

Trust and Semantic Attacks - II

Ponnurangam Kumaraguru

Computation, Organizations and Society

Carnegie Mellon University

Feb 23rd 2006

ponguru@cs.cmu.edu

<http://www.cs.cmu.edu/~ponguru/>

Carnegie Mellon



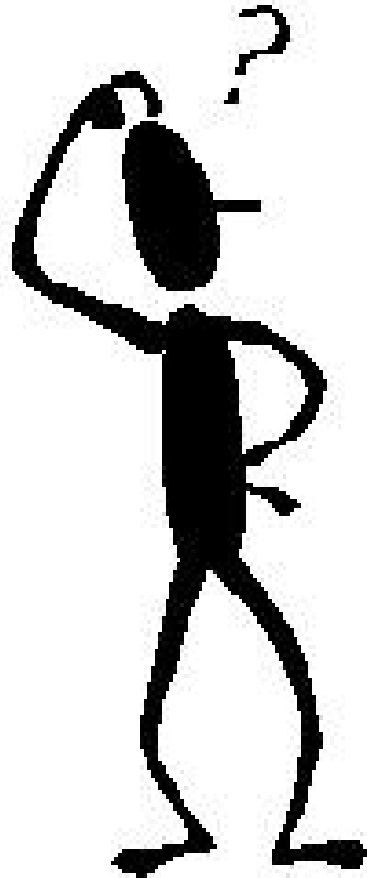
CMU Usable Privacy and Security Laboratory

Outline

- Summary of part I
- Semantic Attacks
- Phishing
- User studies
- Task



What is trust?



- No single definition
- Depends on the situation and the problem
- Many models developed
- Very few models evaluated



Trust Models

■ Positive antecedents

- Benevolence
- Comprehensive information
- Credibility
- Familiarity
- Good feedback
- Propensity
- Reliability
- Usability
- Willingness to transact
- ...

■ Negative antecedents

- Risk
- Transaction cost
- Uncertainty
- ...



Outline

- ✓ Summary of part I
- Semantic Attacks
- Phishing
- User studies
- Task



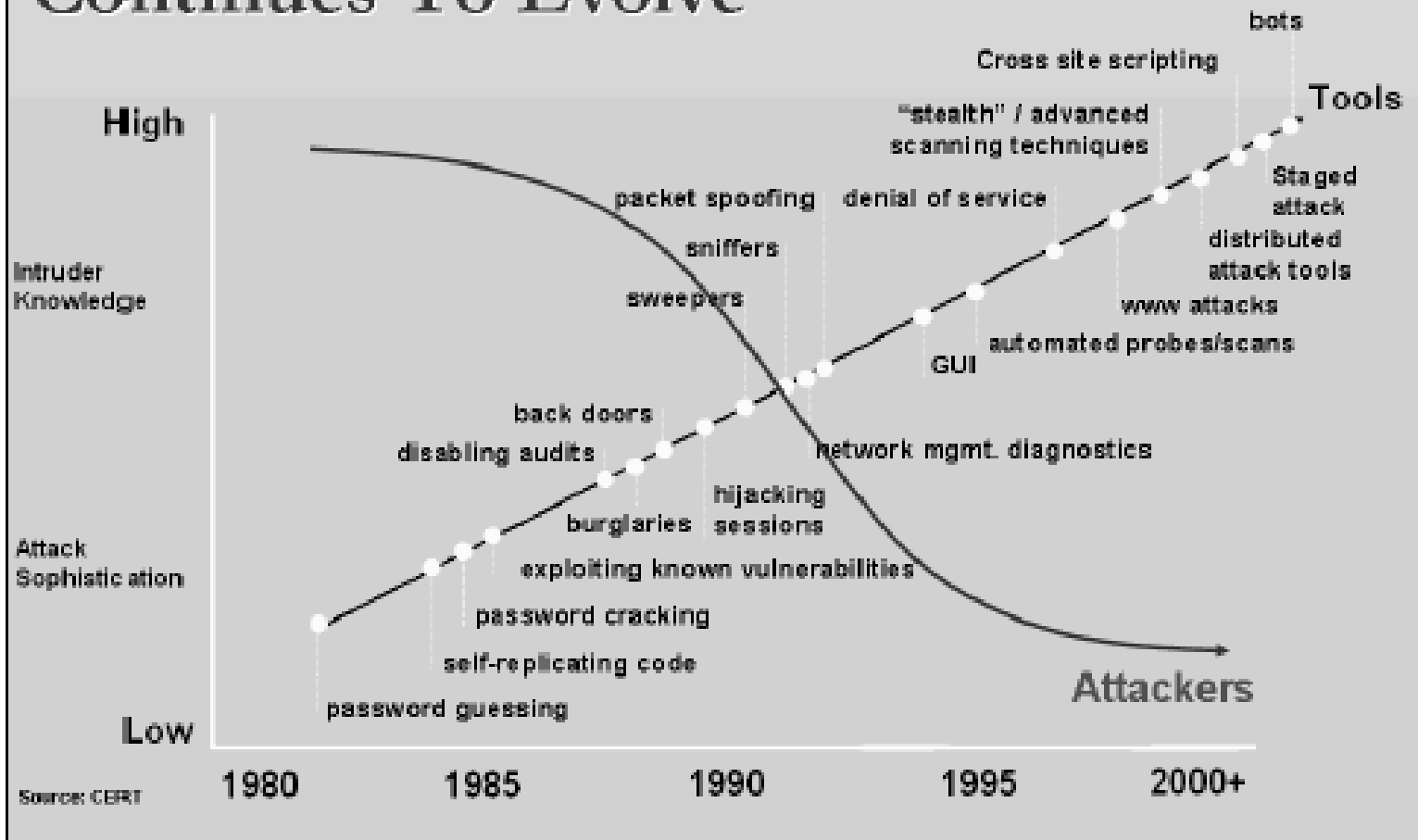
Security Attacks: Waves

- Physical: attack the computers, wires and electronics
 - E.g. physically cutting the network cable
- Syntactic: attack operating logic of the computers and networks
 - E.g. buffer overflows, DDoS
- Semantic: attack the user not the computers
 - E.g. Phishing



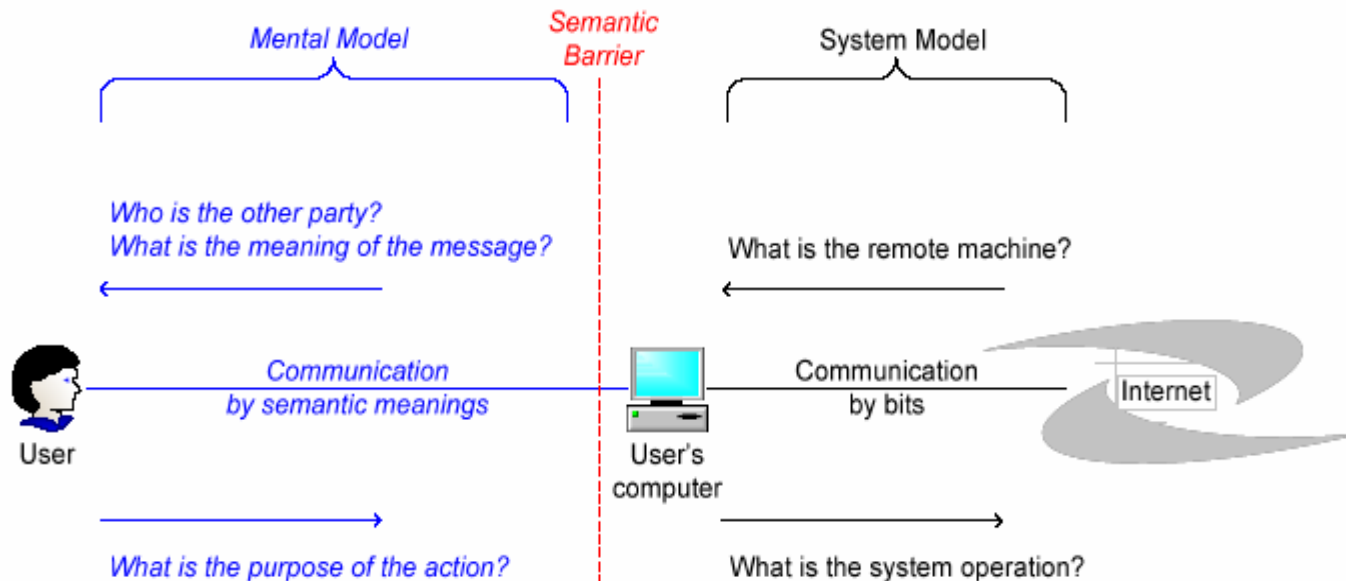
Security Attacks (contd.)

Cyber Attack Sophistication Continues To Evolve



Semantic Attacks

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



Outline

- ✓ Summary of part I
- ✓ Semantic Attacks
 - Phishing
 - User studies
 - Task



Phishing Basics (1)

- Pronounced "fishing"
- Scam to steal personal information
- Also known as "brand spoofing"
- Official-looking e-mail sent to potential victims
 - Pretends to be from their ISP, retail store, etc.,
- One form of semantic attack



Phishing Basics (2)

- Link in e-mail message directs the user to a web page
 - Asks for financial information
 - Page looks genuine
- E-mails sent to people on selected lists or to any list
 - Some % will actually have account
- “Phishing kit”
 - Set of software tools
 - Help novice phisher imitate target Web site
 - Make mass mailings



Phish example

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



Phishing

- *“Successful phishing depends on a discrepancy between the way a user perceives a communication and actual effect of the communication.”*
- *“Phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials.” - APWG*
- *“...the act of sending a forged e-mail (using a bulk mailer) to a recipient, falsely mimicking a legitimate establishment in an attempt to scam the recipient into divulging private information such as credit card numbers or bank account passwords.” – Phishing Exposed*



Phishing: A Growing Problem

- Over 16,000 unique phishing attacks reported in Nov. 2005, about double the number from 2004
- *“Illegal access to checking accounts, often gained via phishing scams, has become the fastest-growing form of consumer theft in the United States, accounting for a staggering \$2.4 billion in fraud in the previous 12 months.”*
– Gartner, late 2004.
- Additional losses due to consumer fears



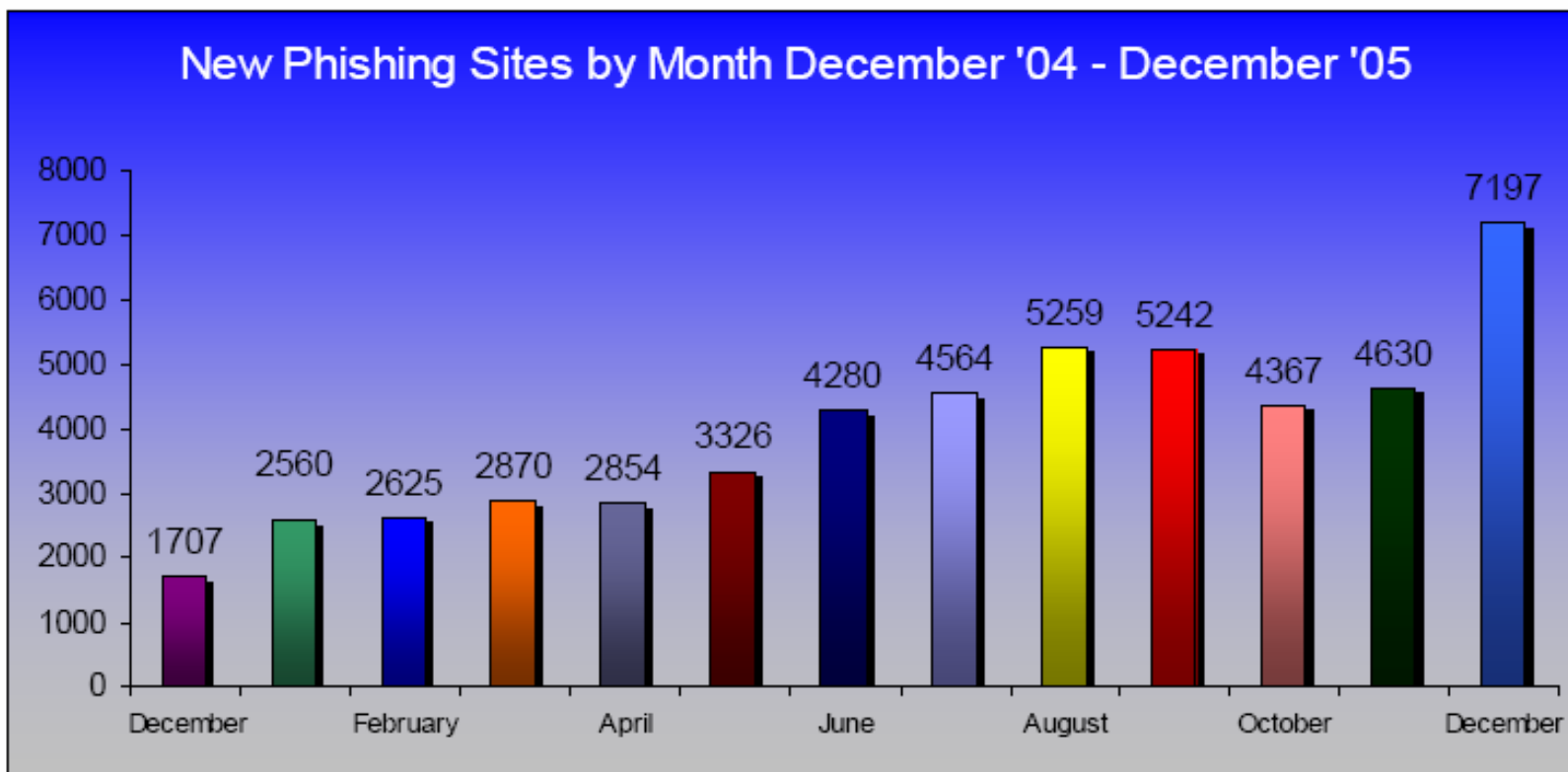
Phishing Trends, Dec 2005



http://apwg.org/reports/apwg_report_DEC2005_FINAL.pdf



Phishing Trends, Dec 2005 (contd.)



Phishing Trends, Dec 2005 (contd.)

- Number of unique phishing reports received in December: 15244
- Number of unique phishing sites received in December: 7197
- Number of brands hijacked by phishing campaigns in December: 121 (highest)
- Average time online for site: 5.3 days
- Longest time online for site: 31 days



Phishing attacks

- Lack of knowledge
 - Lack of computer system knowledge
 - Lack of security and security indicators (security locks, browser chrome, SSL certificates)
- Visual deception
 - Visually deceptive text (vv for w, l for I, 0 for O)
 - Images masking underlying text
 - Windows masking underlying windows
 - Deceptive look and feel
- Bounded attention
 - Lack of attention to security indicators (secondary goal)
 - Lack of attention to the absence of security indicators



Outline

- ✓ Summary of part I
- ✓ Semantic Attacks
- ✓ Phishing
 - User studies
 - Task



Why Phishing Works

■ Goal

- What makes a bogus website credible?

■ Methods

- With-in subjects design
- Analyze about 200 phishing attacks from anti-phishing archive
- Usability Study of 22 participants on 20 websites to determine fraudulent websites

■ Analysis


- Good phishing websites fooled 90% of participants
- On average 40% of the time subjects made mistakes



Bank of the West |

Back Forward Reload Stop Home <http://www.bankofthewest.com/BOW/home/index.html> Go

Friday, July 29, 2005 中文 Chinese | Locations | Employment | Contact Us | Search: GO


BANK OF THE WEST  [PERSONAL](#) [SMALL BUSINESS](#) [COMMERCIAL](#) [ABOUT US](#)

Online Banking


[Learn More](#) | [Enroll Online](#)
eTimeBanker® Sign In:

User Name:


Password:

[Forgot Password?](#) 

Select...



HOME EQUITY

Get in on the Great Rate Lock-in! [Click here for the key](#) 


Locations

State:

ZIP code:


CONSUMER ALERT!

Tips on protecting yourself and how to report suspicious activities

[READ MORE](#) 

News Bulletin

June 14, 2005 | BancWest Corporation Announces Acquisition of Commercial Federal Corporation by Bank of the West [More](#)





Personal Banking


Welcome to your community bank. First job. Last job. New home. College tuition. We're here to help guide your finances through the challenges of every life stage. Stop by a branch to experience our hallmark service for yourself.

[Checking](#) [Wealth & Trust](#)
[Savings & CDs](#) [Consumer Loans](#)
[Debit & Credit Cards](#) [Private Banking](#)
[Online Banking](#) [More ...](#)

Tennis. Beach Games. Rodeo.

Join us for summer fun this week only!



Click on any logo to visit each official event website or [click here](#) to visit our sponsorships page that includes a broadcast schedule for the Classic.

Investments

Retirement planning starts with an investment of about 15 minutes.

Small Business Banking

Taking care of business. Across town. Around the globe.

As you navigate your business through all its cycles, you're not on your own. We assign a dedicated relationship manager to help you make the right financial choices. Give us a call. We pick up the phone!

[Business Checking](#) [Loans & Lines](#)
[Cash Management](#) [SBA Lending](#)
[Merchant Services](#) [More...](#)

Commercial Banking

Your cornerstone of stability and growth. Middle-market to multi-national, our corporate clients give us high marks for flexible financing, fast local decision-making, and a proactive style of client service. Let's talk business.

[Commercial Lending](#) [Equipment Leasing](#)
[Cash Management](#) [International Trade](#)
[Capital Markets](#) [More...](#)

TaxDirect

Pay your business taxes online - quickly and securely.

Done



VeriSign Secured Seal - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://seal.verisign.com

English

13/2/2006 22:44
www.bankofthewest.com uses VeriSign services as follows:

SITE NAME:	www.bankofthewest.com
SSL CERTIFICATE STATUS:	Valid (18-Oct-2005 to 28-Oct-2006)
COMPANY/ ORGANIZATION:	BANK OF THE WEST Walnut Creek California, US

Encrypted Data Transmission This Web site can secure your private information using a VeriSign SSL Certificate. Information exchanged with any address beginning with https is encrypted using SSL before transmission.


Identity Verified BANK OF THE WEST has been verified as the owner or operator of the Web site located at www.bankofthewest.com. Official records confirm BANK OF THE WEST as a valid business.

For your best security while visiting sites, always make sure the address of the visited site matches the address you are expecting to see. Make sure that the URL of this page begins with "https://seal.verisign.com"

>> REPORT SEAL MISUSE

Done seal.verisign.com

Content Analysis Res... 讚美之泉繁體中文 - ... Usable Privacy and S...



Business Banking

... of business. Across town. Around

...igate your business through all its ...
...re not on your own. We assign a ...
...relationship manager to help you ...
...right financial choices. Give us a call. ...
...the phone!

[Checking](#) [Loans & Lines](#)
[Management Services](#) [SBA Lending](#)
[More...](#)

Special Banking

[Cornerstone of stability and growth.](#)
...ket to multi-national, our corporate ...
...us high marks for flexible financing, ...
...ecision-making, and a proactive ...
...ent service. Let's talk business.

[Real Estate Lending](#) [Equipment Leasing](#)
[Management](#) [International Trade](#)
[Markets](#) [More...](#)

Student Loans
Graduate to a great rate or consolidate!

Copyright © 2006 Bank of the West. Member FDIC. Equal Housing Lender

Employment | Consumer Privacy Policy | Terms & Conditions | BancWest | BNP Paribas | Essex Credit | Trinity Capital

Done

start

2 Micr... MINITA... trustpr... Adobe ... 6 Fire... EN 10:44 PM



Why Phishing Works (contd.)

■ Conclusions

- Existing browsing cues are ineffective
- Participants proves vulnerable to phishing attacks
- Lack of knowledge of web fraud
- Erroneous security knowledge

■ Suggestions

- To understand what humans do well and what they do not do well
- Help user to distinguish legitimate and spoofed website



Do Security Toolbars Actually Prevent Phishing attacks?

■ Goal

- To evaluate security toolbar approach to fight phishing?

■ Methods

- Between subjects design
- Subjects as John Smith's personal assistant
- 20 emails from John
- Toolbars tested
 - Neutral-information
 - SSL verification
 - System decision



Spoofstick

- Displays real domain name

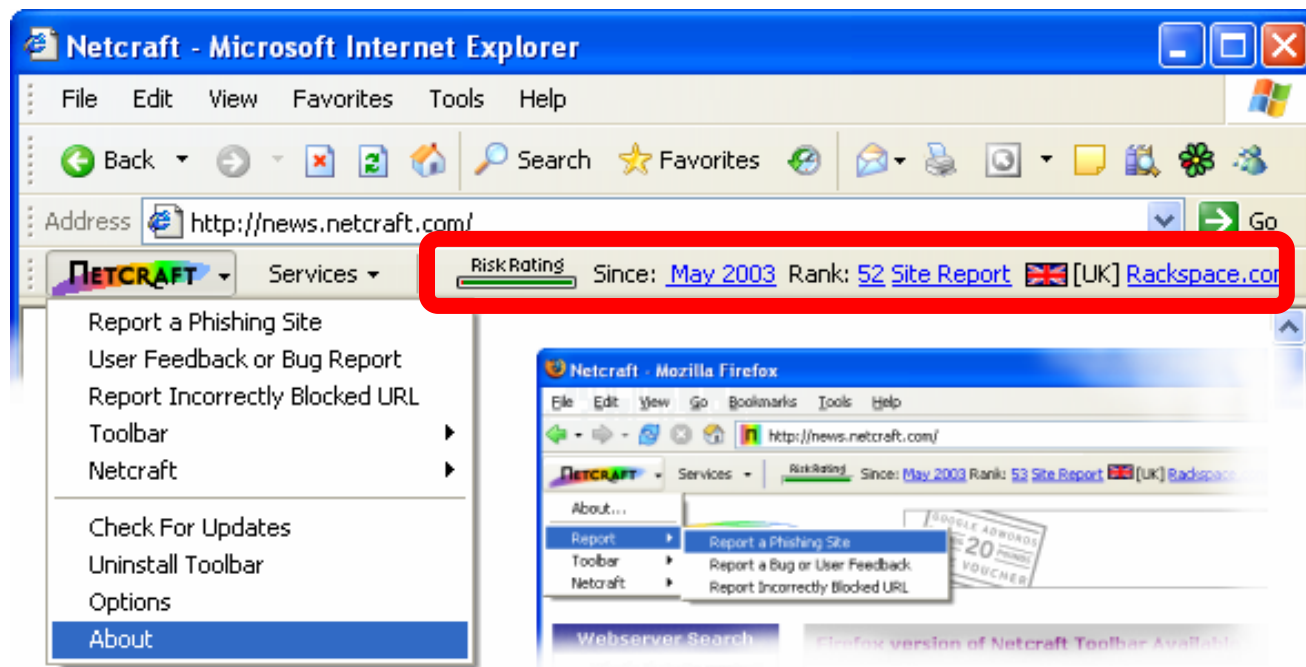
www.paypal.com.wws2.us => wws2.us

- Customize the color and size



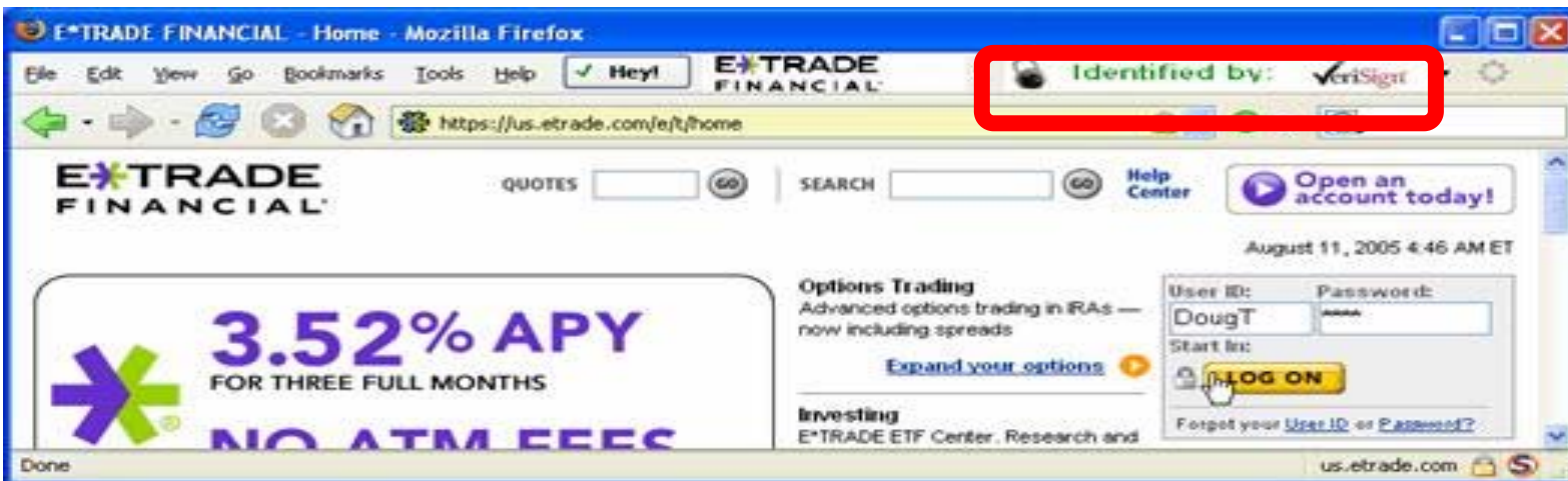
Netcraft

- Displays domain registration date, hosting name and country, and popularity among other users
- Traps suspicious URLs with deceivable characters
- Enforces display of browser navigational controls



Trustbar

- Makes secure connection more visible by displaying logos of the website
- Allowing you to assign a name and/or logo for each of these sites



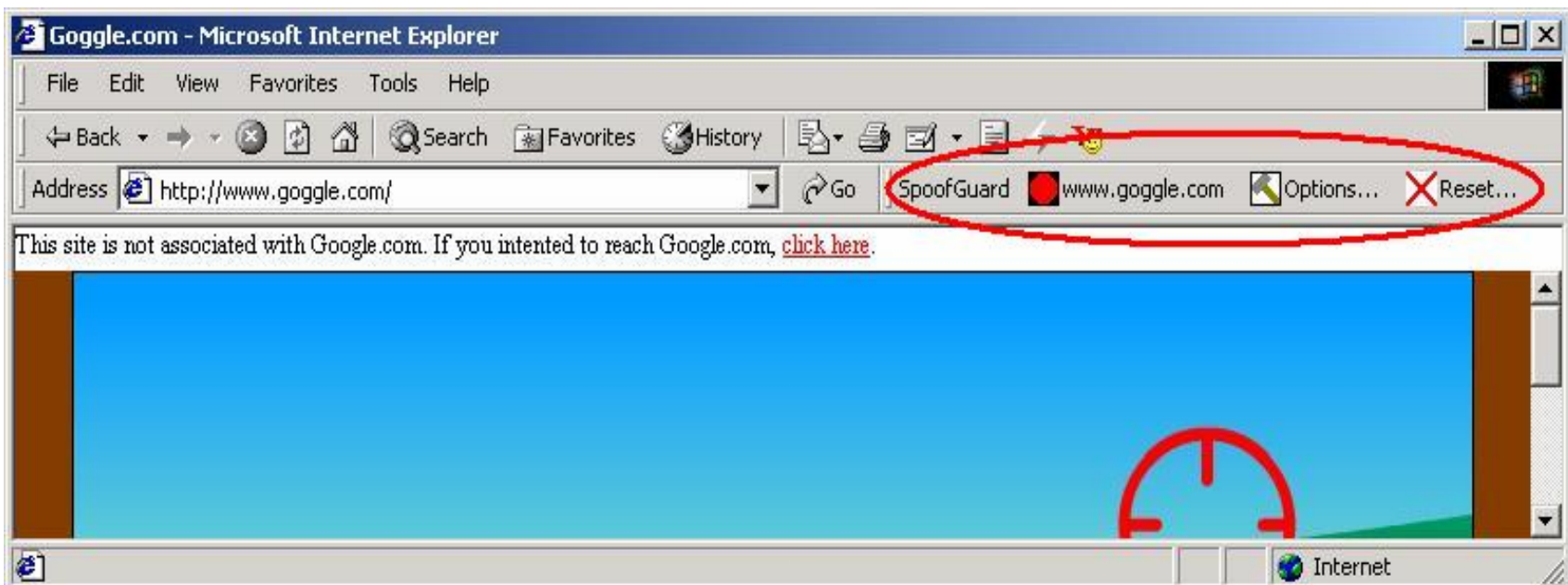
eBay account guard

- Green indicate current site is eBay or paypal, red is a knowing phishing, gray is for all other sites



Spoofguard

- Calculates spoof score from previous attacks
- Red for hostile, yellow for middle and green for safe



Do Security Toolbars Actually Prevents Phishing attacks? (contd.)

■ Analysis

- 34% of the subjects provided information even after notification
- 25% of the subjects did not notice the tool bars at all

■ Conclusions

- Spoof scores of all the toolbars are greater than 0
- Some toolbars would have better spoof rates than others



Potential drawbacks

■ Suggestions

- Active interruptions are effective
- Tutorials are effective
- Knowing the user's intentions will be effective
- User intentions should be respected



Take away points

- Phishing is effective
 - Humans are involved
 - Human interaction with interfaces
 - Social context
- Need better user interfaces
- Need more understanding of users' decision making process
- Need
 - Education
 - Expertise



Outline

- ✓ Summary of part I
- ✓ Semantic Attacks
- ✓ Phishing
- ✓ User studies
- Task



Task - Definition

- Vulnerability - susceptibility to injury or attack (e.g. clicking on the link in the email, giving username and password, etc.)



Task

User type	Vulnerability
Geek	Low
Expert	Low
Savvy	Medium
Novice	High

Design the specifications of a system to train the user type about phishing attacks and help them make trust decisions.



Outline

- ✓ Summary of part I
- ✓ Semantic Attacks
- ✓ Phishing
- ✓ User studies
- ✓ Task



Bibliography

- <http://www.millersmiles.co.uk/>
- <http://cups.cs.cmu.edu/soups/2005/2005proceedings/p77-dhamija.pdf>
- <http://www.simson.net/ref/2006/CHI-security-toolbar-final.pdf>
- http://www.sims.berkeley.edu/~rachna/papers/why_phishing_works.pdf
- [http://www.cs.berkeley.edu/~tygar/papers/Phishing/Phish and HIPs.pdf](http://www.cs.berkeley.edu/~tygar/papers/Phishing/Phish_and_HIPs.pdf)
- <http://www.spoofstick.com/>
- <http://toolbar.netcraft.com/>
- <http://trustbar.mozdev.org/>
- http://pages.ebay.com/ebay_toolbar/
- <http://crypto.stanford.edu/SpoofGuard/>



Thanks to

- Supporting Trust Decision project members



National Science Foundation
WHERE DISCOVERIES BEGIN

