

Computer Systems and Society

3.1 System Design

Parts of a System:

The parts of a system include the **Motherboard** which is the connection between all the components, the **CPU** which is mounted on the motherboard which provides the processing power of the system. The motherboard has many slots in it (PCI) which allow for many other components to be added on. Cards that fit into these slots include, a **Video Card**, this is what the monitor connects to. **The Sound Card** drives all your speakers and also allows you to plug in a **Joystick** or other similar control device. The **Hard Drive** is where all the data is stored, and all programs are run off of, the hard disk also works with the **RAM**, which creates temporary space for apps and programs to be run in. A **Modem**, it allows you to connect to other computers, and access the internet, it operates over the phone line. **Network** cards are also gaining popularity as the internet can be accessed via a network now, network cards also allow you to make a home network connecting all the computers in the house together. A **CDROM** drive is also required with today's computers, other types of cd drives include, **CDR**, which record onto CDs and **DVD** drives, which support the new digital video disk format. A vital part of the system is the **Monitor**, this is where you will view everything on your computer so it is a very important component. A **Keyboard** and **Mouse** are also a must in with a computer system, they are your interface with the computer. A **Printer** is not a required piece of equipment but it is a nice peripheral to have because you can print out documents and files. **Scanner** is another non essential item yet it is very handy for making hardcopies of something into a digital copy. **Floppy Disk** drive is also an essential to the system, it is the only way to get a computer started up and running.

Data to be processed

In the situation outlined in the Case Study: "The use of computers at a large bank". The data which must be stored and processed includes; the customer's account number, the personal identification number (PIN), the bank's branch code, customer's withdrawal limit and the amount withdrawn in the last time period, ex. day. All this information must be stored in a large database because the amount of users is around 20 million, it is the only way to keep all the accounts organized. The information also has to be stored very efficiently in order to make retrieval the least amount of time possible.

Data Capture and Presentation

Data capture in this case occurs on two ends of the system. One on the customer's end of the system, the Automated Teller Machine (ATM). On this end of the system, nothing can be directly changed, except for a balance. The user is

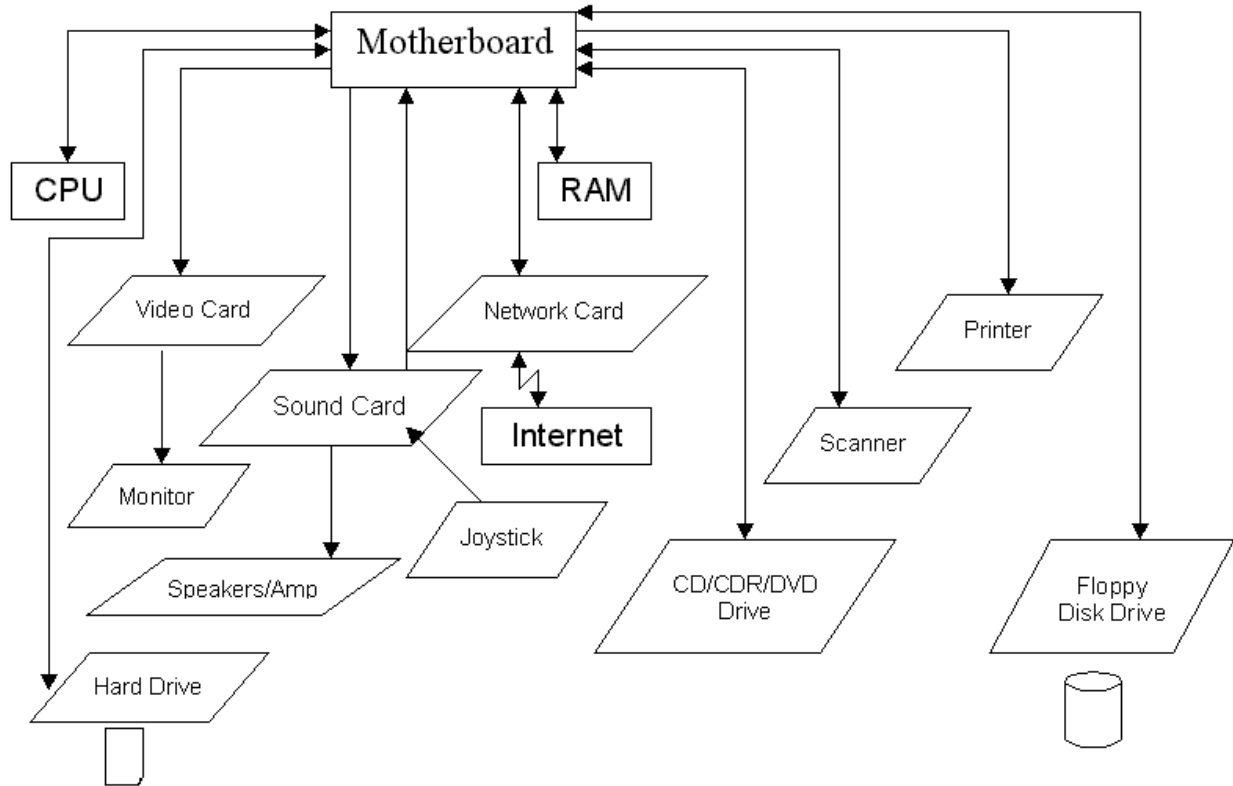
restricted to withdrawing cash only, no other options are available. In order for anything else to be changed in an account a bank employee has to use. On this end of the system all the properties of each account can be accessed. Cash can be withdrawn from tellers as well, but most often they are used for deposits or inquiries related to your account or account status.

On the ATM side of the system users are asked to insert a Interac card, or debit card. This card holds all the information on accessing their account and can be used at the ATMs. Once the card is inserted the user can withdraw money directly from his or her account. Users are also presented with an account statement, for the purpose of notifying the user on their account status.

Data Protection, Error Detection, Data Recovery methods

Data protection is a very important element with banks, because of the amounts of money be moved every day, any leak in data protection could cause a great loss. One prevention system in place is the shadow system. This system is on stand by 24 hours a day, and if any situation the main server goes down, the shadow system takes over. The shadow system is updated every time some data changes on the main system. This system makes it very difficult for any unwanted users to tamper with the system if the main system goes down. When dealing with bank machines, matching information is what it is all based on. If information inputted by the user does not correspond with what the bank has in its system the an error is reported and the users attempt to make a transaction fails. Windows has a data recovery method which is meant to protect users from losing a file they accidentally delete, this feature is disputed by some because by deleting a file you really aren't deleting it, just moving it to a temporary directory.

System Flowchart



Integrity and Security of Data

Refers to the validity of data. Data integrity can be compromised in a number of ways:

- Human errors when data is entered
- Errors that occur when data is transmitted from one computer to another
- Software bugs or viruses
- Hardware malfunctions, such as disk crashes
- Natural disasters, such as fires and floods

There are many ways to minimize these threats to data integrity. These include:

- Backing up data regularly
- Controlling access to data via security mechanisms
- Designing user interface that prevent the input of invalid data
- Using error detection and correction software when transmitting data

Data Security is more an issue is the data protected from who it should not be accessed by. Passwords are the most popular way of restricting access to files and data that is to be protected. Passwords are very effective, but often they can be worked around, with many gates into parts of the system, passwords can be changed by some professional hackers. In some high level security system, and

physical connection is needed for data access, therefore there are moving parts in the system, which will only make a connection when a correct password is entered. Backing up files is also very important, not only backing up but encrypted backup is very important to be sure that leaks cannot be made into the backed up system files.

Data Encryption: The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text ; encrypted data is referred to as cipher text. There are two types of encryptions, Public Key Encryption, this methods works by everyone giving out their encryption code, but not giving out the decryption code, this allows people to send and receive files safely. The other is Symmetric Encryption, this method uses the same key for both ends of the data transfer.