Advanced Network Security

Phishing

Amir Mahdi Sadeghzadeh, Ph.D.

Most slides have been adapted from Mehdi Kharrazi, CE40-817, Sharif University of Technology, 2015

What is Phishing?

- "Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials”
  - Anti-phishing Working Group

How Phishing Works

- "Legitimate" emails seem to originate from trusted sources – banks or online retailers
- Social engineering tactics convince the reader that their information is needed
  - Fear is the #1 tactic
  - Solicitation of help
- Links and email look very real
  - Account Update
  - http://www.ebay.com/myaccount/update.asp
    - actually links to http://187.34.123.231

How Phishing Works

- Techniques
  - Misspelled URLs (http://www.welllsfargo.com/account)
  - Spoofing URLs (http://www.google.com@members.tripod.com)
  - Javascript
  - International Domain Names

How Phishing Works

- The Stolen Results
  - Voluntary! Remember you gave it to them.
  - Login
    - Username
    - Password
- Update Information
  - Social Security Number
  - Address
  - Bank Account Number
  - Credit Card Number

Phishing Example

Subj: **Your Bank of Oklahoma Account could be Suspended**
Date: 10/31/2005 9:17:23 PM W. Europe Standard Time
From: department@bankofoklahoma.com
To: rsutton603@aol.com
Sent from the Internet (Details)

BANK OF OKLAHOMA
You're Better Off At BOk!

Security Alert

Please note that Your B
there is a problem with y
your information,please use the
our Account:

http://secure.bankofoklah oma.com/cgi-bin/dll87443/update/default.asp

Bank of Oklahoma Security Department
Thank you.

Please Note: Bank of Oklahoma always contacts its costumers about acount expiration.That is how we show our *qualify* and *respect* to our clients.However your information are 100% safe in our 128-ssl dabatase.

Actually links to
http://212.45.13.185/bank/index.php

[Pejović]

Phishing Example

SouthTrust

Dear SouthTrust customer,

We recently reviewed your account, and we suspect an unauthorized ATM and/or PIN- based point of sale transaction on your account. Protecting your account is our primary concern.Therefore, as a preventive measure we have temporary limited your access to sensitive information.
SouthTrust Bank features.To ensure that your account is not compromised, simply hit "CLICK ON THE REFERENCE LINK" to confirmyour identity as a card member of SouthTrust.

Login to your SouthTrust Online Banking with your SouthTrust username and password.

Confirm your identity as a card memeber of SouthTrust.

View your transaction history and report suspicious activity or any unauthorized change.

https://southtrustonlinebanking.com/retail/

If you are not enrolled for SouthTrust Online Banking get started today! Complete the steps below and takeadvantage of our online services today!

Select your account: Personal Accounts, Business Acounts, Credit Card Premiere Line or Credit Line Only.
It`s that easy. If you still need assistance, just click the "Help" button within Internet Banking, or contact us. We`re here to help you 24 hours a day, 7 days a week.

*Please do not reply to this message. Mail sent to this address cannot be answered.

*For assistance, log to your SouthTrust Bank Account and chose

Thomas D. B. Graff, Member FDIC

Another false link!

VeriSign Secure Site Click to verify

Phishing Example

Subject: **Sharif University of Technology (WEBMAIL ACCOUNT SUPPORT)**
From: Support Team <supportteam@sharif.ir>
Reply-To: sharifmail@Alum.com
Date: 9/16/08 1:04 AM
To: undisclosed-recipients:;

Dear Subscriber,
Due to the incessant rate of Scam we are currently upgrading our
webmail with a hard spam protector as such all web mail users must
respond to
this Email immediately by entering your password here (**********)

USER NAME:
PASSWORD:

Failure to comply with the above instruction will immediately render your email ACCOUNT
deactivated from our database. You can also confirm your email address by logging into your web mail account.Thank you for using our web mail!

THE SUPPORT TEAM
(http://www.sharif.ir)
WEBMAIL ACCOUNT SUPPORT.
Sharif University of Technology

2008, Sharif University of Technology, Tehran, Iran

This message was sent using IMP, the Internet Messaging Program.

--
Este mensaje ha sido analizado por **MailScanner**
en busca de virus y otros contenidos peligrosos,
y se considera que está limpio.

Consequences

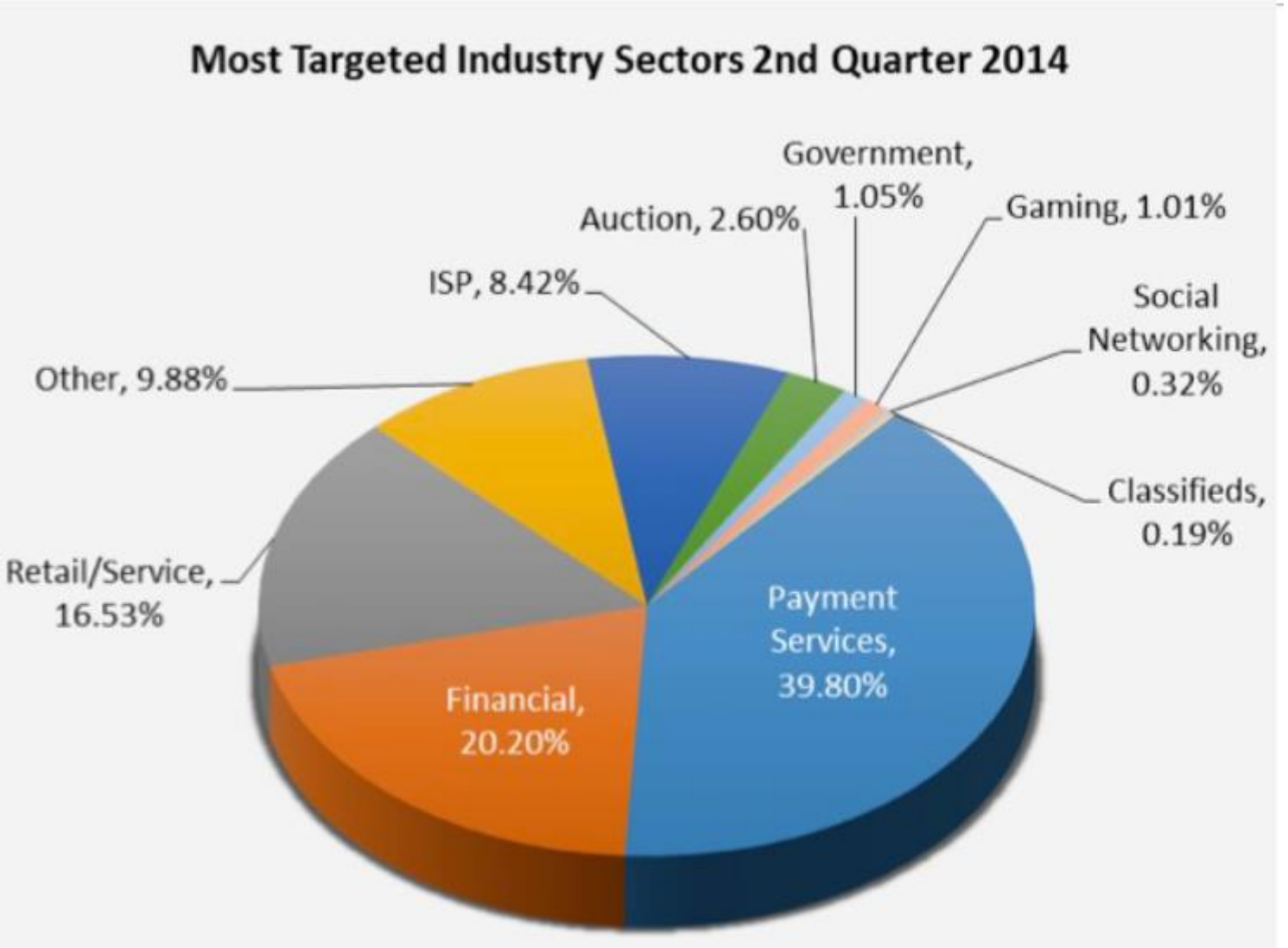
- Customers:
  - Financial consequences – stolen financial information
  - Trust and effective communication can suffer

- Service providers (banks, retailers...)
  - Diminishes value of a brand
  - Customer loss
  - Could affect stakeholders

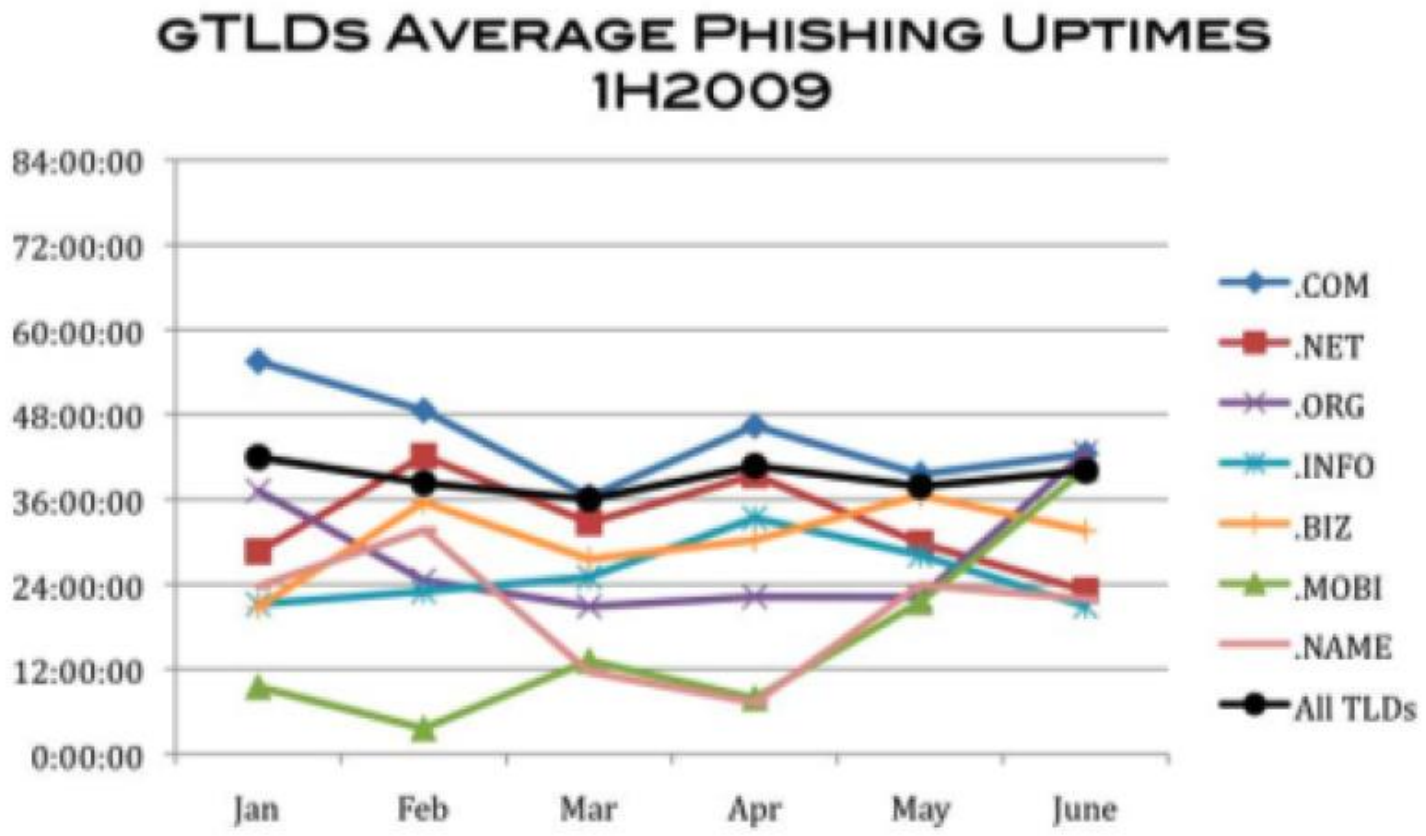
Phishing is a Plague on the Internet

- Estimated 3.5 million people have fallen for phishing
- Estimated to cost $1-2.8 billion a year (and growing)
  - 9255 unique phishing sites reported in June 2006
  - 40621 unique phishing sites reported in August 2009
  - 26402 unique phishing sites reported in March 2011
  - 44407 unique phishing sites reported in May 2014
- The number of phished brands was 339 in January 2011
- The number of phished brands was 531 in 2014Q2
- Easier (and safer) to phish than rob a bank

Most Targeted Industry



Phishing Uptime



Phishing Targets

- Users lack computer knowledge
  - Elderly
- Users lack security knowledge
  - Elderly
  - Teens
  - New Computer Users
  - Infrequent Computer Users

Spear Phishing

Spear Phishing

- Targeted at a specific company, government agency, organization, or group
  - Phisher gets an e-mail address of an administrator/colleague
  - Spoofed e-mail asks employees to log on to a corporate network
  - A key-logger application records passwords
  - Phisher can access corporate information

Whaling Attacks

- Phishing attack directed at high profile executives
- From “The Register” 16th April 2008:
  - Highly targeted email scam that singled out as many as 20,000 senior corporate executives
  - Messages masquerade as an official subpoena requiring the recipient to appear before a federal grand jury
  - The emails correctly address their full name and include their phone number and company name
  - Recipients who click on a link that offers a more detailed copy of the subpoena are taken to a website that informs them they must install a browser add-on in order to read the document
  - a backdoor is installed and key logging software that steals log-in credentials used on websites for banks and other sensitive organizations.
  - About 2,000 executives took the bait on the first day

Phishing Techniques

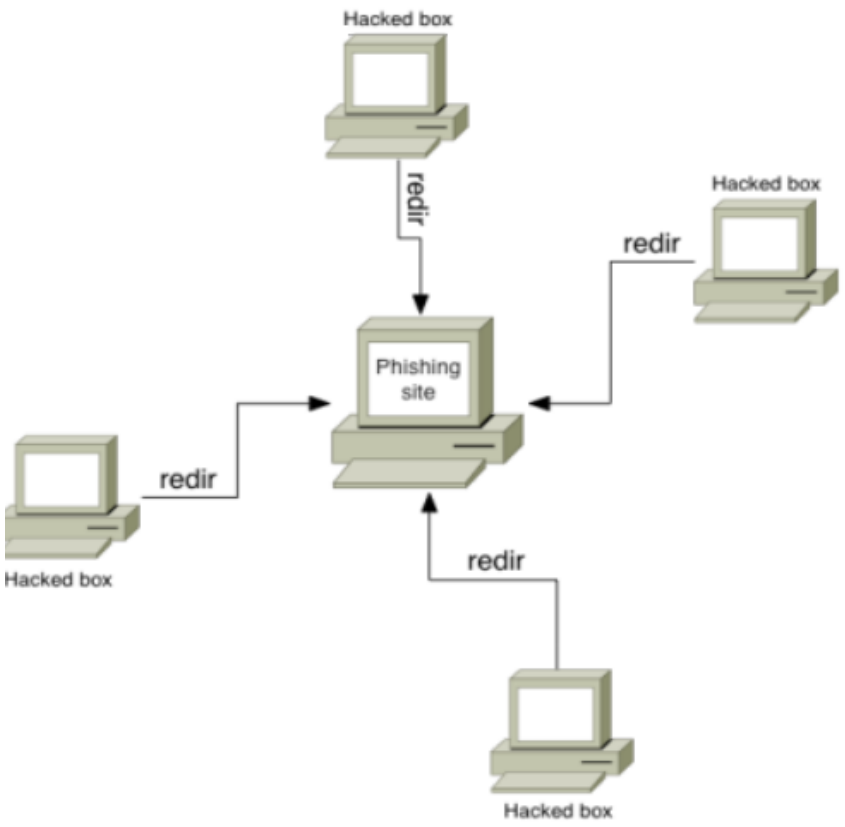
- Phishing through compromised web servers
  - Find vulnerable servers
  - Gain access to the server
  - Pre-built phishing web sites are up
  - Mass emailing tools are downloaded and used to advertise the fake web site via spam email
  - Web traffic begins to arrive at the phishing web site and potential victims access the malicious content

Phishing Techniques

- Phishing through port redirection
  - Find vulnerable servers
  - Install software that will forward port 80 traffic to a remote server
  - Make sure that it is running even after a reboot
  - Try not to get detected
  - Web traffic begins to arrive at the phishing web site and potential victims access the malicious content

Phishing Techniques

- Combined technique
  - If a remote host is lost other will continue to phish
  - If the central phishing site is lost, compromise another and update redirections
  - Faster configuration setup, concurrent adjustments can be made



Phishing Techniques

- Additional approaches
  - Register similar sounding DNS domains and setting up fake web sites, e.g. www.paypa1.com www.welsfargo.com
  - Configure the fake phishing web site to record any input data that the user submits silently log them and then forward the user to the real web site

Phishing Techniques

- Transfer of funds
  - International transfers are monitored, find an intermediate person to send the money
  - “Hello! We finding Europe persons, who can Send/Receive bank wires from our sellings, from our European clients. To not pay TAXES from international transfers in Russia. We offer 10% percent from amount u receive and pay all fees, for sending funds back. Amount from 1000 euro per day. All this activity are legal in Europe, Thank you, FINANCIE LTD.”

Pharming

- Typing URL e.g. www.newegg.com Translates to IP address 216.52.208.185
- DNS – a dictionary with pairs URL - IP
- What happens if somebody hacks the DNS?
  - Instead of 216.52.208.185 , www.newegg.com might take us to 192.168.10.103
  - Usually, a false web page is there

Pharming

- How hard is it to perform DNS poisoning?
  - Local DNS cache
  - Local DNS
  - Wireless routers

Phishing Prevention

- Public Education
  - Do not believe anyone addressing you as a 'Dear Customer' 'Dear business partner', etc.
  - Do not respond to an e-mail requesting username, password, bank account number, etc.
  - Do not click on the link provided in an e-mail message

CANTINA: A Content-Based Approach to Detecting Phishing Web Sites

Yue Zhang, University of Pittsburgh, Jason I. Hong, Lorrie F. Cranor
Carnegie Mellon University, www2007.

Strategies to Counter Phishing

- Make it invisible
  - Taking down phishing web pages
  - Filtering out phishing email
  - Detecting phishing web pages (SpoofGuard, etc)
- Provide better user interfaces
  - Extended certificate verification
  - Anti-phishing toolbars (SpoofGuard, eBay, Netcraft, etc)
- Train the users
  - Games (Sheng et al, SOUPS 2007)

Two Ways of Detecting Phishing Pages

- Human-verified Blacklists
  - No false positives, easy to implement, robust to new attacks
  - But tedious, slow to update, and not comprehensive
  - Only one toolbar found more than 60% phishing sites (Egelman et al, NDSS 2007)
- Heuristics
  - Fast to find new phishing sites (zero-day)
  - But false positives, may be fragile to new attacks
  - Not much work in this area
  - Our work contributes to the understanding of heuristics

Our Solution: CANTINA

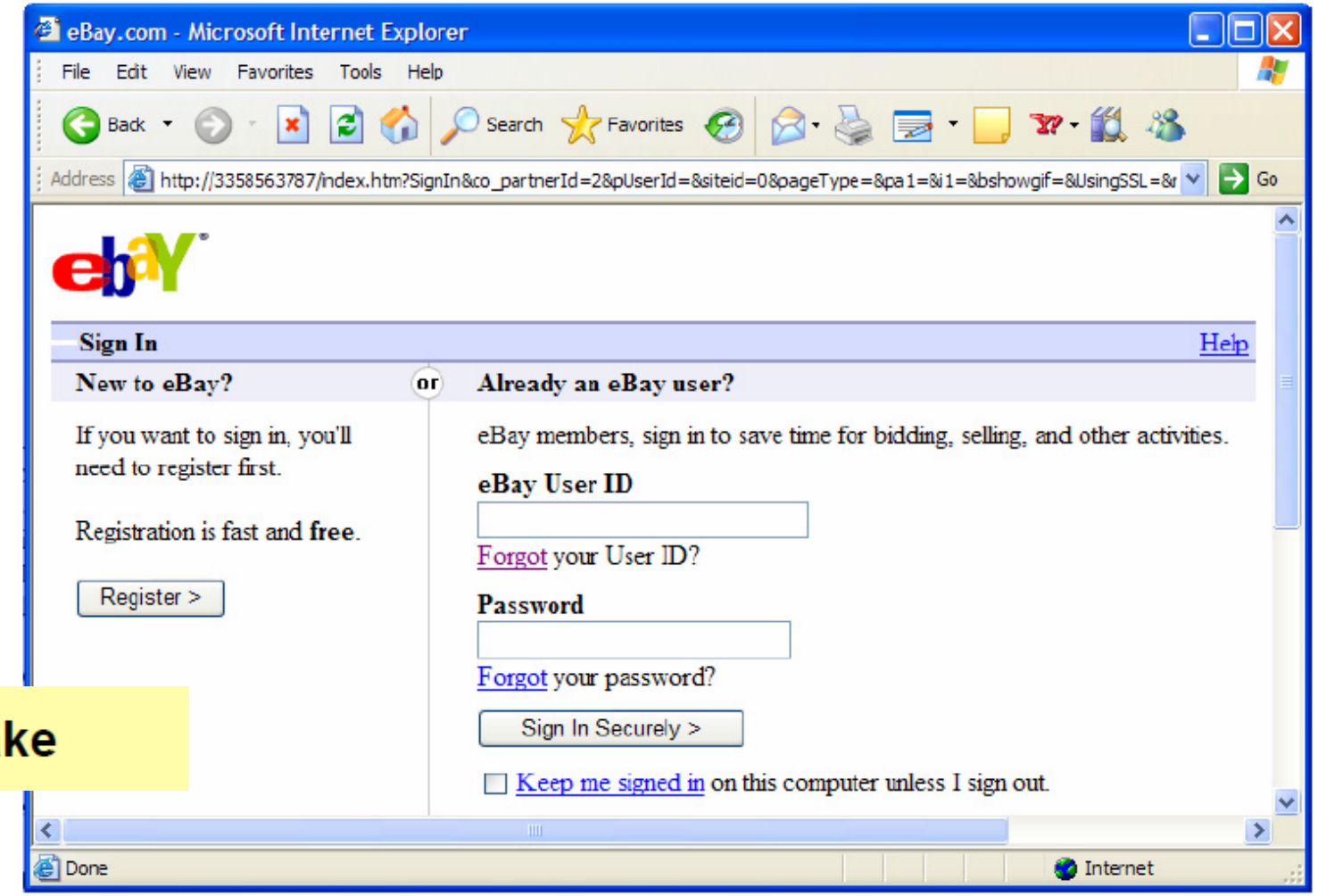
- CANTINA uses a simple content-based approach
  - Examines content of a web page and creates a "fingerprint"
  - Sends that fingerprint as a query to a search engine
  - Sees if the web page in question is in the top search results
    - If so, then we label it legitimate
    - Otherwise, we label it phishing
- Nice properties:
  - Fast
  - Scales well
  - No maintenance by us (done by search engines)
  - Highly accurate

How Robust Hyperlinks Work

- Developed by Phelps and Wilensky to solve “404 not found” problem (D-Lib Magazine 2000)
- Add lexical signature to URLs
  - If link doesn’t work, then feed signature to search engine
  - Ex. http://abc.com/page.html?sig=“word1+word2+...+word5”
- How to generate useful signatures?
  - Term Frequency / Inverse Document Frequency (TF-IDF)
  - Their informal evaluation found using top five words as scored by TF-IDF was surprisingly effective

Adapting TF-IDF for Anti-Phishing

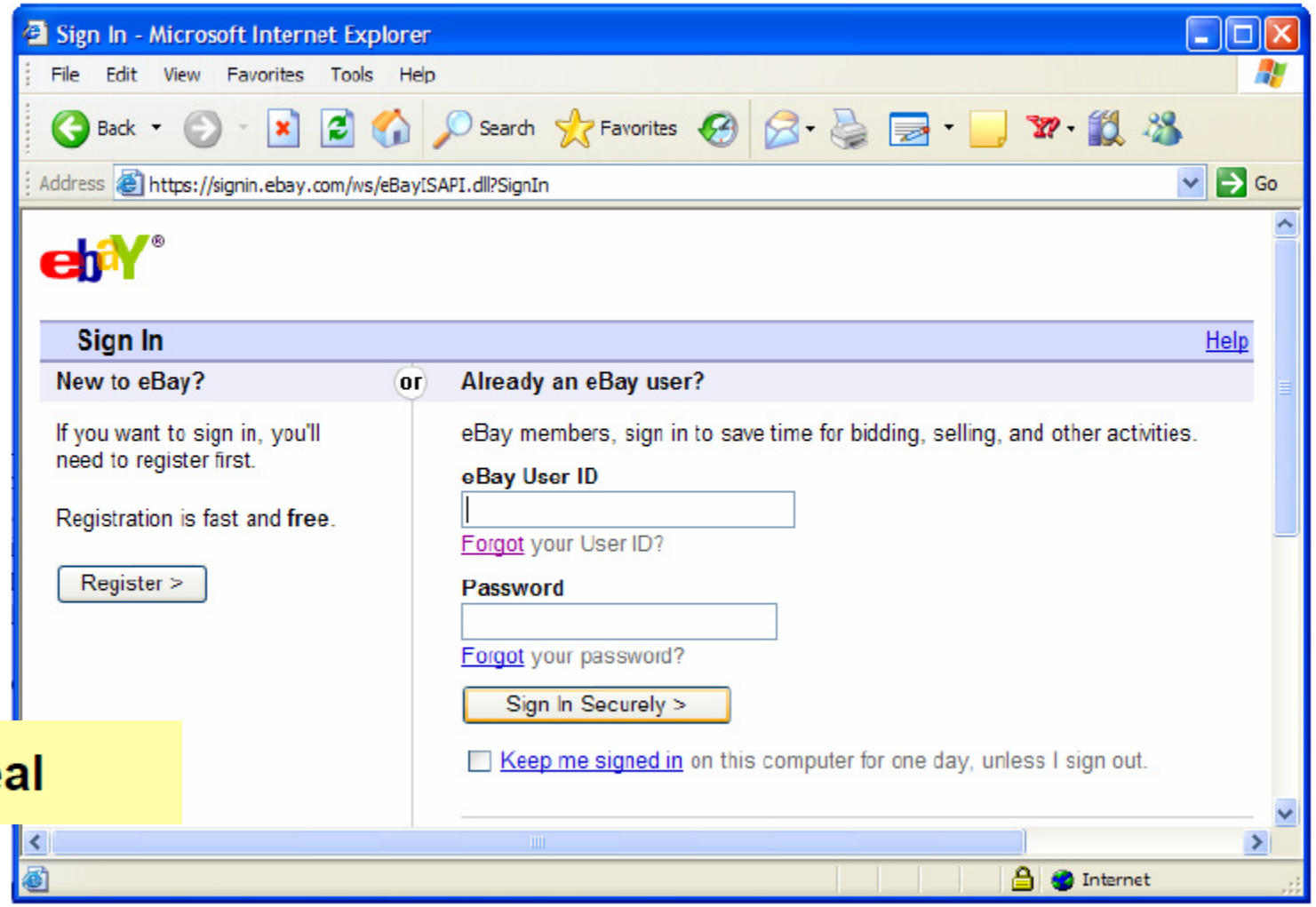
- Can same basic approach be used for anti-phishing?
  - Scammers often directly copy legitimate web pages or include keywords like name of legitimate organization



Fake

Adapting TF-IDF for Anti-Phishing

- Can same basic approach be used for anti-phishing?
  - Scammers often directly copy legitimate web pages or include keywords like name of legitimate organization



Real

Adapting TF-IDF for Anti-Phishing

- Can same basic approach be used for anti-phishing?
- Scammers often directly copy legitimate web pages or include keywords like name of legitimate organization
- With Google, phishing site should have low page rank
  - APWG states that phishing sites alive 4.5 days
  - Few sites link to phishing sites
  - Hence, phishing sites unlikely to be in top search results

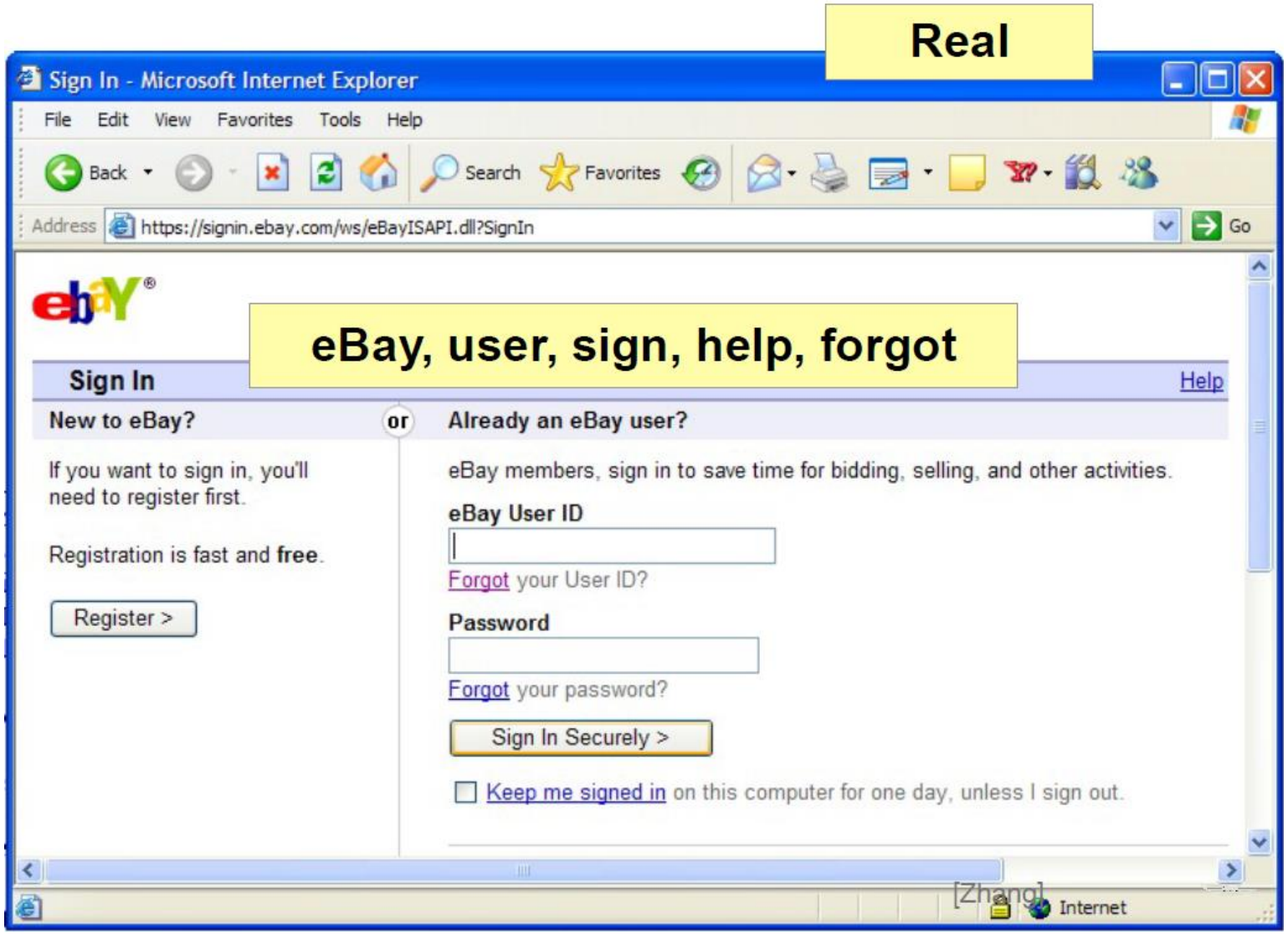
How CANTINA Works (Iteration #1)

- Given a web page, calculate TF-IDF score for each word in that page
- Take five words with highest TF-IDF weights
- Feed these five words into a search engine (Google)
- If domain name of current web page is in top N search results, we consider it legitimate
  - N=30 worked well
  - No improvement by increasing N

How CANTINA Works (Iteration #1)

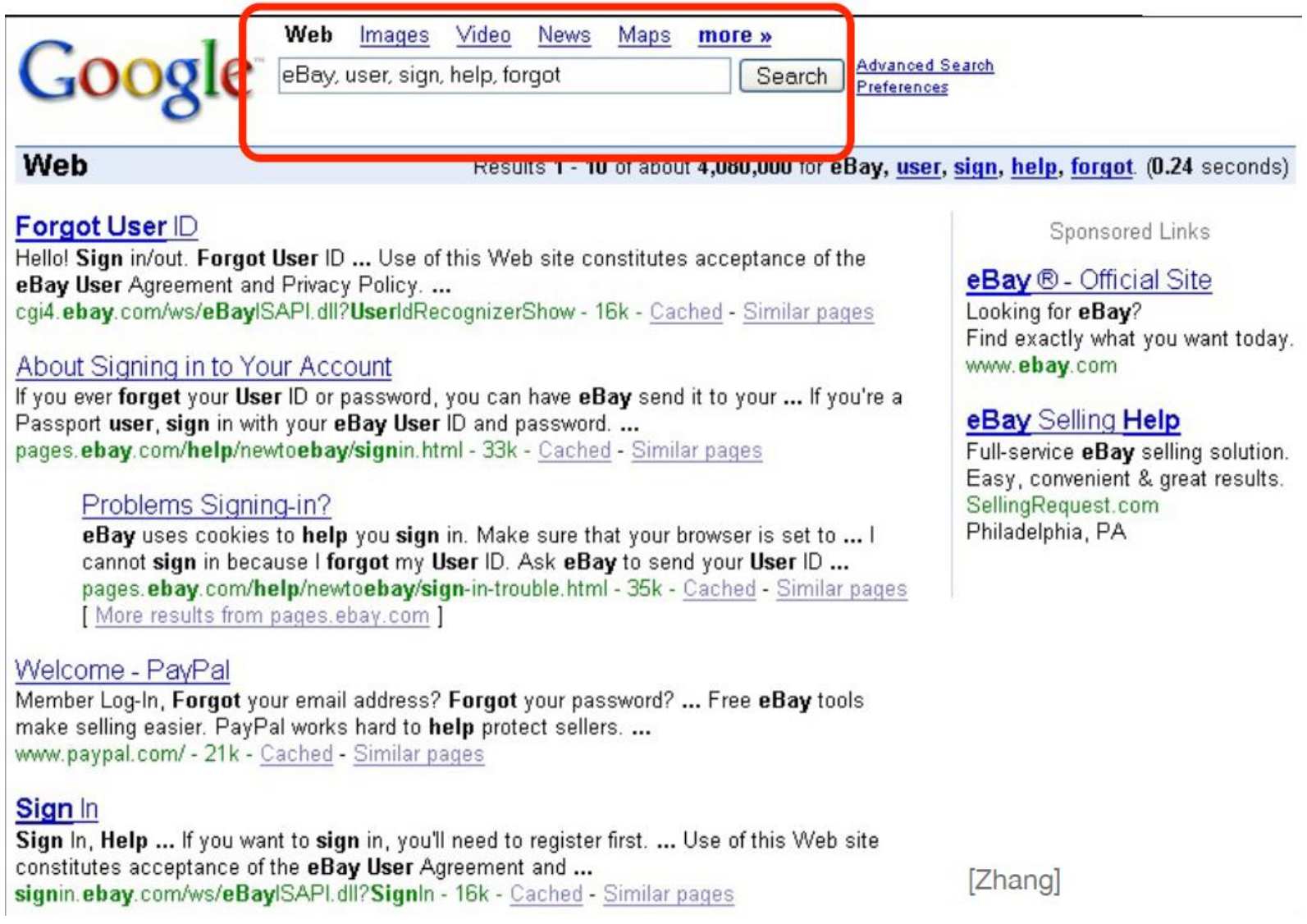
[Zhang]

How CANTINA Works (Iteration #1)



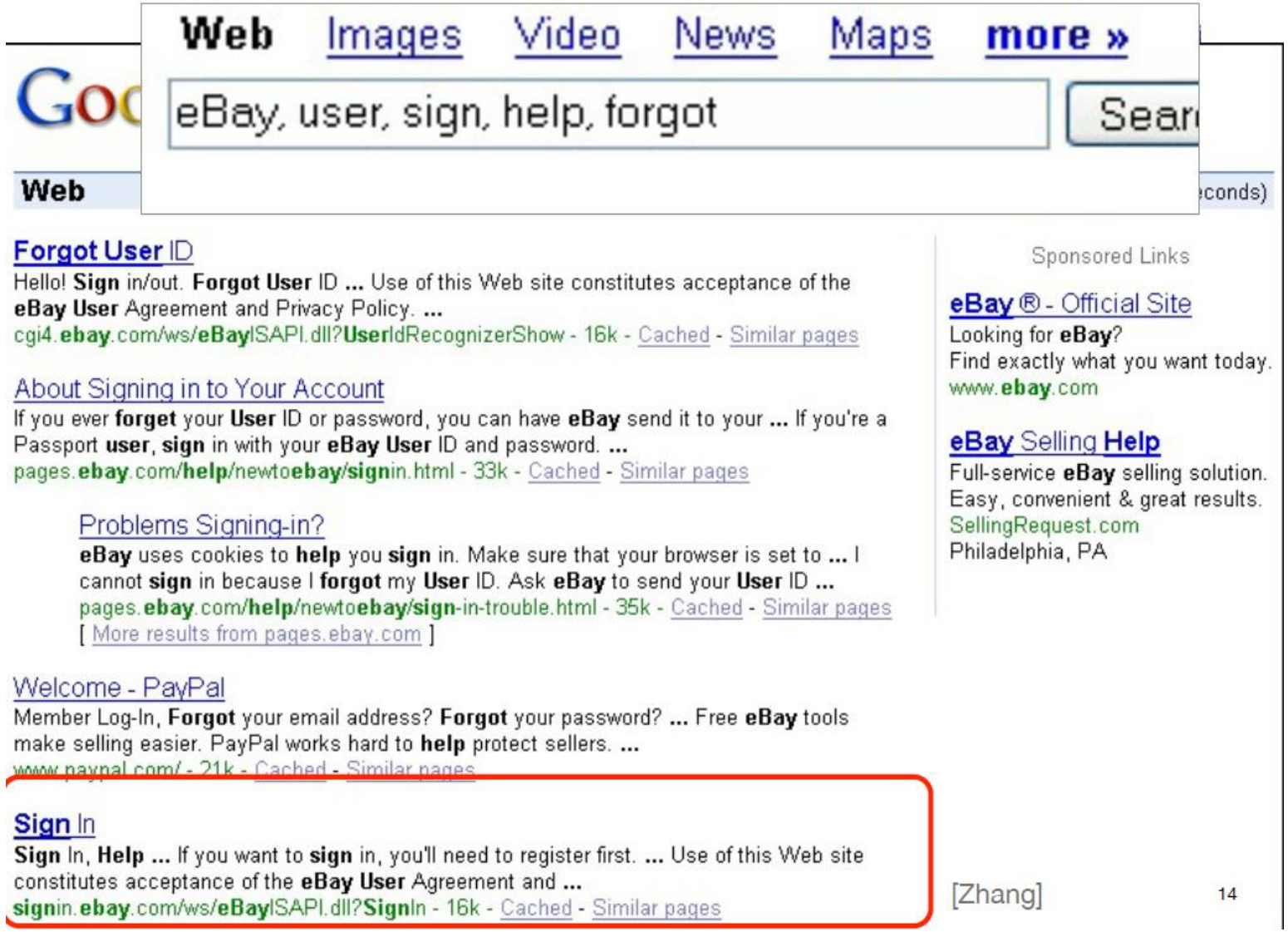
[Zhang]

How CANTINA Works (Iteration #1)



[Zhang]

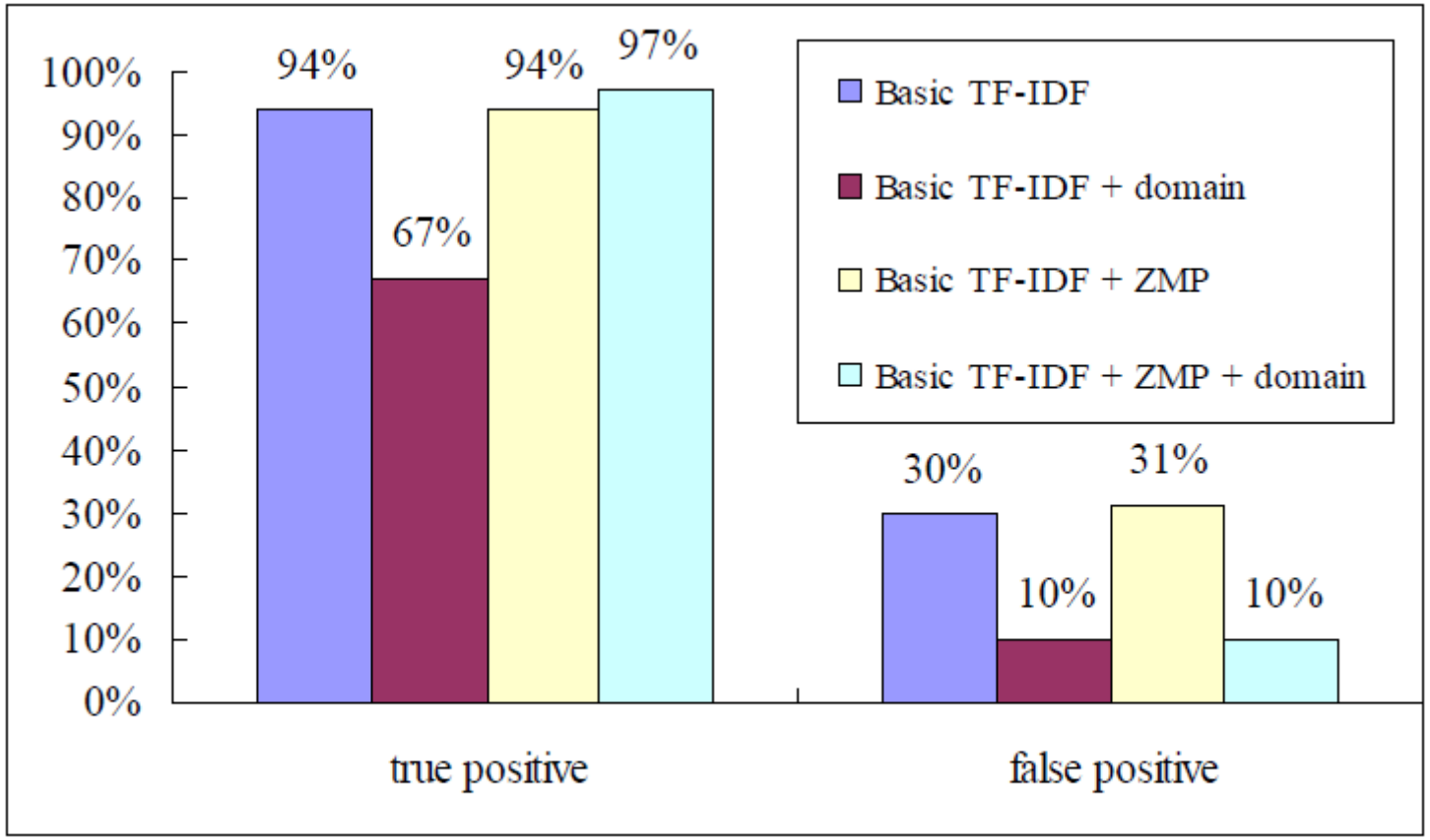
How CANTINA Works (Iteration #1)



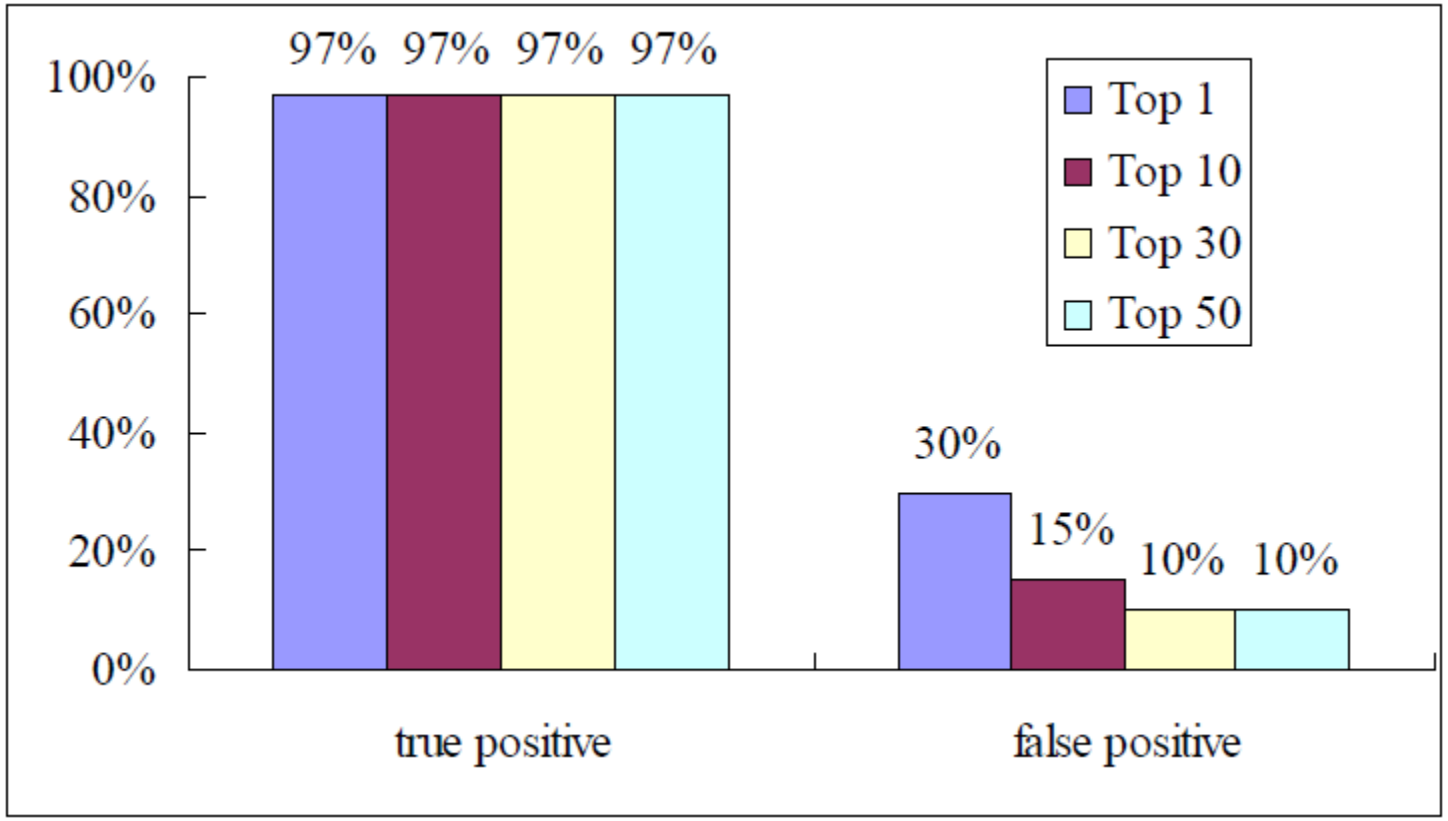
Evaluating CANTINA (Iteration #1)

- 100 phishing URLs from PhishTank.com
  - We used unverified URLs, manually verified them ourselves
- 100 legitimate URLs from another study on phishing
  - From 3Sharp, popular web sites, banks, etc
- Four conditions
  - Basic TF-IDF
  - Basic TF-IDF + domain name (ebay.com -> “ebay”)
  - Basic TF-IDF + ZMP (zero results means phishing)
  - Basic TF-IDF + domain name + ZMP

Evaluating CANTINA (Iteration #1)



Evaluating CANTINA (Iteration #1)



How CANTINA Works (Iteration #2)

- Wanted to reduce false positives
- Added several heuristics from SpoofGuard and PILFER
  - Age of domain
  - Known images (logos)
  - Page is at suspicious URL (has @ or -)
  - Page contains suspicious links
  - IP Address in URL
  - Dots in URL (>= 5 dots)
  - Page contains text entry fields
  - TF-IDF

How CANTINA Works (Iteration #2)

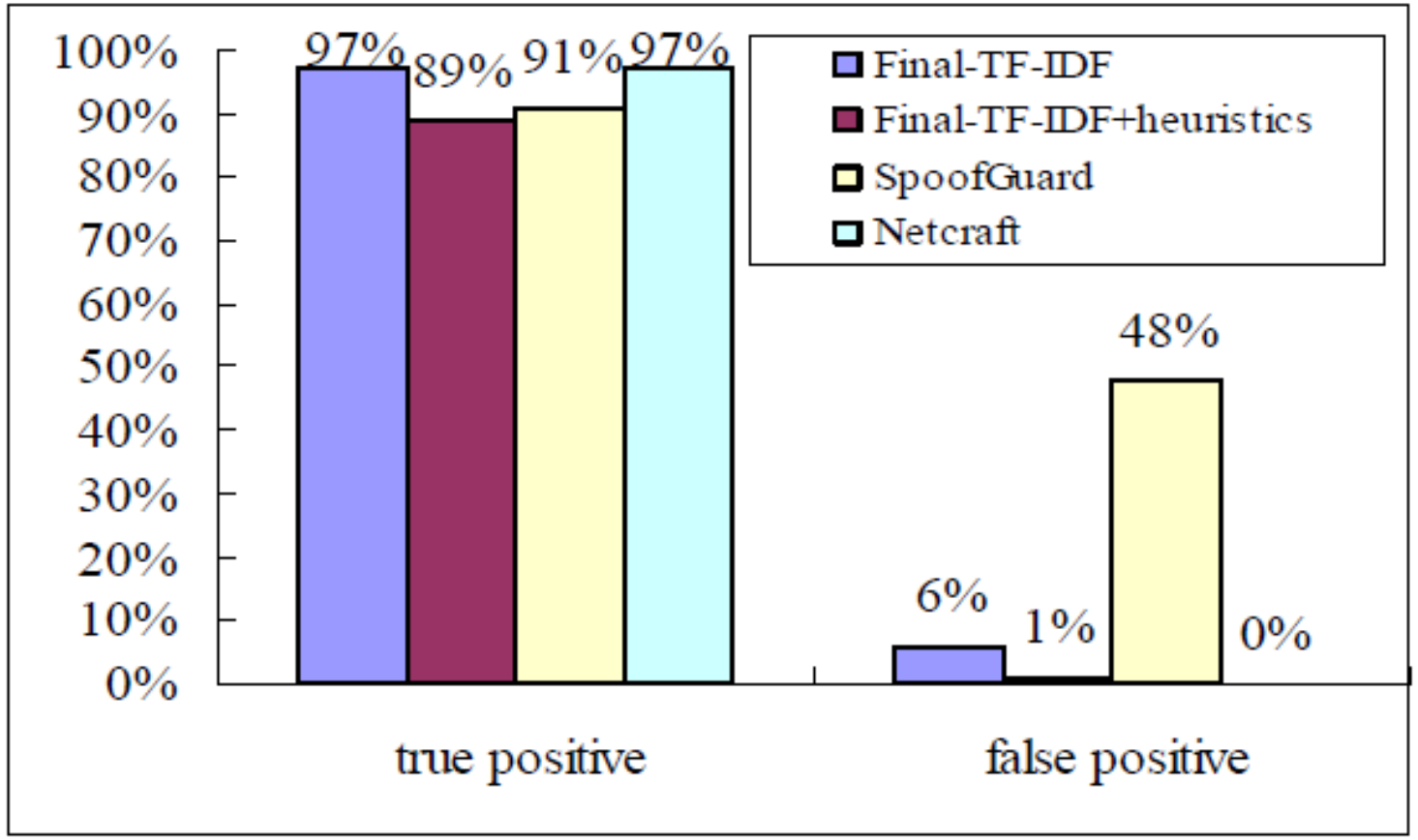
- Used simple forward linear model to weight these
  - The more effective a heuristic, the larger the weight
  - Used 100 phishing URLs, 100 legitimate to find weights

Heuristic	True Positive	False Positive	Effect	Weight
Age of Domain	87%	30%	57.0	0.18
Known Images	37%	0%	37.0	0.12
Suspicious URL	6%	3%	3.0	0.01
Suspicious Links	8%	25%	0.0	0.00
IP Address	22%	0%	22.0	0.07
Dots in URL	45%	3%	42.0	0.13
Forms	94%	27%	67.0	0.21
TF-IDF-Final	99%	10%	89.0	0.28

Evaluating CANTINA (Iteration #2)

- Compared CANTINA to SpoofGuard and NetCraft
  - SpoofGuard uses all heuristics
  - NetCraft 1.7.0 uses heuristics and extensive blacklist
- 100 phishing URLs from PhishTank.com
- 100 legitimate URLs
  - 35 sites often attacked (citibank, paypal)
  - 35 top pages from Alexa (most popular sites)
  - 30 random web pages from random.yahoo.com

Evaluating CANTINA (Iteration #2)



Discussion of CANTINA Overall

- Limitations
  - Does not work well for non-English web sites (TF-IDF)
  - System performance (querying Google each time)
    - Early results from our latest work => low latency crucial
    - CANTINA may be better for backend work than browser
- Attacks by criminals
  - Using images instead of words
    - But has to look legitimate
  - Invisible text
  - But phishing page still has to be in top search results
    - Circumventing TF-IDF and PageRank (hard in practice?)

An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants

Jason Franklin, Vern Paxon, Adrian Perrig, and Stefan Savage

Commoditization of eCrime

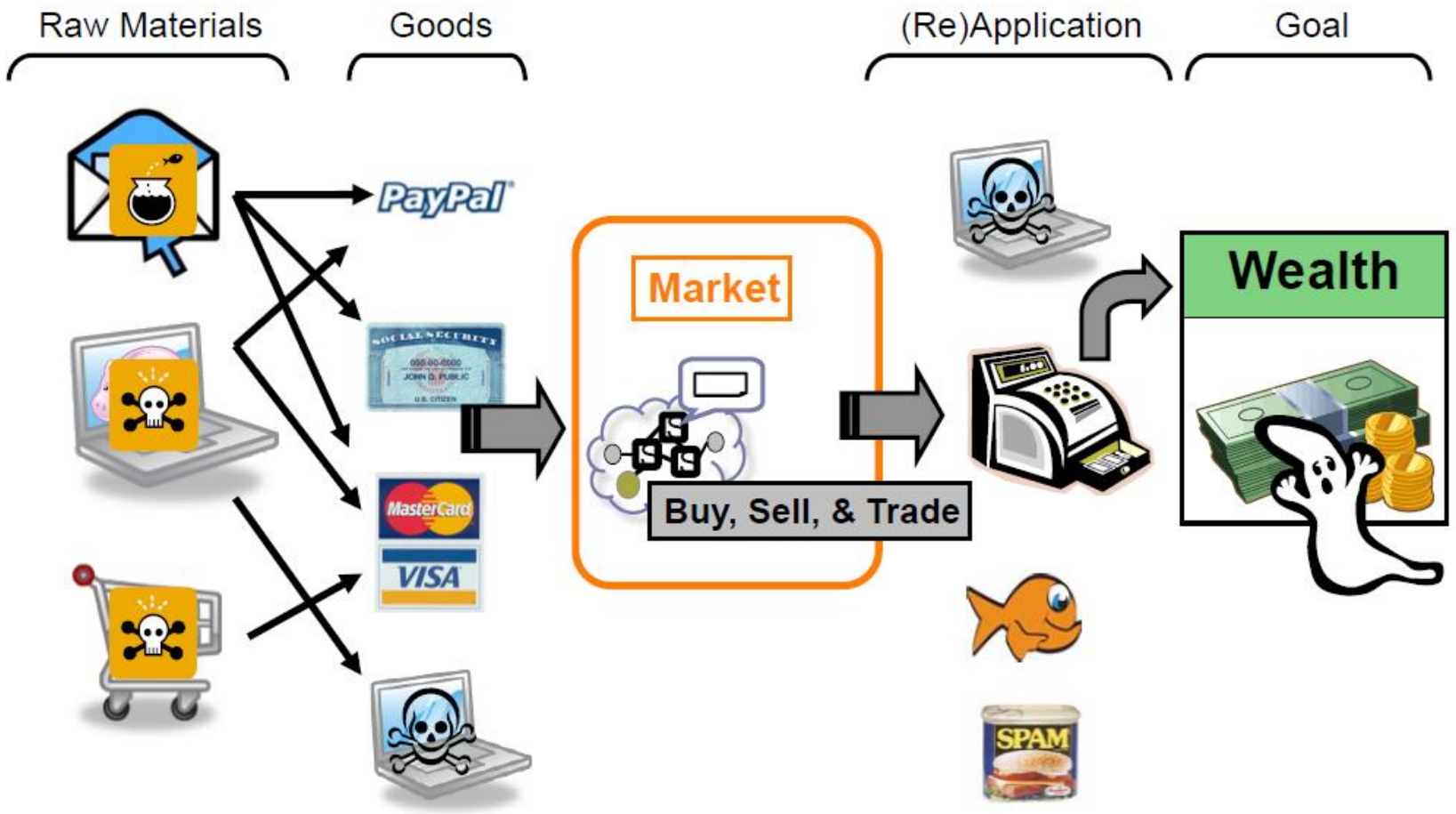
Shift from Hacking For Fun to For Profit

- Observation 1: Internet-based crime shifting from reputation economy to cash economy
  - Today, large fraction of Internet-based crime is profit driven
  - Can be modeled roughly as rational behavior
- Observation 2: eCrime has expanded and evolved to exceed capacity of closed group
  - There now exists diverse on-line market economy that trades in illicit goods and services in support of criminal activity
- Markets are public, bustling with activity, easy to access
  - Lower barrier to entry for eCrime, increase profitability, and contribute to overall level of Internet-based criminal activity

Contributions

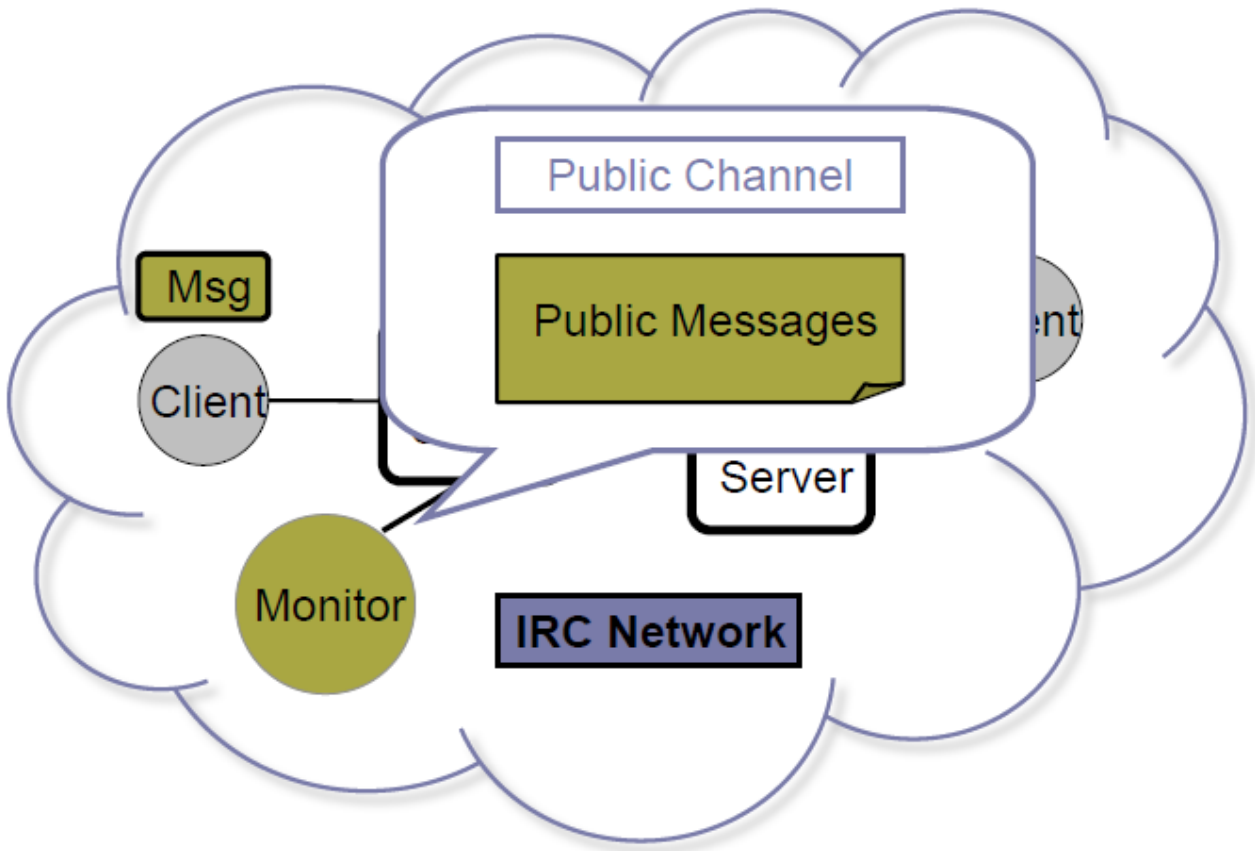
- First systematic exploration into measuring and analyzing eCrime market
- Characterize participants and explore goods and services offered
- Discuss beneficial uses of market data
- Discuss market disruption

eCrime Market Operation



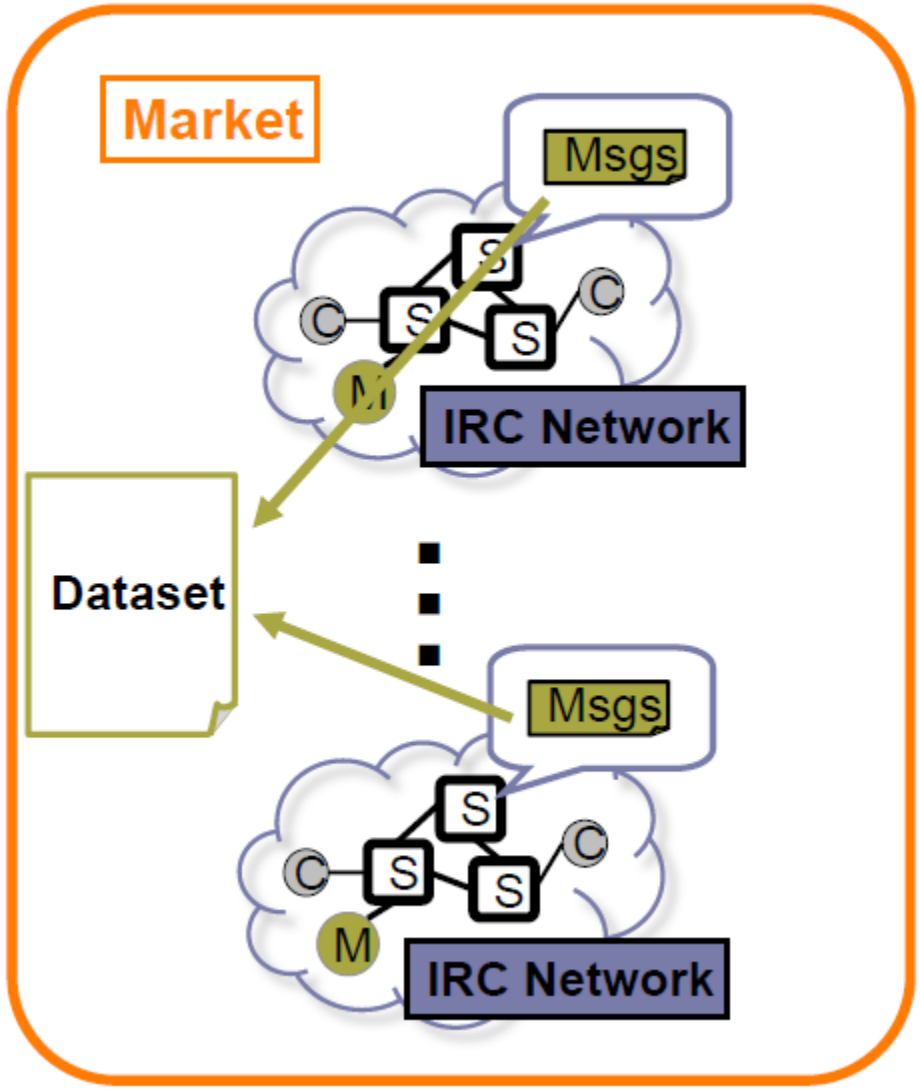
Buying a Targeted Phishing Campaign

Market Data Collection



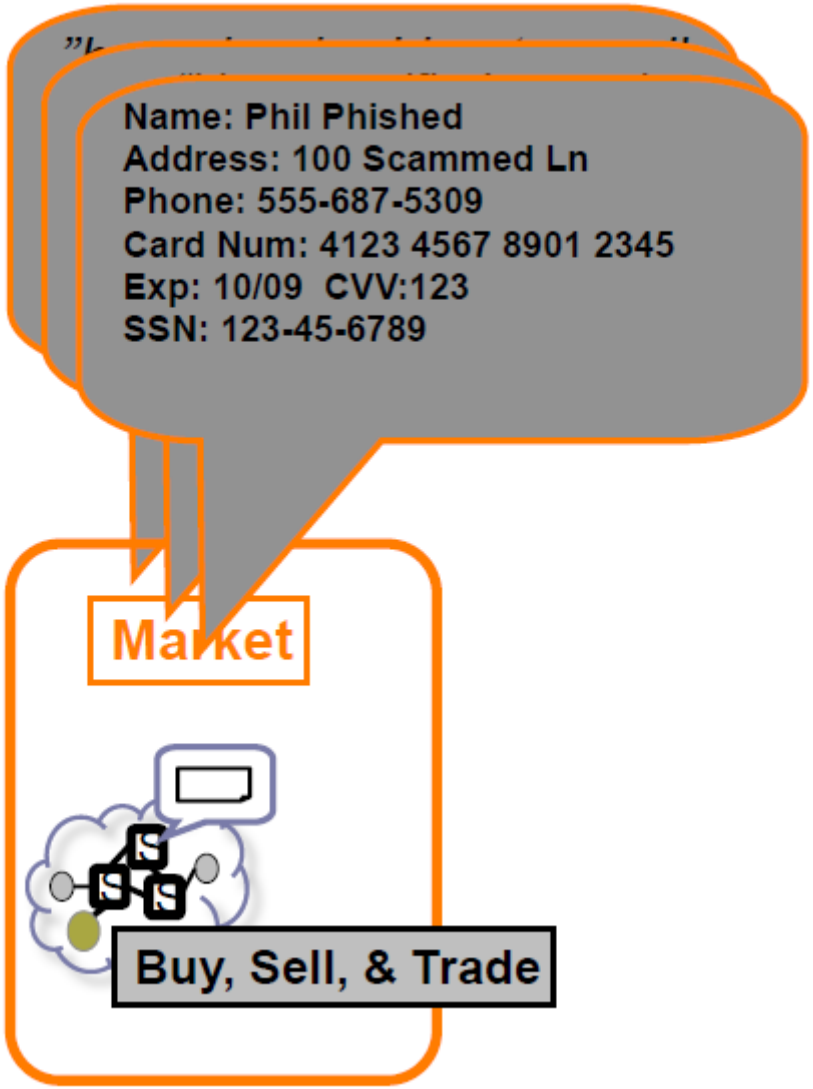
Market Organization and Data Collection

- Market is public channel active on independent IRC networks
- Common channel activity and admin. creates unified market
- IRC log dataset (2.4GB)
  - 13 million public messages
  - From Jan. ’06 to Aug. ‘06



Market Activity

- 1. Posting advertisements
  - Sales and want ads for goods and services
- 2. Posting sensitive personal information
  - Full personal information freely pasted to channel
  - Establishes credibility
- Need automatic techniques to identify ads and sensitive data



Measurement Methodology

- Three classes of measurement:
  - 1. Manual -> (Labeled dataset)
    - Manual classification of >3,500 messages with 60+ labels
      - Messages selected uniformly at random from corpus

Advertisement	Classification Label(s)
"have hacked hosts, mail lists, php mailer send to all inbox"	Hacked Host Sale Mailing List Sale Mailer Sale Ad
"i need 1 mastercard I give 1 linux hacked root"	Credit Card Want Hacked Host Sale

Measurement Methodology

- Three classes of measurement:
  - 2. Syntactic
    - Using regular expressions to pattern match structured sensitive data such as credit card numbers and SSNs

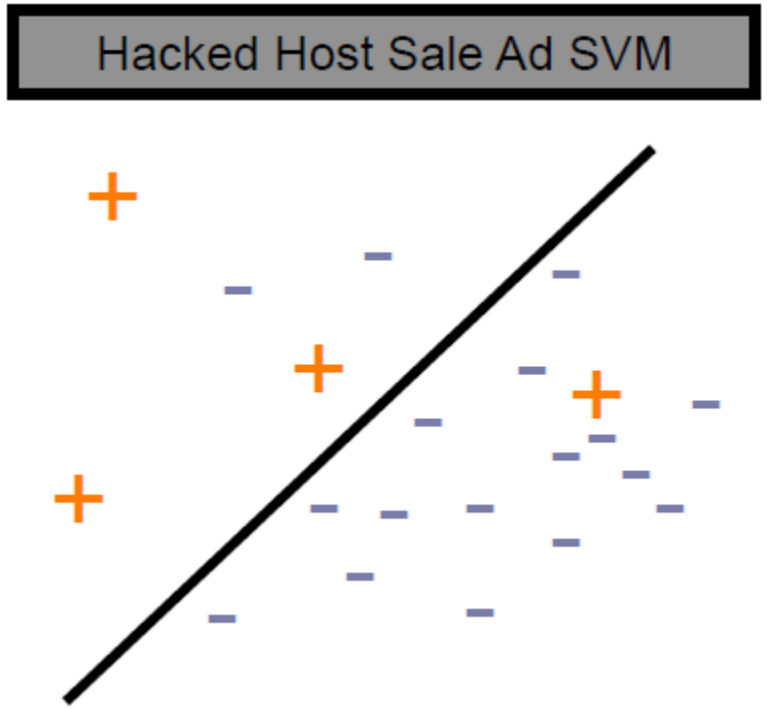
$cc = / \s\d{16}\s /;

```
HaX0R: Free VISA! Name: Adrian Per... Num: 4123456789101234
HaX0R: SSN: 123-456-7859
```

Measurement Methodology

- Three classes of measurement:
  - 3. Semantic
    - Train binary SVM classifiers for each label using labeled dataset
    - Automatically classify messages

"have hacked hosts, mail lists, php mailer send to all inbox"

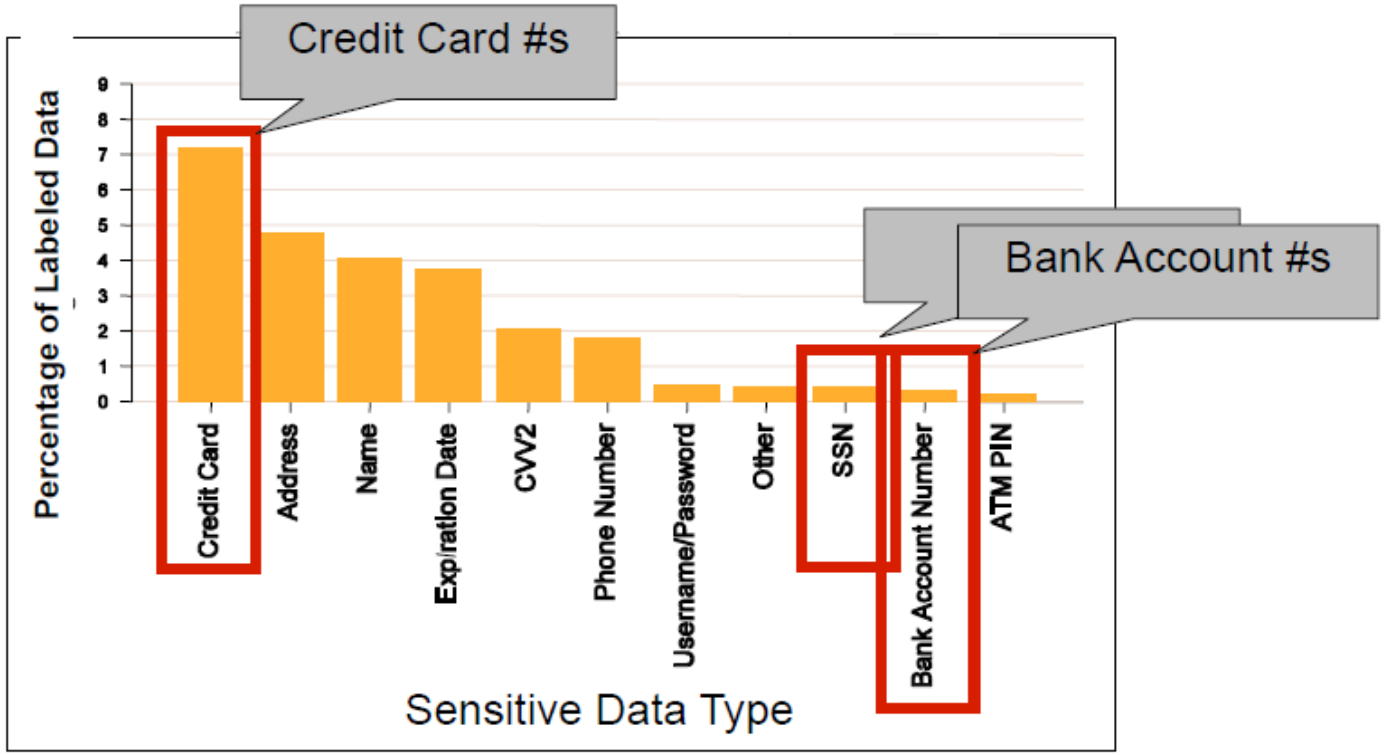


Measurement Complexities and Limitations

- No private messages
  - Limited transaction details and prices
- Assertions are not intentions
  - “Rippers” may advertise items they do not have
- Public market may bias behavior of miscreants
- Key Challenge: Validate data
  - Check Luhn digit, formats, valid ranges of SSNs
  - Cross-validate with other lists of compromised data
  - Need to collaborate with CC companies or law enforcement

Sensitive Data and Market Significance

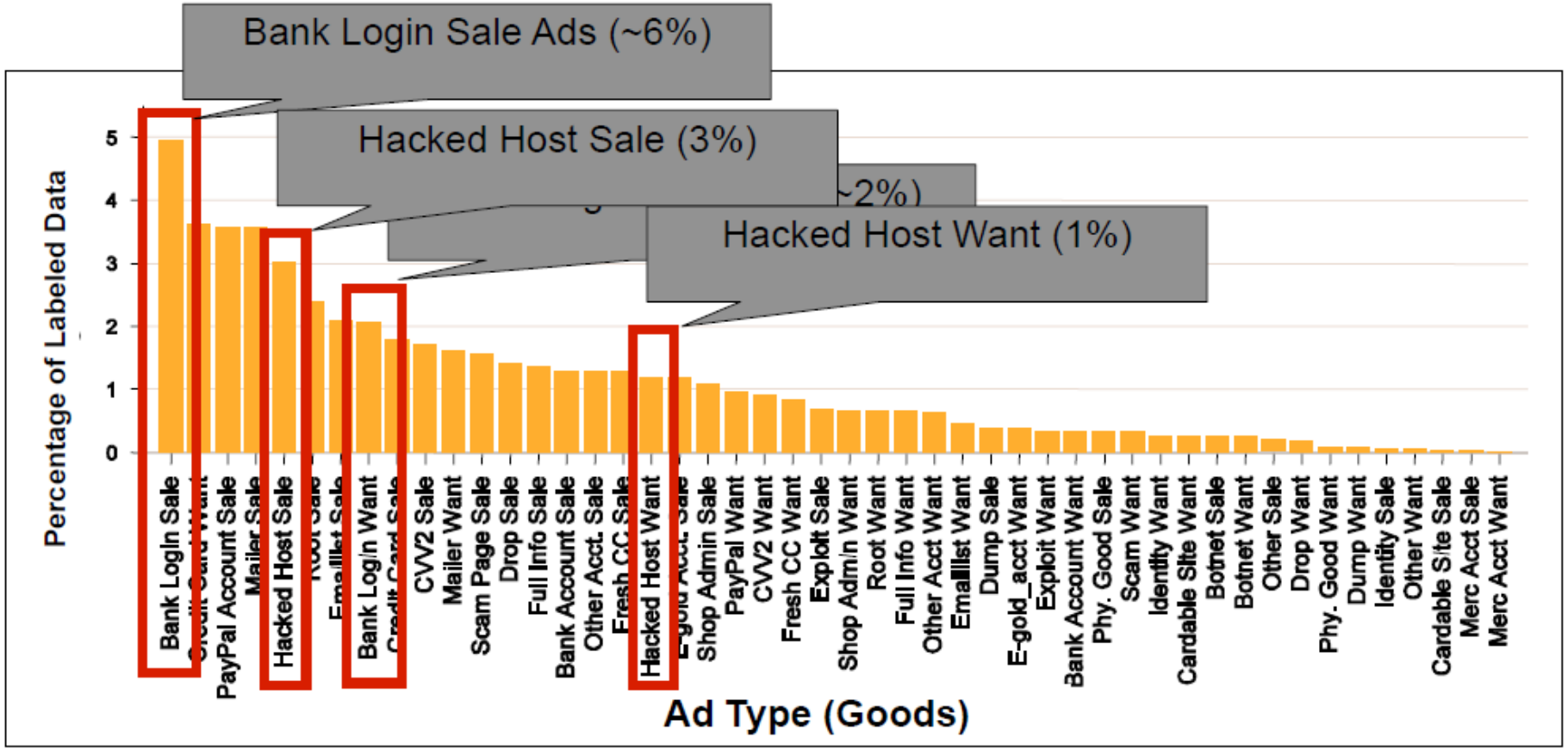
- Measurement Results:
  - Credit cards compose 7% of labeled data
    - Estimate: 13 million line corpus * 7% = 910k (100k unique)
  - SSNs and bank accounts fall in 0.5 – 0.2% range



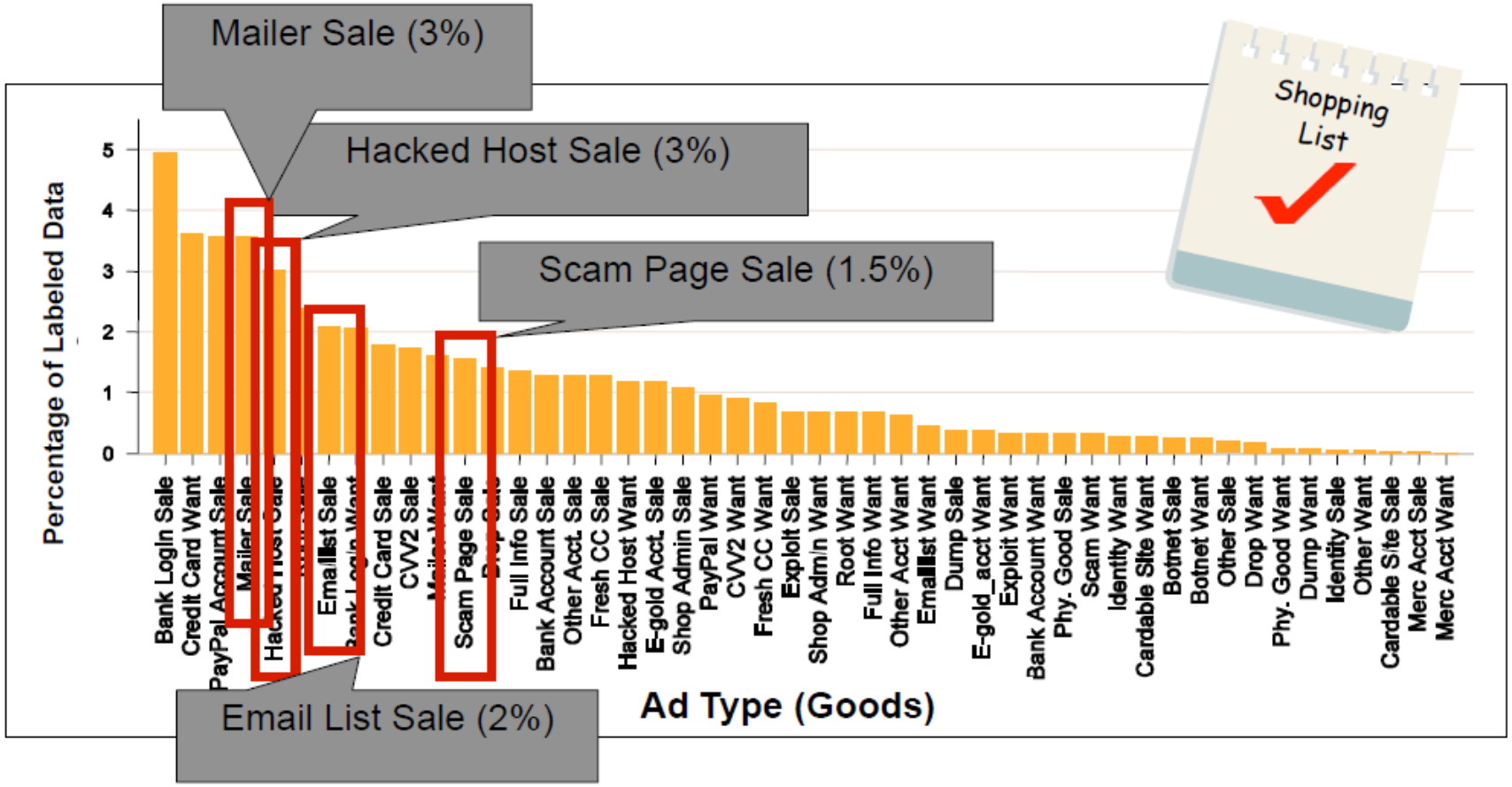
Estimating Wealth of Miscreants

- Goal: Estimate wealth stolen by market
- Measurement Methodology:
  - Transactions hidden by private channels
  - Median loss amount for credit/debit fraud = $427.501
  - Syntactic matches + Luhn check resulted in 87,143 potential cards
  - Include financial account data
- Measurement Results:
  - Credit card wealth = $37 million
  - Total: $93 million

Distribution of Goods in Labeled Data

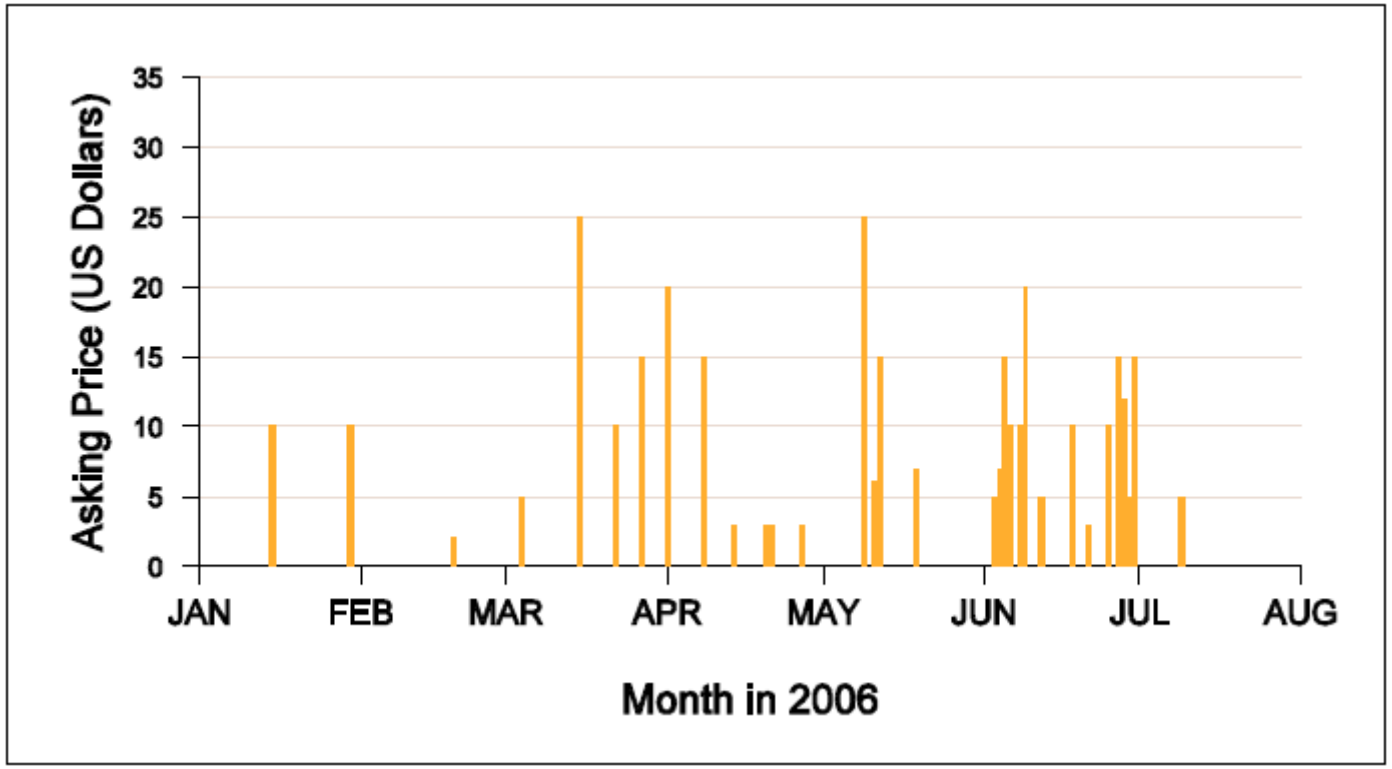


Distribution of Goods in Labeled Data



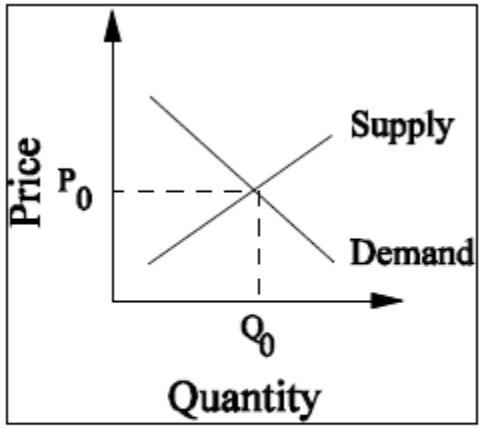
Asking Prices for Compromised Hosts

- Establishes cost to buy resources
  - May be useful to state strength of adversary in monetary terms
  - Cost to buy perhaps useful security metric?

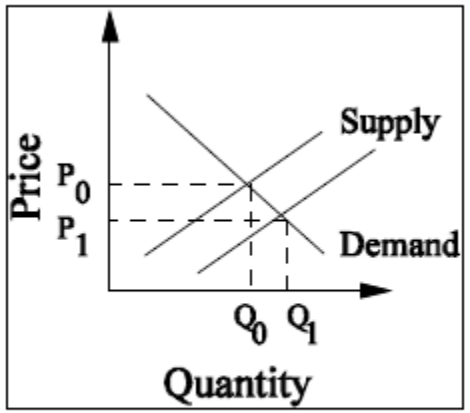


World 0: A Wealth of Information

- Market may enable measurement of global trends and statistics
  - Idea: Price of a good in efficient market provides intersection of supply and demand curves
    - Assume a short-term constant demand
    - Then changes in price are result of shifts in supply curve
      - Increases or decreases in the quantity supplied



Supply and demand curves.



Shift of supply curve.

World 1: Markets Pose Security Threat

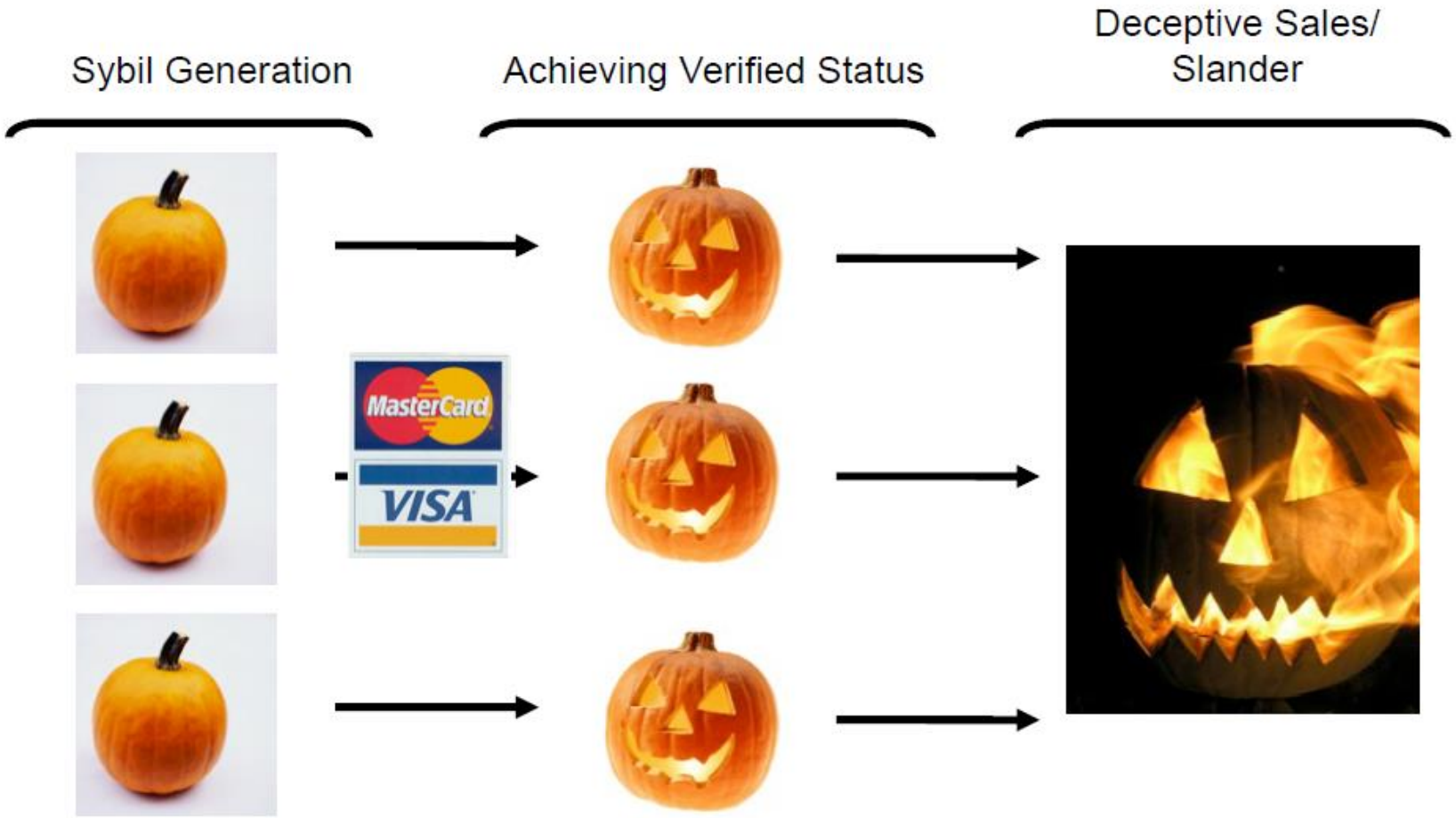
- Markets target of law enforcement activity:
  - U.S. Secret Service's Operation Firewall
    - July 2003 – late 2004, targeted administration
    - Required sting operation, inter-state, and multi-national cooperation
      - UK, Canada, Bulgaria, Belarus, Poland, Sweden, Netherlands, Ukraine
  - Resulted in arrest of 28, in 8 states, 6 countries
- Market reemerged after arrests
  - Decentralized, global nature of market makes traditional law enforcement activity time consuming and expensive
- Motivates need for more efficient low-cost countermeasures

Efficient Countermeasures

- Goal: Raise barrier to entry for eCrime
  - Reduce number of successful transactions
  - Push market towards closed market
- Approach: Establish environment which exhibits asymmetric information similar to Lemon Market
  - Buyers can't distinguish quality of sellers
- Insight: Criminals will likely prefer anonymity over stronger verification system which relies on identity
  - Or we ease law enforcement's job

Efficient Countermeasures

- Sybil and Slander Attack



Conclusion

- Shift from hacking “for fun” to “for profit” opens possible of modeling Internet-based crime as rational behavior (for profit)
- First study to systematically measure and analyze eCrime market
- Explored some beneficial uses of market-derived data & countermeasures
- Limitations of this study:
  - Soundness of measurement
    - Need for better verification and cross-validation
  - Completeness of measurement
    - What percentage of eCrime market activity are we seeing?
  - Applicability of measurements/conclusions
    - Can we apply our techniques to other eCrime markets?

Acknowledgments/References

- [Zhang] CANTINA: A Content-Based Approach to Detecting Phishing Web Sites was presented at, Yue Zhang, Jason I. Hong (presentation obtained from his website), and Lorrie F. Cranor, presented at www 2007.
- [Franklin] An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants, Jason Franklin (presentation obtained from his website), Vern Paxon, Adrian Perrig, and Stefan Savage, presented at ACM CCS'07, Alexandria, VA, Nov. 2007.