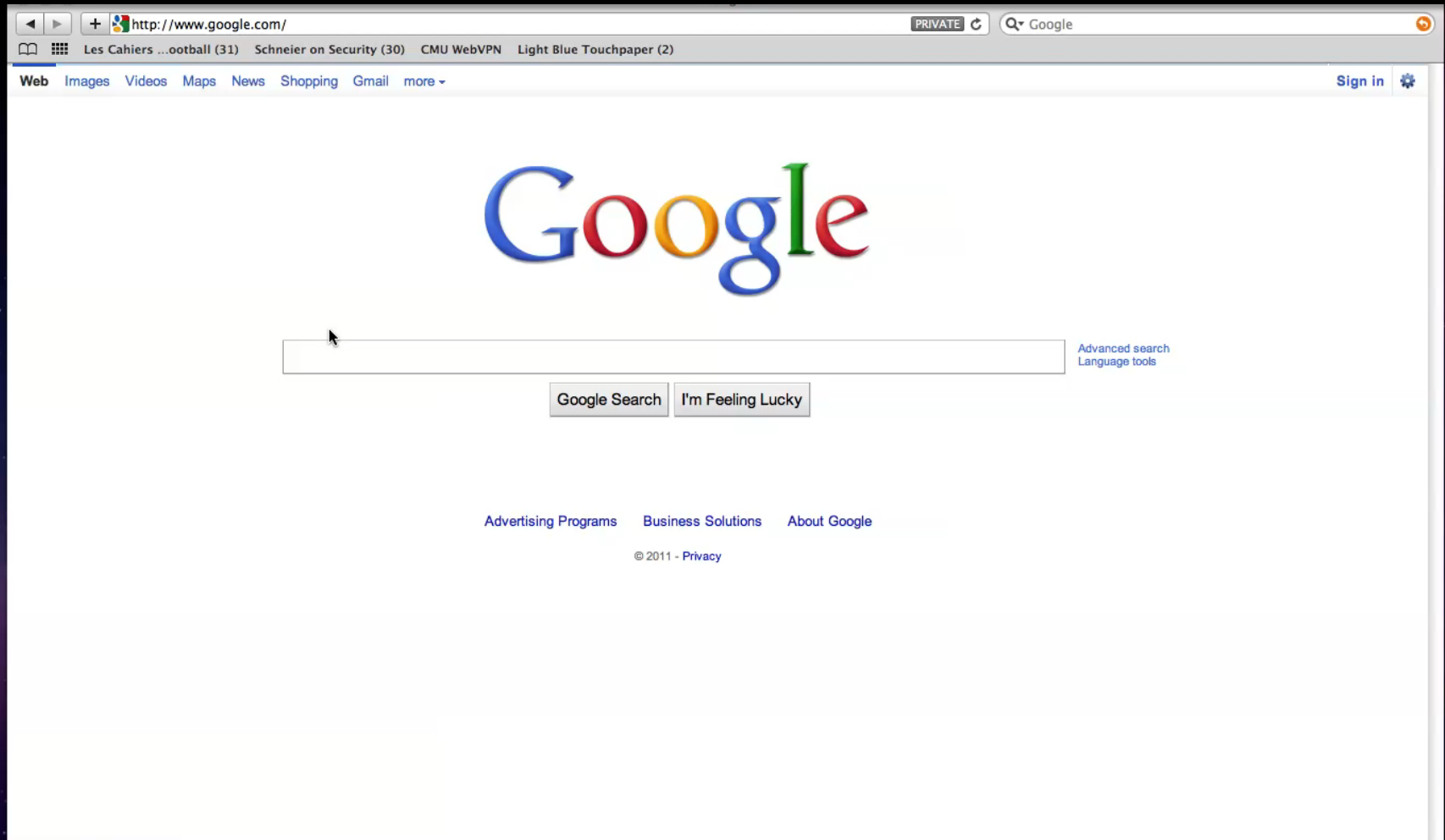
Targeted to users looking for a
product

Probably better conversion
rates

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

Search-redirection attack

[LMC, USENIX Sec'11]



Attack modus operandi

Bob runs a query on Google
(e.g. no prescription cialis)

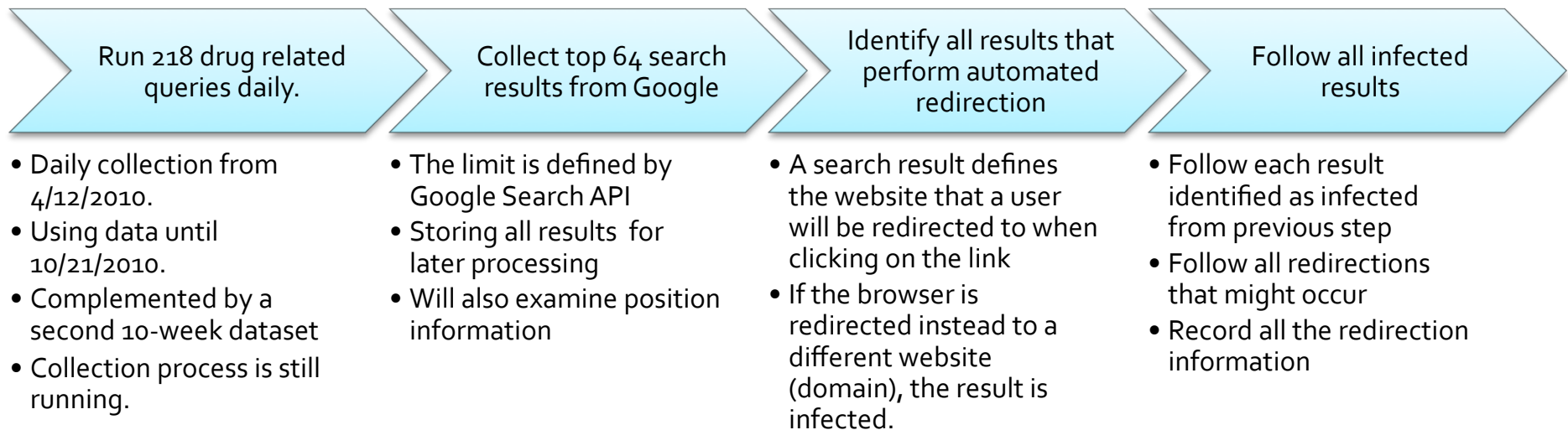
Results will include infected websites

Clicking on an infected result
triggers injected code at the
infected web server

One or more HTTP 302
redirections occur

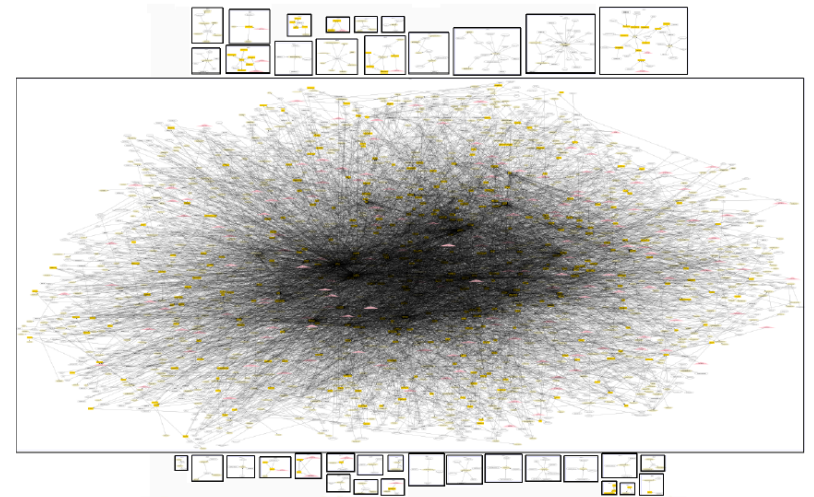
Bob lands on an online pharmacy store

Data collection process



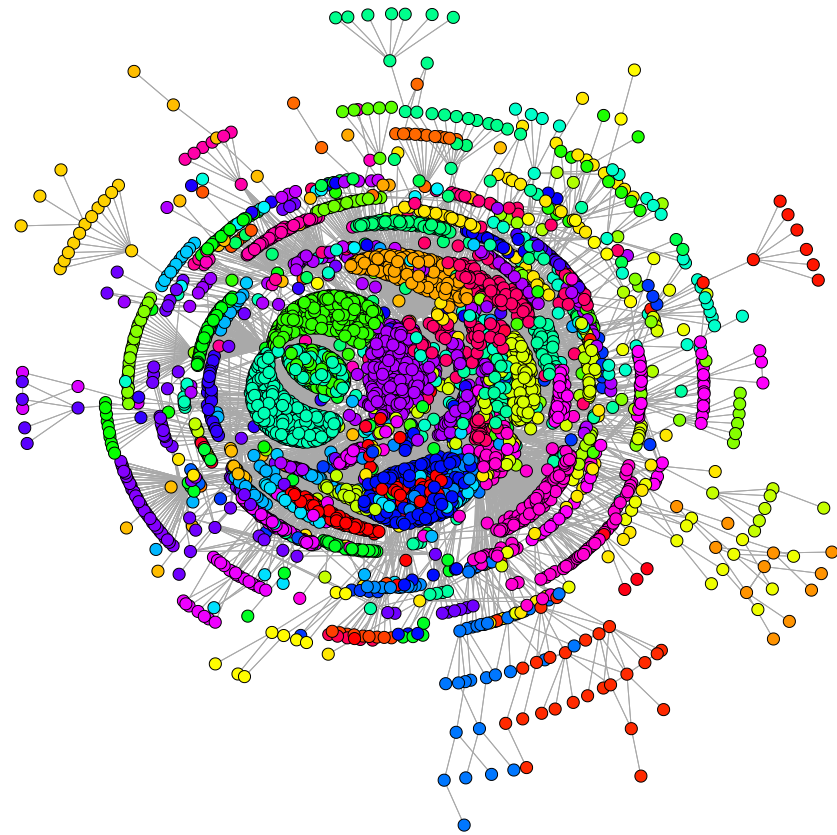
Connected components

- 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



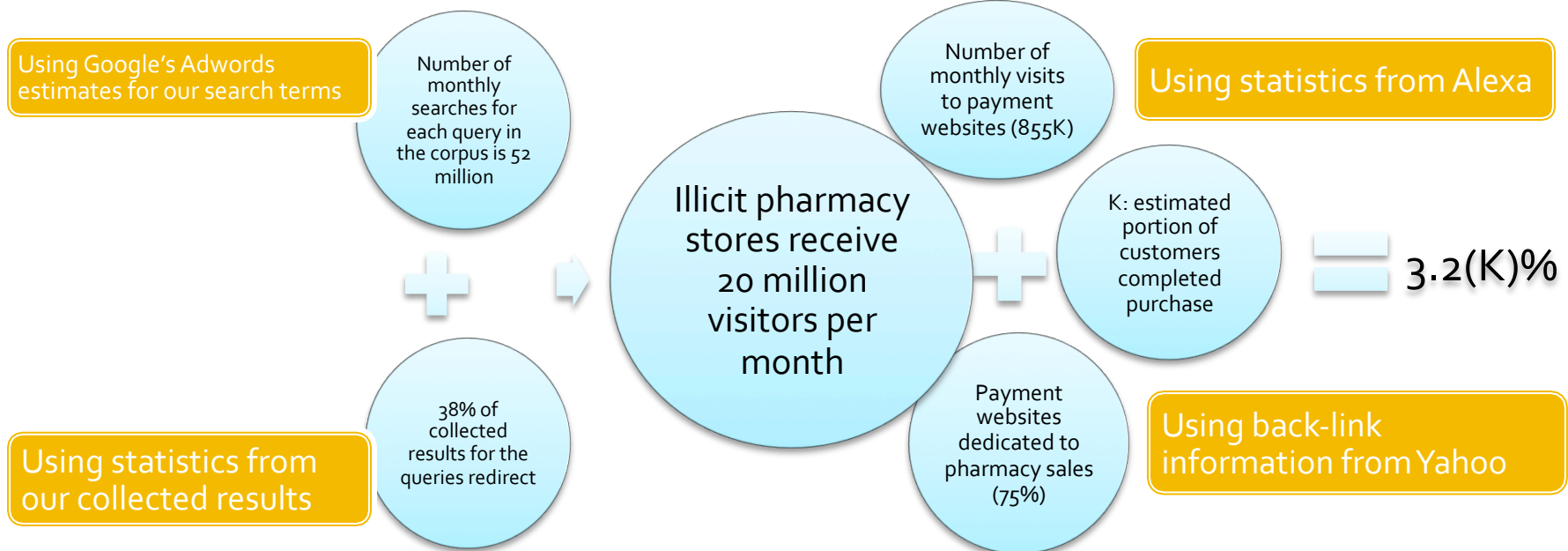
Identifying the main players

- 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



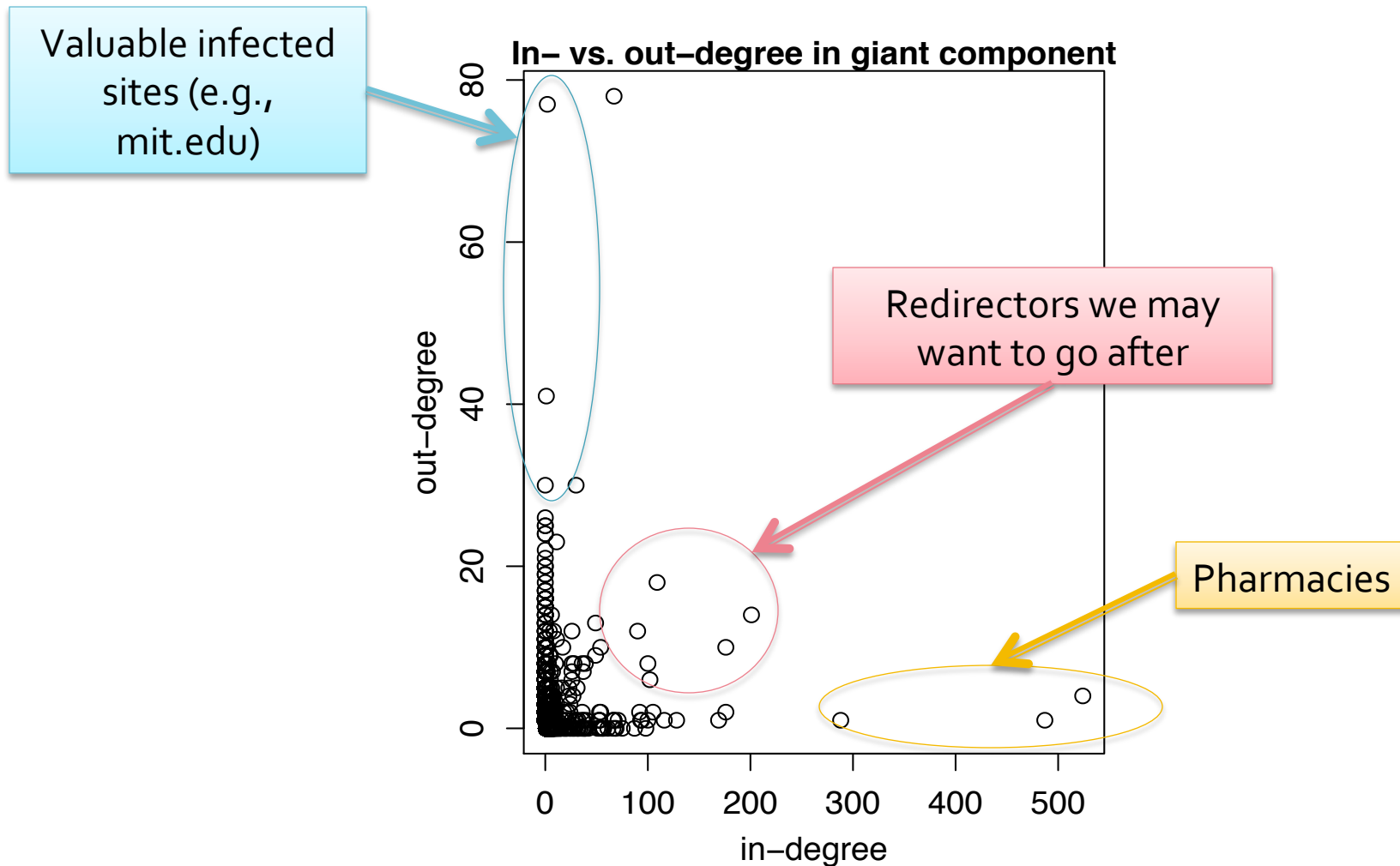
Conversion rate*

*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



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

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

©2008 Google - [Discuss](#) - [Terms of Use](#) - [Privacy Policy](#) - [Help](#)

- News topics change fast
- Associated “trending terms” also change fast
 - “Haiti earthquake”, “Fukushima”, “Herman Cain”, ...

Trending-term exploitation: MFA

Stay Connected / Friday, December 17, 2010

eWorldPost

HOME SCI & TECH WORLD ENTERTAINMENT DOMAINING WEBSITE REVIEWS WEBMASTERING
BUSINESS SPORTS POLITICS HEALTH TRAVEL GENERAL SOFTWARE RELIGION ARTS

ABOUT US RECOMMEND WEBSITE REVIEW SUBMIT A PRESS RELEASE

Dark Knight Rises, the next fiesta for Batman fans, by Nolan!

Boston Coupons www.Groupon.com/Boston
1 ridiculously huge coupon a day. It's like doing Boston at 90% off!

Take an IMAX Thrill Ride www.mos.org
Ride Wild Rollercoasters - Only At The Museum of Science. Buy Tix Now!

Batman & Robin xfinitytv.fancast.com
The Adventures of Batman & Robin. Catch Up On Your Favorite Shows.

Ads by Google

- Batman
- Batman Begin 2
- Memento
- Batman & Robin
- Ads by Google**
- The New Batman
- Dark Knight
- Film Noir
- Batman T Shirt
- Ads by Google**
- Batman Blu Ray
- Film Narration
- Batman Im Kino
- Batman TV Show

Free Batman Games Online
Find more sources/options for Free Batman Games Online
www.webcrawler.com

How to Draw Batman
Access Step-by-Step Instructions Learn How to Draw Batman
howtotutorials.net

Robbie the Reindeer Fan?
See The Illusionist - Nominated For 5 Annie Awards Incl. Best Picture!
SonyClassics.com/TheIllusionist

Batman Costumes & Access.
Also 15,000+ other quality costumes
Guaranteed low prices.
Costumes4Less.com

Ads by Google

LATEST NEWS

Ac.Milan Vs Sampdoria 1-1 Serie A Highlights- Sampdoria Manage To Halt The Leaders
The leader of the Serie A Italian football, AC Milan drew 1-1 with Sampdoria in Stadio Comunale Luigi Ferraris over in...

Newark to Oslo Daily Nonstop

Check out our great deals

After a long wait from fans, Christopher Nolan

Trending term exploitation: Malware

UPDATED: 07 :41 a.m. EST, February 09, 2010

CLEVELAND.COM
Everything Cleveland

NEWS LOCAL BUSINESS SPORTS

SUN

Sponsored By:
Bryant & Stratton College

BLOGS
Breaking News from **The Sun Star** RSS

- State Road's southbound lane closed in North Royalton 6:43 a.m. ET
- Southern Hills Church in North Royalton to have free showing of 'Flywheel' 9:12 a.m. ET
- Royalton Players to stage murder mystery comedy 8:50 a.m. ET
- [More Breaking News](#)

Thursday, Jan
• Something
Both of these
MORE STORIES

Multiple threat detection

File	Infection	Result
C:\Documents and Settings\Administrator\Lo...	Virus identified JS/Psyme.O\W	Infected
C:\Documents and Settings\Administrator\Lo...	Virus identified JS/Psyme.O\W	Infected

Remove threat as Power User

Process Name: C:\PROGRA~1\INTERN~1\ie\explore.exe
 Process ID: 11264
 Detected on open.
[More information about this threat...](#)

Community Home

SHARE THIS STORY

SME CLEVELAND
SALES & MARKETING EXECUTIVE

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

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

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

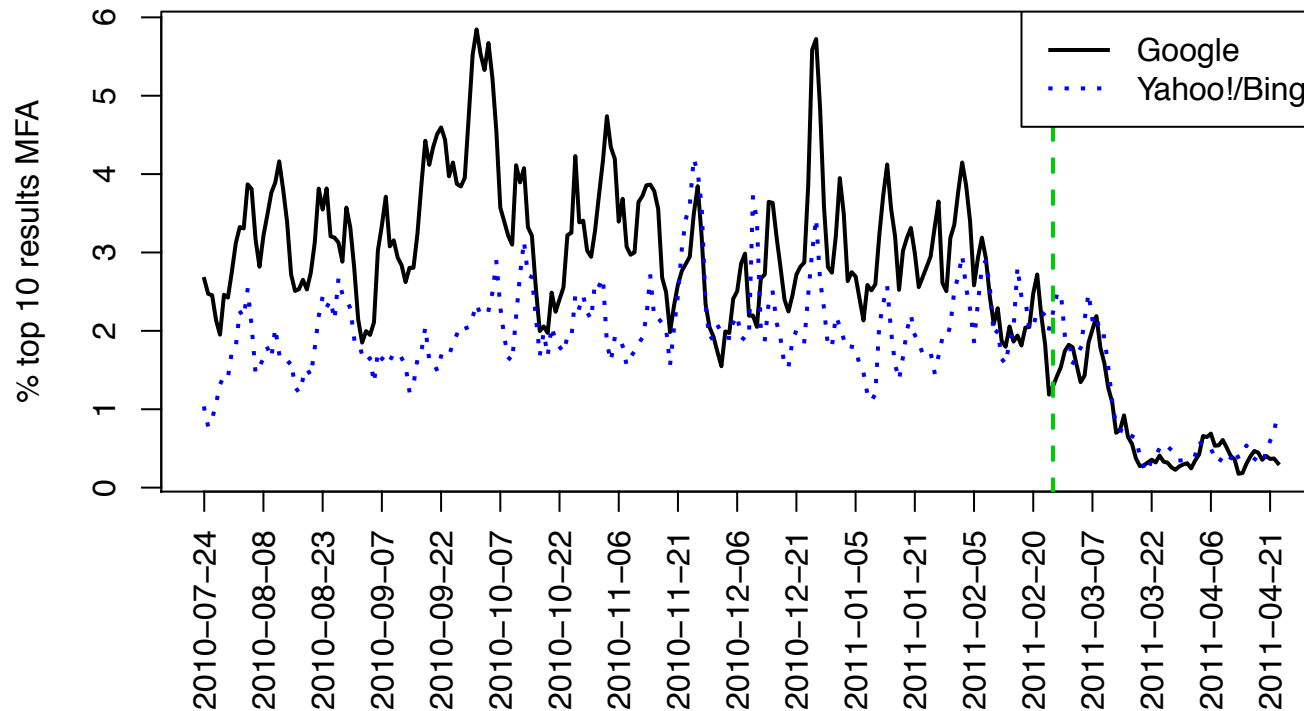
- Using our measurements yields:

- $R_{\text{MFA}}(1 \text{ month}) \approx \$97\,637$ Visits
- $R_{\text{mal}}(1 \text{ month}) \approx \$61\,356$

Expected value
generated per visit

- 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

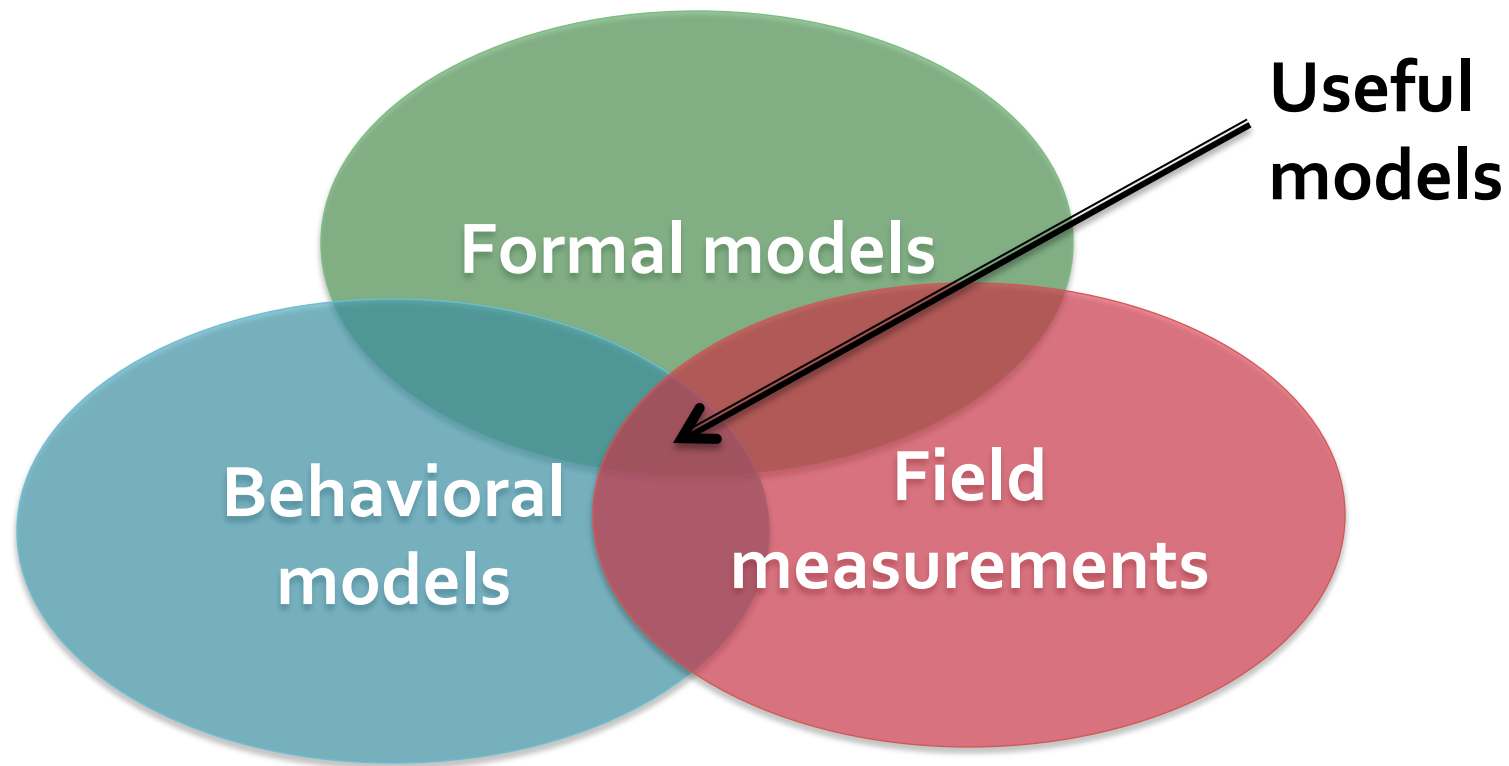


- Google changed algorithm in late Feb 2011
 - Noticeable drop in activity (-47%)
 - Yahoo!/Bing tracks Google more closely (+11%)!

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