Class announcements

- Final Exam:
  - Monday, June 3, 2009, 7:30 - 10:30 pm
  - Classroom unit 2

Student Presentations

- Samir Chaudry
- Robert Culpi
- Ledsey Rosales

Final Review

- Chapter 13 Trustworthiness (Availability and Security)
  - What fraction of time must the system be running to meet business needs?
  - Examples: WebCT? Online banking? Payroll?
  - What is the tolerance for downtime?
  - Planned outages (maintenance, upgrade, etc. - with sensitivity to timing)
    - We probably don't want to be doing maintenance on the financial aid system during the first week of the quarter
  - Unplanned outages
    - Emergency maintenance, system crashes, intrusion, file corruption, power outages
  - What is the application's intrinsic reliability - does it operate correctly in all circumstances?
Intrinsic reliability

- What conditions can affect the reliability of the application?
  - Software bugs
  - Component changes
  - Hardware failures
  - Insufficiently tested changes
  - Incompatibility with system software

Security

Security and network layers

Security and Network Layers

- This is one approach to identifying issues related to security. It is also intended to reinforce concepts of network layering.
- A brief description of each layer is provided followed by potential vulnerabilities and controls or mitigations to counteract the vulnerabilities

Security and network layers

Layer 1 - Physical

- Cable plant
- -Wiring closets
- -WAN connections
- -Network interfaces
- Networking and computing equipment
- -Routers
- -Hubs
- -Switches
- -Servers
- Physical Facilities
- -Data centers
- -Equipment rooms
- -Utilities
**Physical Layer Vulnerabilities**

- Loss of power
- Loss of environmental control
- Physical theft of data and hardware
- Physical damage or destruction of data and hardware
- Unauthorized changes to the functional environment (data connections, removable media, adding/removing resources)
- Disconnection of physical data links
- Undetectable interception of data keystroke & other input logging

Source: Adapted from SANS Institute

"Applying the OSI Seven Layer Network Model To Information Security"

---

**Examples of controls to counter physical layer vulnerabilities**

- Redundant power sources
- Fire suppressant systems
- Locked facilities and enclosures
- Access control mechanisms for logging entry and authorization
- Video and audio surveillance
- PIN and password secured locks
- Biometric authentication systems
- Encrypted data storage

Source: Adapted from SANS Institute

"Applying the OSI Seven Layer Network Model To Information Security"

---

**Security and network layers**

- Application
- Presentation
- Session
- Transport
- Network
- Link
- Physical

---

**Layer 2 - Link Functions**

- Communicating with the network layer
- Segmenting packets into frames that can be handled by the hardware
- Organizing data to be transmitted
- Communicating with the physical layer

---

**Link Layer Vulnerabilities Examples**

- MAC address spoofing
- Bypassing subnets and firewalls
- Errors in transmitting packets caused by intentional or accidental mis-routing
- Weak authentication or weak encryption allowing unauthorized access (wireless)
- Switch configuration problems that allow unintended interception of data

Source: Adapted from SANS Institute

"Applying the OSI Seven Layer Network Model To Information Security"

---

**Examples of controls to counter link layer vulnerabilities**

- VPNs protecting the links between networks
- Network Intrusion Detection Systems (NIDS) watching traffic for attacks
- Host Intrusion Detection Systems (HIDS) protecting connections to critical servers/hosts
- Virus scanning taking place on traffic coming in from outside the customer's network
- Built-in encryption, authentication and MAC filtering for wireless networks

Source: Adapted from SANS Institute

"Applying the OSI Seven Layer Network Model To Information Security"
Security and network layers

Layer 3 - Network Layer
- Concerned with network topology
- Determines the path a packet will travel to its destination.
- Uses IP addresses and routing tables to identify paths

Network Layer Vulnerabilities
- IP address spoofing
- DNS 'poisoning'

Examples of controls to counter network layer vulnerabilities
- Firewalls
- Routing filters
- Packet/traffic shaping
- Network monitoring software

Layer 4 - Transport
- Transmission of data streams into the lower layers of the model
- Packaging data streams for transport
- Where data conversations to a given host are multiplexed and sorted

Transport Layer Vulnerabilities
- Poor handling of undefined, unexpected or 'illegal' conditions
- Overloading port numbers by reusing for multiple functions
- Lack of validation controls resulting in 'forged' packets
- Hidden commands in packets to compromise systems

Source: Adapted from SANS Institute
“Applying the OSI Seven Layer Network Model To Information Security”
Examples of controls to counter transport layer vulnerabilities

- Strict firewall rules to limit access
- Inspection of firewall to disallow bad traffic
- Protocol inspection by firewalls triggered by imbedded commands
- Intrusion detection systems - packet analysis

Source: Adapted from SANS Institute
"Applying the OSI Seven Layer Network Model To Information Security"

Layer 7 - Application

Deals with high-level functions of programs that may utilize the network. User interface and primary application function and all other functions not pertaining directly to network operation occur at this level. It is the catchall for any issues not addressed within the other layers.

Application Layer Vulnerabilities

- Poor application coding (logic flaws, bugs)
- Back doors into applications
  - Intentional, e.g. for maintenance or troubleshooting
  - Unintentional, e.g. developer introduced either unauthorized or overlooked
  - Malicious, e.g. spyware, trojan, virus, etc.
- Overly complex security controls lead to shortcuts or avoidance
- Access by unauthorized individuals
- Weak identity management

Examples of controls to counter application layer vulnerabilities

- Employ application development lifecycle model that includes strong security components
- Anti-virus, anti-spyware
- Patching systems
- Follow best practices in security for application development
- Implement account management processes including provisioning, termination, and audit
- Identification, authentication, authorization mechanisms
- Change default accounts, passwords

Final Review

O’Brien (p. 39): framework for information systems knowledge needed by business professionals

- BPR decisions: streamline or reengineer
- Calculate NPV and make project decisions
- Productivity paradox, text p. 99
- Evaluation of Porter comp. model, strategy
- BPR vs. IT, text p. 79
- SIS, TPS, MIS, DSS
- IT to enable Porter strategies
- IT to benefit Porter value chain
- ERP types: text p. 79
- HHC rollout, Frito Lay
- Company-wide ERP rollout, Cisco
- Struggling startup co., Alibris
- Business function vs. process; BPR
- Push vs. pull IT
- Data vs. information; metadata
- Metcalfe’s Law
**Multiple choice question: terms and definitions**

The higher-level system functionality that arises by interconnecting subsystems is best called:

- A. Emergence
- B. Divergence
- C. Convergence
- D. Integration

**Alphabet Soup (across, then down)**

<table>
<thead>
<tr>
<th>LAN</th>
<th>CDN</th>
<th>ADN</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSN</td>
<td>NSP</td>
<td>NAP</td>
</tr>
<tr>
<td>ISP</td>
<td>IAP</td>
<td>ESI</td>
</tr>
<tr>
<td>.NET</td>
<td>NOC</td>
<td>TCO</td>
</tr>
<tr>
<td>IBM</td>
<td>EDS</td>
<td>SAP</td>
</tr>
<tr>
<td>ROI</td>
<td>NPV</td>
<td>IRR, IROR</td>
</tr>
<tr>
<td>TQM</td>
<td>MIS</td>
<td>BPR</td>
</tr>
<tr>
<td>POP (1)</td>
<td>POP (2)</td>
<td>ERP</td>
</tr>
</tbody>
</table>

**Review: terms to know**

- OSS BSD GPL
- workflow copyleft
- disintermediate
- thin client host
- replication regeneration
- ISP ISV LOB
- Java end-to-end solution

**Short answer question: buy, outsource, or build**

State one advantage and one disadvantage for each of the three approaches to acquiring application software.

1. Buying COTS
   - + less time and cost
   - + benefits of using a "standard" solution
   - + support available
   - - must mold org to app
   - - no potential for competitive advantage

2. Outsourcing
   - + developers not as familiar with org as you
   - + more opportunity for customizing than off the shelf
   - - contractor may share knowledge with competitors
   - - contractor may have too much bargaining power

3. Building
   - + most customizable of 3
   - + easier iteration between conceptualization and development needed
   - - most risky
   - - org may lack competency to do it

**Build vs. Buy?**

**Application Lifecycle**

**Stages:**

1. Conceptualization
2. Analysis
3. Architecture Design
4. Development Evolution
5. Testing and Evaluation
6. Deployment
7. Operations, Maintenance, and Upgrade
From an economics perspective, an inherent difference between information goods (examples: software, music CDs, videos) and manufactured goods (examples: cars, computers) is:

- A. The cost of producing an additional copy (in other words, marginal cost) of an information good is extremely small as compared to the cost of making another copy of a manufactured good.
- B. It is possible to produce copies of information goods but not manufactured goods.
- C. The cost of reproducing an information good is extremely high as compared to the cost of reproducing manufactured goods.
- D. The revenue of selling an additional copy of an information good is always extremely small, whereas that is not the case with manufactured goods.

**Concepts from Chapter 8**

- Externality
- Network effects
- Critical mass
- Positive feedback
- Standardization
- Lock-in
- Switching costs
- Phases in supplying content (create, replicate, distribute)
- Software economies
- Sunk costs
- Intellectual property
- Copyright
- Patent
- Privacy policy
- Privacy regulation

**Porter Models**

- Five forces
  - Buyers
  - Suppliers
  - New entrants
  - Substitutes
  - Rivals
- Value chain
- Competitive strategies
  - Primary
  - Supporting

**Porter's Five Forces, Cisco 3750**

**Supplier Power:**
- Suppliers are both partners and competitors. (Broadcom and Marvell)

**Buyer Power:**
- Many customers & few suppliers
  - Fortune 1000 enterprises
  - Government and education service providers

**Competition:**
- Cisco, HP, 3Com, Nortel

**Substitutes:**
- Lower cost unmanaged switches
  - Commodity copies of older generation products

**Government:**
- Antitrust (Microsoft, Intel, GE)

**Barriers to Entry:**
- Technical sales force
  - ASIC expertise
  - Large software team
  - Feature velocity prevents commoditization

**Review: Frito-Lay corporate strategy**

- Low-cost strategy
- Innovation

**Alibris: four ecommerce steps**

- Messerschmitt, page 85: (1) matching buyers and sellers, (2) negotiating terms and conditions, (3) consumption, and (4) customer service.

- How does the Alibris business model develop a competitive advantage over existing rare book sales channels in each of these four steps?
Alibris: four ecommerce steps

- How does the Alibris business model develop a competitive advantage over existing rare book sales channels in each of these four steps?
  - (1) Matching buyers and sellers: an expanded version of Interloc’s database listing helps buyers find their titles.
  - (2) Terms and conditions: significant 20%+ markup (hence bigger profits) compared to other rare book sellers. Alibris sells books for more than the brick-and-mortar price.
  - (3) Consummation: warehouse provides order consolidation and improves fulfillment performance compared to individual shops.
  - (4) Customer service: not mentioned in case study. Could argue that book quality is now guaranteed through warehouse inspections, and customers have a single point of contact (Alibris).

Alibris

- What added value does Alibris offer that Amazon and eBay do not?

- Applying Porter’s five-strategy model, what combination of strategies is Alibris using?
  - → Differentiation based on: (a) innovation, (b) growth, or (c) alliances?

Cisco Case

- Drivers of change
- Corporate strategy
- Vendor selection process
- Conference room prototyping
- Success factors
- Mistakes
- Lessons learned

Cisco’s “Market Adjacencies”

- Strategy: Use existing customer relationships and core competencies to move into different markets
- Usually timed with a “market disruption”
- Recent examples:
  - IP Telephony
  - Telepresence
  - Webex conferencing
  - Data center

E-Commerce

- Categories:
  - B2B
  - B2C
  - C2C
- Steps
  - Matching buyers and sellers
  - Negotiating terms
  - Consummation
  - Customer service
- Procurement
  - Direct, indirect, EDI, SCM

Multiple choice question: IT fundamentals from the text

- Which software layer is responsible for correctly interpreting that a collection of bits residing on a hard drive is actually a text file, and for sharing that interpretation with software in higher layers?
  - A. application
  - B. middleware
  - C. operating system
  - D. drive controller microcode
Stovepipe vs. Integrated Infrastructure

**Stovepipe Architecture**

--- OR ---

**Turnkey Solution**

- Single supplier provides all encompassing solution
- (complete with infrastructure)

**Integrated Infrastructure**

- Separate infrastructure that can support many applications

Amazon Kindle: stovepipe or integrated infrastructure? What about Kindle’s networking functionality?

- Does each Kindle have a:
  - MAC address?
  - IPv4 address?
  - What networks does it use?
  - What bandwidth is required, and how does Amazon pay for it?

Metcalfe’s Law (Nolan, p. 17)

- Gilder proposed “Metcalf’s Law of the Telecosm” - now a widely accepted heuristic
  - Interconnecting N computers results in a potential value of \((N^2)\)
  - Can apply to other types of networks (roads, telephones, fax machines) as well as computer networks

Intuition from Metcalf’s Law: the “Network Effect”

- We expect the value of a computer network to show increasing returns to scale
  - This gives positive feedback: large networks get larger, the rich get richer
  - Example: eBay grew because more people traded there, so more people wanted to trade there. A larger trading network is more valuable!
  - Be careful: some bad business models were formed to chase network effects! (Pets.com...)

Vertical Integration vs. Diversification

- A company is **vertically integrated** when it makes rather than buys the subsystems in it’s products.
- A **diversified** company produces products across different industry segments.

Vertical Integration vs. Diversification

- Why do customers favor less vertical integration?
  - Prefer competition amongst component suppliers
  - Mix and match components
  - Reduced lock in
- Disadvantages??
  - Customer needs to integrate components from different suppliers.
From stovepipe to layering

Data Voice Video

Application-dependent infrastructure

Many applications

Integrated Infrastructure (Maybe broken into Additional layers.)

Application-independent

Multiple choice question: case studies

- Which of the following is NOT a reason why Alibris invested in a fulfillment center?
  - A. for checking the quality of used books before shipping
  - B. to become a virtual intermediary for its dealer network
  - C. to ensure quick and correct delivery of used books
  - D. for order consolidation

Database technology

Given the segmentation of the database market that we studied, which of the following companies is classified incorrectly?
- A. Oracle: large enterprise-wide data market
- B. IBM: large web site market
- C. Microsoft: small enterprise-wide data market
- D. MySQL: small web site market

Networking technology

The network layer protocol (and a spanning layer) that allows geographically distant hosts to communicate is
- A. the Ethernet Protocol
- B. the Internet Protocol
- C. the Transmission Control Protocol
- D. the Hypertext Transfer Protocol

Link and Network Layer Interaction


- Time Division Multiplexing
  - Gives each connection the use of the link a fixed fraction of time
  - Fixed fraction of resources reserved for each connection
  - Technology called circuit switching

- Problem
  - When A is silent, A's fraction of link goes unused.
4. Statistical multiplexing

- Link shared in such a way that connections are not assigned a fixed fraction of the link (unlike TDM)
- A and B unlikely to offer peak rate at the same time.
  - $\max(A+B) < \max(A) + \max(B)$

Sun N-tier

SUN 3 - Tier

2009 content / application delivery network competitors

Wrap up