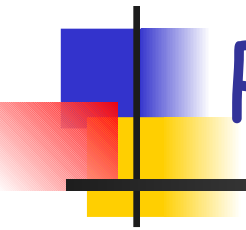
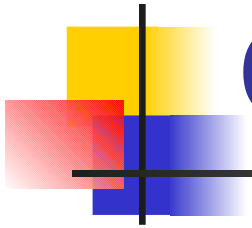


Online Social Networks based Phishing: offense and defense



Outline

- Motivation
- Introduction
- State-of-the-art detections
- Next steps

Motivation

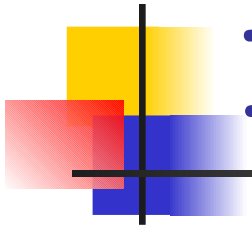
- Phishing is a Plague on the Internet

١. Estimated 3.5 million people have fallen for phishing scams
٢. Estimated $350million-$2billion indirect losses a year
٣. 9255 unique phishing sites reported in June 2006

- Growing # of social networking sites

١. Myspace
٢. Facebook
٣. LinkedIn
٤. Orkut
٥. Identified "Circles of friends"
٦. Facility for a phisher to harvest large amounts of reliable social network information

- Phishing attacks continue to evolve over time, making it harder to defend, however, an effective detection of phishing attacks is indispensable.



Introduction

- Definition

  Phishing is a criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

  - from Wikipedia

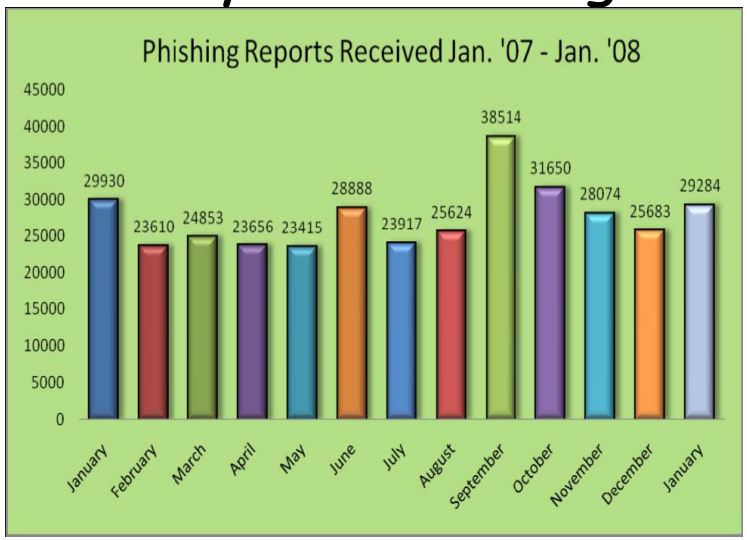
Introduction (cont.)

- How phishing works?

١. "Legitimate" emails seem to originate from trusted sources, such as banks, online retailers, or your friend's email-address
٢. Social engineering tactics convince the reader that their information is needed
٣. Links and emails look very real
٤. Techniques
   - Mis-spelled URLs (http://www.welllsfargo.com/account)
   - Spoofing URLs (http://www.google.com@members.tripod.com)
   - Javascript
   - Cross Site Scripting
   - International Domain Names

Introduction (cont.)

- Damage
- Phishing are badly threatening user's security.



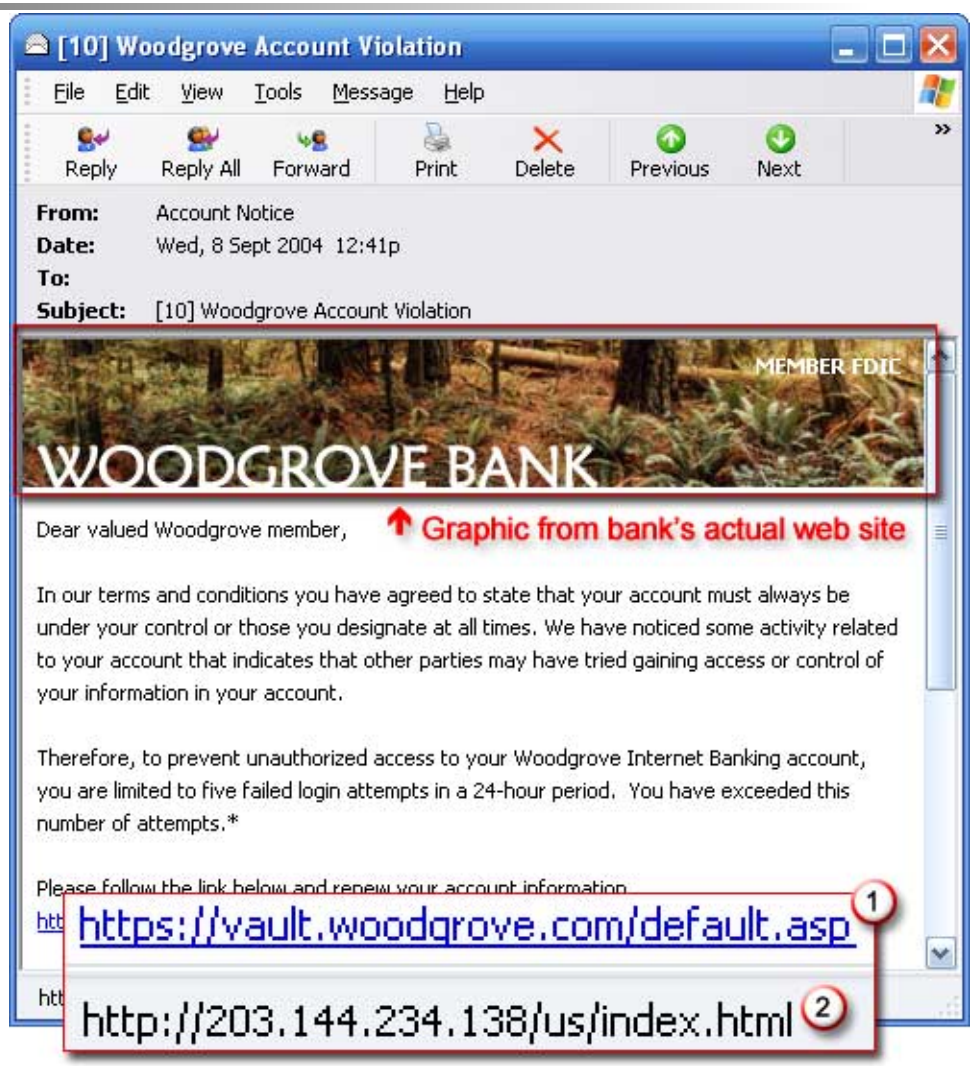
- Causing monetary & identity loss.

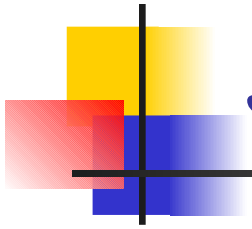
Introduction (cont.)

What phishing looks like?

(1) The link that appears "legitimate"

(2) The actual destination when you click on the link





State-of-the-art defense

- Four categories in anti-phishing:
  1. Studies to understand why people fall for phishing attacks
  2. Methods of training people not to fall for phishing attacks
  3. User interfaces for helping people make better decision about trustworthy emails and web sites
  4. Automated tools to detect phishing.

State-of-the-art defense (Cont.)

- Existing features for automatic detection

1. IP-based URL, a link in email whose host is an IP-address, e.g., http://192.168.0.1/paypal.cgi?fix account
2. Age of linked-to domains, phishing domains often have a limited life
3. Non-matching URLs, e.g., paypal.com
4. "Here" links to non-modal domain
5. HTML emails
6. Number of links
7. Number of domains
8. Number of dots
9. Contains javascript
10. Spam filtering techqiues
11. ……

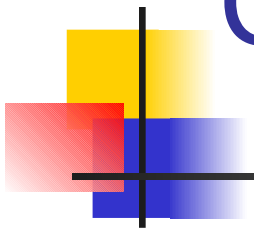
- However, all these features cannot filter phishing emails for social networks, a real example related to Prof. Chen.

  - An "real" email from a classmate's email-address asking him join the student-union, which is also "real".

Next Steps

- Objective: collect phishing attacks that use people's social network
  - Previous work collected phishing attacks involving friends requests made to fake accounts

Collection Methods



- Method 1: Social Honeypots with Friends
  - Have social honeypots make friend requests and and hope people accept them
  - Hope that one of the friends falls prey to a phishing attack and we receive an e-mail
- Method 2: Use existing accounts
  - Go through in-boxes by hand looking for phishing attacks sent from their friends

Pros and Cons

- Method 1
  - Relatively low likelyhood of success per profile
    - Many profiles will have to be created
    - We'll have to wait a long time
  - Not much mail to process
- Method 2
  - Lots of mail to filter through
  - Doesn't require waiting