Usability and Psychology and Economics

Privacy and Security Concerns

- Google buzz abusive ex
- Choicepoint mafia data selling
- Yahoo Chinese activist
- Health status insurance and employment discrimination
- Children online
- Browser/pdf/flash/OS vulnerabilities - most systems can be casually compromised
- Strong underground economy in malware/ SPAM/DDOS/phishing
- (Nearly?) All Internet systems vulnerable to targeted attack

Drexel UNIVERSITY

Web Infections aka Drive-By Downloads

Internet users can be infected simply by *viewing* a compromised website.


```
<body leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">
<script language='JavaScript' type='text/javascript' src='fsvfk.js'></script>
<table width="99" border="1" align="center" cellpadding="0" cellspacing="0" bordercolor="#001D3C">
```

Drexel UNIVERSITY

Usability and Psychology

- 'Why Johnny Can't Encrypt' – study of encryption program PGP – showed that 90% of users couldn't get it right in 90 minutes
- Private / public, encryption / signing keys, plus trust labels was too much – people would delete private keys, or publish them, or whatever
- Security is hard – unmotivated users, abstract security policies, lack of feedback …
- Much better to have safe defaults (e.g. encrypt and sign everything)

Hypotheses

- Data security and privacy are really hard, we are failing despite high investment
- No one cares about security and privacy, so the invisible hand reflects that
- Something is wrong with the market for data privacy and security

Drexel
UNIVERSITY

Hypotheses

- Data security and privacy are really hard, we are failing despite high investment
  - Many things we're not doing (cryptography, extensive code review, self insurance, etc)
  - Software security knowledge is located *precisely nowhere* a developer spends their time.
- No one cares about security and privacy, so the invisible hand reflects that
- Something is wrong with the market for data privacy and security

Drexel UNIVERSITY

Hypotheses

- ~~Data security and privacy are really hard, we are failing despite high investment~~
- No one cares about security and privacy, so the invisible hand reflects that
  - People *say* they care
  - Argument that "rational actors ought to care"
- Something is wrong with the market for data privacy and security

Drexel UNIVERSITY

Hypotheses

- ~~Data security and privacy are really hard, we are failing despite high investment~~
- ~~No one cares about security and privacy, so the invisible hand reflects that~~
- Something is wrong with the market for data privacy and security

Drexel UNIVERSITY

Market Failures

- Markets work when people have incentives to do the "right" thing
- How can they fail?
  - Externalities
  - Asymmetric/Imperfect Information
  - Bounded rationality
  - *All present in information security and privacy!*

Drexel UNIVERSITY

Externalities

- Occur when decisions cause external costs or benefits to stakeholders who did not directly affect the transaction

Drexel UNIVERSITY

Externalities in Web Infections

- Web infections typically affect the end users (browsers)
  - Often don't know that they are infected
    - If they do, they don't know why
  - No incentive for sites to do the right thing
    - Some evidence to suggest overt security measures actually reduce customer confidence
    - Revealing infections can only harm companies brands and reputations
- Most harm is even further removed
  - Attacks carried out/ phishing sites hosted/ SPAM sent from infected machines

Drexel UNIVERSITY

Adverse Selection: Akerlof's Market for Lemons

- Comes from analysis of Used Car market
- *Hidden characteristics*: Buyer doesn't know if the car they are buying is good or a 'lemon'
- Given uncertainty – buyer will not pay much
- Result: *Adverse Selection*, sellers won't sell good cars (can't get a good price) only lemons
- Solution: Reduce customer uncertainty (Independent Inspections, Guarantees, etc)

Drexel UNIVERSITY

Asymmetric Information in Web Insecurity

- End user doesn't know if site they visit is safe or attacking them
- Hosting provider doesn't know if webmaster is incompetent or malicious
- Webmasters don't know if hosting provider is secure
- Adverse selection: Takes resources to be secure, so why bother if no one can notice?

Drexel UNIVERSITY

Bounded Rationality

- Market assumes not only perfect information, but also perfect rationality
- Reality - Behavioral distortions
  - Humans bad at assessing risk
    - Tend to pick the first reasonable sounding

Drexel UNIVERSITY

Consumer Webmasters

- Most webmasters are not tech geeks
  - Just want things to work
  - Use off the shelf software
  - Do not believe they are infected
  - Do not know how to evaluate security properties of hosting providers (or that they should)
  - Can not identify or remove malware

Drexel UNIVERSITY

Security Decisions

unzip this file?

Share dropbox folder?

Make a firewall exception?

Share this post?

Allow user bob access?

Choose a password

buy from amazon.com

Download this attachment.

Open this email?

Install this software?

Plug Carol's usb key into my laptop?

update this app?

allow access to your contacts?

Hard for Machines and Humans

- Context-dependent
- Require specialized knowledge
- Dynamic: sophisticated adversaries and emerging threats
- Complex risk analysis requiring
  - Large knowledge base and rationality

Usability and Psychology (2)

- 1980s concerns with passwords: technical (crack /etc/passwd, LAN sniffer, retry counter)
- 1990s concerns: weak defaults, attacks at point of entry (vertical ATM keypads), can the user choose a good password and not write it down?
- Our 1998 password trial: control group, versus random passwords, versus passphrase
- The compliance problem; and can someone who chooses a bad password harm only himself?

Network Security Attacks

Network attacks are three types:

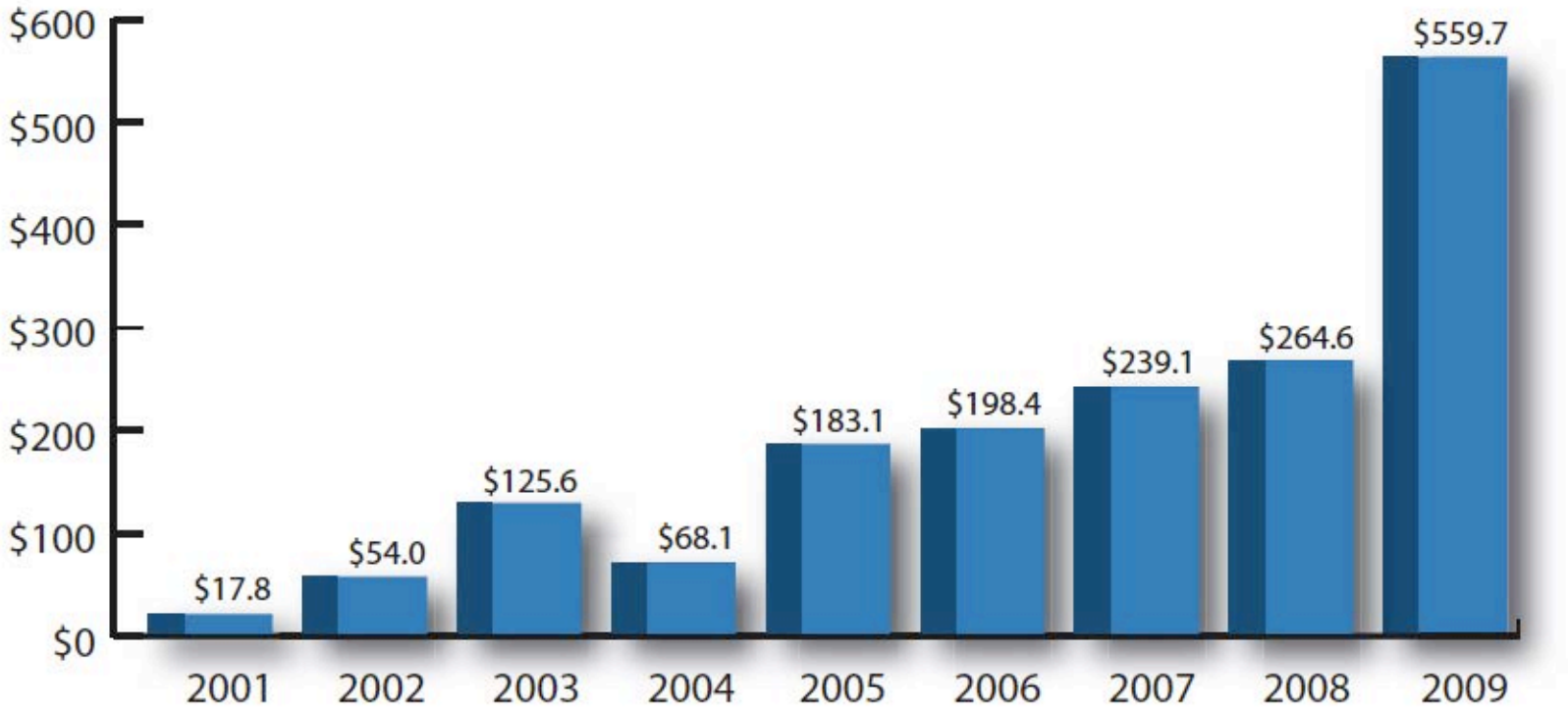
- Physical attacks
  - target the the computers, wires, and electronics
- Syntactic attacks
  - target the operating logic of computers and networks, software vulnerabilities
- Semantic attacks
  - target humans

Social Engineering

- Social Engineering is the process of exploiting people through social interactions to obtain sensitive information.

- Example of this attacks:
  - Spam/phishing with/without malicious attachment
  - Internet Fraud
  - Business scheme

Yearly Dollar Loss (in millions) in Internet Fraud



Why social engineering works

- Psychology
- Usability
- Economics of Information Security

Psychology

- Trust in authority
- Scarcity
- Personalization
- Persuasion
- Capture errors
- Social proof

Usability

- Dhamija et. al. conduct a usability study

  to test the hypotheses

  – Lack of understanding about Internet

  – Visual deception:

    - www.paypal.com@fake.com

  – Bounded attention

- 22 participants are shown 20 web sites and ask to distinguish the fraud sites from the real ones

  – 7 real, 9 phishing, 3 constructed phishing, 1 forged ssl

Result Summary

- 90% people trust sites based on the look.
- 9% (2) participants relied checked URLs, also checked the certificate that was presented.
- Two participants in the study that they would only question a website's legitimacy if more than the username and password was requested.

- Schechter et. al. perform a usability study of website authentication measures:
- Will customers of an online bank enter their passwords even if
  - their browsers' HTTPS indicators are missing?
  - their site-authentication images are missing?
  - they are presented with an IE7 warning page?

Results

- All participants entered passwords without https
- 97% entered passwords without site authentication images
- 57% entered passwords in spite the warning page

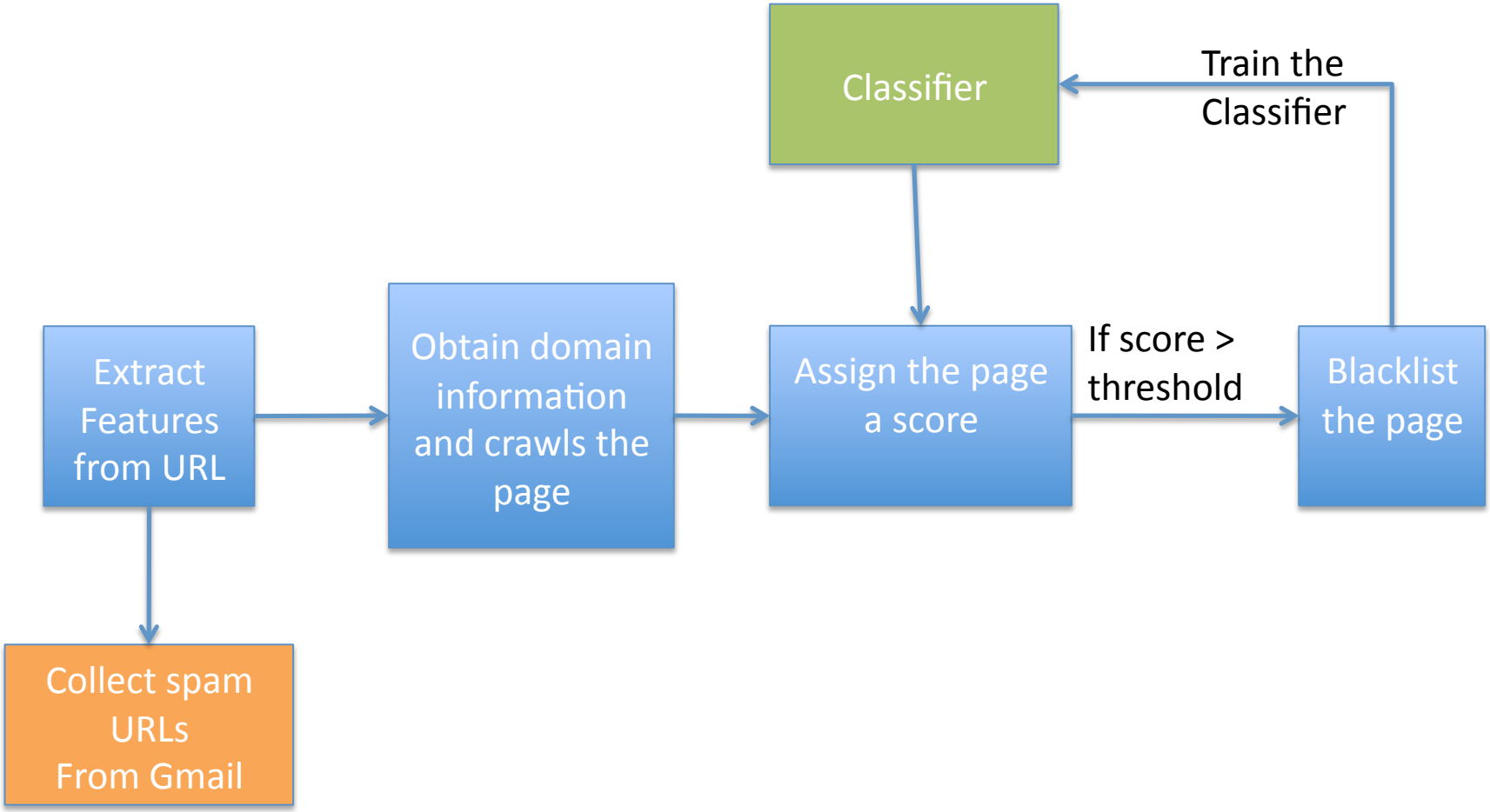
Economics of Information Security

- Security investment:
  - what is the optimal amount of investment for information security for a given company?
- Security as externality:
- Incentive misalignment
  - Anderson and Moore indicates that incentive misalignment significantly undermines information

Countermeasures

- Technical : only for phishing, malware, spam
- Legal
- Education and awareness

Google Safe Browsing API



- Phisher can bypass the system:
  - By disguising as a non-phishing page
  - By manipulating the training classifier
  - By slowing down page fetching
  - By hiding the phishing page from Google

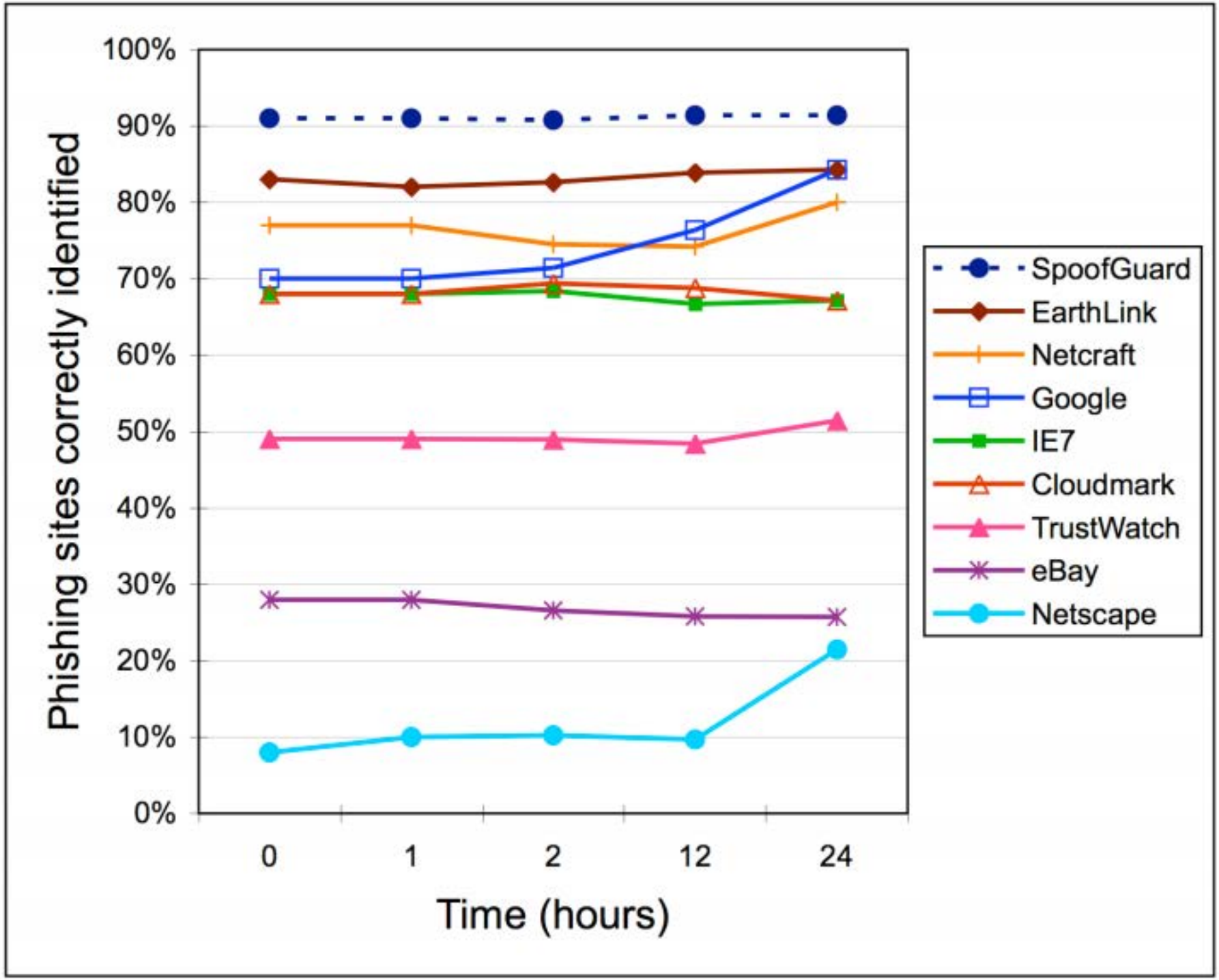
Evaluation of tools

- 10 Anti-phishing tools examined are CallingID Toolbar, Cloudmark Anti-Fraud Toolbar, EarthLink Toolbar, eBay Toolbar, Firefox 2/ Google, GeoTrust TrustWatch Toolbar, Microsoft Phishing Filter in Windows Internet, Explorer 7, Netcraft Anti-Phishing Toolbar, Netscape Browser 8.1, SpoofGuard.

- Toolbars method:
  - Blacklisting
  - Check content/URL of the page
  - Machine learning

- Evaluation of accuracy:
  - 100 phishing sites
  - 516 legitimate URLs

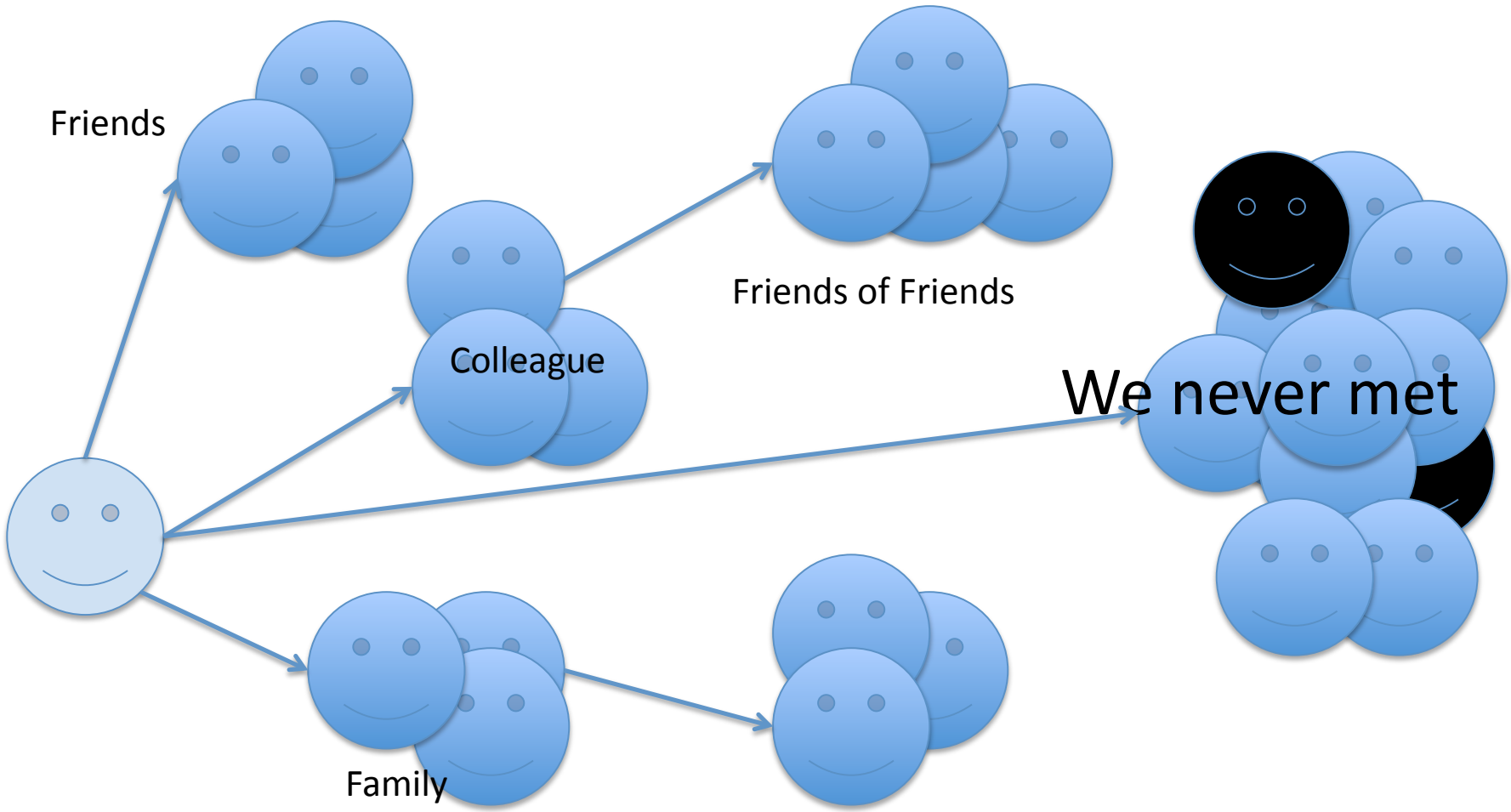
- Evaluation of vulnerability:
  - Changing the URL
  - Increasing the page load time


Phishing sites correctly identified
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
0
1
2
12
24
Time (hours)
SpoofGuard
EarthLink
Netcraft
Google
IE7
Cloudmark
TrustWatch
eBay
Netscape

Results

- Phishing detection depends on the freshness of the URLs
- Most tools detect phishing sites accurately after 12 or 24 hours, but more than 70% attacks happen within first 12 hours.
- Anti-phishing tools detections can easily circumvented.

Impact of social network



Our whole life is on the internet!

twitter

flickr™

foursquare

facebook

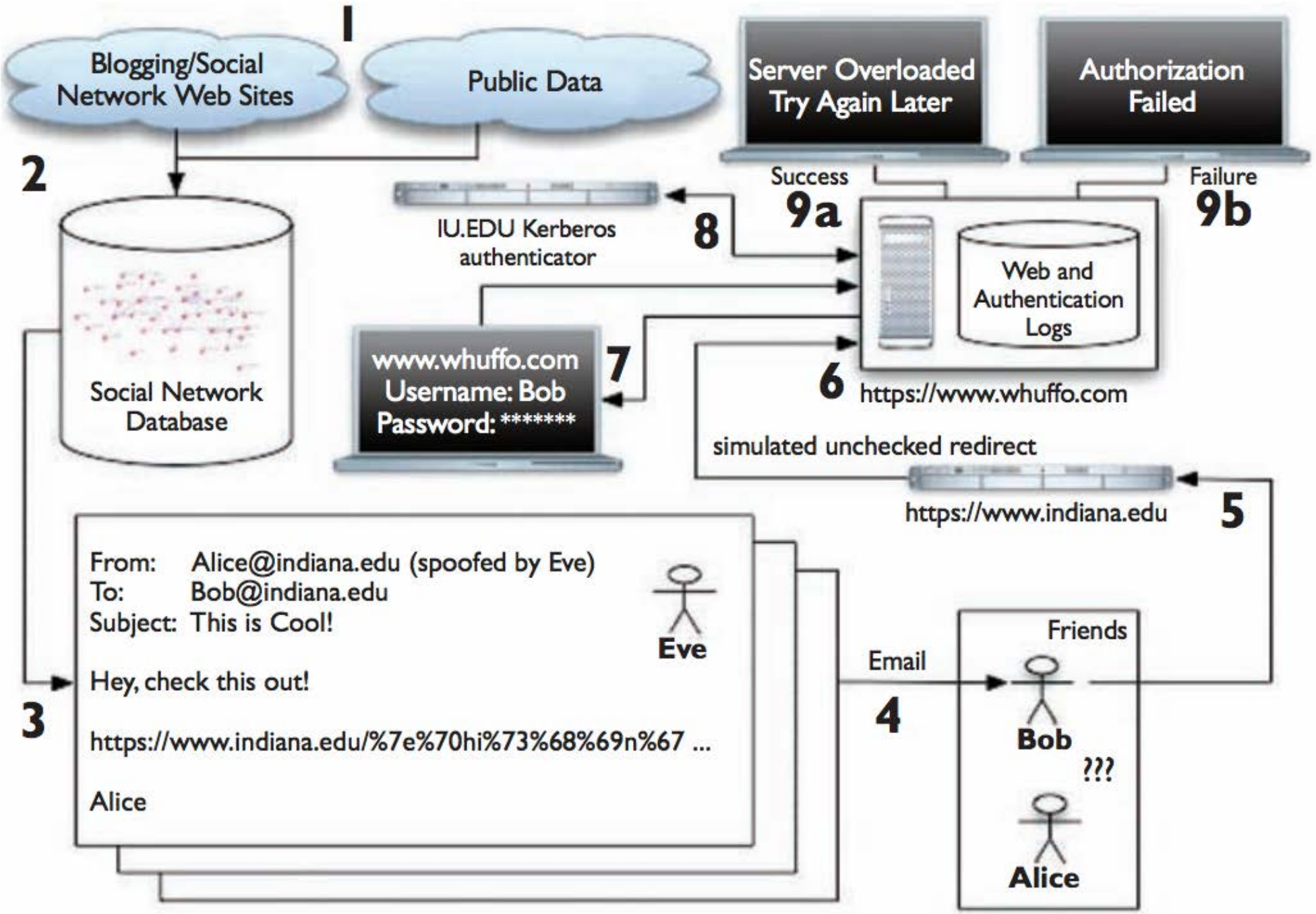
blippy

Social Phishing

Jagatic et. al demonstrate the effectiveness of social phishing
Research questions:
1. How much information you can collect?
2. How valuable are they?

Research method:
A total of 1,731 Indiana University students of age 18 to 24 years are selected based on the amount of publicly available information

After harvesting the data, the researchers conduct phishing attack on two groups of subjects: social network group and control group.


1
Blogging/Social Network Web Sites
Public Data
Server Overloaded Try Again Later
Authorization Failed
2
Success
9a
Failure
9b
IU.EDU Kerberos authenticator
8
Web and Authentication Logs
Social Network Database
www.whuffo.com
Username: Bob
Password: *******
7
6
https://www.whuffo.com
simulated unchecked redirect
https://www.indiana.edu
5
From: Alice@indiana.edu (spoofed by Eve)
To: Bob@indiana.edu
Subject: This is Cool!
Hey, check this out!
https://www.indiana.edu/%7e%70hi%73%68%69n%67 ...
Alice
Eve
3
Email
4
Friends
Bob
???
Alice

Results

- Effectiveness of Social Phishing: 72%
- Effectiveness of Regular Phishing: 16%
- 15% more effective if the sender is of opposite sex
- Female students are more susceptible to phishing.
- Social phishing lower people's guard against attacks.
- Students with technology major are less vulnerable than others.

Privacy Risks at Social Network

- Thomas et. al explore how much information can be inferred about a user on social network from people in his network.
- A privacy conflict occurs when two users disagree on who can access the content.
- Two scenarios are tested -friendship and wall posts.
- Friendship:
  - Alice hides her friendlist
  - Bob reveals his friendlist
  - If Alice and Bob are friends, it is known from Bob.
- Wall posts:
  - Alice's wall is private
  - Bob's wall is public
  - Alice posts anything on Bob's wall, everybody can see that.
  - Skipping work with @Alice and hitting the bars at 9am.

- Three classifier are implemented:
  - Baseline Classifier:
    - Predict user's attributes based on his own profile
  - Friend Classifier:
    - Predict user's attributes based on his friends' profiles
  - Wall Classifier:
    - Predict user's attributes based on his wall posts on his friends' profiles

Results

Profile Attribute	# of Labels	Baseline	Friend	Wall Content
Gender	2	61.91%	67.08%	**76.29%**
Political Views	6	51.53%	**58.07%**	49.38%
Religious Views	7	75.45%	**83.52%**	53.80%
Relation Status	7	39.45%	**45.68%**	44.24%
Favorite Music	604	30.29%	**43.33%**	-
Favorite Movies	490	44.30%	**51.34%**	-
Favorite TV Shows	205	59.19%	**66.08%**	-
Favorite Books	173	42.23%	**44.23%**	-

Social Engineering on Social Network

- Grier et. al. explored spam and phishing on Twitter
- Twitter features:
  - Twitter restricts Tweets to 140 characters
  - URLs are posted using URL shortening services
  - Mentions: @justinbieber PLEASE FOLLOOWW MEEE!!! <3333
  - Retweets: RT @JBieberCrewz: RT this if u <3 justin bieber
  - Hashtags: Get free followers #FF #Follow Justin Bieber
- Twitter uses Google's Safebrowsing API to detect spam

- Spam features specific to Twitter:
  - Call outs: 3.5-10% of spam
    - Win an iTouch AND a $150 Apple gift card @victim!http://spam.com
  - Retweets: 1.8-11.4% are retweets of blacklisted URLs
    - RT @scammer: check out the Ipads there having a giveaway http://spam.com
  - Tweet hijacking:
    - 23% of phishing and malware retweets
  - Trend setting:
    - Buy more followers! http://spam.com #fwlr
  - Trend hijacking:
    - Help donate to #haiti relief: http://spam.com

Results

- 90% users visit spam sites before it is blacklisted
- 97.7% of URLs receive no clicks, but those that do accumulate over 1.6 million visitors
- Mostly used twitter feature is current trends
- Successful spam accounts are compromised accounts and number of followers in that account

Mule recruitment

- Proportion of spam devoted to recruitment shows that this is a significant bottleneck
- Aegis, Lux Capital, Sydney Car Centre, etc
  - mixture of real firms and invented ones
  - some "fast-flux" hosting involved
- Only the vigilantes are taking these down
  - impersonated are clueless and/or unmotivated
- Long-lived sites usually indexed by Google

1. Regional Sales Manager

Status: Part-time

Job description:

- Work as a member of a group, helping to enlarge a base of customers in countries all over the world and liaise with head office on a daily basis;
- Deliver high standards of customer service ensuring high delivery speed and quality of orders;
- Manage a part of a sales cycle – ensure fast remittance of payments through your bank account and then - through world wide Western Union system and calculate fees at each step;
- Create and maintain positive relationships with existing clients that result in new customers, lead to and maximise opportunities for expansions and renewals to enhance revenue stream.

Employees should be able to perform:

- Excellent spoken English & communication skills (oral and written).
- Professional approach on the phone conversations
- PC literate: Microsoft Outlook and Word as a minimum
- Proven ability to communicate effectively at all levels in a relaxed confident manner.
- Extroverted and outgoing, with a positive outlook.
- Significant attention to detail.
- Excellent organisational skills.
- Customer focused.
- Focused on own personal goals, integrating the achievement of company objectives.
- Ability to work unsupervised No previous sale or accounting experience is necessary, though it will be valued.

Your Personal situation must allow you to travel around your place 1-2 hours a day on company assignments(that would be particularly trips to the bank and Western Union branches)

Apply for this Position

WE OFFER:

- A base salary with generous commissions (10% out of each payment you've dealt with) and expenses .
- Flexible timetable – allows you to chose the most suitable time to deal with company assignments
- Benefits, including Contributory Pension, Life Assurance, Private Medical Insurance, Birthday holiday Day and Childcare vouchers

2. Warehouse supervisor

Status: full-time

Job description:

- Provide health and safety of all staff and visitors to the warehouse and goods in area;
- Make accounting for quality and storing of incoming goods;
- Make stock records of all stock in warehouse;
- Correct assembly of orders against shipping documents;
- Supervise cleanliness of the warehouse and production area;
- Monitor loading of vehicles to meet shipping dates;
- Inspect maintenance of all mechanical handling equipment within the Company.
- Supervise and manage all staff reporting to you.

Employees should be able to perform:

1 Knowledge of Warehouse Operations
2 Stock Control skills
3 Knowledge Warehouse IT Systems
4 Supervision of Staff
5 Professional approach on the phone and in face-to-face meetings.
6 PC literate: Microsoft Excel, Outlook & Word as a minimum

Open Problems

- Improve detection and prevention
- Usability and psychology
- Privacy

Prevention and Detection

- Improving detection rate at the early stage of the attack
- No detection method for targeted attack
- No detection method for false information, hoaxes, fake accounts

Usability and Psychology

- Asymmetry in usability
  - How to detect hoaxes and false information
- Understand user's mental model
- Study of user's bias

Privacy

- Importance of private information
- How to improve privacy

Questions?

References

- Koobface: http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul2009.pdf
- http://www.social-engineer.org/