Web Security

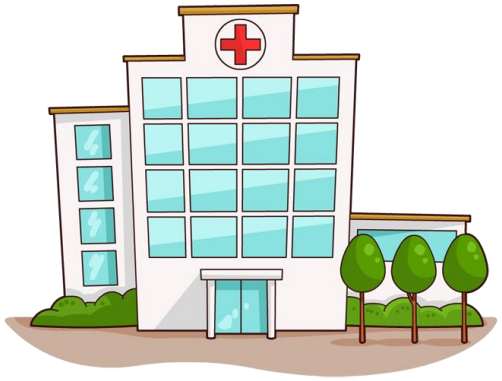
EECS 195

Spring 2019

Zhou Li

Security issues at Web

Email



Hospital Information System

Network

Shared workstation

Attacks:

- *Spam, Phishing*
- *Injection attacks*
- *Malicious webpage*

Website

Objectives

- Background: Web and Browsers
- Attacks against browsers
- Fake and malicious websites
- Attacks targeting sensitive data
- Browser and Web policies
- Injection attacks
- Spam
- Phishing attacks

What is the Web?

- A platform for deploying applications, *portably* and *securely*

client

server

HTML

- Hypertext markup language (HTML)
  - Describes the content and formatting of Web pages
  - Rendered within browser window
- HTML features
  - Static document description language
  - Supports linking to other pages and embedding images by reference
  - User input sent to server via forms
  - Embedding programs in supported languages (e.g., JavaScript, Java) provides dynamic content that interacts with the user

JavaScript

- Powerful web page *programming language*
- Scripts are embedded in web pages returned by web server
- Scripts are executed by browser (client side scripting). Can:
  - Alter page contents
  - Track events (mouse clicks, motion, keystrokes)
  - Read/set cookies
  - Issue web requests, read replies
- *(Note: despite name, has nothing to do with Java!)*

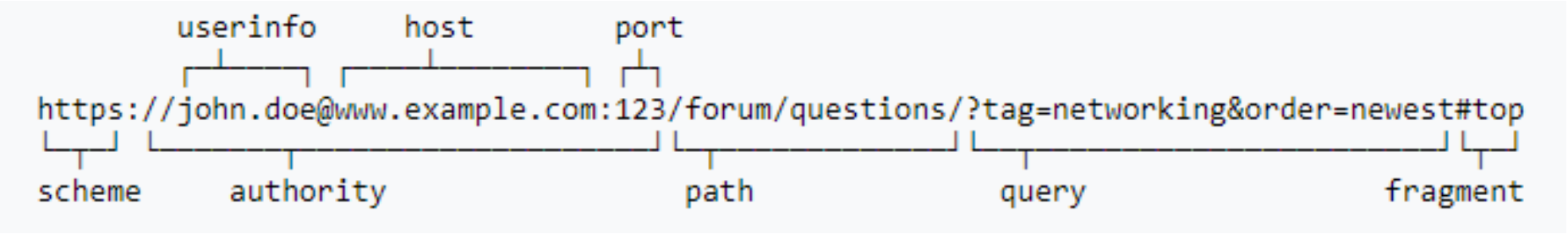
JavaScript

- Code enclosed within **<script>** … **</script>** tags
- Defining functions:

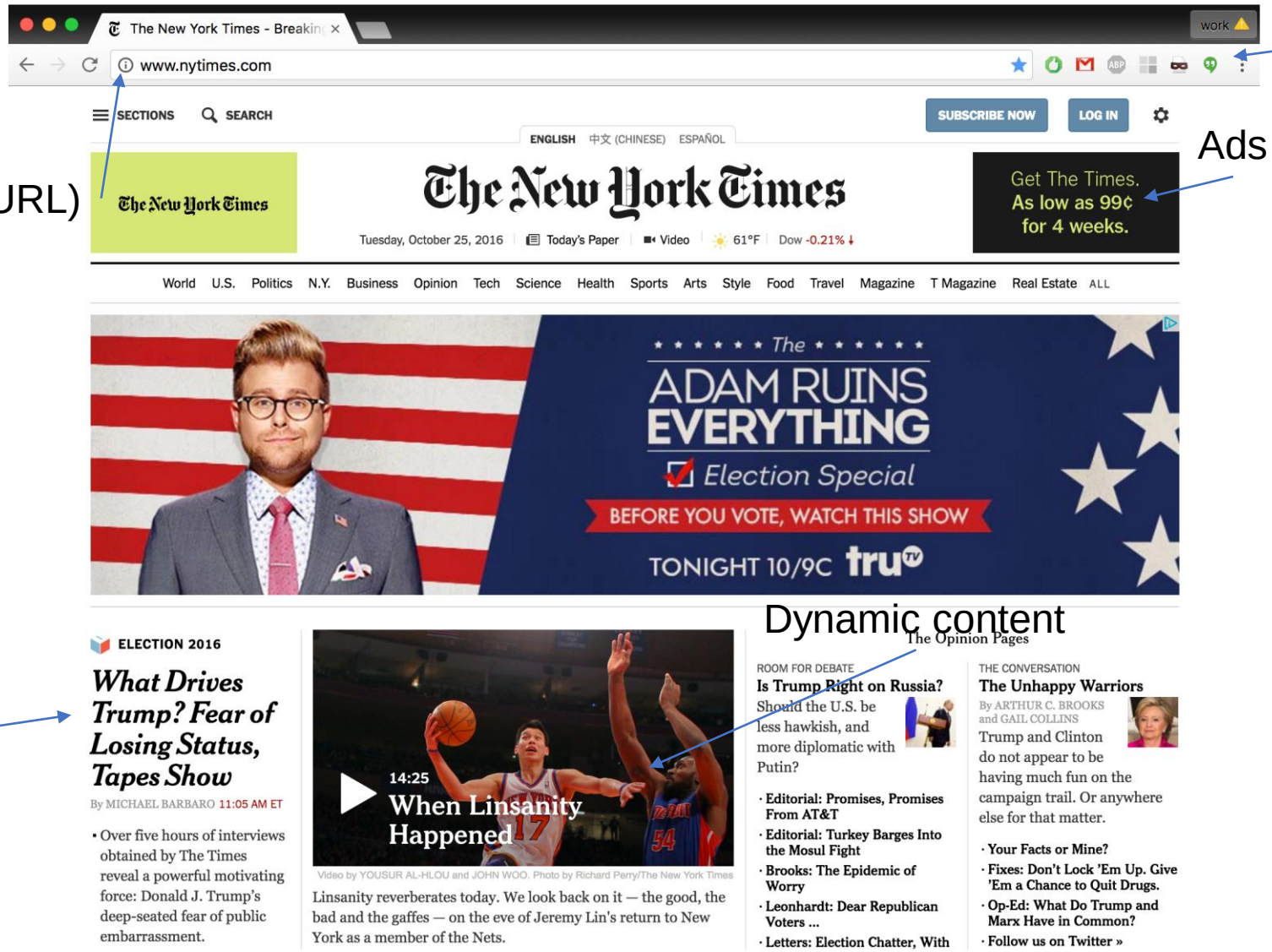
```
<script type="text/javascript">
  function hello() { alert("Hello world!"); }
</script>
```

URLs

- Global identifiers of network-retrievable documents
- Example:



Browser


Add-on
Address bar (URL)
Ads
Dynamic content
HTML
The New York Times - Breaking
work
www.nytimes.com
SECTIONS
SEARCH
SUBSCRIBE NOW
LOG IN
ENGLISH 中文 (CHINESE) ESPAÑOL
The New York Times
Tuesday, October 25, 2016
Today's Paper
Video
61°F
Dow -0.21%
Get The Times.
As low as 99¢
for 4 weeks.
World U.S. Politics N.Y. Business Opinion Tech Science Health Sports Arts Style Food Travel Magazine T Magazine Real Estate ALL
The
ADAM RUINS EVERYTHING
Election Special
BEFORE YOU VOTE, WATCH THIS SHOW
TONIGHT 10/9C truTV
ELECTION 2016
What Drives Trump? Fear of Losing Status, Tapes Show
By MICHAEL BARBARO 11:05 AM ET
• Over five hours of interviews obtained by The Times reveal a powerful motivating force: Donald J. Trump's deep-seated fear of public embarrassment.
14:25
When Linsanity Happened
Video by YOUSUR AL-HLOU and JOHN WOO. Photo by Richard Perry/The New York Times
Linsanity reverberates today. We look back on it — the good, the bad and the gaffes — on the eve of Jeremy Lin's return to New York as a member of the Nets.
The Opinion Pages
ROOM FOR DEBATE
Is Trump Right on Russia?
Should the U.S. be less hawkish, and more diplomatic with Putin?
· Editorial: Promises, Promises From AT&T
· Editorial: Turkey Barges Into the Mosul Fight
· Brooks: The Epidemic of Worry
· Leonhardt: Dear Republican Voters ...
· Letters: Election Chatter, With
THE CONVERSATION
The Unhappy Warriors
By ARTHUR C. BROOKS and GAIL COLLINS
Trump and Clinton do not appear to be having much fun on the campaign trail. Or anywhere else for that matter.
· Your Facts or Mine?
· Fixes: Don't Lock 'Em Up. Give 'Em a Chance to Quit Drugs.
· Op-Ed: What Do Trump and Marx Have in Common?
· Follow us on Twitter »

Security on the web

- Integrity
  - malicious web sites should not be able to tamper with integrity of my computer or my information on other web sites
- Confidentiality
  - malicious web sites should not be able to learn confidential information from my computer or other web sites
- Privacy
  - malicious web sites should not be able to spy on me or my activities online

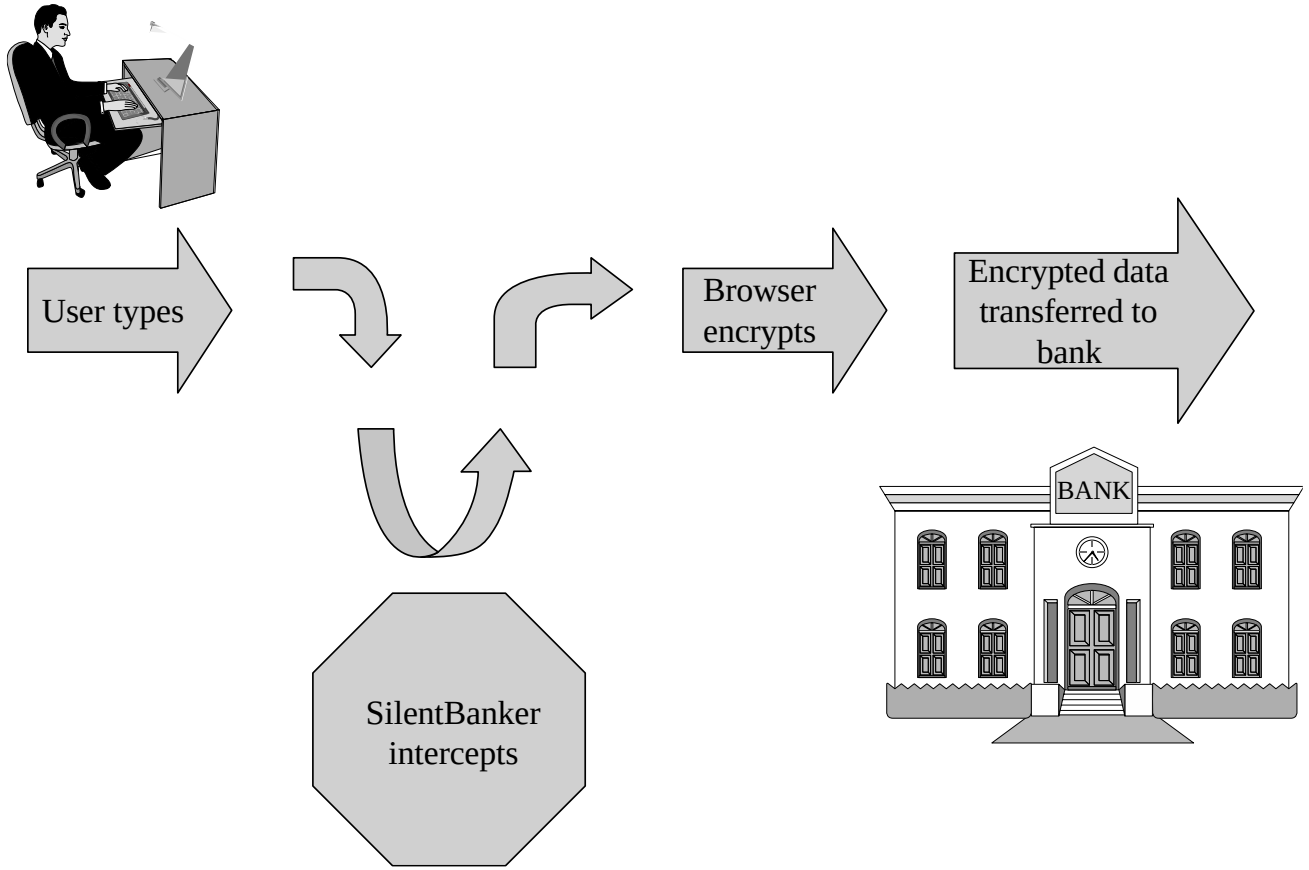
Web Attack by Changing Content

- Man-in-the-browser
- Page-in-the-middle
- Program download substitution
- User-in-the-middle

Man-in-the-Browser

- Trojan horse that intercepts data passing through the browser

- Example: SilentBanker
  - Discovered in 2008
  - Fake browser add-on
  - Intercept users keystrokes on popular banks
  - Redirect keystrokes and customer details to attacker server
  - Even modify account fields

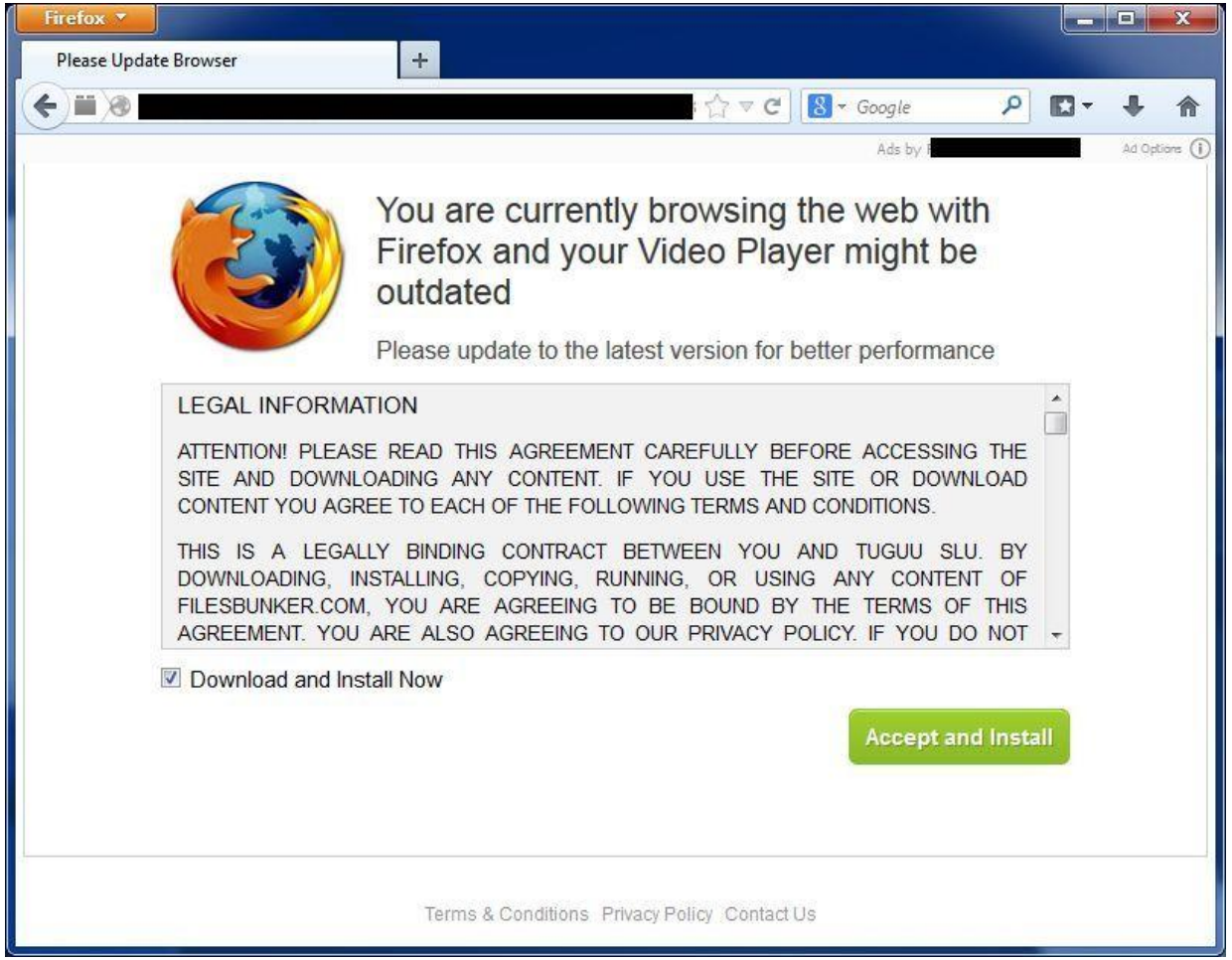


Page-in-the-Middle

- User is directed to a different page than believed or intended
- Similar effect to a man-in-the-browser, where attacker can intercept and modify user input
- Root-cause: no encryption and authentication protection (e.g., using HTTP rather than HTTPS)

Program Download Substitution

- Attacker creates a page with seemingly innocuous and desirable programs for download
- Instead of, or in addition to, the intended functionality, the user installs malware



User-in-the-Middle

- Using click-bait to trick users into solving CAPTCHAs on spammers' behalf

Hackers Offer Free Porn To Beat Security Checks

Spammers are enticing consumers with free porn or games in exchange for help cracking CAPTCHAs on targeted websites, security researchers say.

How browser attacks succeed

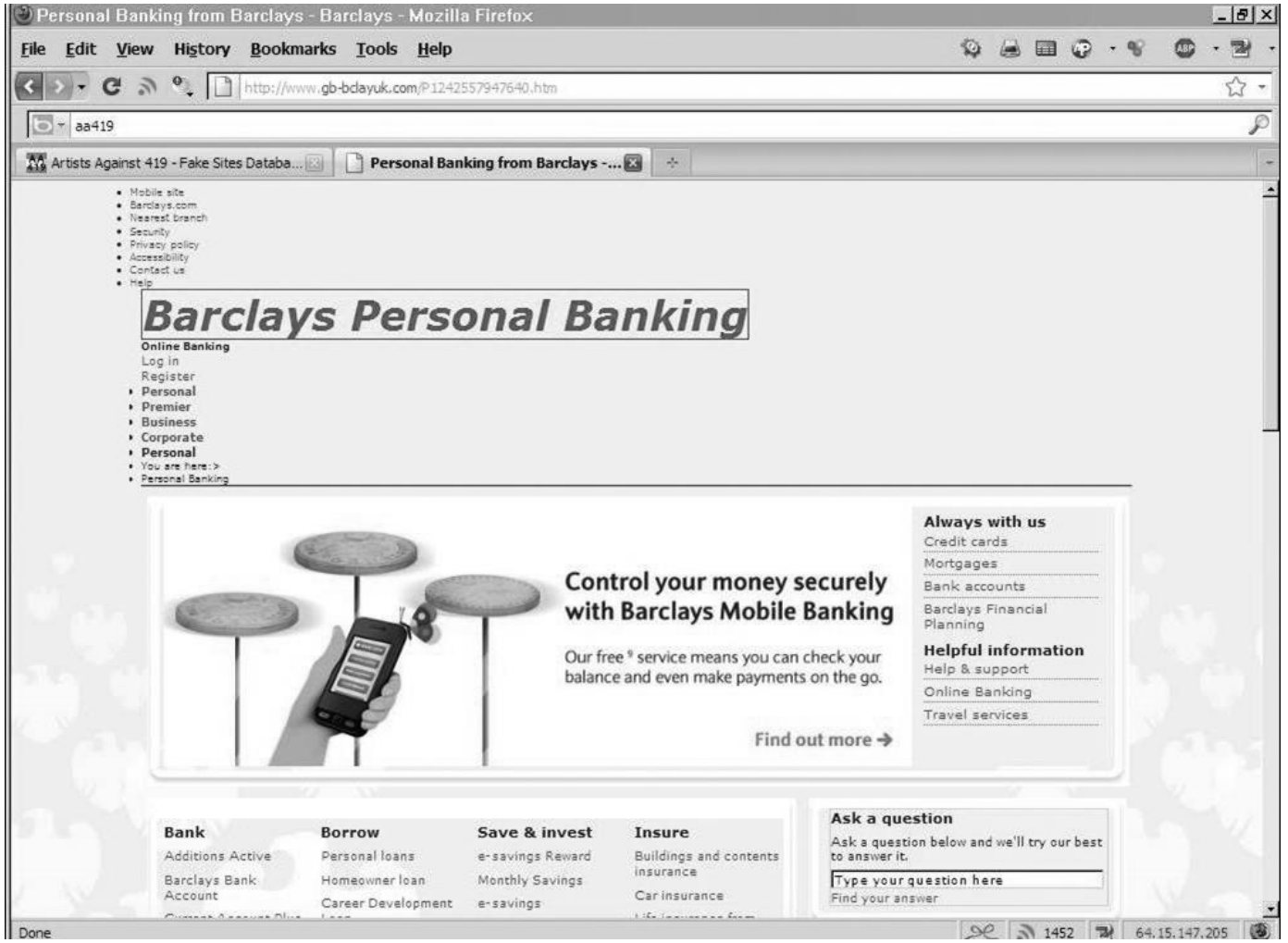
- The attacks listed above are largely failures of authentication
  - How does your bank authenticate you?
  - How do you authenticate your bank?
- Some solutions
  - Encryption and PKI
  - Tokens (e.g., USB drive distributed by bank)
  - Out-of-band communication (PIN mailed by bank)
  - Continuous authentication

Fingerprint scanner for bank website

Protecting website against change

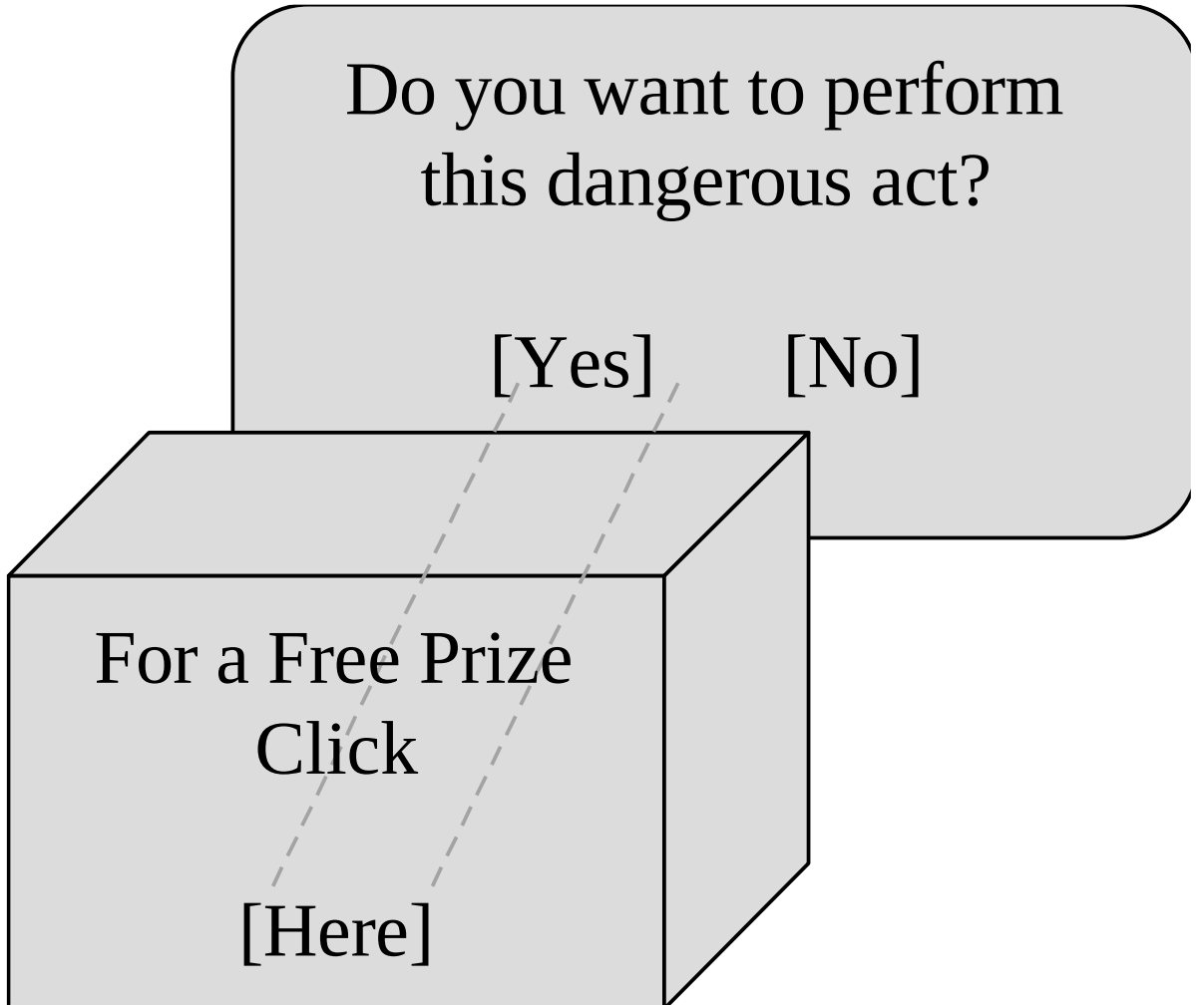
- Integrity checksums
  - Detect altered content on a website
  - The web owner runs the check frequently
  - Problem: what if a website is developed by third-party or using third-party libraries?
- Signed code or data
  - A signer creates digital signatures for program and data
  - The web user verifies the digital signature
  - Infrastructure of PKI can be leveraged

Fake Website (Phishing)



Clickjacking

- Tricking a user into clicking a link by disguising what the link points to
- Can be done through dialog overlaying



JavaScript for Clickjacking

- Built-in functions can change content of window: **Click-jacking attack**

```
<a onMouseUp="window.open(‘http://www.evilsite.com’)"
href="http://www.trustedsite.com/">Trust me!</a>
```

Drive-By Download

- Code is downloaded, installed, and executed on a computer without the user's knowledge
- May be the result of clickjacking, fake code, program download subsitution, browser vulnerabilities, etc.
- Popular exploited vulnerabilities
  - JavaScript
  - Adobe Flash
  - Java applet
  - ActiveX component