CPSC155b: Solution Set for Fourth Homework Assignment

Q1
Two examples from B2B:
- Consider an online B2B marketplace, in which the participants are large firms using EDI. The legacy technology here is EDI (electronic data interchange), which "provides computerized documents through which business can exchange the considerable information that business-to-business transactions require." The online B2B marketplace should provide a convenient interface to the EDI systems. The B2B data format should be converted so that the EDI systems can understand it. Otherwise, firms that have invested years of effort in EDI and rely on EDI-based systems to function will be reluctant to participate in the B2B. Glushko's paper "How XML Enables Internet Trading Communities" explains CommerceOne's proposed migration path from EDI to XML.
- Consider a company that uses the Internet for communication between its two branches. The legacy technology here is a MRP system, which "enables companies to more efficiently track what they need to purchase based on their production schedules." The two branches may exchange information about purchases through the Internet. This information should be in a format compatible with the MRP system.

Examples from earlier in the course include:
- Fax was a technological innovation that was compatible with the legacy telephone system. Because fax traffic was sent over ordinary phone lines and fax machines could be plugged into ordinary phone jacks, adoption of fax technology was easy.
- DVDs are compatible with CDs. So, if you buy a new computer with a DVD-ROM drive, you can still use all of the data that you have stored on CDs. Here the innovation is the DVD format, and the legacy technology is the CD format.

Q2
The answer to the first part of this question is in the lecture notes for March 1 and in the FTC report:
  (a) a horizontal marketplace serves many different industries, while a vertical marketplace serves a single industry;
  (b) a horizontal marketplace has "a broad product focus," while a vertical marketplace has a product focus on "the supply chain of one product category" or on "expertise and in-depth content knowledge for one industry."

Examples of horizontal B2Bs include HotOffTheWire, NTE, and equalFooting.
Examples of vertical B2Bs include Covisint, MetalSite, and BuyProduce.

In my opinion, participant ownership is potentially more problematic in vertical B2Bs. Participants are likely to be established companies that are direct competitors, and there is significant potential for collusion in order to fix prices or to exclude new competitors or small companies that serve niche markets. You can get full credit for the opinion that participant ownership is more problematic in horizontal B2Bs if you give a good justification.

Q3

Many of the principles that were relevant in our discussion of security technology's role in online content distribution are relevant here as well. Digital signatures and public-key certificates are helpful if the entity whose key is being certified is "known" to the verifier of the signature; in practice this usually means that the known entity is a company with an established "real-world" reputation. Firewalls are helpful in guarding against unauthorized access to machines if they are properly configured and competently administered. Encryption keys, passwords, and other secret information can be used to achieve confidentiality or authentication, but only if it can truly be kept secret; this is essentially incompatible with storing it on a networked PC.

Scenarios in which information-security technologies can solve problems include:
- Company A orders some products of Company B in a B2B marketplace. Suppose A can get B's public-key certificate from a reliable CA. Then A can verify B's digital signature on every message to ensure that it is really from B.
- In the same B2B marketplace, company A can set up an encrypted communication channel with company B and keep its order information confidential. If B has a certified public key, a standard protocol such as SSL should be able to accomplish this.
- A customer of an auction service (either buyer or seller) can verify that he is really connected to the service (and not to an impostor), using standard protocols, certified keys, *etc.* Similarly, he can verify that he is connected to an established payment or escrow service.
- Both B2B and C2C sites (such as Covisint, eBay, *etc.*) can protect their confidential data by storing it on machines that are guarded by well-administered firewalls or other access-control technology.

Scenarios in which information-security technologies cannot completely solve problems include:
- Two customers of a C2C auction service can send each other signed messages once they've decided to do business, but, unless these customers actually "know" each other in the "real world," the signatures won't be very meaningful. Alice can't really conclude anything from the fact that PK_{BOB} correctly verifies a signature and that Verisign says PK_{BOB} belongs to Bob unless she knows something about Bob's trustworthiness, creditworthiness, *etc.*
- Similarly, two customers of a C2C auction service can send each other encrypted messages. If the item being sold is a digital good, the seller can transfer it to the buyer in encrypted form. But the decryption keys are at risk of being stolen if they are stored on ordinary networked PCs.
- Customers of both C2C and B2C services can rely on secure-communication protocols such as SSL to stop eavesdroppers from capturing their transaction information as it is being transferred. But they cannot necessarily stop the e-commerce services themselves from selling the information to unsavory partners or from turning it over to law-enforcement agencies.

Q4

(a) The four words or phrases that I had in mind are "online catalog," "printer," "purchase order," and "invoice." You will also get full credit if you chose "catalog" instead of "online catalog."

(b) A DTD for invoice:

```
<!DOCTYPE DOCINVOICE [
<!ELEMENT invoice (customer, product, price, time, signature)>
<!ELEMENT customer (#PCDATA)+>
<!ELEMENT product (#PCDATA)+>
<!ELEMENT price (#PCDATA)+>
<!ELEMENT time (#PCDATA)+>
<!ELEMENT signature (#PCDATA)+>
<!ATTLIST invoice invoiceid ID #REQUIRED>
]>
```

A DTD for online catalog:

```
<!DOCTYPE DOCCAT [
<!ELEMENT onlinecatalog (entryno, product, type, description, price)+>
<!ELEMENT entryno (#PCDATA)+>
<!ELEMENT product (#PCDATA)+>
<!ELEMENT type (#PCDATA)+>
<!ELEMENT description (#PCDATA)+>
<!ELEMENT price (#PCDATA)+>
<!ATTLIST price  unit CDATA #REQUIRED
                 currency CDATA #REQUIRED>
]>
```

A DTD for printer:

```
<!DOCTYPE DOCPRINTER [
<!ELEMENT printer(type, manufacturer, description, price)>
<!ELEMENT type (#PCDATA)+>
<!ELEMENT manufacturer (#PCDATA)+>
<!ELEMENT description (#PCDATA)+>
<!ELEMENT price (#PCDATA)+>
<!ATTLIST price  currency CDATA #REQUIRED>
]>
```

A DTD for purchase order:

```
<!DOCTYPE DOCORDER [
<!ELEMENT purchaseorder(suborder+, totalprice)>
<!ELEMENT suborder (product, type, unitprice, number, subtotal)+>
<!ELEMENT product (#PCDATA)+>
<!ELEMENT type (#PCDATA)+>
<!ELEMENT unitprice (#PCDATA)+>
<!ELEMENT number (#PCDATA)+>
```

```
<!ELEMENT subtotal (#PCDATA)+>
<!ATTLIST unitprice  unit CDATA #REQUIRED
                 currency CDATA #REQUIRED>
<!ATTLIST subtotal  currency CDATA #REQUIRED>
<!ATTLIST total  currency CDATA #REQUIRED>
]>
```

You can find many examples of DTDs in my lecture notes from March 20, in Glushko's lecture notes from March 22, and on the web site http://www.xcbl.org