

Privacy and Security in Online Social Media

Course on NPTEL

NOC21-CS28

Week 7.3

Ponnurangam Kumaraguru (“PK”)

Full Professor

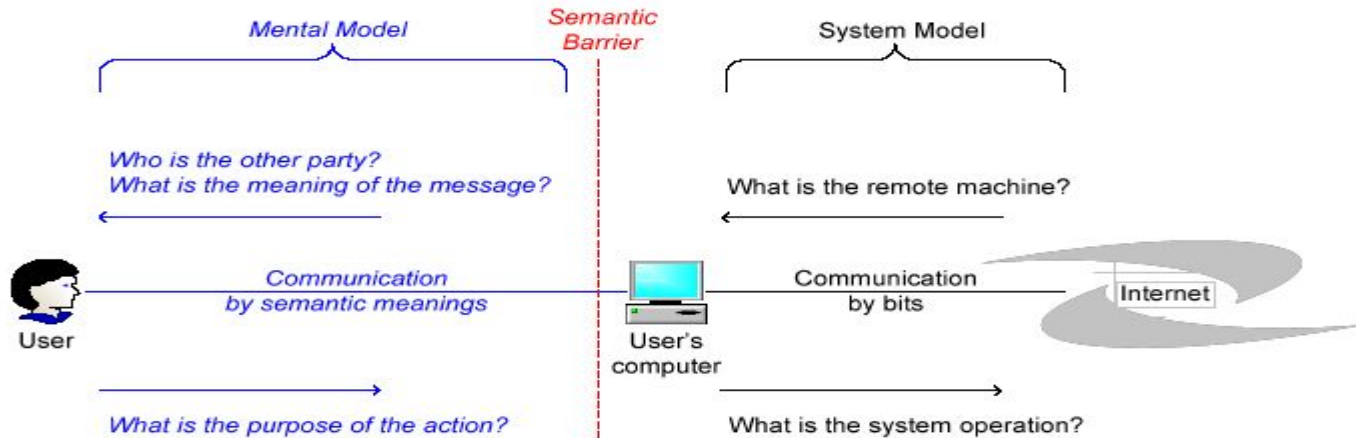
ACM Distinguished Speaker

fb/ponnurangam.kumaraguru, @ponguru

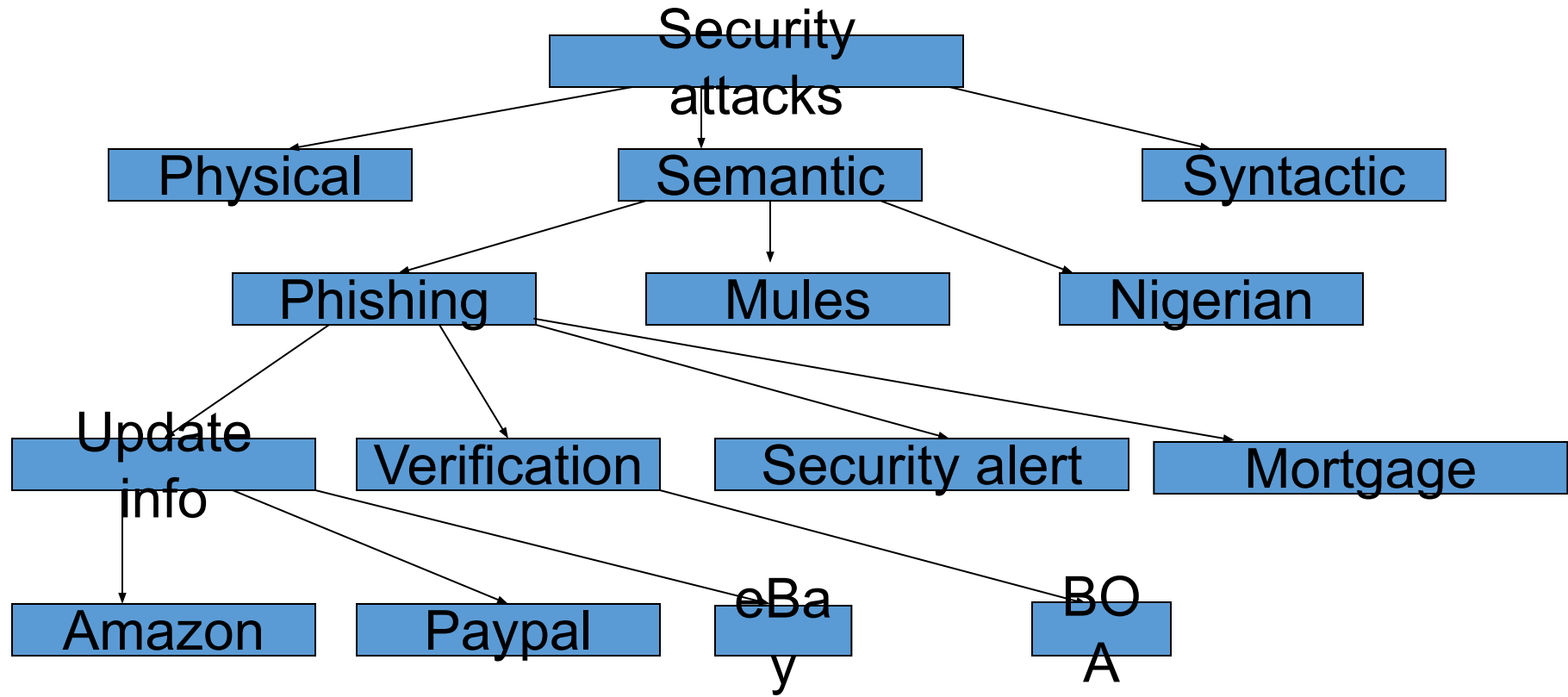


Semantic Attacks

- “Target the way we, as humans, assign meaning to content.”
- System and mental model



Semantic attacks



An email that we get

From: isri-phd-students-indiv-bounces@mailman.srv.cs.cmu.edu on behalf of eBay Inc [supprefnum8304194205199@ebay.com]
To: isri-people@cs.cmu.edu
Cc:
Subject: eBay: urgent security notice [Sun, 05 Feb 2006 18:54:02 -0400]

Sent: Sun 2/5/2006 6:03 PM



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.

To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team

This is an automatic message, please do not reply

Features in the email

From: isri-phd-students-indiv-bounces@mailman.srv.cs.cmu.edu on behalf of eBay Inc [supprefnum8304194205199@ebay.com]

Sent: Sun 2/5/2006 6:03 PM

To: isri-people@cs.cmu.edu

Subject: eBay: Urgent Notification From Billing Department



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.

To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team

This is an automatic message, please do not reply

Features in the email

From: isri-phd-students-indiv-bounces@mailman.srv.cs.cmu.edu on behalf of eBay Inc [supprefrum8304194205199@ebay.com]
To: isri-people@cs.cmu.edu
Cc:
Subject: eBay: urgent security notice [Sun, 05 Feb 2006 18:54:02 -0400]

Sent: Sun 2/5/2006 6:03 PM



We regret to inform you that your eBay account could be suspended if you don't update your account information.

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Features in the email

From: isri-phd-students-indiv-bounces@mailman.srv.cs.cmu.edu on behalf of eBay Inc [supprefnum8304194205199@ebay.com]
To: isri-people@cs.cmu.edu
Cc:
Subject: eBay: urgent security notice [Sun, 05 Feb 2006 18:54:02 -0400]

Sent: Sun 2/5/2006 6:03 PM



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.

To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerid=2&sideid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

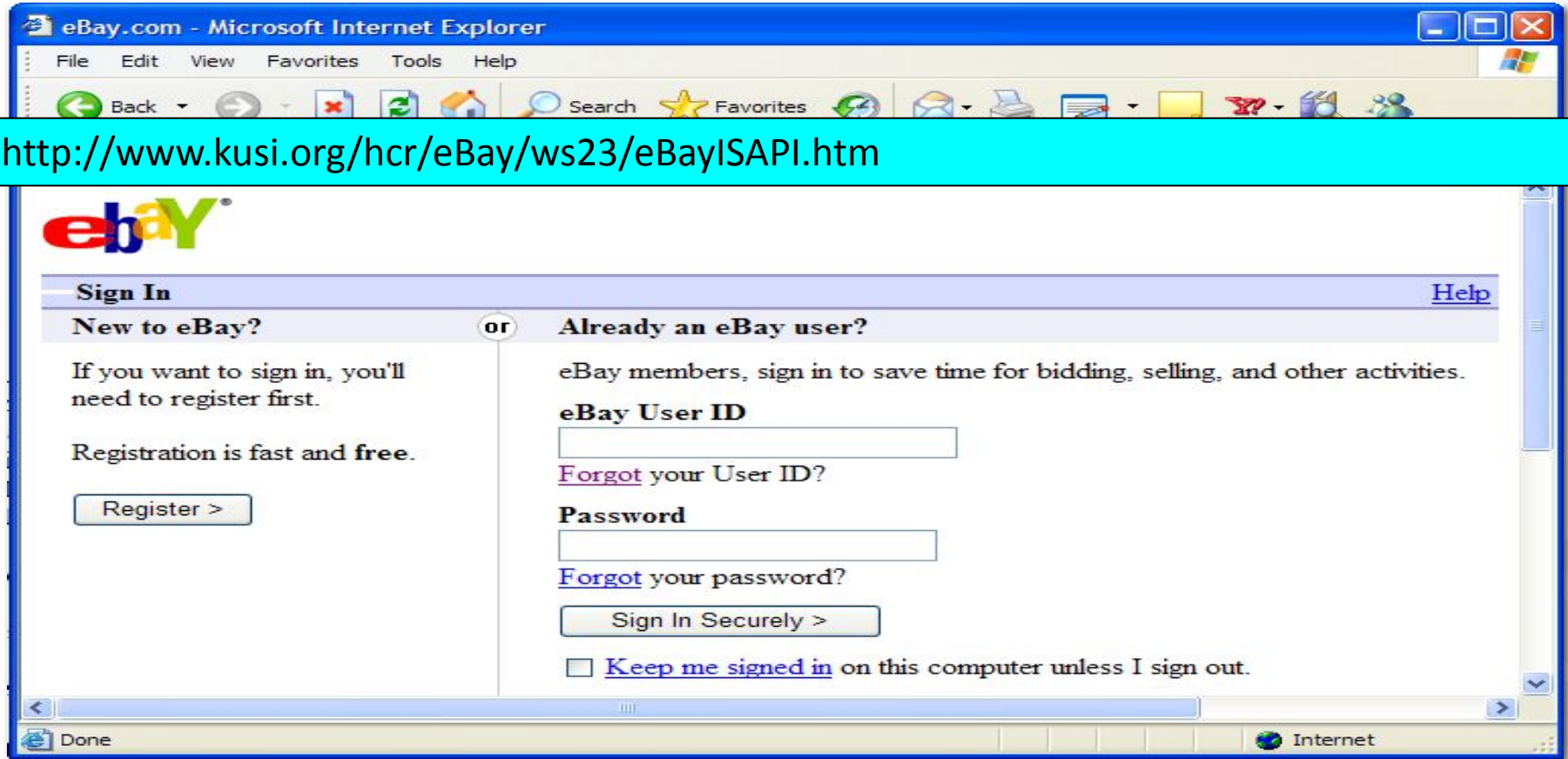
Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team

This is an automatic message, please do not reply

Website to collect information

http://www.kusi.org/hcr/eBay/ws23/eBayISAPI.htm



The image shows a screenshot of a Microsoft Internet Explorer browser window displaying the eBay sign-in page. The browser's address bar shows the URL: http://www.kusi.org/hcr/eBay/ws23/eBayISAPI.htm. The page features the eBay logo at the top left and a navigation bar with a "Sign In" link on the right. Below the navigation bar, there are two main sections: "New to eBay?" and "Already an eBay user?". The "New to eBay?" section includes a registration button. The "Already an eBay user?" section contains input fields for "eBay User ID" and "Password", along with "Forgot your User ID?" and "Forgot your password?" links, a "Sign In Securely >" button, and a checkbox for "Keep me signed in on this computer unless I sign out."

Sign In [Help](#)

New to eBay? **or** **Already an eBay user?**

If you want to sign in, you'll need to register first.

Registration is fast and free.

eBay members, sign in to save time for bidding, selling, and other activities.

eBay User ID

[Forgot](#) your User ID?

Password

[Forgot](#) your password?

[Keep me signed in](#) on this computer unless I sign out.

Done Internet

Phishing Cost

The cost of phishing

Cost for 10,000-employee organization	Cost per employee	Percent cost	
Part 1. The cost to contain malware	\$208,174	\$22	6%
Part 2. The cost of malware not contained	\$338,098	\$35	9%
Part 3. Productivity losses from phishing	\$1,819,923	\$191	48%
Part 4. The cost to contain credential compromises	\$81,920	\$9	2%
Part 5. The cost of credential compromises not contained	\$1,020,705	\$107	27%
Total extrapolated cost \$3,768,820	\$3,768,820	\$395	100%

Types of Phishing Attacks

- Phishing
- Context-aware phishing / spear phishing
- Whaling
- Vishing
- Smsishing
- Social Phishing?



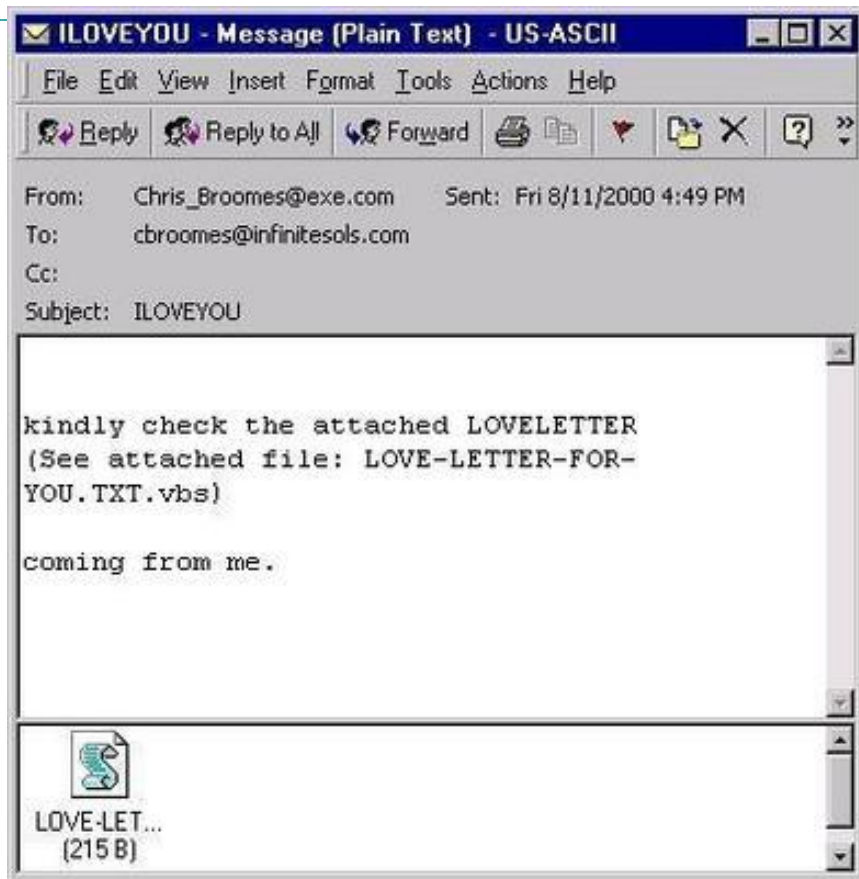
Until now, work that we have seen?

- Using voters database
- Using Medical health database
- Using Pictures from FB



Goal

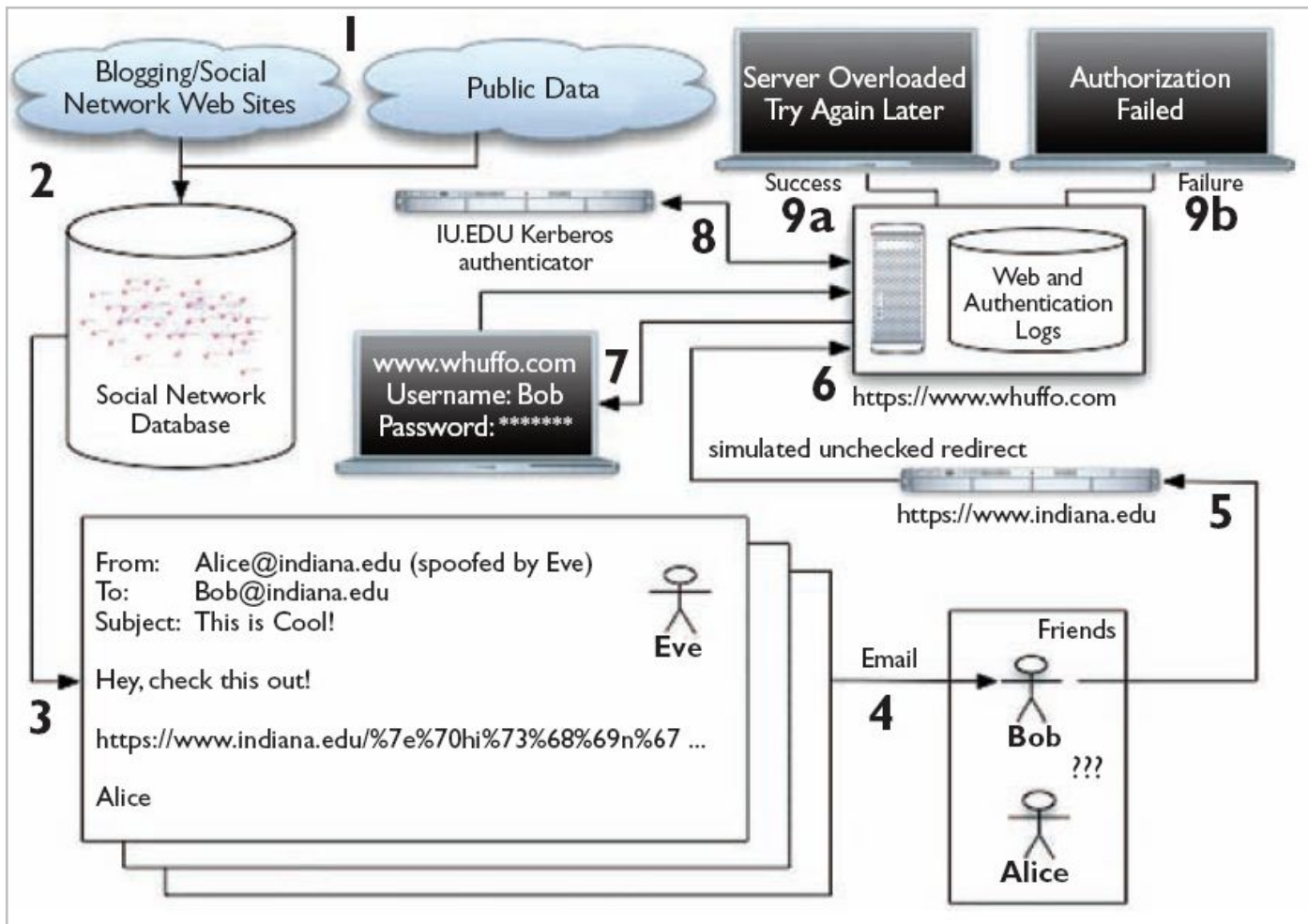
- To see how phishing attacks can be performed by collecting personal information from social networks
 - How easily or effectively can phisher use this information?



Methodology

- Collected publicly available personal information using simple tools like Perl LWP library
- Correlated this data with IU's address book database
- Launched in April 2005
- Age between 18 – 24





Control Vs. Experiment

- Control: The email from IU email ID, but, from an unknown person
- Experiment: From a friend in IU



Methodology

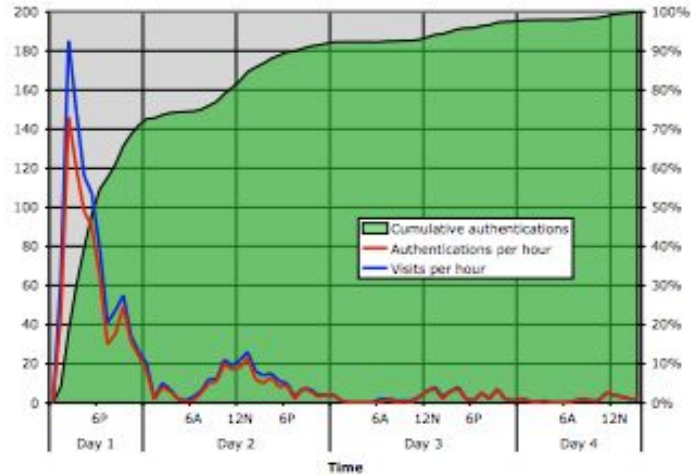
- Blogging, social network, and other public data is harvested
- Data is correlated and stored in a relational database
- Heuristics are used to craft spoofed email message by Eve “as Alice” to Bob (a friend)
- Message is sent to Bob
- Bob follows the link contained within the email message and is sent to an unchecked redirect
- Bob is sent to attacker whuffo.com site
- Bob is prompted for his University credentials
- Bob’s credentials are verified with the University

Victims

	Successful	Targeted	Percentage	95% C.I.
Control	15	94	16%	(9–23)%
Social	349	487	72%	(68–76)%

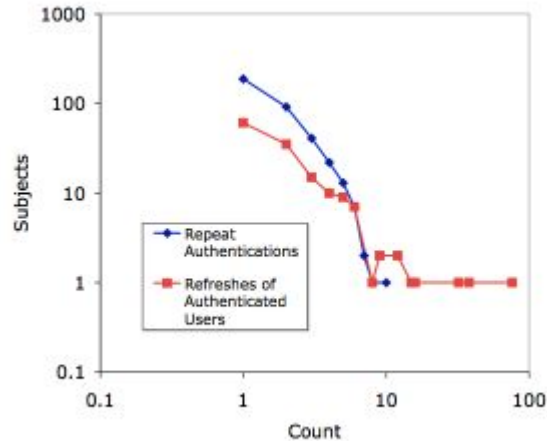
- Control group high – sender email ID was IU
- Experimental condition consistent with other studies

Success rate



- 70% authentications in first 12 hrs
- Takedown has to be successful

Repeated authentications

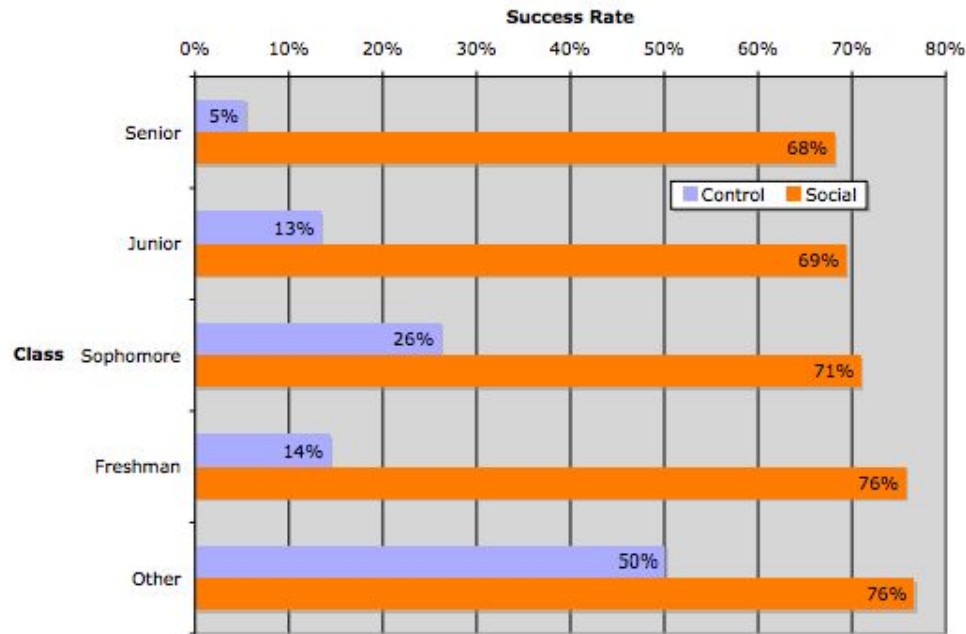


- Subject tried multiple times
- Tried again because “overload” message was shown
- Lower bound of users to fall, continued to be deceived
- Some tried 80 times

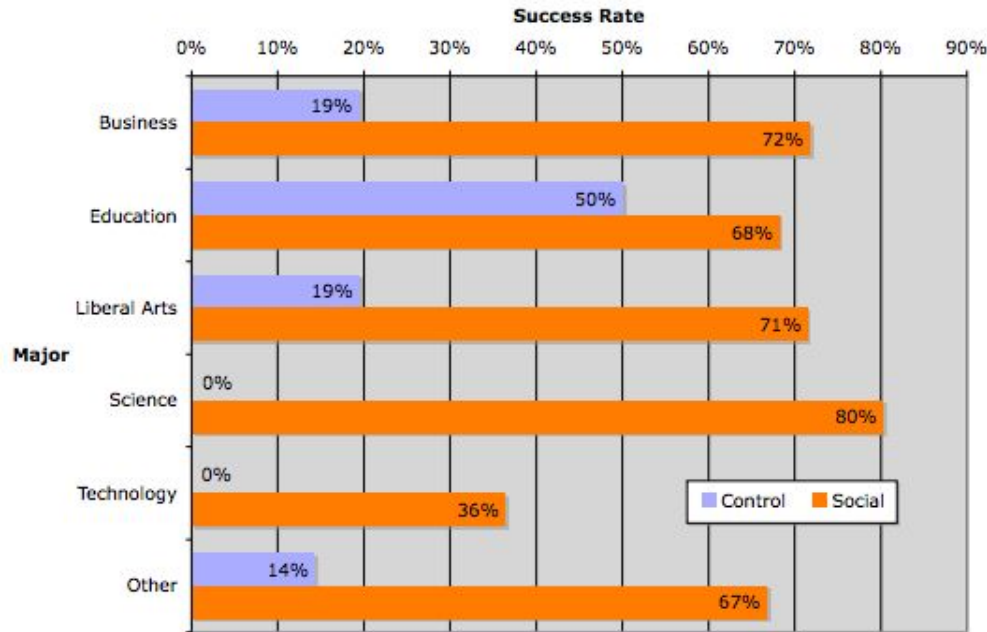
Gender

	To Male	To Female	To Any
From Male	53%	78%	68%
From Female	68%	76%	73%
From Any	65%	77%	72%

- 18,294 Ms and 19,527 Fs
- Overall F more victims
- More successful if it came from opposite gender
- F to M (13%) was more effect than M to F (2%)



- Younger targets more vulnerable



- All majors significant difference between control and experimental
- Max difference in Science
- Technology lowest #satisfying 😊

Reactions

- Anger
 - Unethical, inappropriate, illegal, fraudulent
 - Researchers fired
 - Psychological cost
- Denial
 - Nobody accepted that they fell for it
 - Admitting our vulnerability is hard
- Misunderstanding over spoofing emails
- Underestimation of publicly available information

Conclusions

- Extensive educational campaigns
- Browser solutions
- Digitally signed emails
- OSM provides lot more information for making the attack successful

References

- <http://markus-jakobsson.com/papers/jakobsson-commacm07.pdf>

References

- <http://www.mpi-sws.org/~farshad/TwitterLinkfarming.pdf>
- www.isical.ac.in/~acmsc/TMW2014/N_ganguly.ppt

Thank you

pk@iiitd.ac.in

precog.iiitd.edu.in

[fb/ponnurangam.kumaraguru](https://www.facebook.com/ponnurangam.kumaraguru)