Security Strategies in Web Applications and Social Networking

Chapter 1

From Mainframe to Client/Server to World Wide Web

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

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

Understanding Data, Data Processing and Information

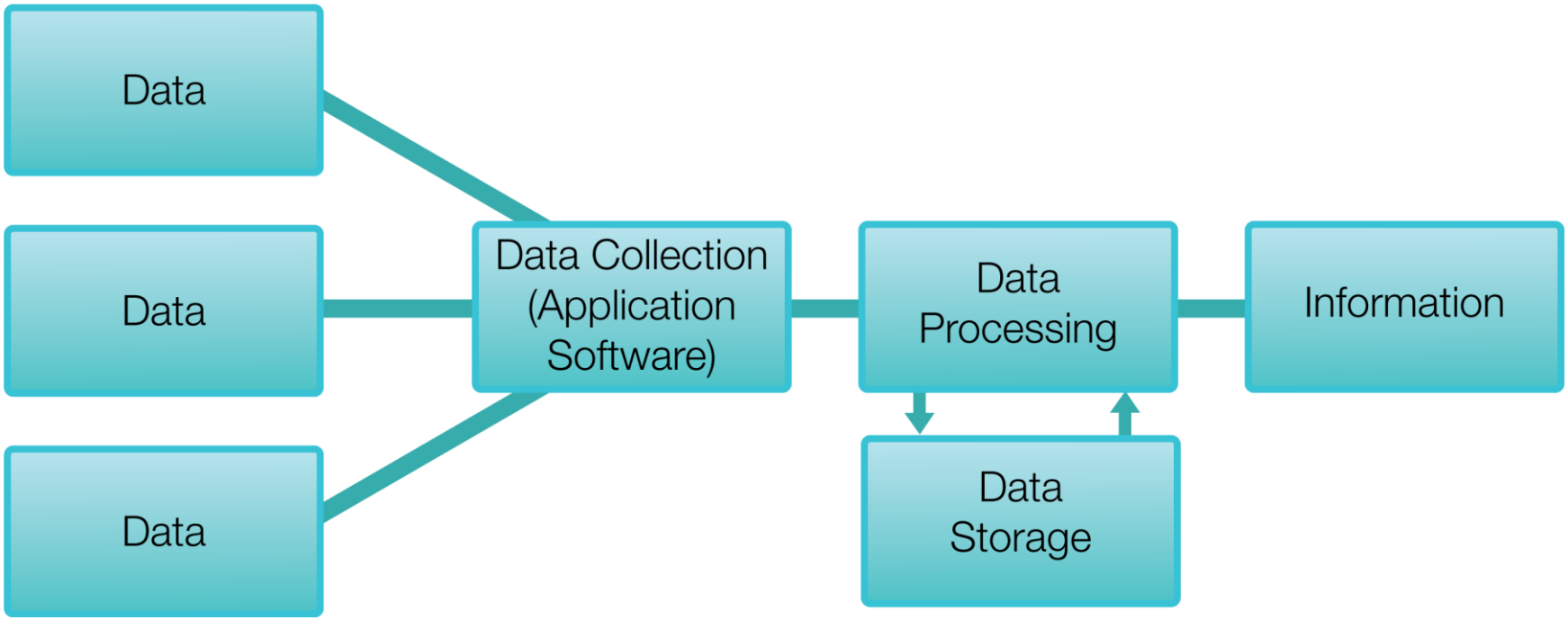
Data

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

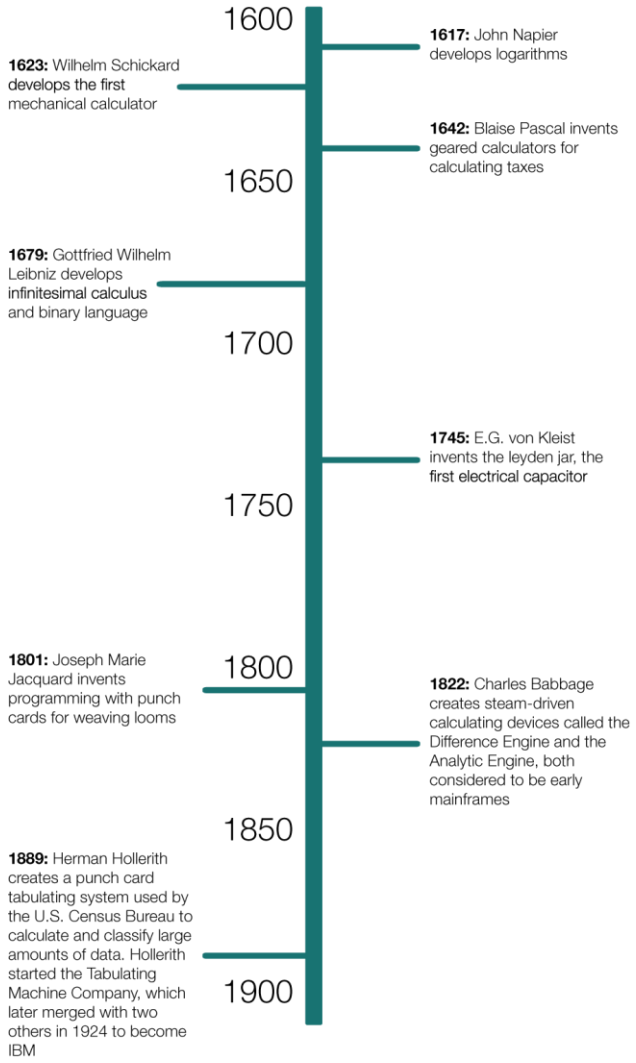
Information

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

Processing Data



Data Processing Timeline



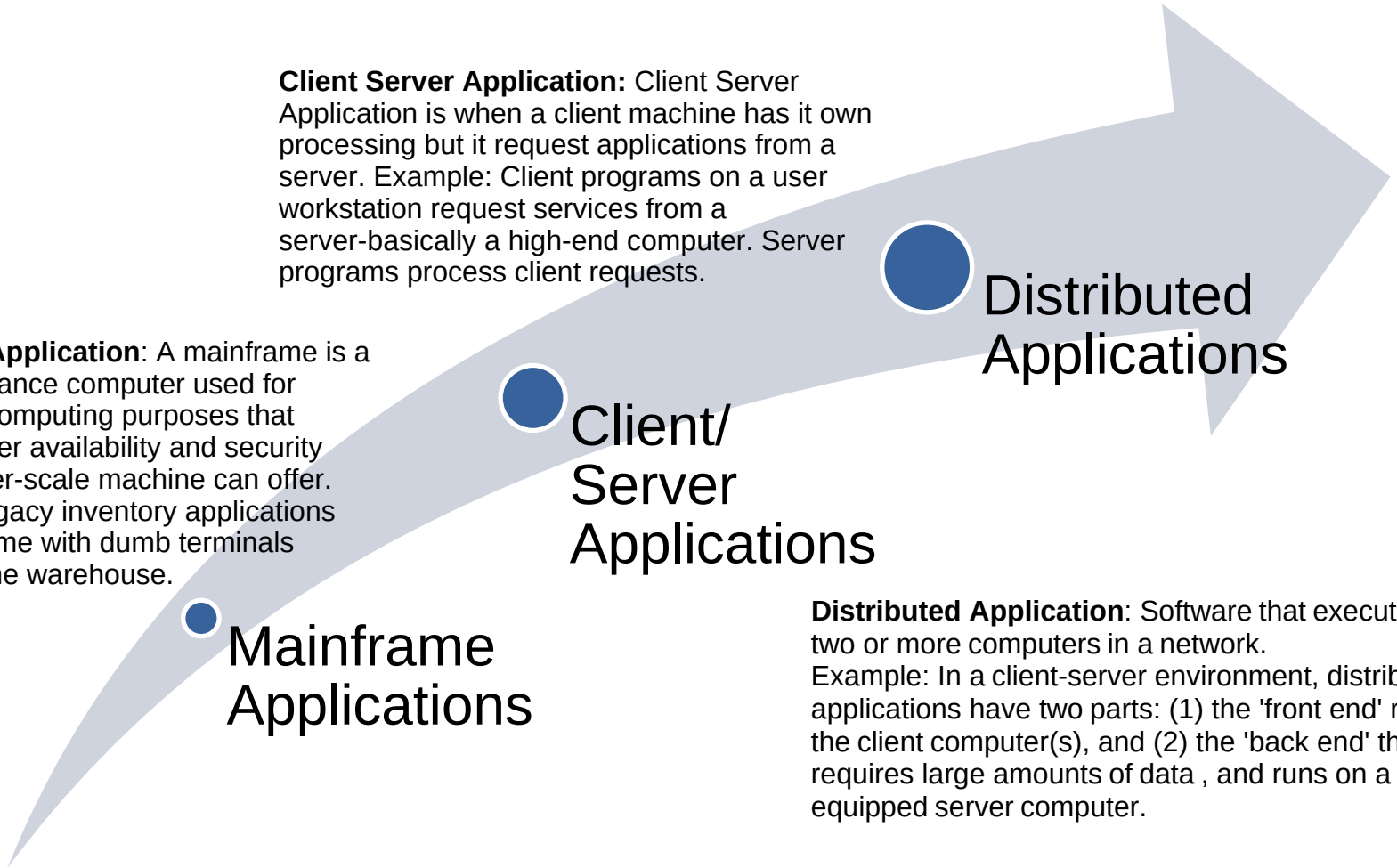
Evolution of Data Processing

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

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.



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.

Mainframe Computers

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

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

downside is that there is only one point of contact

if the server goes down no one able to access it

Distributed Computing

- Server handles centralized data, workstations perform the processing
- Server clusters (farms)
- Greater performance
- Shared workload (balancing)
- Disaster recovery

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

Transformation of Brick-and-Mortar to E-Commerce

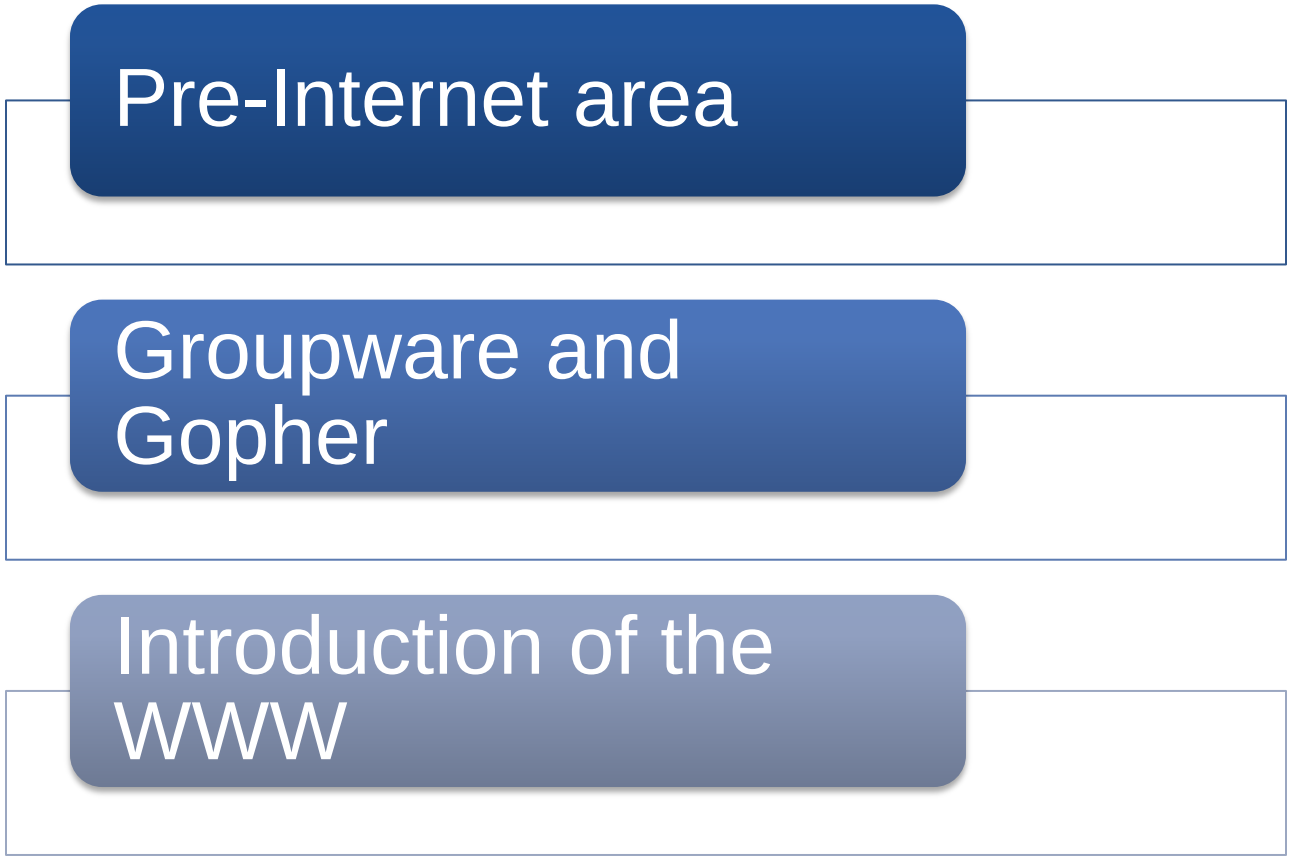
with static web pages, simply presenting the data as information to the end user;
one way traffic; did not need to worry about security; end user does not interact with system

- Started mid-90's
- Key areas of concern for e-commerce:
  - 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

Triad of Information Security (Bindu said):
A -> uthentication
A -> uthorization
A -> ccountability

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

WWW Revolution



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

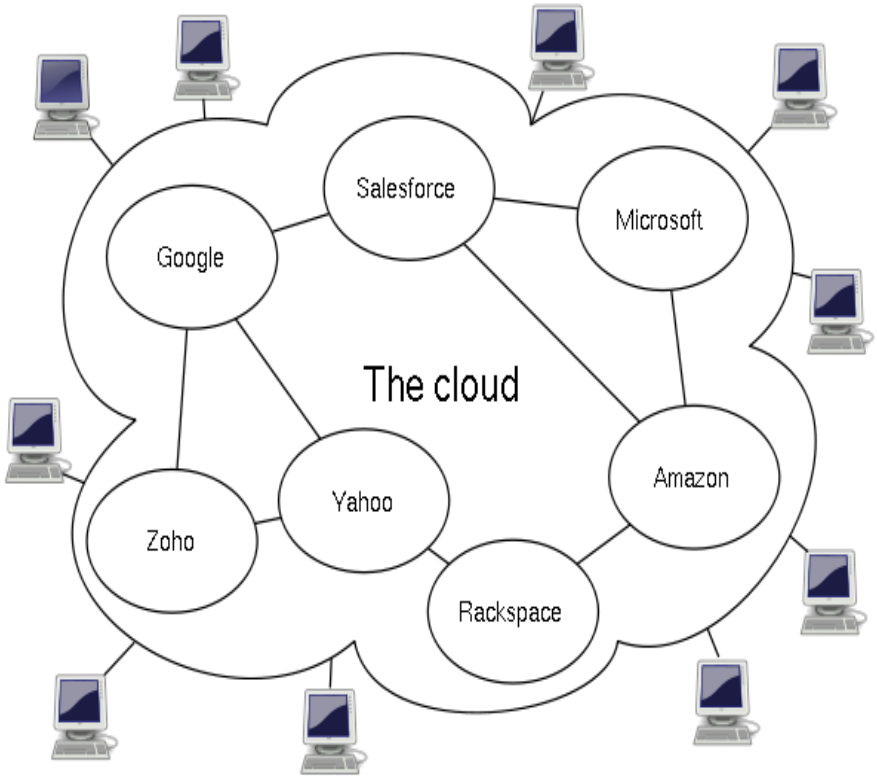
Web 3.0
visionary future

- Semantic Web
- The Web as one big database

Content and services created by skilled individuals using Web 2.0 technologies

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



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

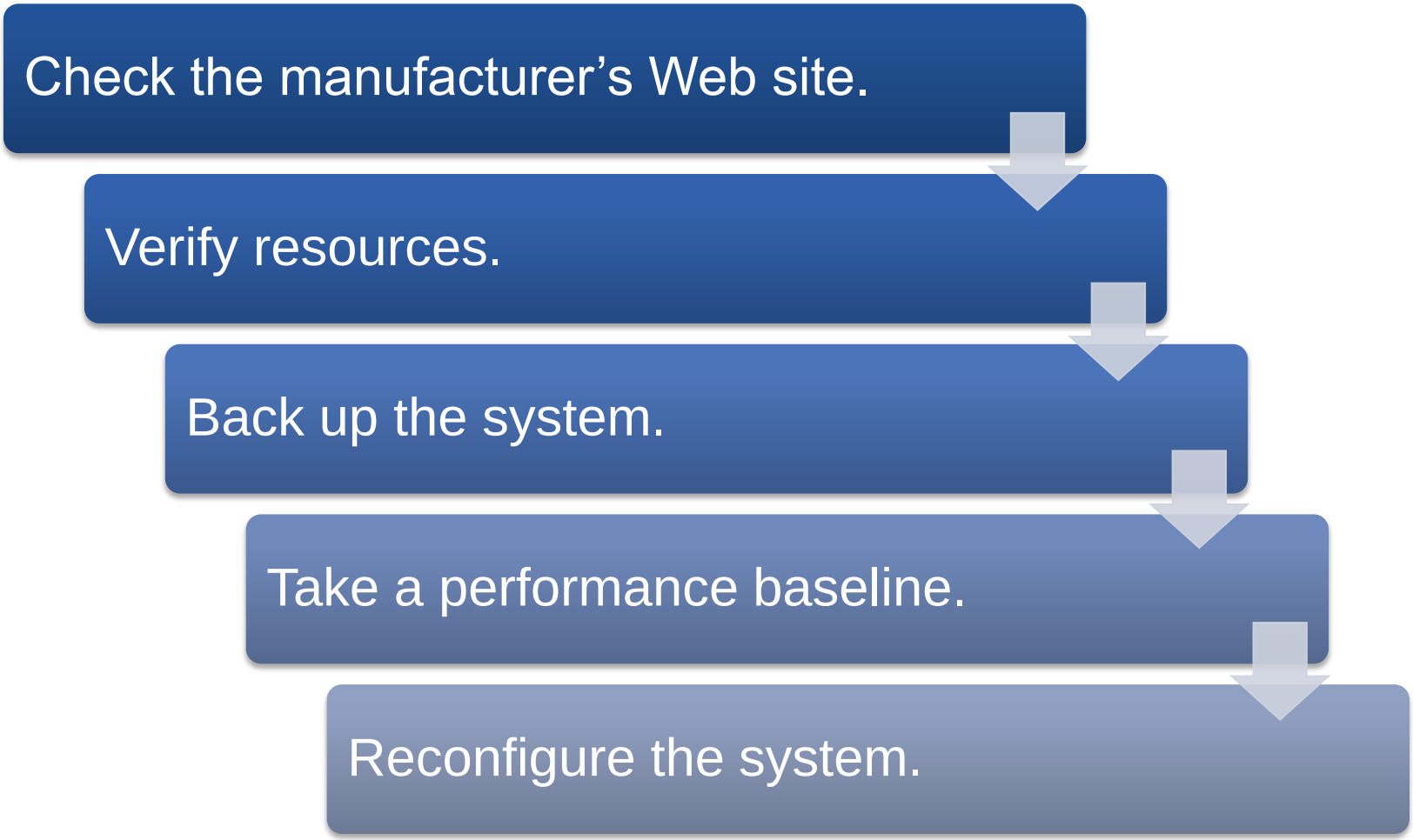
Securing Communications

- 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

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.

Installing Service Packs



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