Security Strategies in Web Applications and Social Networking

Chapter 1

From Mainframe to Client/Server to World Wide Web

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Learning Objective

- Identify the highlights in the evolution of data processing, from mainframes to the World Wide Web (WWW).
- Understand the characteristics of Web 1.0, 2.0, 3.0
- Understand the role of cloud computing
- Identify the functions of service packs
- Review comparison on secure/insecure protocols

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Key Concepts

- Fundamental shift in technology and platforms
- Phases of the WWW: Web 1.0, Web 2.0, Web 3.0
- Key areas of concern for e-commerce
- Lack of security in common WWW protocols
- Securing communications

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Understanding Data, Data Processing and Information

Data

- Facts, figures, raw input
- Collection of observations, stats, recordings

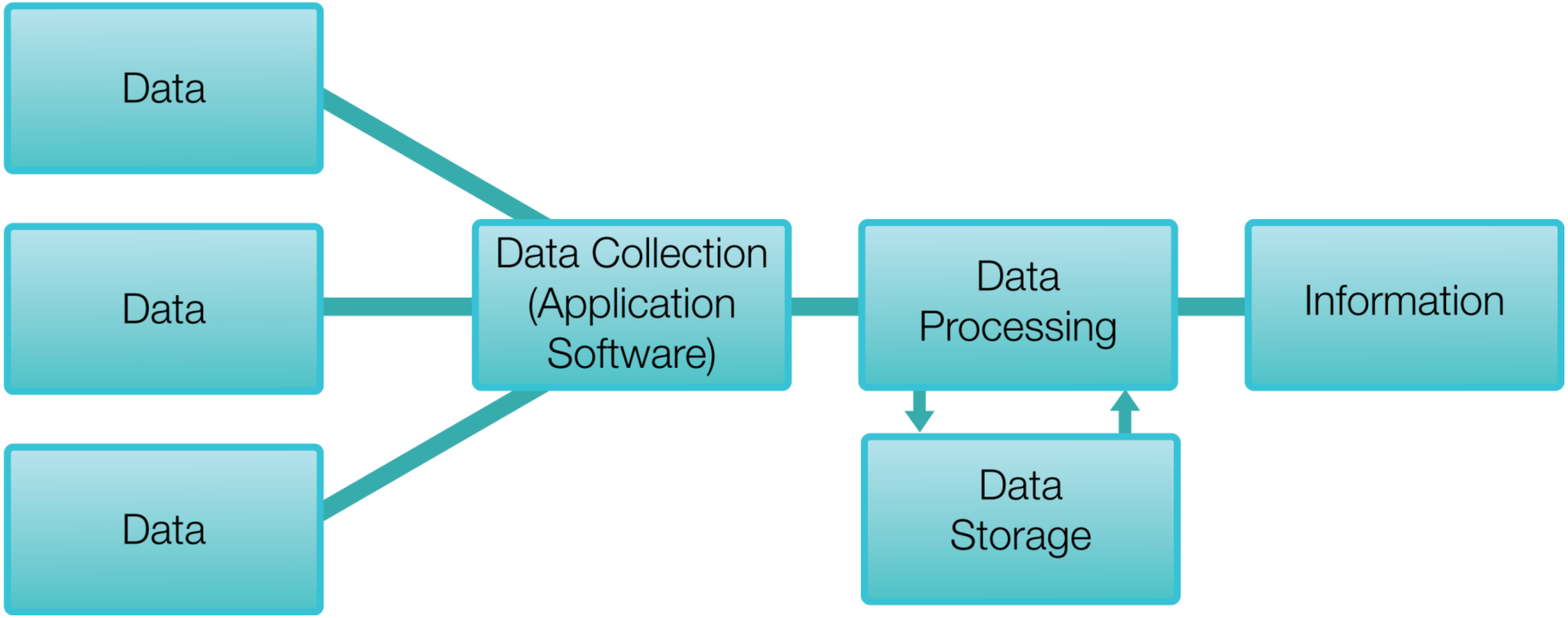
Information

- Conclusions drawn become useful info
- Organized, interpreted within a framework

to have relevance as information, data needs to be recorded, organized, and interpreted within a specifc framework. Data processing refers to the steps data goes through to become information.

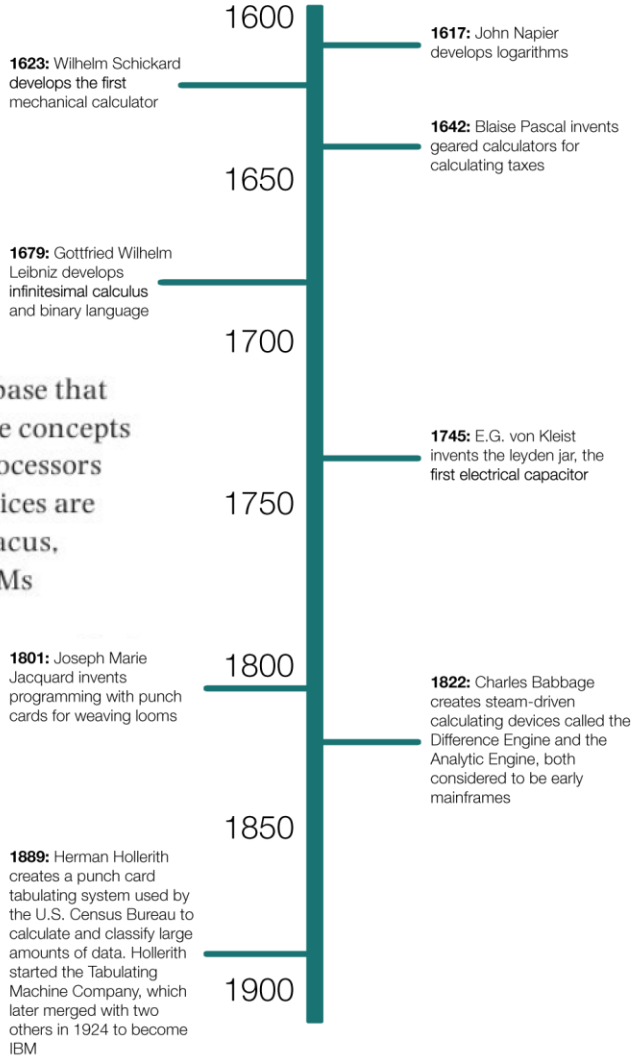
© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Processing Data



© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Data Processing Timeline



1617: John Napier develops logarithms

1623: Wilhelm Schickard develops the first mechanical calculator

1642: Blaise Pascal invents geared calculators for calculating taxes

1679: Gottfried Wilhelm Leibniz develops infinitesimal calculus and binary language

1745: E.G. von Kleist invents the leyden jar, the first electrical capacitor

1801: Joseph Marie Jacquard invents programming with punch cards for weaving looms

1822: Charles Babbage creates steam-driven calculating devices called the Difference Engine and the Analytic Engine, both considered to be early mainframes

1889: Herman Hollerith creates a punch card tabulating system used by the U.S. Census Bureau to calculate and classify large amounts of data. Hollerith started the Tabulating Machine Company, which later merged with two others in 1924 to become IBM

These early technologies formed a knowledge base that was continually built upon over the centuries. The concepts of these early devices still can be found in data processors used today. The designers of these antiquated devices are the true data processing pioneers, making the abacus, sextant, slide rules, and other such devices the IBMs or Intels of their day.

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Evolution of Data Processing

- Early 1900s to 1960s
  - 1924 Hollerith starts IBM
  - 1946 ENIAC British computer (vacuum tubes)

for calculating millitary artilitery firing tables for long range ammo

- 1950s through today
  - 1964 IBM/360 modern mainframe
  - 1977 Apple II with color graphics
  - 1981 IBM PC
  - 1990 Windows 3.0
  - 2002 one billion computers

1971 - Intel 4004, first CPU

1973 - Alto, developed by Xerox, first simple GUI and a mouse-type device for input; designed for offices with workstation systems.

1984 - Apple first Macintosh; first popular computer with GUI and a mouse

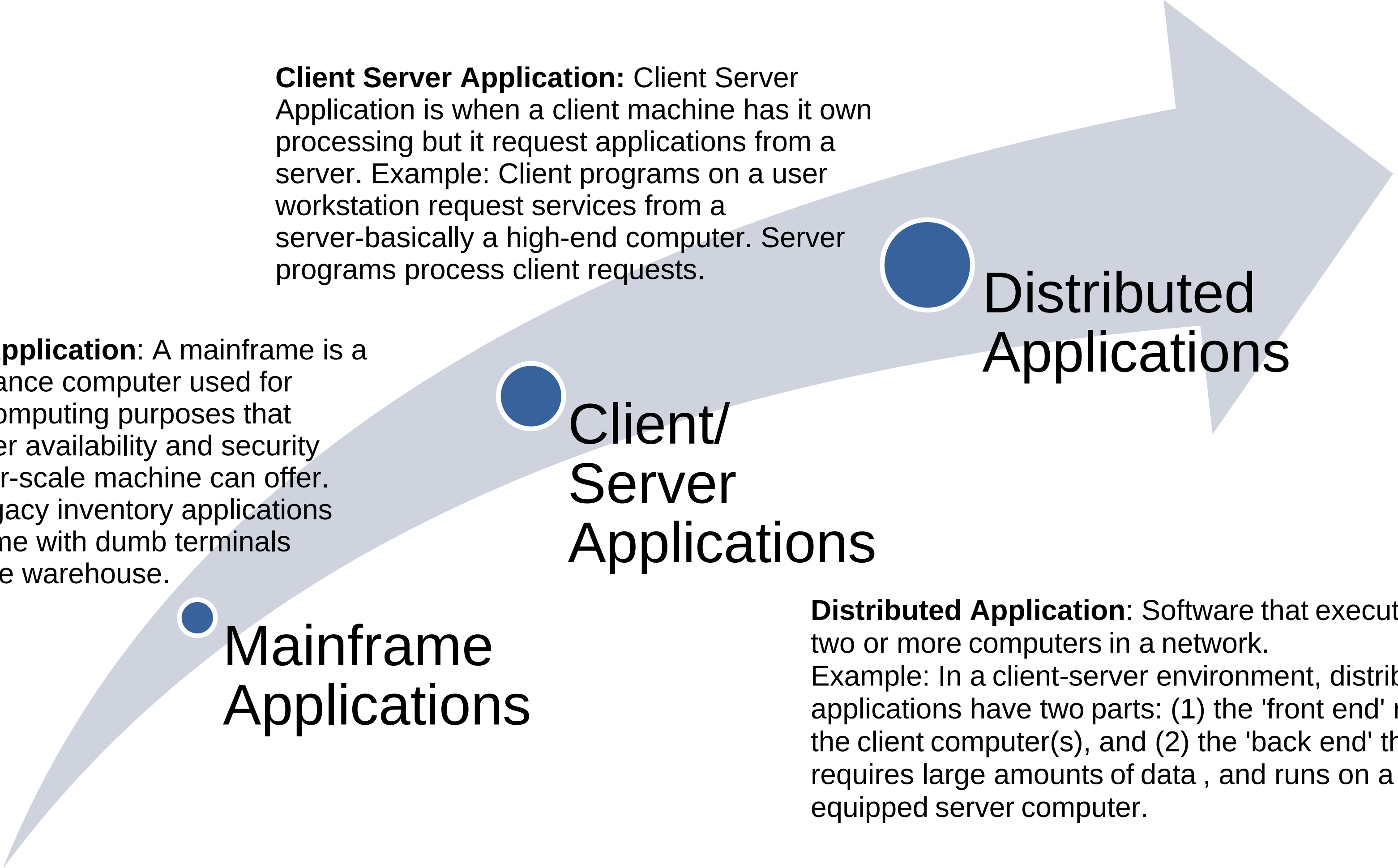
1997
IBM's Deep Blue beat Gary Kasparov in a six-game match of chess.
first time computer beat a human
some consider this a turning point for computing

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Evolution of Application Delivery

Client Server Application: Client Server Application is when a client machine has it own processing but it request applications from a server. Example: Client programs on a user workstation request services from a server-basically a high-end computer. Server programs process client requests.

Mainframe Application: A mainframe is a high-performance computer used for large-scale computing purposes that require greater availability and security than a smaller-scale machine can offer. Example: Legacy inventory applications on a mainframe with dumb terminals throughout the warehouse.



Mainframe Applications

Client/ Server Applications

Distributed Applications

Distributed Application: Software that executes on two or more computers in a network.
Example: In a client-server environment, distributed applications have two parts: (1) the 'front end' runs on the client computer(s), and (2) the 'back end' that requires large amounts of data , and runs on a suitably equipped server computer.

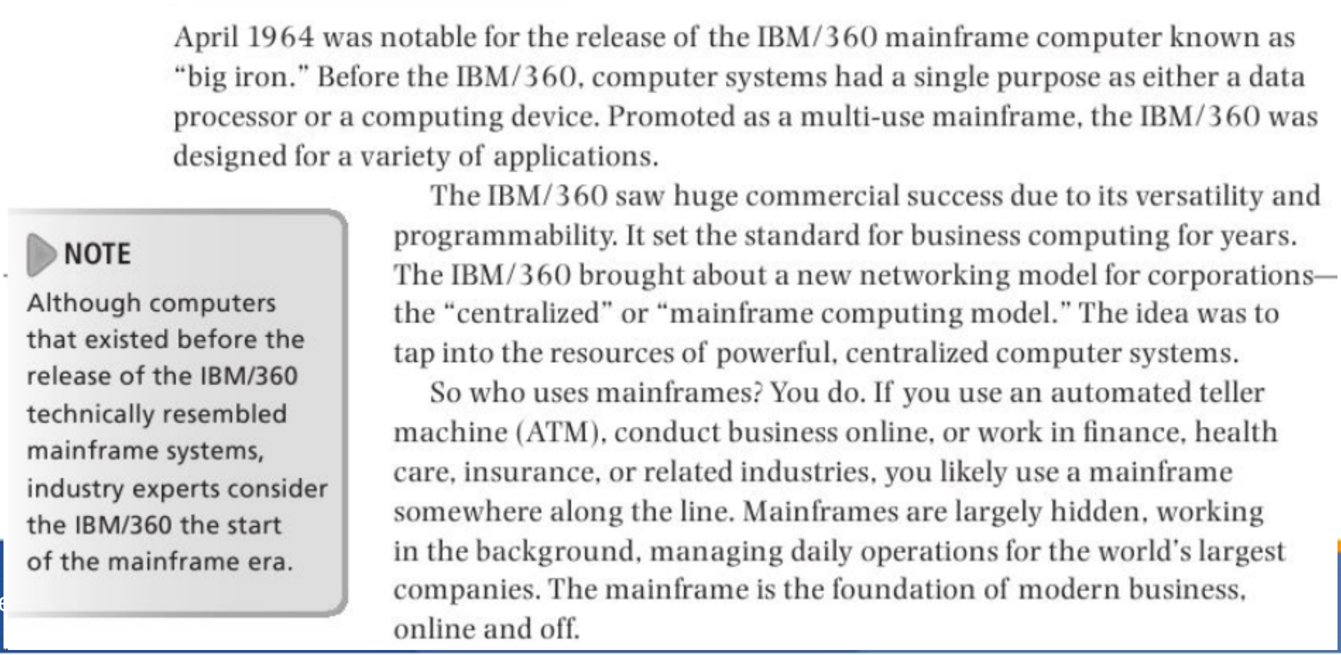
© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Mainframe Computers

maintains the most mission-critical applications in the world due to numerous disaster-recovery and fault tolerant solutions build into their designs

- Processing power (more than network servers and workstations) allows faster more complex apps
- DB management (TB of info)
- User-friendly interface (Web interface)
- App continuity (robust, no down time)
- App security (centralized management)
- DB backups allows centralized management for security and backups of databases

centralized processing/computing
- workstation is merely a gateway to centralized system, all processing, computing and storage takes place on m/f



April 1964 was notable for the release of the IBM/360 mainframe computer known as "big iron." Before the IBM/360, computer systems had a single purpose as either a data processor or a computing device. Promoted as a multi-use mainframe, the IBM/360 was designed for a variety of applications.

The IBM/360 saw huge commercial success due to its versatility and programmability. It set the standard for business computing for years. The IBM/360 brought about a new networking model for corporations—the "centralized" or "mainframe computing model." The idea was to tap into the resources of powerful, centralized computer systems.

So who uses mainframes? You do. If you use an automated teller machine (ATM), conduct business online, or work in finance, health care, insurance, or related industries, you likely use a mainframe somewhere along the line. Mainframes are largely hidden, working in the background, managing daily operations for the world's largest companies. The mainframe is the foundation of modern business, online and off.

NOTE

Although computers that existed before the release of the IBM/360 technically resembled mainframe systems, industry experts consider the IBM/360 the start of the mainframe era.

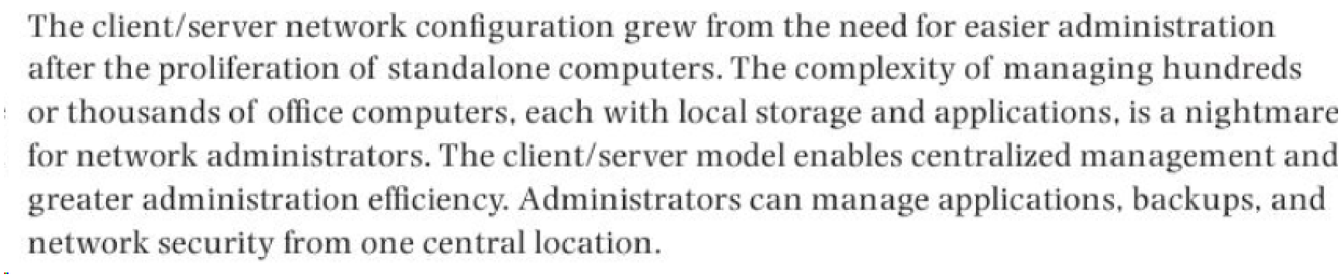
Client/Server

- Scalability (easy to add computers and peripherals)
- Centralization (easier management of resources and user accounts)
- Convenience (one uid/pwd for controlling access to all available network resources)
- Efficiency (one location = easier backup)

access to sensitive data is easier*

- Security (access easier to secure and monitor)
- Protocols that use client/server:
  - FTP
  - SMTP
  - Telnet
  - POP3

  HTTP



The client/server network configuration grew from the need for easier administration after the proliferation of standalone computers. The complexity of managing hundreds or thousands of office computers, each with local storage and applications, is a nightmare for network administrators. The client/server model enables centralized management and greater administration efficiency. Administrators can manage applications, backups, and network security from one central location.

downside is that there is only one point of contact

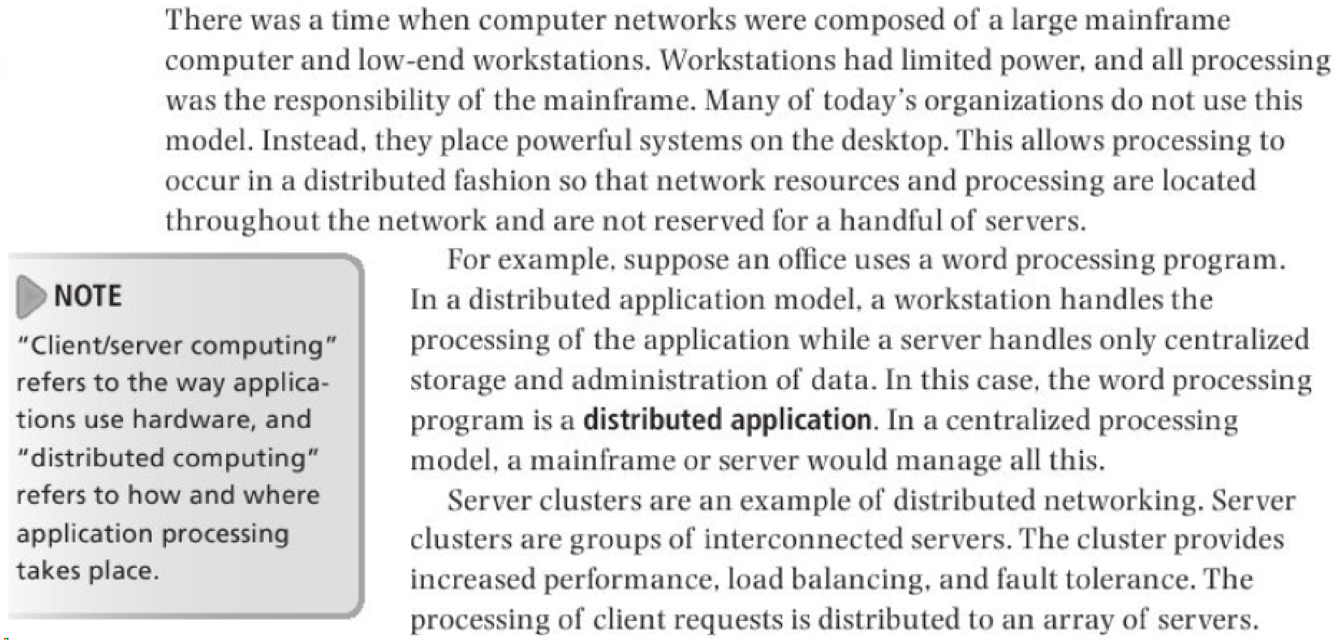
if the server goes down no one able to access it

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

dont have same problem of client/server where we are dependent on the server

Distributed Computing

- Server handles centralized data, workstations perform the processing
- Server clusters (farms)
- Greater performance more rsrcs = more procesing power than single machine
- Shared workload (balancing)
- Disaster recovery



There was a time when computer networks were composed of a large mainframe computer and low-end workstations. Workstations had limited power, and all processing was the responsibility of the mainframe. Many of today's organizations do not use this model. Instead, they place powerful systems on the desktop. This allows processing to occur in a distributed fashion so that network resources and processing are located throughout the network and are not reserved for a handful of servers.

For example, suppose an office uses a word processing program. In a distributed application model, a workstation handles the processing of the application while a server handles only centralized storage and administration of data. In this case, the word processing program is a **distributed application**. In a centralized processing model, a mainframe or server would manage all this.

Server clusters are an example of distributed networking. Server clusters are groups of interconnected servers. The cluster provides increased performance, load balancing, and fault tolerance. The processing of client requests is distributed to an array of servers.

NOTE

"Client/server computing" refers to the way applications use hardware, and "distributed computing" refers to how and where application processing takes place.

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

e-commerce = buying and selling of goods and services over electronic systems such as the Internet

Transformation of Brick-and-Mortar to E-Commerce

with static web pages, simply presenting the data as information to the end user;
one way traffic; did not need to worry about security; end user does not interact with system

- Started mid-90's businesses used websites as advertisement or shopping window
- Key areas of concern for e-commerce: these needed to be addressed before offline can go online
  - Integrity (message was not tampered with in transit)
  - Nonrepudiation (neither party can deny the transaction has taken place)
  - Authentication (verify user identity)
  - Privacy (info stored confidentially)
- New protocols (https, PKI)
- E-commerce today:
  - Catalog
  - Shopping cart
  - Transactions and payment processing
  - Fulfillment system e.g. system monitors whether order shipped, etc.

new protocols helped ensure secure online communications

https
hypertext transfer protocol with Secure Sockets Layer

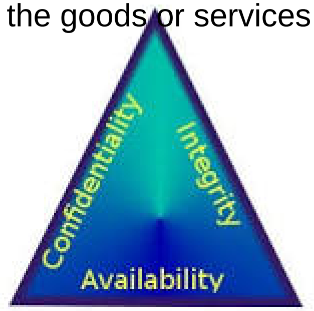
pki
Public Key Infrastructure

For example, the customer must be assured of the seller's identity, the seller must use a secure and trackable form of payment processing, and the seller must use a proof-of-delivery system so that neither party can later deny having processed the data or received the goods or services.

Security Network Login:
A -> uthentication
A -> uthorization
A -> ccountability

Accounting - keep logs to see how often a user has logged in for example.

profile the visitors



CIA triad for Information Security: model designed to guide policies for information security within an organization

Confidentiality - keeping user's info private and not disclosing it
Integrity - correctness of the information, should not be modifiable by "man in the middle" atk for ex., use encryption
Availability - want high availability because hackers may DOS atk to try to bring ur service down

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Email and FTP are services which use the Internet but not the web. The infrastructure of the Internet was established long before the Web loading Web sites using HTTP.

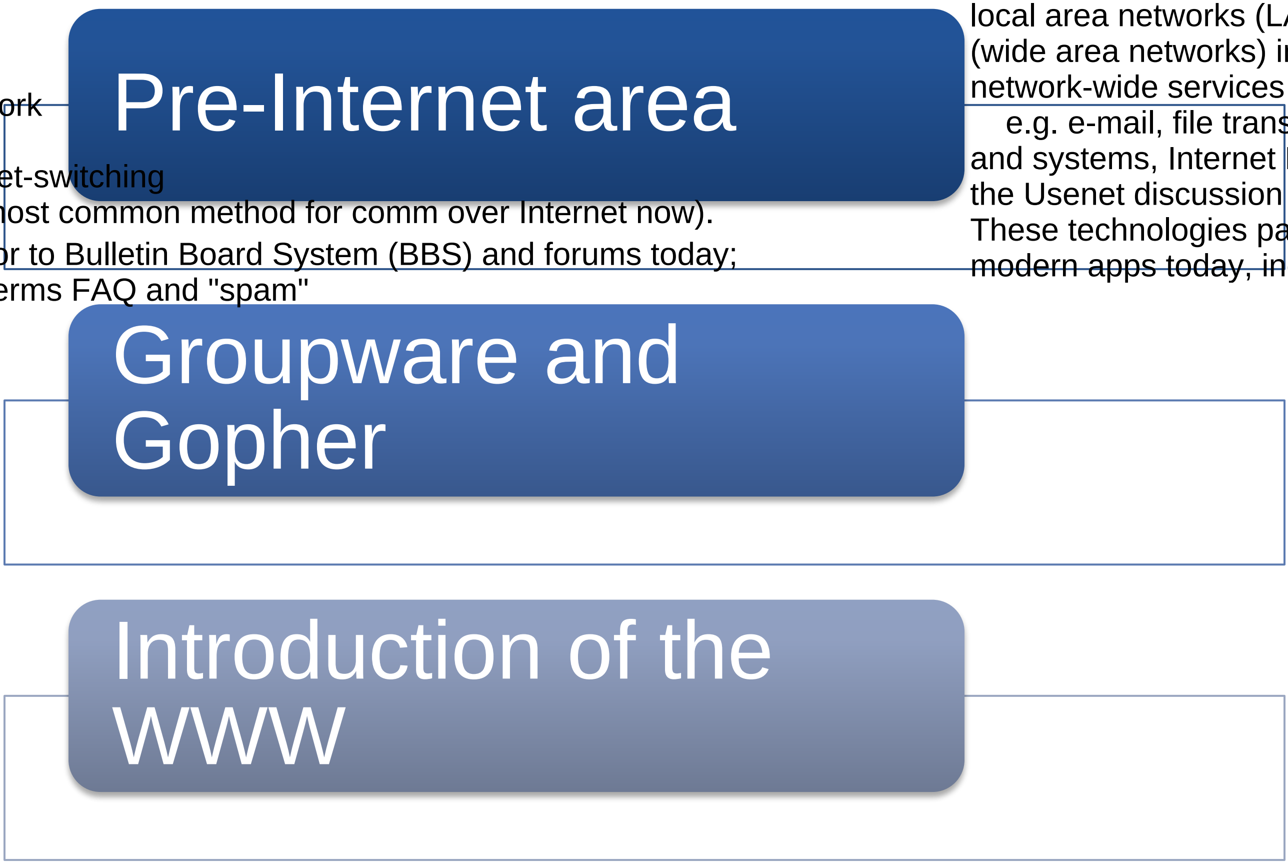
WWW Revolution

Internet vs WWW: Internet (with capital "I") is large, global network consisting of routers, cabling, servers, and all the hardware that create the Internet network infrastructure. The web is simply one of the services deployed on the Internet; it is interconnected system of interlinked hypertext documents accesed via the Internet.

1960s and 1970s
Advanced Research
Project Agency Network
(ARPANET) project:
first operational packet-switching
network (pswitch is most common method for comm over Internet now).

***Usenet predecessor to Bulletin Board System (BBS) and forums today;
Its users coined the terms FAQ and "spam"

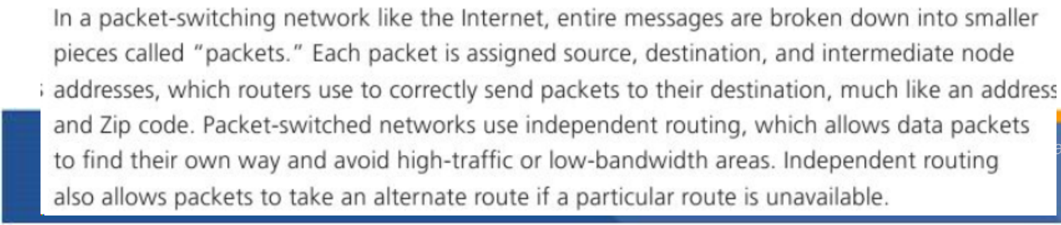
1980s
computers proliferated, became smaller
local area networks (LANs) and WANS
(wide area networks) introduced, new set of
network-wide services
e.g. e-mail, file transfers b/t workstations
and systems, Internet Relay Chat (IRC) and
the Usenet discussion forum
These technologies paved the way for
modern apps today, including the WWW



Pre-Internet area

Groupware and Gopher

Introduction of the WWW



In a packet-switching network like the Internet, entire messages are broken down into smaller pieces called "packets." Each packet is assigned source, destination, and intermediate node addresses, which routers use to correctly send packets to their destination, much like an address and Zip code. Packet-switched networks use independent routing, which allows data packets to find their own way and avoid high-traffic or low-bandwidth areas. Independent routing also allows packets to take an alternate route if a particular route is unavailable.

Phases of the WWW

Web 1.0

1990 - 2003

- Static Web
- Sites are non-interactive
- Directory portals

Refers to the state of the WWW, and any Web site design style used before the advent of Web 2.0 phenomenon

Web 2.0

2003 - present

- User-generated content
- Blogging and social networking
- Wikis

Is commonly associated with the Web applications that facilitate interactive, user-created information

Web 3.0

visionary future

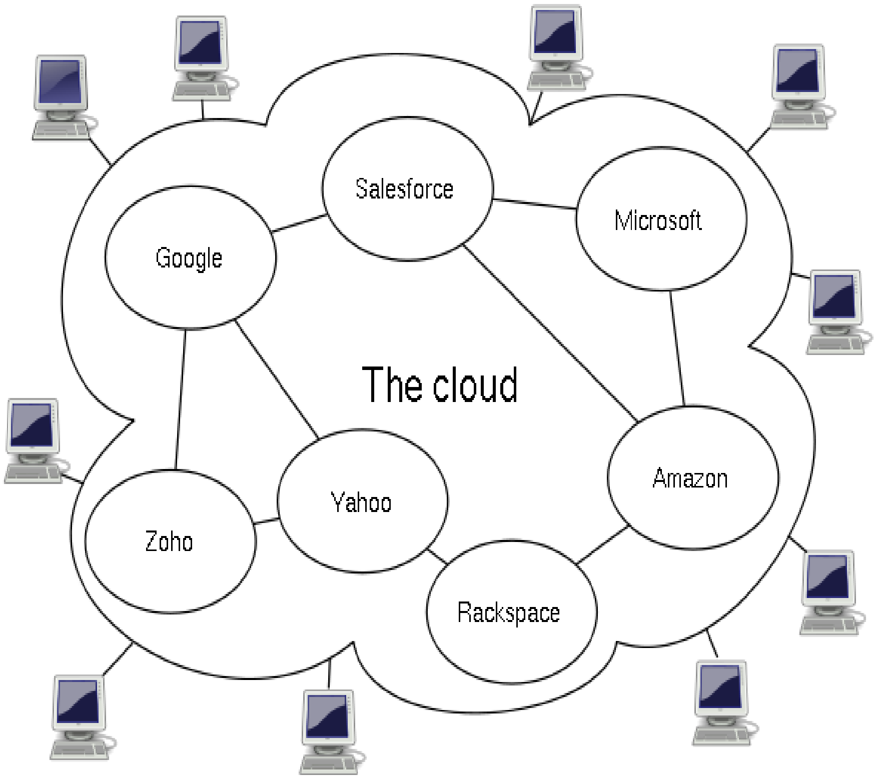
- Semantic Web
- The Web as one big database

Content and services created by skilled individuals using Web 2.0 technologies

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Virtualization and Cloud Computing

- **Virtualization:**
  - The creation of one or more virtual instances of servers running on one or more physical servers
- **Cloud Computing:**
  - Internet-based computing



© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Lack of Inherent Security Within Protocols and Coding

- Internet Protocol Version 4 (IPv4) lacks sufficient security technologies
- Security flaws in software
  - Operating systems and other applications

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Securing Communications

- Use secure versions of insecure protocols
    - IPv4 secured through higher layers (encryption, SSL, HTTPS)
    - IPv6 designed with security built in
- Use IPSec (Internet Security Protocol)
- Prevent different types of attacks:
    - Eavesdropping (intercepts and modifies clear-text)
    - Address spoofing (impersonate an IP address)
    - Man-in-the-middle (use non-repudiation)
    - DoS

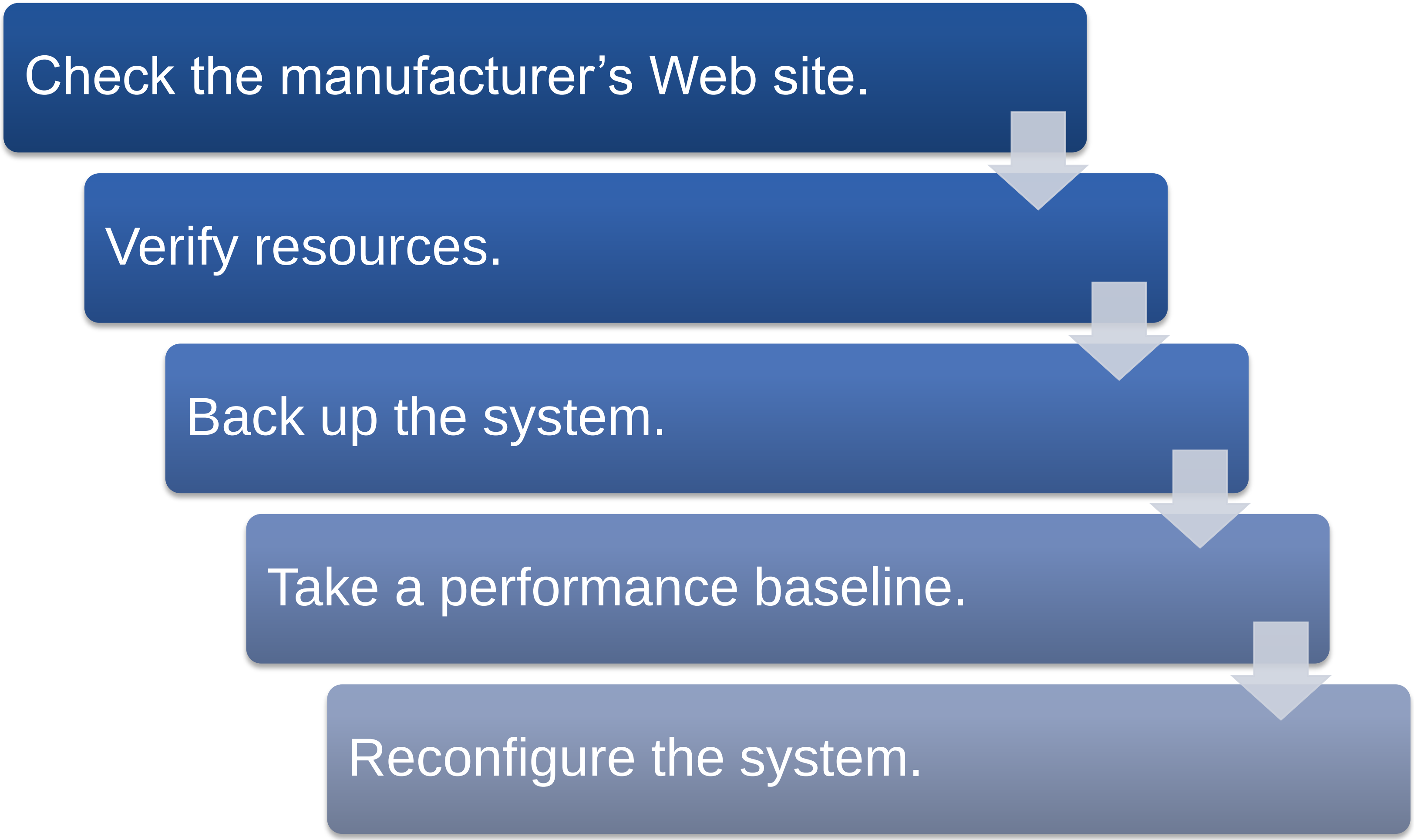
© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Securing Communications (Continued)

- Manage application and coding security
  - Developers plan for security concerns present at the time applications are created.
- Use service packs
  - As new security threats arise, updates, patches, and service packs must be installed to protect the applications.

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Installing Service Packs



Check the manufacturer’s Web site.

Verify resources.

Back up the system.

Take a performance baseline.

Reconfigure the system.

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Summary

- Fundamental shift in technology and platforms
- Phases of the WWW: Web 1.0, Web 2.0, Web 3.0
- Key areas of concern for e-commerce
- Lack of security in common WWW protocols
- Securing communications

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.