SII 199 – Computer Networks and Society

Handout # 11: Spam, Phishing, and Fraud in Internet

Professor Yashar Ganjali
Department of Computer Science
University of Toronto

yganjali@cs.toronto.edu
http://www.cs.toronto.edu/~yganjali
Announcements

- Final project
  - Intermediate report
    - Due: Fri. Nov. 13th
  - In class presentations
    - The last two weeks of classes
    - 15 minute presentation

- Assignment 2
  - Will be marked by the end of this week.

- Volunteer for lecture notes?
The Story ...

- Introduction to computer networks
- The science of networks
- Computer networks and healthcare
- Computer networks and business
- Computer networks and entertainment
- Cloud computing /storage

**This week**: Spam, phishing, and fraud in the Internet
Outline

- Fraud in the Internet
  - Examples
- Spam
  - Detecting spam
- SPIT
  - Detecting SPIT
- Phishing
  - Vishing
Fraud in the Internet

- Internet can hide the identity of people behind e-mails, voice calls, IP numbers.
  - Not easy to find out who they are
- People trust what they see.
  - And usually don’t verify.
- Most communication is not authenticated.
- E-mail is a good example.
  - Receiver does not authenticate the sender
  - Easy to send e-mail that looks like someone else’s

Perfect environment for scammers!
Example 1 - Nigerian Scam

- Politician/businessman with tons of money
- Needs transfer some money
- Help, and you’ll be rich!
  - Give me your account number so that I can transfer the money to your account.
- Started from Nigeria
  - Nowadays, all over the world
Example 2 – Lottery

- You have won the lottery!
  - Even though you never participated in anything relevant!!
- You need to pay a small fee
  - To receive your millions of dollars ...
- And, you need to give them your personal information
  - Bank account numbers
  - After all, they need to transfer the money to your account! 😊
Example 3 – Stock Market

- Scammers invest in a specific stock
- Create a hype about that stock
  - Usually via sending mass messages
- Stock value increases as people invest
- Scammer *dumps* the stock
  - Also called *pump-and-dump*

- Predicting stock prices
  - Start with 1,000,000 people
  - Predict: halve the set
  - After 10 iterations you have 1,000 people
    - Which fully trust your predictions
Example 4 - Check Fraud

- You are selling something online
  - Craigslist, eBay, Kijiji, ...
- Buyer contacts you
  - Needs item immediately
  - Sends check or money order
  - Ask you to ship item immediately
- Check is fake
- Item has already been shipped
Example 5 - Overpayment Scam

- You are selling an item online
- Buyer contacts and tells you he/she will send you a check for a much larger amount
- You can keep some
  - But need to return some
- Original check is forged
  - It might take sometime for you to find this out

- The list goes on ...
Outline

- Fraud in the Internet
  - Examples
- Spam
  - Detecting spam
- SPIT
  - Detecting SPIT
- Phishing
  - Vishing
Spam in the Internet

- Unwanted e-mail, or phone call
  - Well, usually!
- Bulk
  - Usually, using machines which are compromised
    - Botnets
- Automated
  - Producing large number of e-mails and phone calls needs automated tools to be effective
  - Why?
- Some studies say up to 98% of e-mails are spam.
Types of Spam

- Spam in e-mails
  - Junk mails – not of interest for us here
- Chat rooms, and instant messages
- Weblogs, or any other online forums
- Popups
- Voice calls
  - To voice applications, or
  - Landlines and cell phones
Objectives of Spammers

- Sell a product
  - Advertising products and services

- Steal personal information
  - Usually through *phishing* attacks
  - Identity theft
    - Financial information can be used to transfer funds or purchase product

- Gain control of victim’s machine
  - Use as a botnet node
  - Launch attacks against others
Collecting User E-mails

• Crawling the web
  • Use image instead of text
  • Even simple tweaks seem to help a lot with this
    • My last name at cs dot Toronto dot edu

• Collecting and selling user registration data
  • Sometimes offer legitimate product or service
  • Fine prints ...

• Dictionary attacks
How Spammers Send Spam

- User computers infected by viruses
  - Large network of such machines, called botnets
  - Thousands to hundreds of thousands of machines in each botnet
- Spammer controls the botnet
  - Used to attack other machines
  - Or generate spam
- Very difficult to trace
- Very cheap for spammer
Detecting Spam

- **User feedback**
  - Ideally, we want the user to tell us what she/he considers spam

- **Getting user feedback is very costly**
  - In terms of user time
  - And annoying in long-term

- **Detect specific keywords used in spam**
  - Use artificial intelligence to classify documents
  - How?
  - What if they send pictures rather than text?
Detecting Spam – Cont’d

- Identify hosts which send spam
  - And block them (black-listing)
  - How?

- Identify good senders
  - And only allow them (white-listing)
  - How?

- Challenge the sender
  - Computational puzzles
  - Captcha (reCaptcha)
Protecting Against Spam

- If you can detect spam, clearly you can block it.
  - On the server, or locally.
  - Pros and cons of each?
- You can also make it costly for the spammer to send spam
  - Small fee to deliver e-mail?
  - Tons of research in this area
- Disposable e-mail addresses
  - Useful when registering on a site that you can’t trust
- Blocking outbound traffic
  - Mostly by your ISP, or e-mail service providers
Protecting Against Spam – Cont’d

- Having lots of information makes spam detection easier
- Feedback from a large group of users
  - Less work for individual user
- We can take advantage of social networks
  - Friend-of-friend relationships
- Google, Yahoo, ... have large datasets
  - And that’s why they can do a good job in spam detection
- Education is a big part of this process which has been overlooked.
More Challenges

- Detecting spam is challenging.
- No universal definition
  - What you consider spam might be a legitimate e-mail for someone else.
  - And vice versa.
  - Example: bank offering life insurance to all its customers
- Personalization can be extremely difficult
  - Not as much training data
  - Giving feedback is a pain for the user
  - User might make a mistake
Outline

- Fraud in the Internet
  - Examples
- Spam
  - Detecting spam
- SPIT
  - Detecting SPIT
- Phishing
  - Vishing
SPam in Internet Telephony (SPIT)

- Similar to e-mail spam
  - But use voice as the medium
- Call a large number of users
  - Mostly for advertising, or to steal some information
  - Can use botnets

- Seems to be increasing
  - Shift to Voice over IP (VoIP) systems
  - Lower cost of VoIP calls
    - Sometimes free
  - Easier to gain control of VoIP boxes
    - Compared to traditional phone systems
Challenges of Detecting SPIT

- SPIT is more annoying than spam.
- Most phones are not equipped with the appropriate tools.
  - Unlike e-mail which is received by computers
- Detection needs to be real-time
  - Unlike e-mail which is offline
- Detection before the user picks up the phone
  - Therefore without having access to the content of the call
- Processing voice is more complex than processing text
  - Needs more resources and is more costly
- Handling SPIT not straight-forward
  - Just mark as SPIT, forward to voice mail, drop the call, ...?
SPIT Detection

- Using call logs
  - Who called whom, at what time, for how long
- How can we do this?
- Strong ties property
  - People spend more than 80% of their time talking to 4-5 of their friends.
- Weak ties property
  - People talk to at least 10% of their friends for more than 1 minute.
  - It’s hard for the spammer to keep 10% of people on the line for more than 1 minute.

Spammers need to generate large volume of calls. Spammers can’t easily forge strong ties and weak ties.
User Challenge for SPIT Detection

- Ask the user to repeat a sentence
  - Machine needs to understand what you said
  - And to repeat it in an understandable manner
- Verify the user to see if he actually said that sentence
- Check to see if the sentence is said by a human
  - They can’t simply replay the sentence
- Block if user fails to pass the test
User Challenge - Characteristics

• Natural and easy
  • Easy for a real human, difficult for machines

• Accessible
  • For people with disabilities
  • And, for the times when using keyboard is not easy
    • E.g. while driving
Outline

• Fraud in the Internet
  • Examples

• Spam
  • Detecting spam

• SPIT
  • Detecting SPIT

• Phishing
  • Vishing
Phishing Attacks

- Pose as someone else to ...
  - Gain personal information
    - Account numbers
    - Authentication information
    - Social insurance number
- Individual target, or mass e-mail attack
  - Asking you to verify or update your account information
Phishing Example

A MasterCard to build credit
From: OrchardBankCreditCard <orchardmgl@bukewebserices.net> Add to Contacts
To: updates2407168@bukewebserices.net

Orchard Bank Credit Card

The Best card for Rebuilding Credit Just Got Better

You could begin rebuilding your credit today with the power of an Orchard Bank® MasterCard®. Our flexible process makes it easier to get pre-qualified for any of our cards, even if your history is less than perfect. Start Now!

Best of all, our no-risk inquiry means we can pre-qualify you in as little as 30 seconds, with no negative impact to your credit score. Click here to find out what offer is best for you.

This message is a solicitation for an Orchard Bank Credit Card account.

It is our goal to offer you the credit card that best fits your credit profile. You may be offered a secured credit card with other terms and conditions, which will be disclosed before your application is processed.

The Orchard Bank® MasterCard® is issued by HSBC Bank Nevada, N.A. and is serviced by HSBC Card Services Inc. and/or HSBC Card Services (IL) Inc.

http://go.centerlinktech.com/CTYZLHcplHyJpDUkQ7UfrEiobsaFeBZcmDzBYXxKsaraiGeUBwKLVggqNVobsxOwFnaOkRTS
Simple Countermeasures for Phishing

- Never click on links from untrusted sources
- Hoover over the link to see what it looks like
  - Sometimes they hide the actual URL
- Use common sense
  - PayPal already knows your password!
  - They don’t need to ask you to repeat!
Vishing Attacks

• Attack via voice, i.e. phone call
  • Fake number pretending to be a bank, government, ...
  • Asking personal information to prove who you are
    • Bank account number, social insurance number, ...
  • Or a message asking you to call a specific number

• Harder to detect than phishing
  • Similar to SPIT detection problem

• Web sites which can provide information
  • Mostly user feedback
  • Sometimes confusing data
Simple Countermeasures for Vishing

- If they ask you to call a specific number verify it first
  - Government can verify numbers for you.
  - Check online resources
  - Call the number you have rather than the number they give you
    - Like the number on the back of your credit card

- Use common sense
  - Before verifying their identity don’t give sensitive information.
    - Your bank knows your account number already! They can’t expect you to provide that information before proving who they are.
Conclusion

- Fraud is a big problem in today’s Internet.
  - Criminals hide their identity, and
  - Try to steal yours!
- Spam, and phishing are serious problems today.
  - Impact on performance of e-mail systems
  - User time wasted
- SPIT and vishing not as big of a problem.
  - But they are growing,
  - Are more difficult to detect, and
  - Are more annoying for users
- **Question.** How do you think we can solve these problems?
  - Technically?
  - Any other way?