University of BRISTOL

Computer System- B Security

Introduction to Web Security P2

Cookies, session IDs, Phishing (URL obfuscation)

Sanjay Rawat

bristol.ac.uk

HTTP vs HTTPS

- HTTP send request/response in clear text
  - Information can be sniffed (confidentiality is lost)
- We do not know if we are connected to the right server
  - Identity/authenticity is not variable.
- HTTPS (secure) solves this by using crypto.
  - Encryption
  - Signature
  - MAC
- Example: SSL/TSL (later in the unit)

HTTP is stateless

HTTP is stateless

- The notion of a **session**
  - encapsulates information about a visitor
  - Allows user to relate multiple requests

HTTP is stateless

- The notion of a **session**
  - encapsulates information about a visitor
  - Allows user to relate multiple requests
- Session information should be considered extremely sensitive

HTTP is stateless

- The notion of a **session**
  - encapsulates information about a visitor
  - Allows user to relate multiple requests
- Session information should be considered extremely sensitive
- Thus, a class of attacks known as session hijacking

Sessions Using GET or POST

Sessions Using GET or POST

- Pass session information to the web server each time the user navigates to a new page using GET or POST requests.

Sessions Using GET or POST

- Pass session information to the web server each time the user navigates to a new page using GET or POST requests.
- This method is particularly susceptible to man-in-the-middle attacks, unfortunately, since HTTP requests are unencrypted.

Sessions Using GET or POST

- Pass session information to the web server each time the user navigates to a new page using GET or POST requests.
- This method is particularly susceptible to man-in-the-middle attacks, unfortunately, since HTTP requests are unencrypted.
- Use HTTPS.

Cookies

Cookies

- Small packets of data, called cookies, which are sent to the client by the web server and stored on the client’s machine.

Cookies

- Small packets of data, called cookies, which are sent to the client by the web server and stored on the client’s machine.
- When the user revisits the web site, these cookies are returned, unchanged, to the server, which can then “remember” that user and access their session information.

Cookies

- Small packets of data, called cookies, which are sent to the client by the web server and stored on the client’s machine.
- When the user revisits the web site, these cookies are returned, unchanged, to the server, which can then “remember” that user and access their session information.
- SOP policy is applicable to who access the cookies

Cookies

- Small packets of data, called cookies, which are sent to the client by the web server and stored on the client's machine.
- When the user revisits the web site, these cookies are returned, unchanged, to the server, which can then "remember" that user and access their session information.
- SOP policy is applicable to who access the cookies
- Contains sensitive information!

Session Hijacking

- Leakage of HTTP session information may lead to an attack called *session hijacking.*
  - Stealing of session ID/cookies allows an attacker to impersonate an ongoing session
  - Replay of a session to repeat some important action.

Phishing

Phishing

- Forged web pages created to fraudulently acquire sensitive information

Phishing

- Forged web pages created to fraudulently acquire sensitive information
- User typically solicited to access phished page from spam email

Phishing

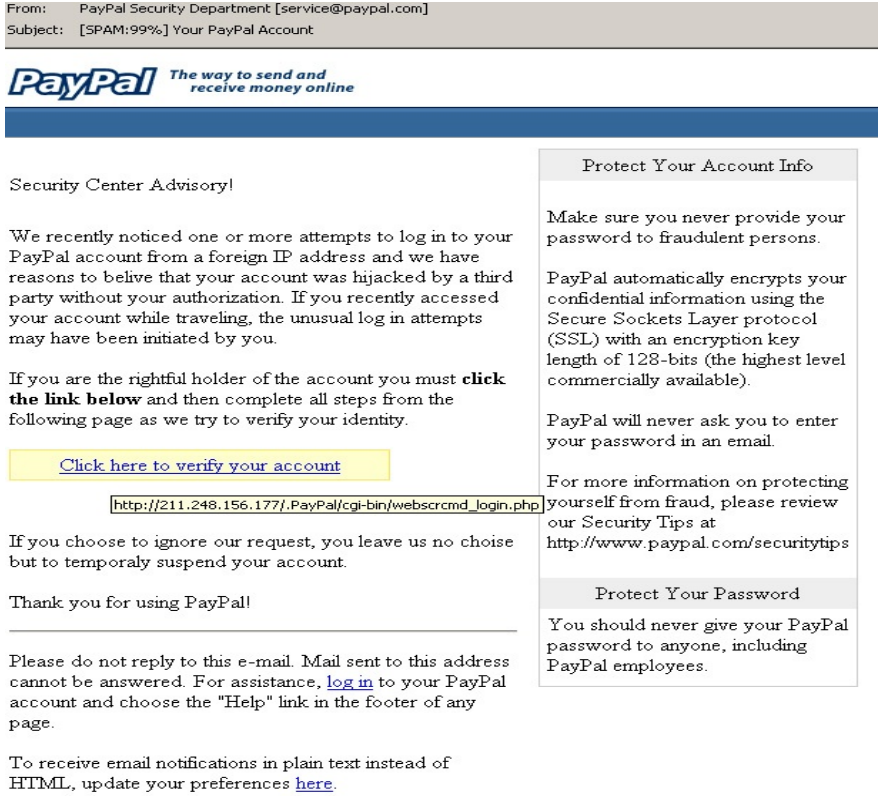
- Forged web pages created to fraudulently acquire sensitive information
- User typically solicited to access phished page from spam email
- Most targeted sites
  - Financial services (e.g., Citibank)
  - Payment services (e.g., PayPal)
  - Auctions (e..g, eBay)

Phishing

- Forged web pages created to fraudulently acquire sensitive information
- User typically solicited to access phished page from spam email
- Most targeted sites
  - Financial services (e.g., Citibank)
  - Payment services (e.g., PayPal)
  - Auctions (e..g, eBay)
- Methods to avoid detection
  - Misspelled URL
  - URL obfuscation
  - Removed or forged address bar

Phishing

- Forged web pages created to fraudulently acquire sensitive information
- User typically solicited to access phished page from spam email
- Most targeted sites
  - Financial services (e.g., Citibank)
  - Payment services (e.g., PayPal)
  - Auctions (e..g, eBay)
- Methods to avoid detection
  - Misspelled URL
  - URL obfuscation
  - Removed or forged address bar



From: PayPal Security Department [service@paypal.com]
Subject: [SPAM:99%] Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

http://211.248.156.177/.PayPal/cgi-bin/webscrcmd_login.php

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal!

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

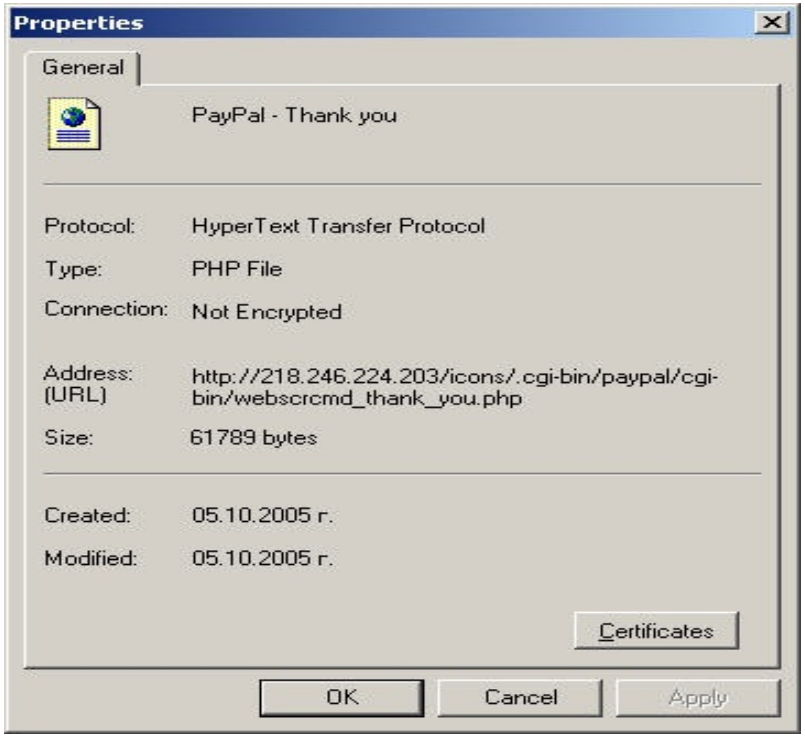
For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

URL Obfuscation

- Properties of page in previous slide
  - Actual URL different from spoofed URL displayed in address bar
- URL escape character attack
  - Old versions of Internet Explorer did not display anything past the Esc or null character
  - Displayed vs. actual site http://trusted.com%01%00@malicious.com
- Unicode attack
  - Domains names with Unicode characters can be registered
  - Identical, or very similar, graphic rendering for some characters
  - E.g., Cyrillic and Latin “p”
  - Phishing attack on paypal.com



Click-Jacking

Click-Jacking

- Click-jacking is a form of web site exploitation

Click-Jacking

- Click-jacking is a form of web site exploitation
- A user’s mouse click on a page is used in a way that was not intended by the user

Click-Jacking

- Click-jacking is a form of web site exploitation
- A user’s mouse click on a page is used in a way that was not intended by the user
- For example

Click-Jacking

- Click-jacking is a form of web site exploitation
- A user’s mouse click on a page is used in a way that was not intended by the user
- For example
- `<a onMouseUp=window.open("http://www.evilsite.com") href="http://www.trustedsite.com/">Trust me!</a>`