

1.264 Final Exam Solutions
Fall, 2005

Name: _____

Exam guidelines:

1. 3 hours are allowed to complete the exam.
2. Open notes, open book.
3. No laptop computers or calculators are allowed. You have some arithmetic to do by hand in one question. You may approximate to within 20%.
4. No cell phones or messaging devices are allowed. Please turn off any that you have brought.
5. Short answer questions: Your answers are limited to a maximum of 2-4 sentences or phrases. Demonstrate that you understand the principles and key points. You will receive full credit for an answer if you make the principal observation(s) that the question is asking for. Details are not necessary.

1. Security (20 points)

In public key encryption, a digital certificate is stored on computers that must communicate securely. You are in charge of security for a transportation or supply chain application to manage purchases of retail items from suppliers. It was bought from a third party vendor and configured for your company's or agency's use. You decide to use SSL to protect the network connections between your computers and those of the merchandise vendors. You use a variety of other measures to protect the clients and servers in the system. (If you're an MST student, imagine this is a system in which you purchase spare parts for bus and rail vehicles from a variety of vendors, similar to the aircraft parts vendors.)

For the SSL portion of security, you make a presentation to your management and they ask you a series of questions as you go along. Please answer them below:

a. Does the certificate contain the computer's public key? If not, where is the public key kept? Suggest a good place if it is not in the certificate.

Yes. It is sent to other computers that send secure information to this computer.

b. Does the certificate contain the computer's private key? If not, where is the private key kept? Suggest a good place if it is not in the certificate.

No. The private key is not in the certificate, since the certificate is sent to other computers 'in the clear'. The private key can be kept in an encrypted file on your computer, protected by a password (your Windows password on Internet Explorer and by browser-specific passwords for other browsers).

c. Must the certificate be protected from attackers?

No. It is sent on request to any computer that requests it.

d. How is the private key protected from attackers?

Through a password, as mentioned above.

e. If a public key is obtained by an attacker, what is the risk? What measures should be taken to eliminate the risk if the public key is thought to be compromised?

No risk; no measures needed.

f. If a private key is obtained by an attacker, what is the risk? What measures should be taken to eliminate the risk if the private key is thought to be compromised?

The compromised computer can be impersonated by the attacker. The certificate of the attacked computer must be revoked by being placed on the certificate revocation list that browsers check.

g. Digital signatures can be generated by certificates. The sender signs the message with his or her private key, and the message is then verified by the receiver using the sender's public key. What risks are there in accepting a digital signature of this sort? How secure is a digital signature versus a paper signature or a PIN number entered by a user to verify, for example, that they are making a transaction? (Your system is replacing letters, faxes and physical transactions with credit cards with system-to-system transactions.)

The risks are that the computer may have been compromised by a virus, which can send transactions, or the private key may have been compromised by an attacker, who has obtained it. Thus, the transaction may not be known by, or approved by, the user. The risks of digital signatures are perceived to be higher than those of paper signatures, where the risk is of forgery. It is also perceived as higher than those of PINs, which are entered by humans and cannot be triggered by viruses or other software attacks. Digital signature attacks are difficult to repudiate; forgeries can be determined and PIN numbers require having a physical card (credit card) that must be stolen first, whose absence will be noticed by its owner.

h. You tell the management that the software vendor has excellent software process, and that this enhances security. What is the relationship between software process and security? Does good software process improve security?

Yes. Systems built to defined requirements and design, and reviewed and tested against that design, will have fewer application errors, which are the most common security hole. Few cryptographic or security systems are broken by attackers; it is usually simpler to find bugs in the application that can be exploited.

i. You gave a talk the previous week on system architecture, and one of the managers remembers part of it. What is the relationship between the virtual storage hierarchy that we discussed in class and security? Briefly describe any security issues that the virtual storage hierarchy creates.

Program memory can be written to disk, kept indefinitely in main memory, or cache, or registers, and is vulnerable to attack. For example, private keys could be exposed. Computers should allow the option of encrypting exposed data, but essentially none do.

j. The merchandise purchasing system uses passwords to protect parts of the system. How long must a password be to provide the same protection as a 128 bit symmetric key? Name one method to allow users to reasonably remember and use a password of this length.

Password characters have between 1.5-2 bits of entropy per character. Using 2 bits/character, passwords would be 64 characters long to meet our criterion. Using passphrases, strings of human language words, allows long passphrases to be remembered.

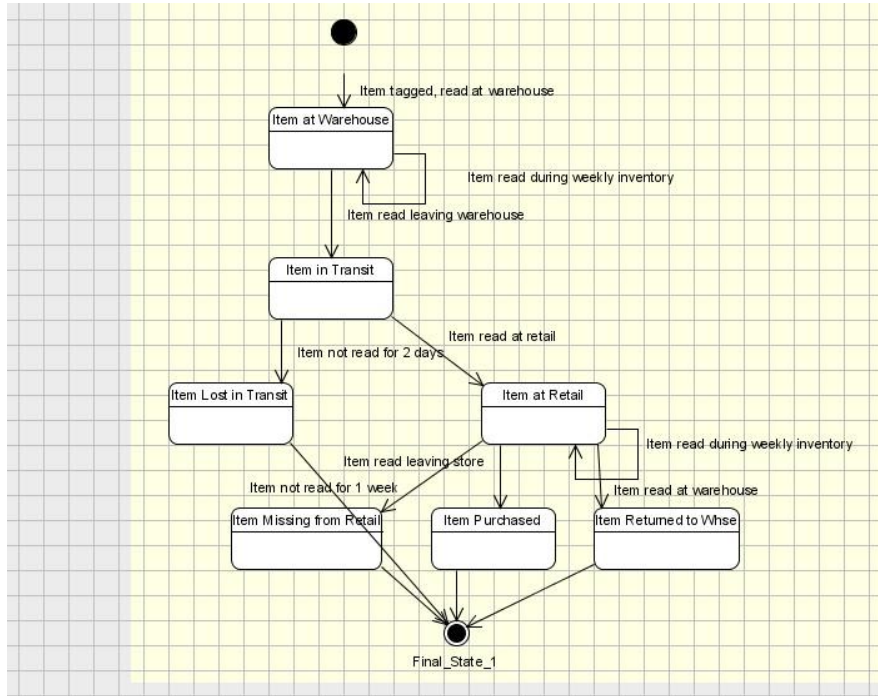
2. UML (20 points)

Your inbound supply chain is based on receiving products that have RFID tags on them. The tags are placed on every item (not every case or pallet) shipped from a warehouse to the retailer. The retailer is a high-end retailer; the average item price is \$300; and many items are custom or one-of-a-kind jewelry or artwork, so the cost of an RFID tag on each item is minor. Items are shipped overnight. (If you're an MST student, you may consider the items to be replacement parts for bus or rail vehicles, which are high cost and come in many variations, and are shipped from a warehouse to transit agency maintenance facilities.)

An item with a tag may have the following events occur:

- Tag placed on item and read at warehouse
- Tag read at warehouse during weekly inventory, with handheld RFID reader
- Tag read leaving warehouse
- Tag read arriving at retail store (or transit maintenance facility)
- Tag read leaving retail store as purchase (or installed on vehicle)
- Tag read at warehouse after having been read at retail: returned or defective
- Tag read at retail during weekly inventory, with handheld RFID reader
- (Tag not read at retail during weekly inventory, and not read leaving store, and not read at warehouse: item is missing)
- (Tag read leaving warehouse, but never read at store: item is missing)

a. Draw a UML state diagram to represent the possibilities listed above. Label the states and transitions (events).



b. What other type of UML diagram could you use to represent the same requirements? Name at least one, and contrast it with the state model.

Sequence diagram could be used: it would capture the events directly but would not easily capture the states.

3. Data model (20 points)

Each retailer has a par level, or desired inventory level, of each product. A product is, for example, a pair of gold earrings in a specific style. The retailer (store) will specify what quantity (number of items) of each product it wants to carry. High-end retail stores often carry just a few (1, 2 or 3 items) of many different products.

These stores are serviced by well-paid (on commission) sales reps, who have what is called ‘trunk stock’: they have inventory of certain products in their vehicles. When a product is sold and a store needs another one, the sales rep drives it over, often the same day. Sales reps have a numerical sales rep ID that is unique (for example, 5334). Stores have text store names that are unique (for example, MIT Fashion City). Some of them

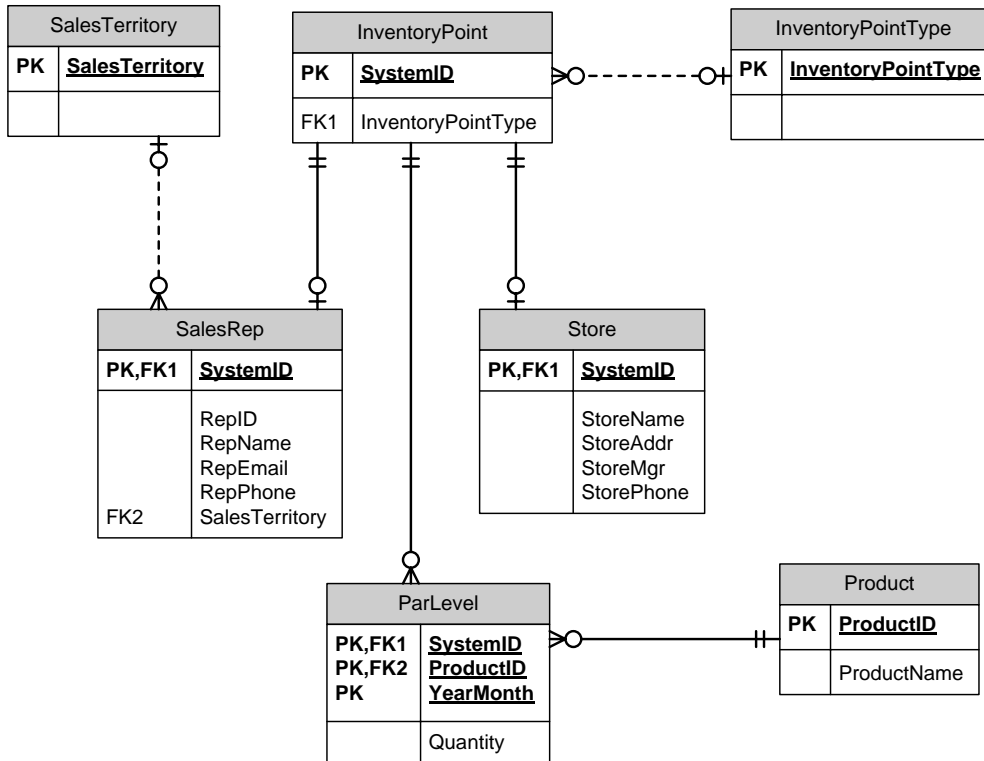
may be numbers; a store could be called 007, for example. There is a different par level every month, for every store and every sales rep, for each product.

Each store has an address (treat it as just one column), a manager, and a phone number. Each sales rep has a name, sales territory he or she covers, an email address, and a phone number. Each product has a unique ID and a name.

~~a~~ Model this scenario elegantly. (There is probably no perfect answer.)

Draw a data model for these entities and attributes.

- Draw a box for each entity; give each an appropriate name.
- List the attributes in the box for each entity.
- Indicate the primary key for each entity by placing the phrase (PK) next to its name.
- Draw all relationships between the entities in the model.
- Indicate foreign keys by placing the phrase (FK) next to attributes that are foreign keys.
- Indicate the cardinality of each relationship: many-many, many-one or one-one. Use crow's foot notation; if you use another notation, define it.
- Include the appropriate domain tables.
- The model must be fully normalized.



4. XML (20 points)

Assume that you are using XML for data transfer. Write out a DTD file that corresponds to the portion of your data model that defines the par level for **a store** (not a sales rep) for all products and all time periods (year/month). This DTD should validate an XML document that will be sent from the warehouse to one inventory point at the start of a month informing it of the planned stock levels for that month for all products that they carry.

- Assume that all fields are parsed character data
- The DTD must enforce the business rules contained in your data model.
- You must send the system ID of the inventory point, and optionally send its type (store or sales rep)
- You must send the store name, address, and you may send the manager and phone number.
- All other data elements in the XML document are required
- The document is for only one period (year/month). Send the year/month variable only once in the XML document. E.g., 01-06 (January 2006)

a. Write the DTD file:

```
<?xml version="1.0"?>
<!ELEMENT InventoryTransaction (InventoryPoint, YearMonth,
ParLevel+)>

<!ELEMENT InventoryPoint(SystemID, InventoryPointType?,
StoreName, StoreAddr, StoreMgr?, StorePhone?)>

<!ELEMENT ParLevel(ProductID, Quantity)

<!ELEMENT SystemID(#PCDATA)>
<!ELEMENT InventoryPointType (#PCDATA)>
<!ELEMENT StoreName(#PCDATA)>
<!ELEMENT StoreAddr (#PCDATA)>
<!ELEMENT StoreMgr(#PCDATA)>
<!ELEMENT StorePhone (#PCDATA)>

<!ELEMENT ProductID (#PCDATA)>
<!ELEMENT YearMonth (#PCDATA)>
<!ELEMENT Quantity (#PCDATA)>
```

b. Write out an appropriate XML document for the following par levels:

- InventoryPoint SystemID: 334
- InventoryPointType: Store
- YearMonth: 01-06
- StoreName: MIT Fashion Warehouse
- StoreAddress: 77 Massachusetts Ave, Cambridge MA 02139
- Par level:
 - i. ProductID A22, quantity 3
 - ii. ProductID G555, quantity 2

XML file:

```
<?xml version="1.0" encoding="utf-8"?>
<InventoryTransaction>
  <InventoryPoint>
    <SystemID>334</SystemID>
    <InventoryPointType>Store</InventoryPointType>
    <StoreName>MIT Fashion Warehouse</StoreName>
    <StoreAddr>77 Massachusetts Ave, Cambridge MA
02139</StoreAddr>
  </InventoryPoint>
  <YearMonth>01-06</YearMonth>
  <ParLevel>
    <ProductID>A22</ProductID>
    <Quantity>3</Quantity>
  </ParLevel>
  <ParLevel>
    <ProductID>G555</ProductID>
    <Quantity>2</Quantity>
  </ParLevel>
</InventoryTransaction>
```