Introduction

WEB DEVELOPMENT FUNDAMENTALS

Introduction

- Objectives
  - To explain the aims and objectives of the course
  - To construct a simple web page using an ASCII text editor
  - To display that page using a browser
- Contents
  - Course administration
  - Course aims and objectives
  - Web introduction
  - The Internet, Intranets and Extranets
  - Web browsers
  - Web server software
  - Development tools
- Practical exercise
  - Building a simple web page
- Summary

2

Administration

- Front door security
- Name card
- Chairs

- Fire exits
- Toilets
- Smoking
- Coffee Room

- Timing
- Breaks
- Lunch

- Downloads & Viruses
- Admin support
- Messages

- Taxis
- Trains/Coaches
- Hotels

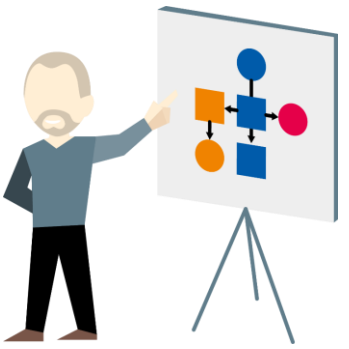
- First Aid

- Telephones/Mobiles

3

Course delivery

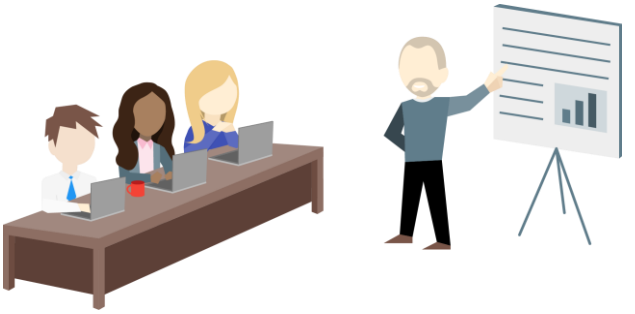
- The course material is covered in a number of ways
  - Lecture material
  - Demonstrations
  - Course workbooks
  - Practical exercise sessions



4

The training experience

- A course should be
  - A two-way process
  - A group process
  - An individual experience



5

Introductions

- Please say a few words about yourself, for the benefit of the group...
- What is your job?
- What is your experience of
  - HTML?
  - Web Administration?
  - Programming?
- What do you want from the course?

6

Course aims and objectives

At the end of this course you will be able to:

- Appreciate the underlying web technologies including URLs, HTTP and MIME
- Use the most common functions of HTML and work with graphics
- Build HTML forms
- Work with linked, embedded and inline CSS
- Understand absolute and relative CSS positioning
- Understand the principles of client side scripting with JavaScript

7

Evolution of the Web

- Hypertext
  - Text with embedded pointers to other text and pictures
  - Works by association, a metaphor for the human mind
  - Hypermedia extends concept to any media format
- Hypertext/Hypermedia systems
  - Ted Nelson's Project Xanadu (1964)
  - Interactive CD ROM
  - The World Wide Web (WWW)
- Gopher - Menu based Hypertext system
- World Wide Web - Tim Berners-Lee at CERN (1989)
  - First text clients in February 1991; Mosaic adds graphics in 1993

8

Terminology

- Browser
  - What the user sees: the client
- The term 'server' refers both to
  - A computer holding all the pages and resources for a web site
  - The HTTP server software
- HTTP = Hypertext Transfer Protocol
  - How the browser communicates with the server over a network
- HTML = Hypertext Markup Language
  - The page description language for web pages
  - Consists of text with markup tags

9

Why is the Web popular?

- Simple and open specifications
  - Specifications freely available over the Internet
  - Easy for developers to implement
- Client-Server model
  - Anyone can set-up a Web site
  - Web servers only satisfy HTTP requests
  - Intelligent Web clients (browsers) understand many different Internet protocols
- HyperText Markup Language (HTML)
  - Lightweight markup language
  - Describes document structure, not formatting
  - Portable over a range of browsers (braille, text, GUI)

10

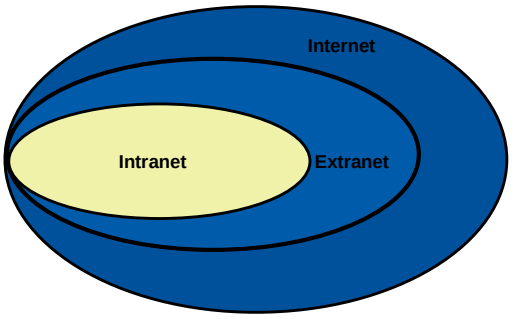
Intranets

- Based on the Internet technology using high-bandwidth available on corporate LANs
  - Corporates have both the need and the hardware
  - Internet technology is providing the software
- Benefits to an organisation include:
  - Easy information dissemination
  - Highly extensible
  - Low cost
  - Re-use of existing systems
    - Corporates can create interfaces between HTML forms and legacy applications
  - Universal Client
    - Familiar tools
    - Browsers exist for all major client systems

11

Internet, Intranets & Extranets

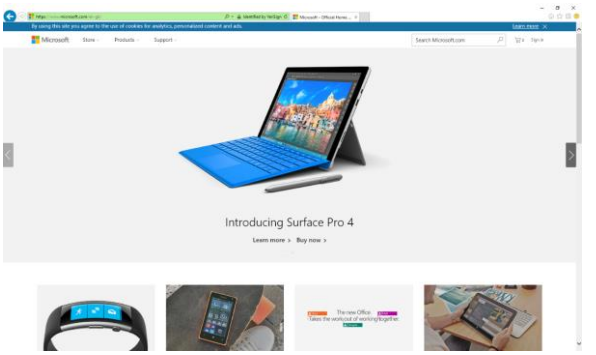
- Intranet is an internal corporate network, with access available to authorised employees only
- Extranet allows extended access to key business partners and customers



12

WWW browsers

- Multiple platforms
- GUI browsers
  - Internet Explorer / Edge
  - Firefox / Mozilla
  - Safari
  - Opera
  - Chrome
- Non-desktop browsers
  - WebTV
  - Wireless devices - Hand-held devices, Mobile phones
  - Speech synthesisers, Braille



13

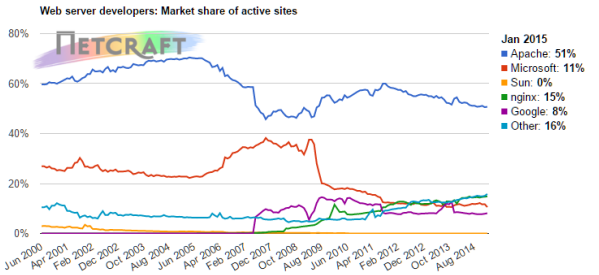
Exercise 1a

- Create and open your first web page

14

Web server software

- Web Server Software
  - Apache
  - Microsoft Internet Information Server
  - ngix (pronounced as "engine X")
  - lighttpd (pronounced "Light-TPD", abbreviated "Lighty")
  - Sun Web Server 7



- Market Share for Top Servers Across All Domains

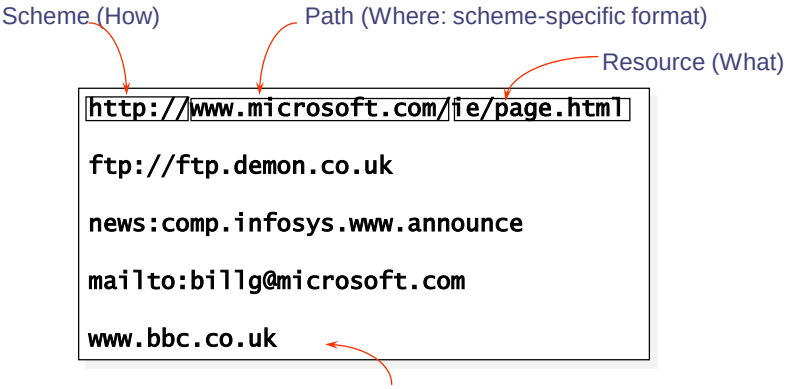
15

Introduction to URLs

- Uniform Resource Locators (URL)
  - Identifies location and protocol to access a resource
  - URLs are a form of Uniform Resource Identifier (URI)

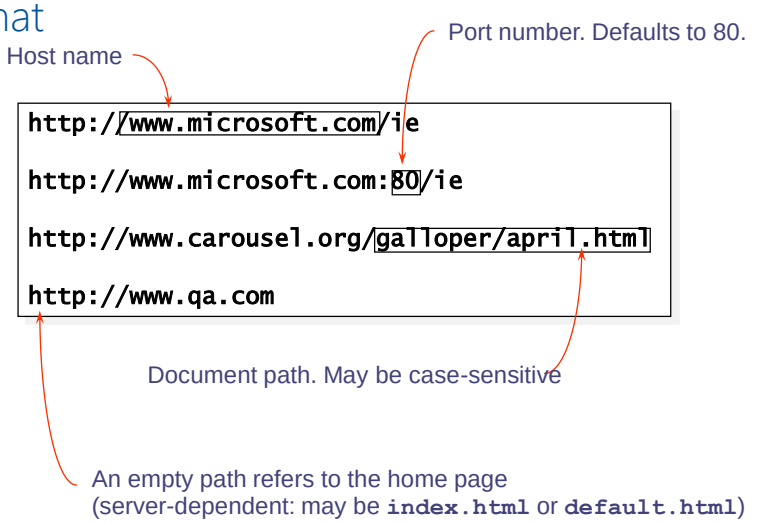
16

URL Syntax



17

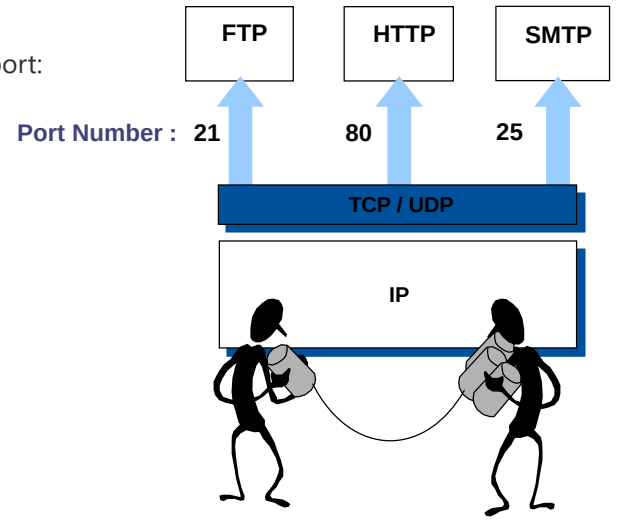
HTTP URL Format



18

Ports in Action

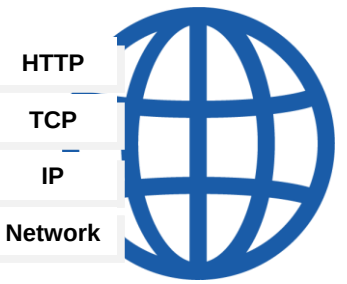
- Each process uses a different port:



19

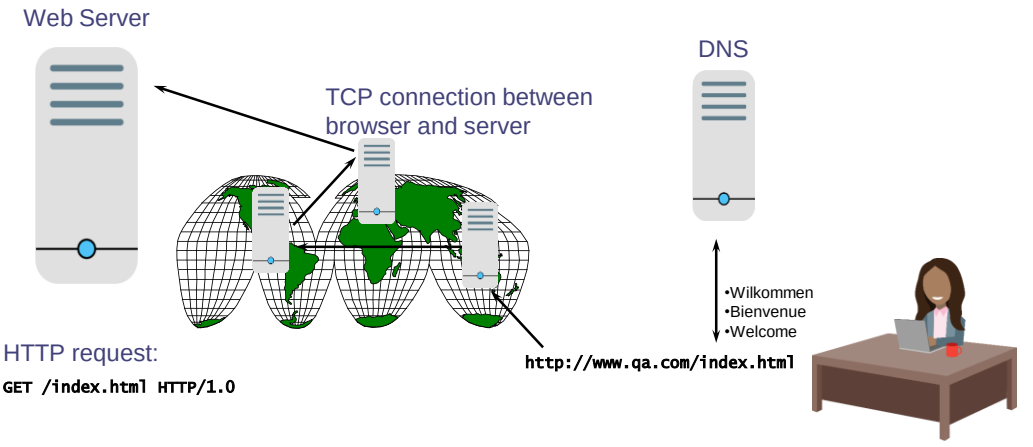
HyperText Transfer Protocol (HTTP)

- Application Level Protocol
  - Technical information at http://www.w3.org
  - TCP-based
  - Current version is 1.1
- Lightweight
  - Easy to implement clients and servers
  - Stateless: each request is independent from the others
    - Other technologies required in order to enable e-commerce, online banking, etc.
- Request/response paradigm



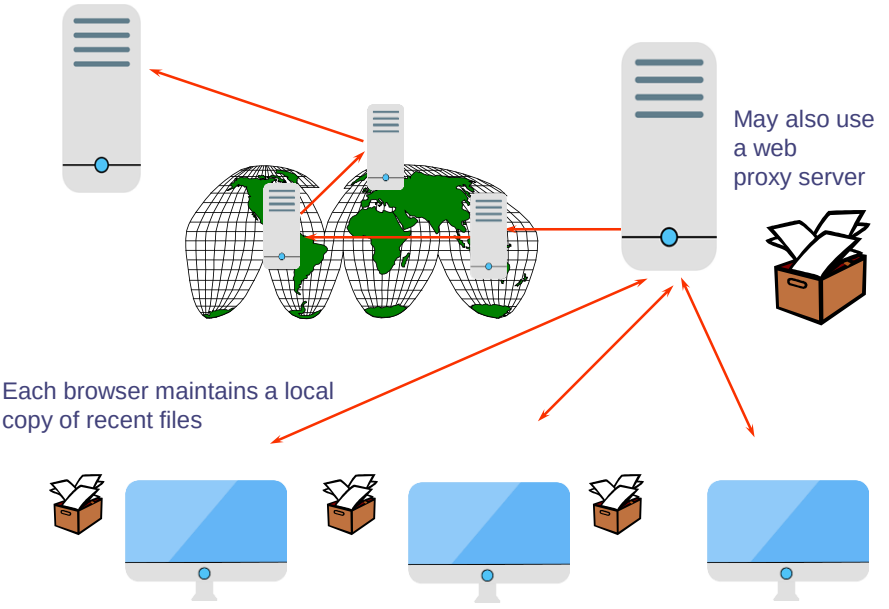
20

Principles of Browser Operation



21

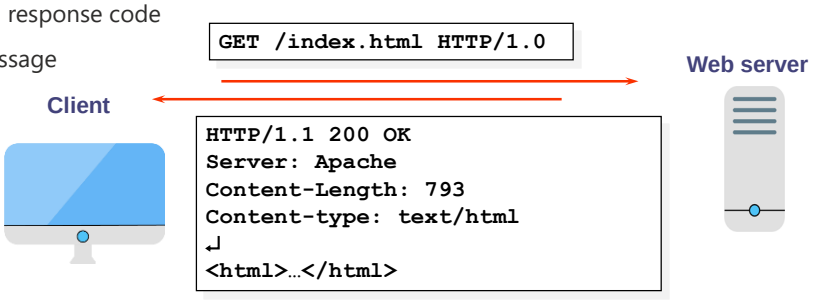
Caches



22

HTTP Interactions

- Client Request:
  - Method, Resource, HTTP version
  - MIME type header and message
- Server Response:
  - HTTP version and standard response code
  - MIME type header and message



23

HTTP Client Request

- Method
  - Action to perform on resource - GET, HEAD, POST
- Uniform Resource Identifier
  - Identifies a networked resource
  - Absolute URI used with a proxy server
  - Request URI used with an origin server
- HTTP Version
  - Major.minor version - Default (no version given) is 0.9
  - Version 1.1 now the most popular
  - Browsers and Servers must also understand both 0.9 and 1.0
- MIME-like message - Contains request modifiers and forms data

24

HTTP Server Response

- Simple Response/Full Response
- Status line
  - HTTP version
  - Standard status code
  - Reason phrase
- MIME like message
  - Generated by Web server or by backend script
  - Header fields describe the requested resource
  - Modified using HTML <meta> tag
  - Requested data
  - Header and Data are separated by CRLF pair

25

MIME and HTTP

- Multipurpose Internet Mail Extensions
  - Based on Internet Mail (RFC 822)
  - MIME is defined in RFC 1521
  - HTTP usage differs from RFC 1521
- Transmission of Multimedia Objects over Internet
  - Header consists of colon-separated fields
  - Data contains requested object
  - Content-Type field describes object
- Object Types
  - Defined by IANA
  - Consist of type/subtype
  - Unofficial types preceded by x- (x-world/x-vrml)
- Multipart Messages
  - Multiple MIME messages each containing a header specifying the type of body data

26

Exercise 1b

- Place your web page on a web server

27

Security

WEB DEVELOPMENT FUNDAMENTALS

HTTP Authentication Mechanisms

- Possible authentication mechanisms
- User/Password
  - Can allow all access (anonymous)
  - Clear-text uuencoded username and password
  - Server-specific extensions

29

Security Issues

- Preventing Eavesdropping:
  - Use of encryption
- Preventing Modification/Fabrication:
  - Authenticating Messages
- Preventing Impersonation:
  - Authenticating clients and servers

30

Protection through Encryption

- Encryption can provide protection from network data attacks
  - Internet links are not secure
  - Intranet links can be insecure
  - Encryption provides protection from Data Snooping

31

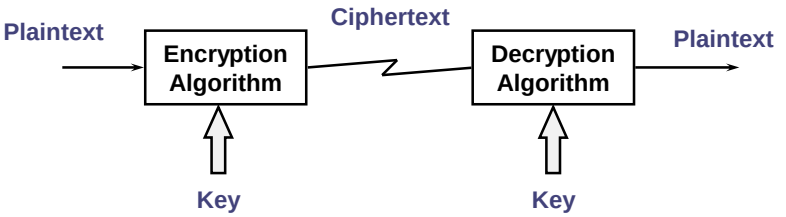
Encryption Algorithms

- Encryption algorithms have been developed over time
- Development of Cryptography
  - Early cryptography evolved well over 3000 years ago
  - Complex mathematically secure cryptography evolved 80 years ago
  - Modern public/private algorithms are 20 years old or younger
- Modern algorithms break into two classes -
  - Private Key (or Symmetric) algorithms
  - Public Key (or Asymmetric) algorithms

32

Private Key Algorithms

- Private Key (or Symmetric Algorithms)
- A single key is used for both encryption and decryption
- Security depends on algorithm and key size
  - Usually the bigger the key size the better
  - But larger key sizes impact on performance



33

Key Distribution and Management

- Primary problem with Private Key algorithms
  - How to securely transmit the key to other parties
  - The key management problem
  - Problematic until 1976 and the advent of public key cryptography
  - Private key must be kept securely
- Solutions
  - Secure and restrict access to the private key
  - A known secure communications link can transmit the private key
- Current solutions
  - Public key algorithms have become the modern solution to the key management problem

34

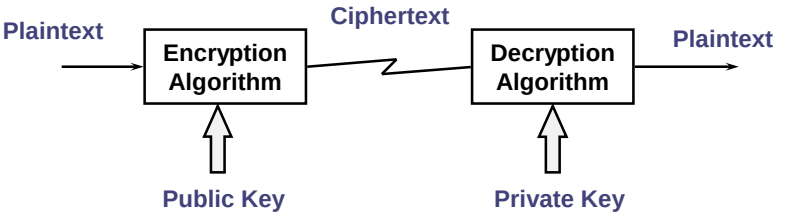
Public Key Cryptography

- Each entity (user etc.) has two mathematically related keys
- The private key is told to *no-one*
- The public key is made freely available
- Data encrypted with one key can be decrypted with the other

35

Public Key Algorithms

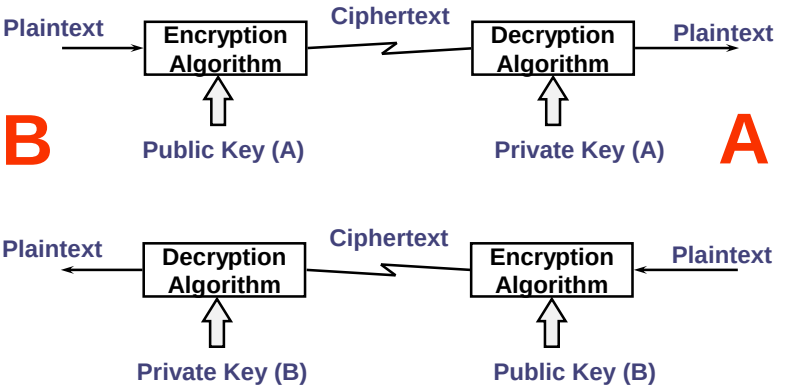
- Public Key (or Asymmetric Algorithms)
- A pair of keys are used for encryption and decryption
- One key is kept private and used for decryption, the other is made public and used for encryption
- The private key cannot (practically) be derived from the public key



36

Public Key Algorithms (2)

- By using two pairs of keys, one for each party, a secure two way channel can be established ...



37

Public Key Algorithms (3)

- Advantages
  - Solves the key management problem
- Disadvantages
  - Slow performance (Symetric algorithms are up to 1,000 times faster than Public algorithms)
  - Needs large key sizes (512 bits is weak, 1024 is reasonably secure)
  - Vulnerable to certain types of attacks (plaintext and timing attacks)

38

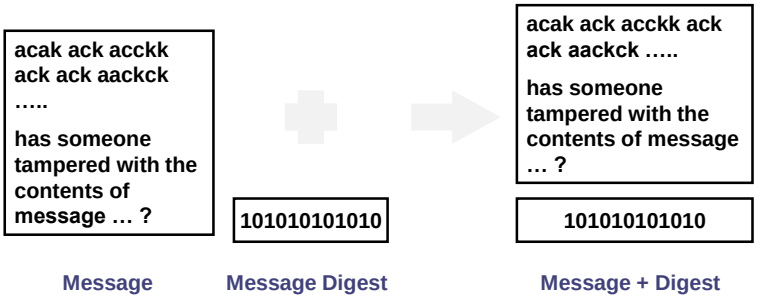
Protection through Authentication

- Encryption provides us with the ability to hide data from third parties - but …
  - Do we know the data came from who we think it came from?
  - Do we know that it hasn't been tampered with?
  - Do they positively know who we are?
- Authentication provides the answers …
  - Individual messages can be protected from tampering
  - We can positively authenticate parties who connect to us
  - We can positively authenticate ourselves to other parties

39

Message Authentication

- To check that a message has not been altered en-route
- Hashing algorithm used to create a fixed-size message digest appended to the end
- Popular algorithms include MD5 and SHA



40

Digital Signatures

- How can we be sure that the contents and the message digest are both unaltered?
- We use "Digital Signatures"
  - Public key encryption in reverse
  - Data encrypted with a private key can only be decrypted using the corresponding public key
  - Recipient is already in possession of a public key they know belongs to you
  - If the message can be decrypted using public key it came from you
- In practice, we combine digital signatures with message digests…
  - Public key encryption is too slow to use on the whole message
  - So we just sign the message digest, so that cannot be tampered with

41

Digital Certificates

- Certificates bind a public key to a particular entity
- Certificates contain information about an entity...
  - Certificate information, e.g. system name and public key
  - Server's digital signature
  - The most commonly used certificates are based upon the ITU-T X.509 standard
  - X.509 certificates are those used in SSL and other common authentication mechanisms
- Certificates are issued by a trusted body
  - The Certification Authority
  - You trust them to check that the certificate really does belong to whoever claims to own it

42

Certificates and Digital IDs

- A certificate contains your "distinguished name" and public key
- It is digitally signed by a "Certificate Authority"(CA)
- If you have obtained the CA's public key from a reputable source, then you can verify that they issued this certificate
- If you trust the CA, then you can be sure that the holder of the certificate is who he claims to be

43

Certification Authorities

- Issue Certificates
- Verisign, RSA Data Security, etc.
- Process of applying for certificate
  - When applying for key, the CA needs detailed information on the person/company
  - The CA's job it to ensure that you are who claim to be, how thorough they are determines how trustworthy their judgement is
  - Generally, the more expensive the certificate, the more checking and the more trustworthy

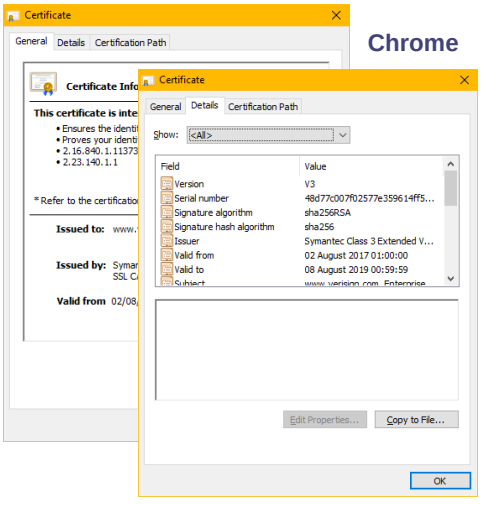
44

Breaking Public Key Cryptography

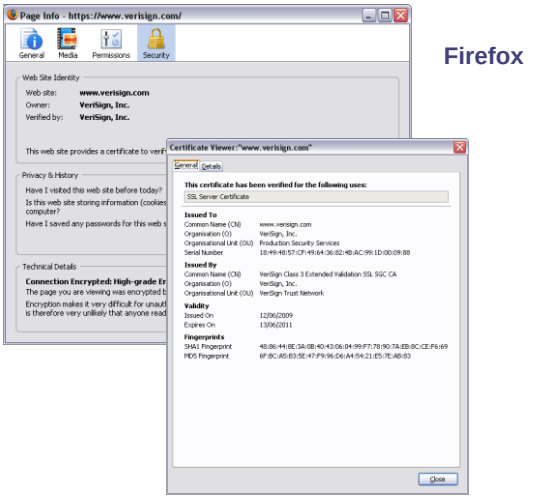
- Obtain the private key by deception, bribery, etc.
- Deduce private key by “brute force”
  - Try every possible key in succession
- Larger key size gives greater protection against brute force attack
  - More possible keys
- Standard “maximum strength” key is 128 bits
- SSL2.0 uses 256 bit private keys

45

Checking a Certificate



Chrome



Firefox

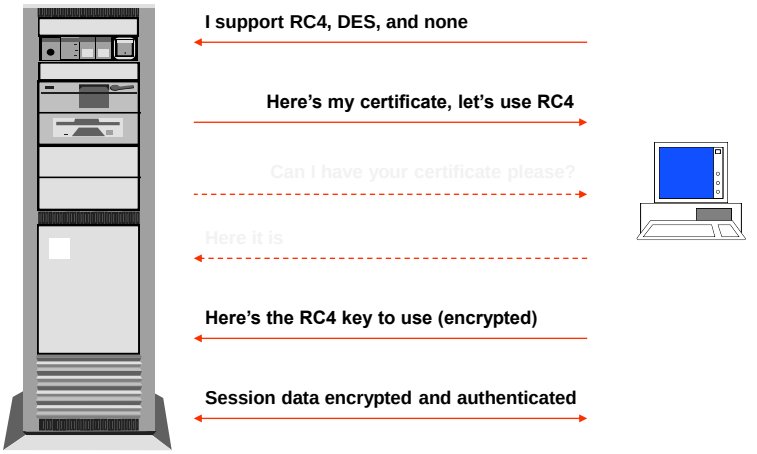
46

SSL

- SSL designed by Netscape
- Open standard before the IETF
- Includes server and client authentication, data encryption and compression, and message authentication

47

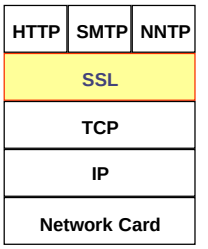
SSL Session Overview



48

SSL and HTTP

- SSL is a Presentation Layer protocol, sitting between the application and TCP/IP
- Can be used by any application, which requires its features
- Largely invisible to application
- https URLs are used to specify HTTP over SSL



49

Development Tools

WEB DEVELOPMENT FUNDAMENTALS

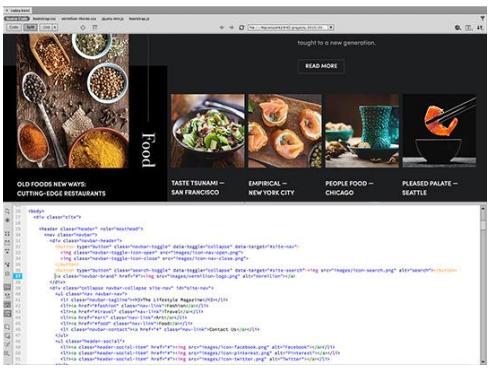
Web Tools

- Objectives
  - To describe the various editors available to us
  - To use a tool to create and edit Web pages
  - To compare HTML editors
  - A first look at some modern developer tools
- Summary

51

DreamWeaver

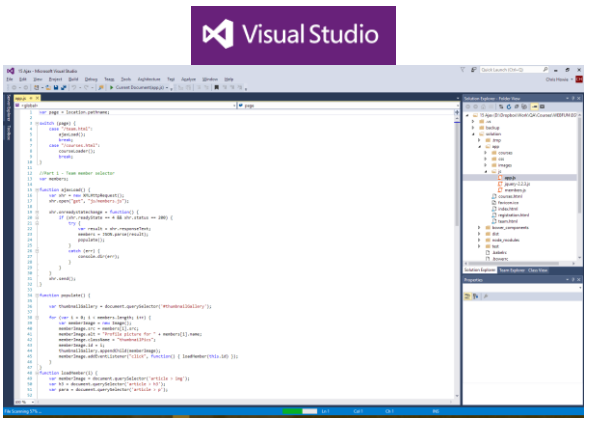
- WYSIWYG editor
  - DTP quality content positioning on the page with Fluid Grid Layout
- Supports style sheets, including a CSS designer
- Allows direct HTML editing
- Supports JavaScript
- Site management



52

Microsoft Visual Studio

- Developer-oriented tools for Windows and the Web
  - Builds interactive Web pages
  - Builds mobile Web pages
  - Can build Windows based Applications
  - Builds Smart device Applications
- Visual Studio Community (Free for individuals)



53

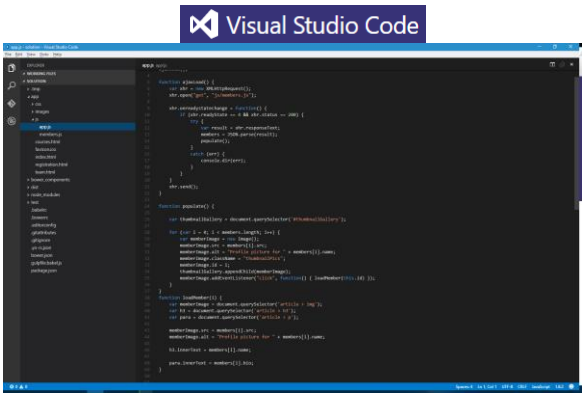
Aptana Studio

- Broad Web Standards Support
- HTML5 Intellisense
- Integrated Debugger
- Deployment Mechanisms
- Code Tracking
- Editing
  - IntelliSense and color-coding for HTML, CSS, JavaScript, etc.
  - Real-time standards validation

54

Microsoft Visual Studio Code

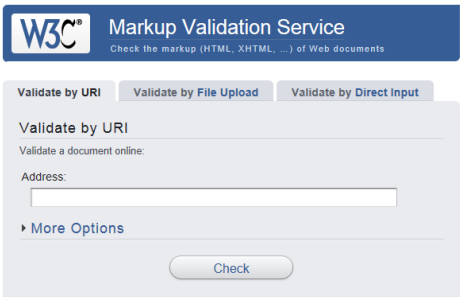
- Cross-platform code editor for modern web and cloud apps
  - Built in Git source control
  - Hundreds of community built extensions
  - File and folder based
  - Free!



55

Consistency Checkers and Validators

- On-line validators
  - http://www.netmechanic.com
  - http://validator.w3.org
- W3C Web Accessibility Initiative
  - Complete list of web accessibility evaluation tools
  - http://www.w3.org/WAI/ER/tools/complete



56

Using the Tools of the Modern Web

WEB DEVELOPMENT FUNDAMENTALS

Introduction

- The Open Web Development Stack
  - Automation support and Continuous Development
    - Grunt
    - Yeoman
    - Bower
    - Gulp
    - Node.js
  - Working with the Command Line and Terminal
  - Continuous Development and a DevOps Methodology

58

What is Grunt?

- Grunt is a task based command line tool for JavaScript projects
  - Grunt is an open source project
    - Hundreds of packages
    - Ability to build your own projects
  - It helps you to rapidly start up web dev projects
  - Tasks can include:
    - Unit testing
    - JS linting
    - Minification
    - SASS
    - AngularJS

59

What is Yeoman

- Yeoman provides a way to scaffold workflows
  - It scaffolds out a new application
  - Options include Angular, Backbone, Ember
- Yeoman scaffolds out a new application
  - It writes your grunt file
  - Pulls in relevant Grunt tasks
  - Plus Bower dependencies

60

What is Bower?

- Modern web aps often rely upon multiple packages e.g.
  - AngularJS, jQuery, Bootstrap, NodeJS in a single app
  - Managing these packages and making sure they are up-to-date is difficult
- Bower is a package manager
  - It helps with package dependencies
  - Use it to search for packages
  - Perform updates and version control

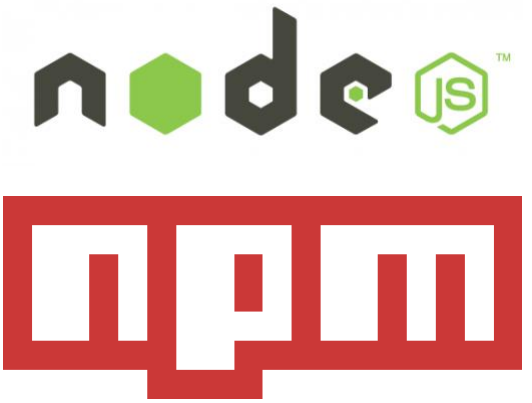
61

What is Gulp

- Gulp is a build automation tool
  - Entirely JS based
- Gulp is built on Node
  - A competitor to Grunt
  - Do much of the same thing
  - Gulp plug-ins only do a single thing
  - Gulp uses leaner, simpler JavaScript code

62

Node & NPM



63

Conclusion

- The Open Web Development Stack
  - Automation support and Continuous Development
    - Grunt
    - Yeoman
    - Bower
    - Gulp
    - Node.js

64

Summary

- Course Outline
- What is the web?
- Intranets and Extranets
- WWW browsers
- Principles of Browser operation
- Security
- Development tools
- Modern web tools

65