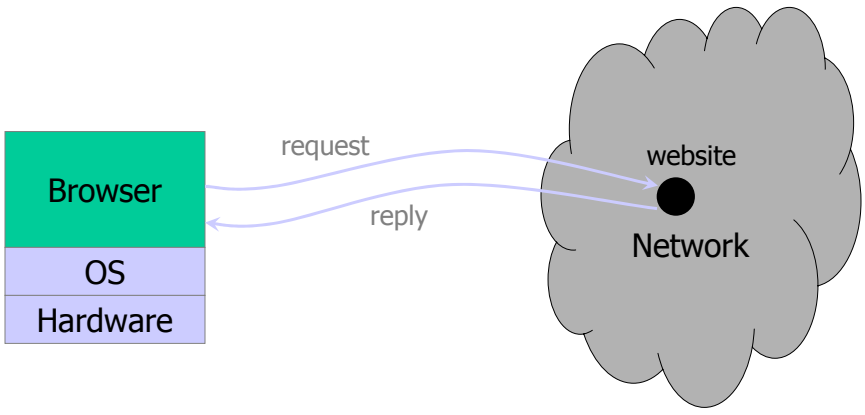
Web Security

Web basics

http security

1

Browser and network



2

INTERNETWEEK.com
CONNECTING THE ENTERPRISE, CUSTOMERS & SUPPLIERS

February 12, 2002

Microsoft Issues New IE Browser Security Patch

By Richard Karpinski

- Microsoft has released a security patch that closes some major holes in its Internet Explorer browser
- The so-called "cumulative patch" fixes six different IE problems
- Affected browsers include Internet Explorer 5.01, 5.5 and 6.0
- Microsoft rated the potential security breaches as "critical"

3

Fixed by the February 2002 patch

- Buffer overrun associated with an HTML directive
  - Could be used by hackers to run malicious code on a user's system
- Scripting vulnerability
  - Lets an attacker read files on a user's system
- Vulnerability related to the display of file names
  - Hackers could misrepresent the name of a file and trick a user into downloading an unsafe file
- … and many more

On April 13, 2004, MS announced 20 new vulnerabilities

4

October 12, 2004

Microsoft Security Bulletin MS04-038

If a user is logged on with administrative privileges, an attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. […] Microsoft recommends that customers install the update immediately.

Cascading Style Sheets (CSS) Heap Memory Corruption Vulnerability	Critical
Similar Method Name Redirection Cross Domain Vulnerability	Critical
Install Engine Vulnerability	Critical
SSL Caching Vulnerability	Moderate
Aggregate Severity of All Vulnerabilities	**Critical**

5

December 13, 2005

Microsoft Security Bulletin MS05-054

If a user is logged on with administrative user rights, an attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. […] We recommend that customers apply the update immediately.

File Download Dialog Box Manipulation Vulnerability	Moderate
HTTPS Proxy Vulnerability	Moderate
COM Object Instantiation Memory Corruption Vulnerability	Critical
Mismatched Document Object Model Objects Memory Corruption Vulnerability	Critical
Aggregate Severity of All Vulnerabilities	**Critical**

6

January 7, 2007

Microsoft Security Bulletin MS07-004

A remote code execution vulnerability exists in the Vector Markup Language (VML) implementation in Microsoft Windows. An attacker could exploit the vulnerability by constructing a specially crafted Web page or HTML e-mail that could potentially allow remote code execution if a user visited the Web page or viewed the message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Maximum Severity Rating: Critical

Recommendation: Customers should apply the update immediately

7

Many other vulnerabilities

- Check out http://www.microsoft.com/technet/security/
- 44 "critical" updates related to Internet Explorer 6.0 between October 10, 2001, and January 9, 2007

8

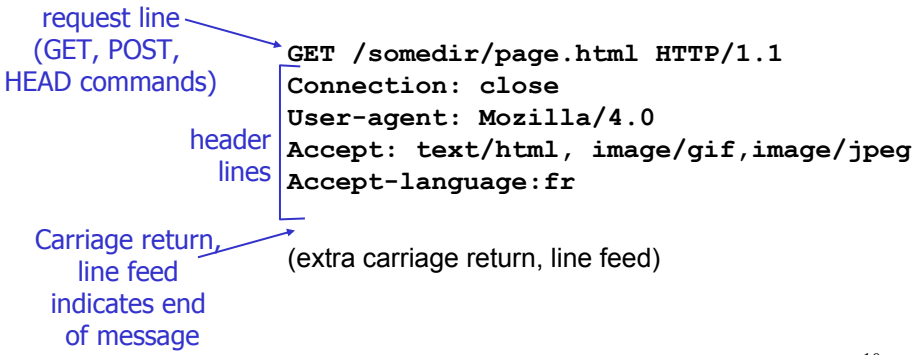
HTTP: HyperText Transfer Protocol

- Used to request and return data
  - Methods: GET, POST, HEAD, …
- Stateless request/response protocol
  - Each request is independent of previous requests
  - Statelessness has a significant impact on design and implementation of applications
- Evolution
  - HTTP 1.0: simple
  - HTTP 1.1: more complex

9

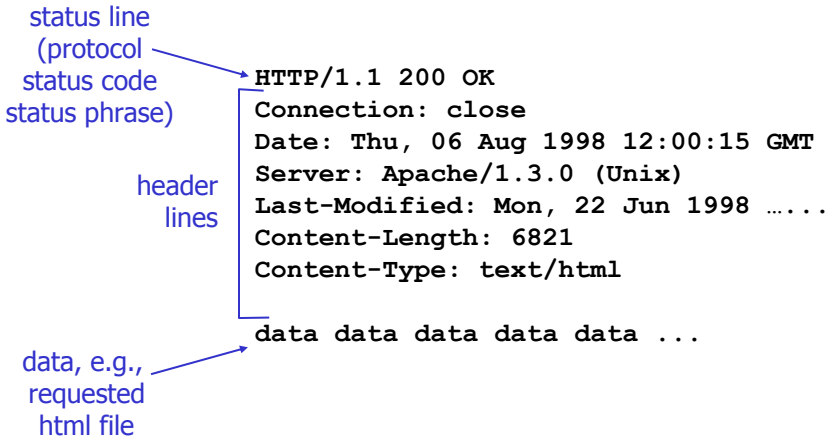
HTTP protocol message format:

- Two types of http messages: *request*, *response*
- http request message:
  - ASCII (human-readable format)



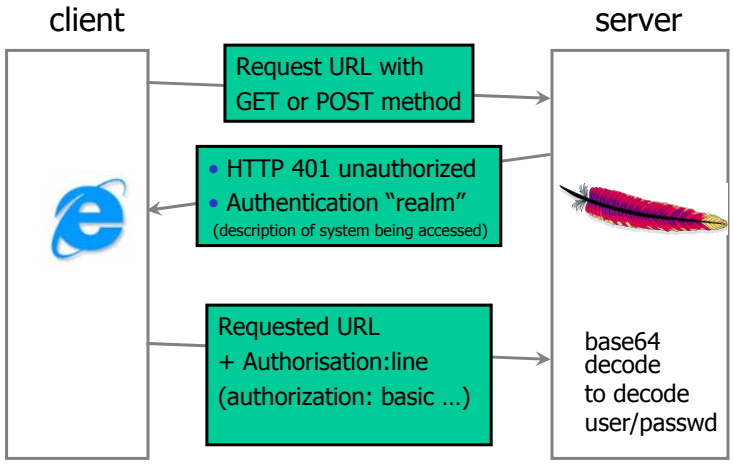
10

HTTP message format: reply



11

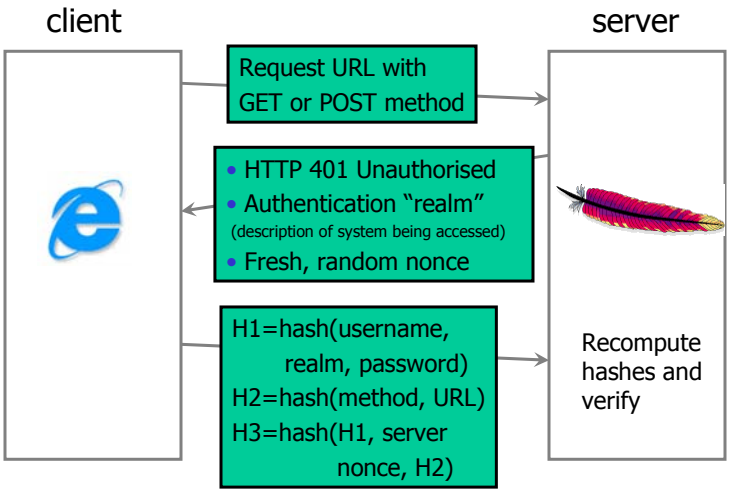
HTTP authentication



E.g.: Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

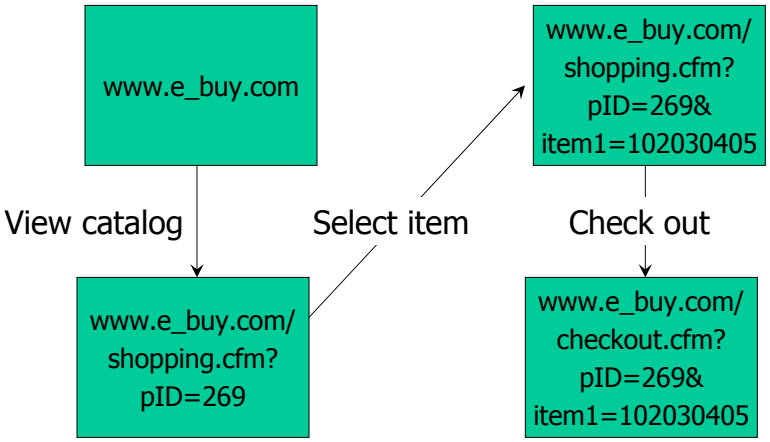
12

HTTP digest authentication



13

Primitive browser session



Store session information in URL; easily read on network

14

FatBrain.com circa 1999 [due to Fu et al.]

- User logs into website, authenticator is generated, user is given special URL containing authenticator

  https://www.fatbrain.com/HelpAccount.asp?
  t=0&p1=me@me.com&p2=540555758

  - Special URL, user doesn't need to re-authenticate
    Reasoning: user could not have not known the special URL without authenticating first. That's true, BUT…
- Authenticators are global sequence numbers
  - It's easy to guess sequence number for another user

    https://www.fatbrain.com/HelpAccount.asp?
    t=0&p1=SomeoneElse&p2=540555752

  - Fix: use random authenticators

15

Bad idea: encoding state in URL

- Unstable, frequently changing URLs
- Vulnerable to eavesdropping / Web proxies!
- There is no guarantee that URL is private
  - Early versions of Opera used to send entire browsing history, including all visited URLs, to Google

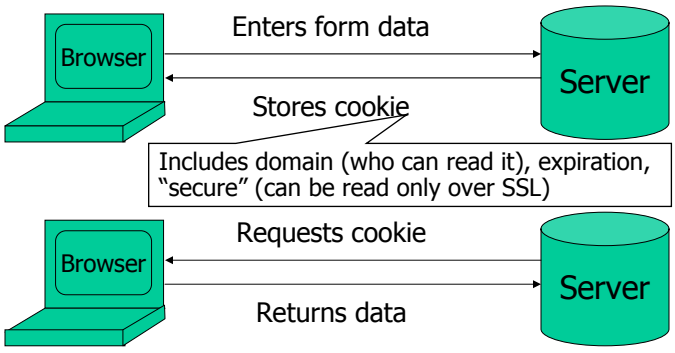
16

Cookies

17

Storing info across sessions

- A cookie is a file created by an Internet site to store information on your computer



HTTP is a stateless protocol; cookies add state

18

What are cookies used for?

- Authentication
  - Use the fact that the user authenticated correctly in the past to make future authentication quicker
- Personalization
  - Recognize the user from a previous visit
- Tracking
  - Follow the user from site to site; learn his/her browsing behavior, preferences, and so on

19

Cookie management

- Cookie ownership
  - Once a cookie is saved on your computer, only the website that created the cookie can read it
- Variations
  - Temporary cookies
    - Stored until you quit your browser
  - Persistent cookies
    - Remain until deleted or expire
  - Third-party cookies
    - Originates on or sent to another website

20

Privacy issues with cookies

- Cookie may include any information about you known by the website that created it
  - Browsing activity, account information, etc.
- Sites can share this information
  - Advertising networks
  - 2o7.net tracking cookie
- Browser attacks could invade your "privacy"

  November 8, 2001:

  Users of Microsoft's browser and e-mail programs could be vulnerable to having their browser cookies stolen or modified due to a new security bug in Internet Explorer (IE), the company warned today

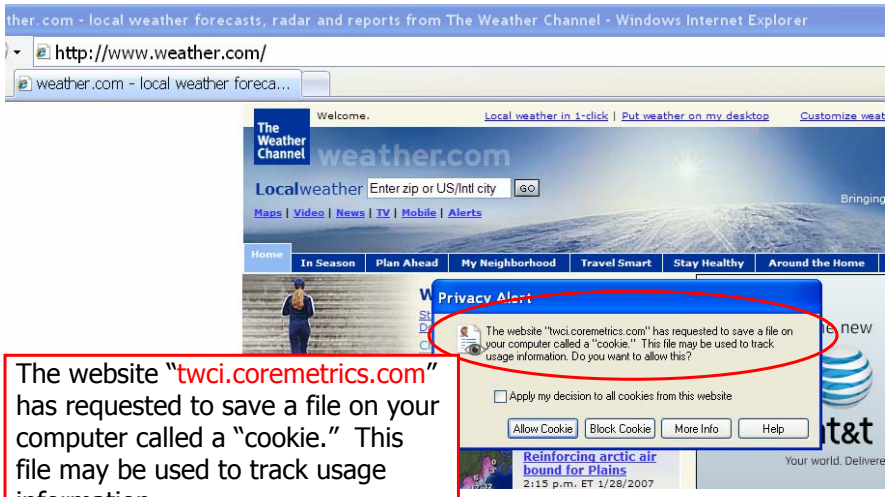
21

Austin American-Statesman

The website "adinterax.com" has requested to save a file on your computer called a "cookie." This file may be used to track usage information…

22

The Weather Channel



The website "twci.coremetrics.com" has requested to save a file on your computer called a "cookie." This file may be used to track usage information…

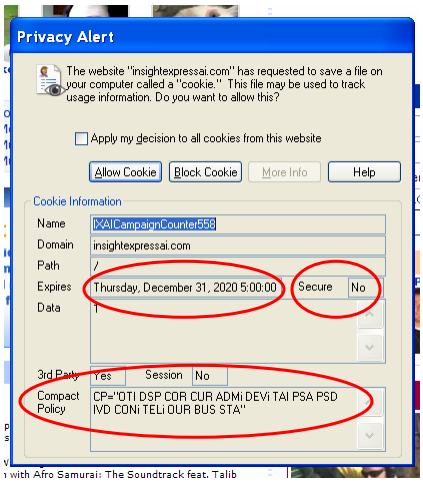
23

MySpace

The website "insightexpressai.com" has requested to save a file on your computer called a "cookie"…

24

Let's take a closer look…



Storing state in browser

- Dansie Shopping Cart (2006)
  - "A premium, comprehensive, Perl shopping cart. Increase your web sales by making it easier for your web store customers to order."

```
<FORM METHOD=POST
 ACTION="http://www.dansie.net/cgi-bin/scripts/cart.pl">

  Black Leather purse with leather straps<

  <INPUT TYPE=HIDDEN NAME=name      VALUE="Black leather purse">
  <INPUT TYPE=HIDDEN NAME=price     VALUE="20.00">
  <INPUT TYPE=HIDDEN NAME=sh        VALUE="1">
  <INPUT TYPE=HIDDEN NAME=img       VALUE="p
  <INPUT TYPE=HIDDEN NAME=custom1   VALUE="B
       with leather straps">

  <INPUT TYPE=SUBMIT NAME="add" VALUE="Put in Shopping Cart">

</FORM>
```

Change this to 2.00

Bargain shopping!

Shopping cart form tampering

http://xforce.iss.net/xforce/xfdb/4621

- Many Web-based shopping cart applications use hidden fields in HTML forms to hold parameters for items in an online store. These parameters can include the item's name, weight, quantity, product ID, and price. Any application that bases price on a hidden field in an HTML form is vulnerable to price changing by a remote user. A remote user can change the price of a particular item they intend to buy, by changing the value for the hidden HTML tag that specifies the price, to purchase products at any price they choose.
- **Platforms Affected:**
  - 3D3.COM Pty Ltd: ShopFactory 5.8 and earlier
  - Adgrafix: Check It Out Any version
  - ComCity Corporation: SalesCart Any version
  - Dansie.net: Dansie Shopping Cart Any version
  - Make-a-Store: Make-a-Store OrderPage Any version
  - McMurtrey/Whitaker & Associates: Cart32 3.0
  - Rich Media Technologies: JustAddCommerce 5.0
  - Web Express: Shoptron 1.2
  - @Retail Corporation: @Retail Any version
  - Baron Consulting Group: WebSite Tool Any version
  - Crested Butte Software: EasyCart Any version
  - Intelligent Vending Systems: Intellivend Any version
  - McMurtrey/Whitaker & Associates: Cart32 2.6
  - pknutsen@nethut.no: CartMan 1.04
  - SmartCart: SmartCart Any version

27

Storing State in Browser Cookies

- Set-cookie: price=299.99
- User edits the cookie… cookie: price=29.99
- What's the solution?
- Add a MAC to every cookie, computed with the server's secret key
  - Price=299.99; HMAC(ServerKey, 299.99)
- But what if the website changes the price?

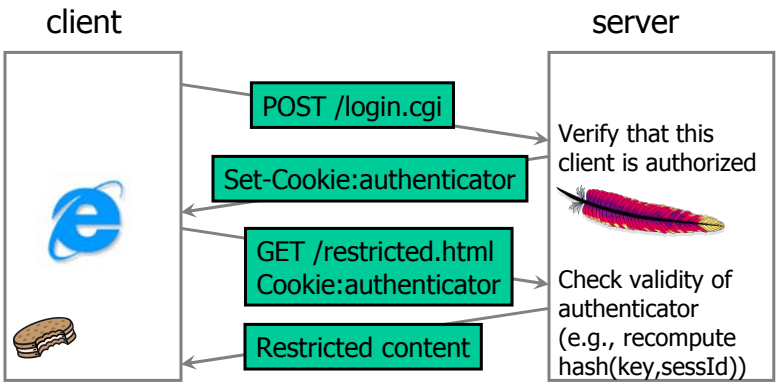
28

Web authentication via cookies

- Need authentication system that works over HTTP and does not require servers to store session data
  - Why is it a bad idea to store session state on server?
- Servers can use cookies to store state on client
  - When session starts, server computes an authenticator and gives it back to browser in the form of a cookie
    - Authenticator is a value that client cannot forge on his own
    - Example: hash(server's secret key, session id)
  - With each request, browser presents the cookie
  - Server recomputes and verifies the authenticator
    - Server does not need to remember the authenticator

29

Typical session with cookies



Authenticators must be unforgeable and tamper-proof
(malicious client shouldn't be able to compute his own or modify an existing authenticator)

30

WSJ.com circa 1999 [due to Fu et al.]

- Idea: use user,hash(user,key) as authenticator
  - Key is secret and known only to the server. Without the key, clients can't forge authenticators.
- Implementation: user,crypt(user,key)
  - crypt() is UNIX hash function for passwords
  - crypt() truncates its input at 8 characters
  - Usernames matching first 8 characters end up with the same authenticator
  - No expiration or revocation
- It gets worse… This scheme can be exploited to extract the server's secret key

31

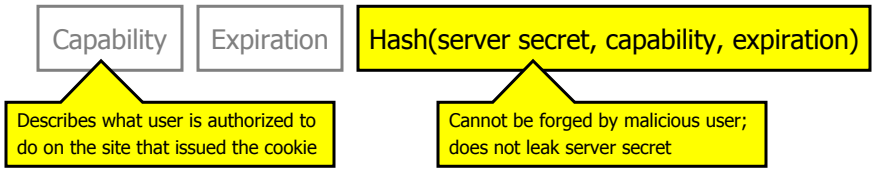
Attack

username	crypt(username,key,"00")	authenticator cookie
VitalySh1	008H8LRfzUXvk	VitalySh1008H8LRfzUXvk
VitalySh2	008H8LRfzUXvk	VitalySh2008H8LRfzUXvk
Create an account with a 7-letter user name…		
VitalySA	0073UYEre5rBQ	Try logging in: access refused
VitalySB	00bkHcfOXBKno	Access refused
VitalySC	00ofSJV6An1QE	Login successful! 1st key symbol is C
Now a 6-letter user name…		
VitalyCA	001mBnBErXRuc	Access refused
VitalyCB	00T3JLLfuspdo	Access refused… and so on

- Only need 128 x 8 queries instead of intended 128^8
- 17 minutes with a simple Perl script vs. 2 billion years

32

Better Cookie Authenticator



- Main lesson: don't roll your own!
  - Homebrewed authentication schemes are often flawed
- There are standard cookie-based schemes
  - We'll see one when discussing IPSec

33