SOFTWARE AUDIT SYSTEM

Gaurav Kumar Nigam
M.Tech (IIIT Allahabad)
Lecturer
Jaypee Institute of Information Technology, Noida
U.P. (INDIA)

Abstract: ***To remotely monitor your computer over the internet, you have to install this software on the remote computer (called as server) as well as on your own computer (called as client). When connected , Software Audit System software gives you the full mouse and keyboard control over your computer and you can see the whole screen of the remote PC on your own desktop. As we know that computer networks within companies and organizations become more extensive and more complex, there is a considerable growth in the number of software programs that are installed and used on the computer systems. In order to increase the reliability and efficiency of computer Systems, it is mandatory that we clearly understand and control all the computer programs that are being used. The problem may also arise when people installing unauthorized or copied computer programs on their Desktop PC's. It is necessary that we provide auditing tools that can facilitate audit data either locally or reside on to a central network manager and it gives the information related to the installed and used computer programs.***

The objective of this paper is to design a system that monitors concurrent activities in an organization or network and stop illegal use of system.

Keywords : ECB,DES,SSL,TLS,JVM

1. INTRODUCTION

As there is a fastest growth in computer networks within companies and organizations that causes a large amount of computer systems to be used by a number of users. All users installed a number of software programs and use their computer for the sake of their company or organization but it is clear that the administrator have a clear understanding of all the programs that are installed and used by the users in order to increase the efficiency and reliability of their computer systems.. As an example, different users use other available versions of a software programs that causes system compatibility problems. The problem may also arise when people installing unauthorized or copied computer programs on their Desktop PC's.

As there is a considerable increase in viruses and other infected programs in the computer systems, it is recommended and mandatory that we have to install anti-virus software on all the computer systems and keep eye on their regular updation. There is a large threat to the computer systems from various computer viruses and many malicious programs [1].

As we know that in order to secure a computer system from malicious computer viruses, it is necessary that anti-virus computer programs have relatively low access and control inside a computer system. Anti-virus software receives the scan requests and process the request on-access or on-demand basis[1]. The data file is first scanned before it is being used. This information is passed directly to anti-virus software, from there it is transferred to the audit agent and it checks what are the programs that are used by the computer system. We can view this audit data as a product of an anti-virus software. The audit data generator efficiently reside on the anti-virus software in such a way that it provides detailed, secure and correct audit data while it consumes low processing overhead.

In an organization there are a number of authorized users that are using the computer systems each having their user name and password but it may happen that the users using unauthorized programs that are not permitted to them by the company or organization. So in order to have a check on their activities the administrator has to monitor their activities so that they should not waste the bandwidth of the company.

The users may watch the movies or load the hard drive with waste material that will cause the system to take more time to process any task. It is significant that each user do the necessary tasks which are assigned to them for the sake of the company. There are different users that employ different versions of the programs that may cause the compatibility problems. The problem may also arise due to the people using unauthorized programs or copied programs.

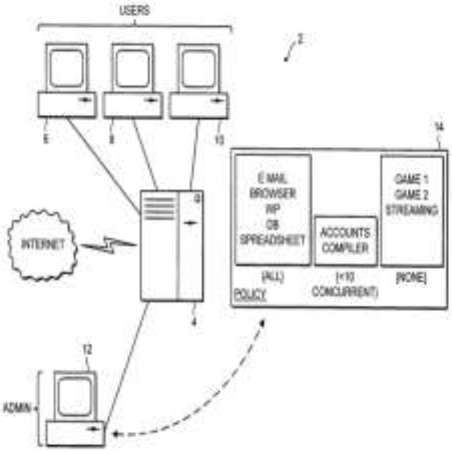


Fig 1.1

Fig 1.1 shows a computer network (let's say 2 in Fig 2.1) that we see in many business organizations. The computer network (let's say 2 in fig 1.1) consists of a central server (let's say 4 in Fig 1.1) and a number of user computers (let's say 6, 8,10 in Fig 1.1) that are directly linked to the central server (let's say 4 in Fig 1.1). A system administrator (let's say 12 in Fig 1.1) has to control the network (let's say 2 in Fig 1.1). The network 2 has directly linked to the internet **adapted from [1].**

Fig 1.2 shows the relationship among an operating system (shown in fig 1.2 as 14), an anti-virus software (shown in fig 1.2 as 16) and an audit data generator (shown in fig 1.2 as 18). The operating system (let's say 14 in Fig 1.2) proceeds its processing when it receives a request to access file that is stored on a HDD (hard disk let's say 20 in Fig 1.2) or stored elsewhere. Operating system will grant access to that process that has valid permissions.

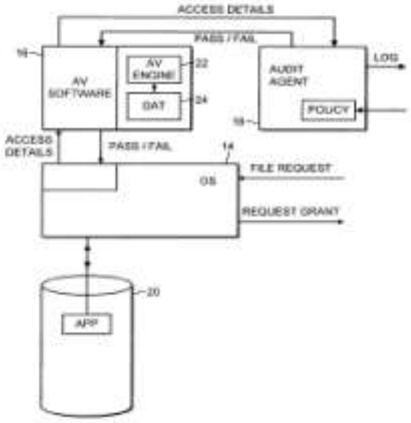


Fig. 1.2

Fig 1.3 shows a flow diagram that explains the operation of an operating system. At the step shown as 26 in Fig 1.3, the operating system (let's say 14 in Fig 1.3) gets a request to access a file that is generated by any application program or by a user command.

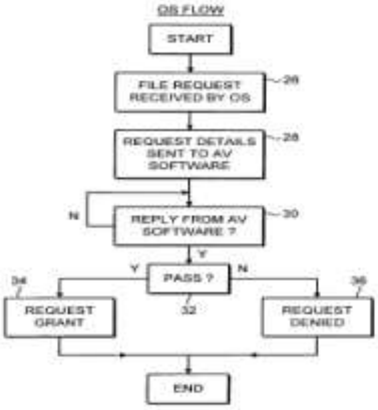


Fig. 1.3

Fig 1.4 shows a flow diagram that demonstrates the processing of the anti-virus software.

As we know that computer networks within companies and organizations become more extensive and more complex, there is a considerable growth in the number of software programs that are installed and used on the computer systems. In order to increase the reliability and efficiency of computer Systems, it is mandatory that we clearly understand and control all the computer programs that are being used. Let's take an example, different users using various versions of programs that cause compatibility problems[1]. The problem may also arise when people installing unauthorized or copied computer programs on their Desktop PC's. It is necessary that we provide auditing tools that can facilitate audit data either locally or reside on to a central network manager and it gives the information related to the installed and used computer programs.

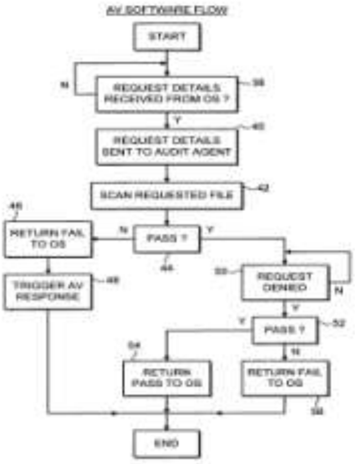


Fig. 1.4

2. METHODS AND ALGORITHM USED

2.1 Electronic Code Book (ECB)

Electronic Code Book (ECB) is defined as a mode of operation for a block of cipher text. In ECB each possible block of plain text has a cipher text value that is defined earlier and vice versa. In other words, the same plaintext value will always produce result in the same cipher text value. In ECB the plaintext is handled 64 bits at one time and each block of plaintext is encrypted using the same key. We use the term codebook because for a given key, there is a unique cipher text for every 64 bits of plain text [22]. We may imagine a large codebook where there is a separate entry for every possible 64 bit of the plain text pattern showing its corresponding cipher text. If we have a message which is larger than 64 bits, then the procedure is that we have to divide the message into 64 bit blocks and use padding for the last block if needed. Decryption is applied by taking one block at a time but always using the same key [21]. In figure, the plain text (you may use padding if necessary) consists of a 64 bit blocks, $P_{1,}$ $P_{2,}$ ..... , P_n and the corresponding cipher blocks is C_1 , C_2 , …., C_n. The ECB is useful for a small amount of data , such as encryption key[21] .Thus we can say that if you have to use ECB then you have to transmit a DES key securely .

We use Electronic Code Book (ECB) when we have a plaintext that is divided into separate blocks, each of which is then encrypted independently of other blocks. The Electronic Code Book has a useful feature to support a separate encryption key for each block type [21]. One of the important properties that ECB have is that if there is the same appearance of 64 bit block of plain text, then it always produces the same cipher text. However, it is recommended that Electronic Code Book is not used for small block sizes (if the size is less than 40 bits) and similar encryption modes. This is because of the reusability of some words and phrases that causes the repetition of blocks of cipher text that came out.

The ECB mode method is not secure for a lengthy message. Because if the message is properly organized, then it is not an easy task for a cryptanalyst to exploit these regularities. For example if a message starts with certain predefined fields, then the cryptanalyst may have a number of choices of known plain-cipher text pairs that he may use [21]. However, security is improved by adding the random pad bits to each block. On the other hand, 64-bit or larger blocks should contain enormous amount of unique features that makes attack to the codebook to be unsuccessful.

2.2 Data Encryption Standard (DES)

This algorithm is adopted in 1977 by National Bureau of Standards, which is now called as National Institute of Standards and Technology (NIST), as Federal Information Processing Standard (FIPS PUB 46) [21]. The algorithm is also referred as the Data Encryption Algorithm (DEA). Data Encryption Standard (DES) is an algorithm that is based on Symmetric Key Algorithm. It means that there is a same key on the both sides for encryption and decryption process. The algorithm transforms 64 bit input into a series of steps into a 64 bit output. The same steps are used with the same key that is used to reverse the encryption. DES algorithm is an insecure algorithm because of its key size. So its later version triple DES was introduced later on after its invention.

DES algorithm takes a plain text of fixed length string and transforms it through a number of consecutive operations into another cipher text which is of the same length. In DES the size of block is 64 bits but out of these only 56 bits is used in the algorithm and the rest of 8 bits are used for checking the parity and after checking they are neglected or discarded.

There are total 16 round of processing in this algorithm. There are two term initial and final permutation (IP and FP).FP does the inverse of IP and vice-versa. Initially, we take 56 bits of the key out of 64 bit by Permuted Choice 1 (PC-1) while the remaining of eight bits are used for parity check bits [17]. The 56 bits are divided into two halves each of 28-bits each. Now each half is thereafter processed one by one separately. There are successive rounds in which there is a circular right or left shift by one or two bits (i.e. specified for each round), and then 48 sub key bits are selected by Permuted Choice 2 (PC-2) which consists of 24 bits from the left half, and 24 from the right[17].

3. TECHNOLOGY USED

3.1 Remote Method Invocation (RMI)

Remote Method Invocation (RMI) facilitates an object function calls among Java Virtual Machines (JVMs). JVMs are found on separate computers but one JVM can call another JVM method that belongs to an object stored in it. Methods can even pass an object that has never been done by a foreign virtual machine, and thus allowing dynamic loading of new classes as required [24]. .

Consider the follow situation:

- Web Developer A writes a service that performs some useful and predefined function. He updates this service regularly according to his need and adding some new features and improved the existing ones.
- Web Developer B tries to use that service that is provided by Web Developer A. However, it is not convenient for A to provide B by regular updating every time.

Java RMI gives a solution for this problem. As we know that RMI load new classes dynamically. Hence, the Web Developer B can use RMI to manage the regular updates for him. Web Developer A maintains a web directory where he places all of his new classes, which can be easily fetched by RMI for new updates when they are required.

3.2 TRANSPORT LAYER SECURITY (TLS) /SECURE SOCKET LAYER (SSL)

One problem that you often face in monitoring a network is to maintain the data security when data is transferred between various applications across an unrecognized network. TLS/SSL may be used in authenticating servers and clients, after that it is being used to encrypt the messages between authenticated parties [26].The protocols TLS, SSL versions 2.0 & 3.0, and the (Private Communications Transport) PCT uses public key cryptography. These protocols are provided by the Security Channel.

The TLS/SSL authentication process consists of sending a message from client to a server, the server first checks whether the response came from the trusted body or not, then it authenticate and reply to the response. When the connection is established, client and server start performing the operation of exchange of their session keys, and after that their authentication dialog process ends. When the authentication process is over, a symmetric encryption key starts the SSL-secured communication between server and client [26].

When the servers authenticate to the clients, TLS/SSL doesn't need to store server keys on a domain controllers or on a database, like the Microsoft Active Directory service [26]. The clients register the server's validity credentials with the certificate of a trusted certification authority's (CA's), which are loaded in installing Microsoft Windows Server 2003.

3.2.1 Merits of TLS/SSL

TLS/SSL allows various merits to clients and servers: [26]

3.2.1.1 Secure authentication, privacy of message, and message integrity

3.2.1.2 Interoperability

3.2.1.3 Algorithm flexibility

3.2.1.4 Ease of deployment

3.2.1.5 Ease of use

3.2.1.1 Secure authentication, privacy of message, and message integrity

TLS/SSL uses the encryption in securing transmitted data. TLS/SSL protocols are used to authenticate the servers and, optionally, in a secured communication the client check the identity of parties' .It provides data integrity via an integrity check value. The TLS/SSL security protocol protects data against various attacks, they are masquerade attacks, man-in-the-middle or bucket brigade attacks, rollback attacks, and replay attacks [26].

3.2.1.2 Interoperability

TLS/SSL starts its working with most available Web browsers, like Internet Explorer and Netscape Navigator, and it operates on many operating systems and Web servers, like the Windows operating system, UNIX, Novell, Apache (version 1.3 and later), Netscape Enterprise Server, and Sun Solaris [26].

3.2.1.3 Algorithm flexibility

TLS/SSL allows various mechanisms that are used for authentication, uses various encryption algorithms for the secure session.

3.2.1.4 Ease of deployment

There are many applications that transparently use TLS/SSL on a Windows Server 2003 operating system. You may use TSL for secure browsing via Internet Explorer and Internet Information Services (IIS).

3.2.1.5 Ease of use

Since TLS/SSL is implemented below the application layer, its most operations are completely not visible to the client. That's why client have less or no knowledge about security of communications but still it is protected from the attackers.

4. IMPLEMENTATION

4.1 Overview: Software Audit System is software that is used by the computer administrator for computer maintenance and providing technical support to someone who needs assistance with his/her system. By using this software you can remotely shutdown or restart computer system.Software Audit System is an open source software that is used for viewing and/or controlling a distant PC.Software Audit System uses RMI (Remote Method Invocation) with SSL/TLS to establish a secured connection between the viewer and the server.Software Audit System is intended to run across different platforms (based on JVM).It also ensures the security of passed information both ways using Data Encryption Standard (DES) algorithm using Electronic Code Book (ECB). The Remote PC is always protected by password. You have to know the password in order for using the Remote PC from the current PC.

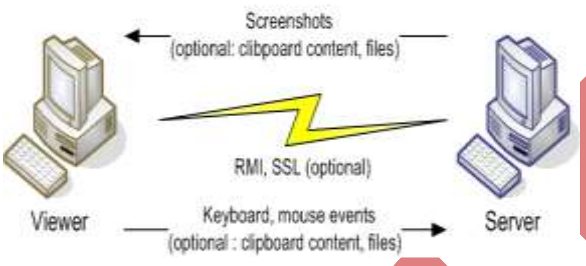
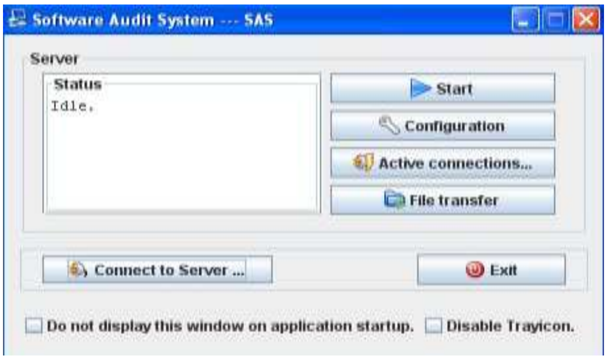

Screenshots
(optional: clipboard content, files)
RMI, SSL (optional)
Viewer
Keyboard, mouse events
(optional : clipboard content, files)
Server

Fig 5

4.2 Main features

- It allows to see the Screenshots of the remote system , manage the transfer of keyboard and mouse.
- It consists of many control functions such as Start, Stop, Pause and Resume, view only, full control.
- There are Screen functions to control the size of screen like full screen, custom size, scale, ...
- It allows Data compression (with level selection)
- You can also use JPEG compression (with level selection)
- It allows Color quality (use full colors, 16 bits, 256 colors, gray color)
- You can transfer file from one system to another.
- You can get the Connection information’s like their duration, transferred data size and speed .
- It allows the process of Authentication & encryption
- You can view Multiple –sessions.

4.3 Snapshots of the Software Audit System :

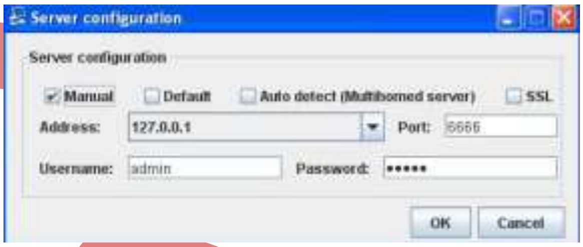


Status

```
Idle.
```

□ Do not display this window on application startup. □ Disable Trayicon.

Fig4.3.1 This is the main window of SAS



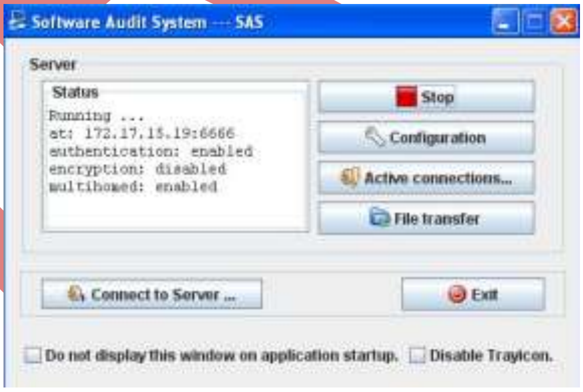
Server configuration

☑ Manual □ Default □ Auto detect (Multihomed server) □ SSL

Address: 127.0.0.1 Port: 6666

Username: admin Password: •••••

Fig4.3.2 SAS Server configuration

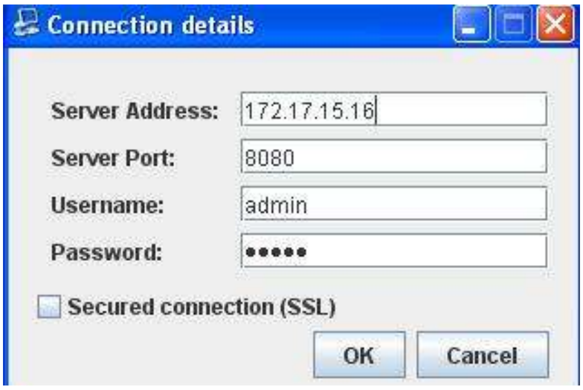


Status

```
Running ...
at: 172.17.15.19:6666
authentication: enabled
encryption: disabled
multihomed: enabled
```

□ Do not display this window on application startup. □ Disable Trayicon.

Fig4.3.3 SAS Main Window after the server is started



Server Address: 172.17.15.16

Server Port: 8080

Username: admin

Password: •••••

□ Secured connection (SSL)

Fig4.3..4 Connection Details

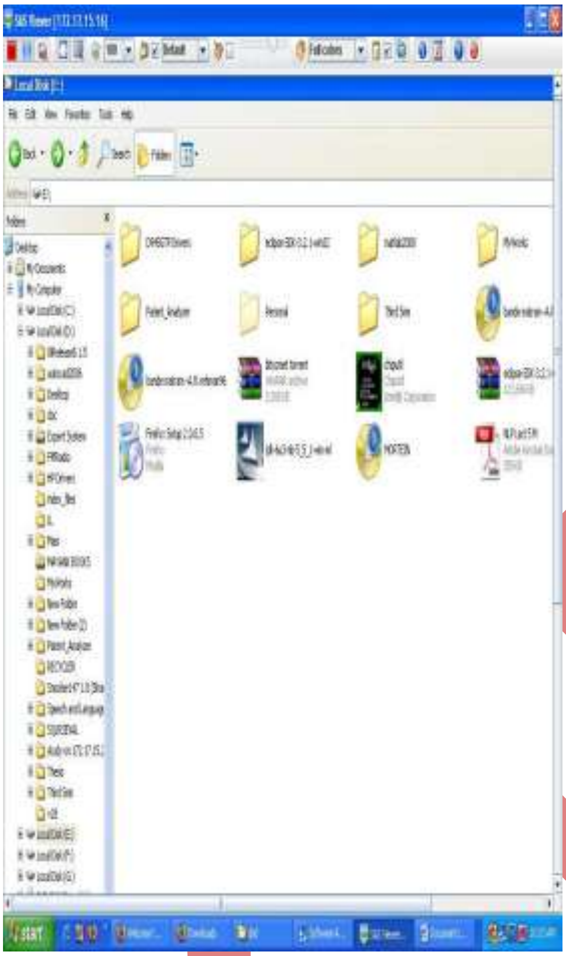


Fig 4.3.5 SAS on Windows XP shows the complete desktop control of the remote PC

5 Conclusion

As we know that computer networks within companies and organizations become more extensive and more complex, there is a considerable growth in the number of software programs that are installed and used on the computer systems. In order to increase the reliability and efficiency of computer Systems, it is mandatory that we clearly understand and control all the computer programs that are being used. Let's take an example, different users using various versions of programs that cause compatibility problems. The problem may also arise when people installing unauthorized or copied computer programs on their Desktop PC's. It is necessary that we provide auditing tools that can facilitate audit data either locally or reside on to a central network manager and it gives the information related to the installed and used computer programs.

References

[1] www.uspto.gov / US Patent Number 7,281,267 Titled "Software Audit System".

[2] IEEE paper on Development of Information System Audit support System by Ingoo han and bomil suh , Graduated school of Management ,korea Advanced Institute of Science and Technology , Seoul , Korea

[3] IEEE paper in International Conference on Computational sciences and Its Applications with topic on Auditing System using rule-based Reasoning in Ubiquitous Computing by Moohun Lee,sunghoon cho,Hyokyung Chang,Junghee Jo,Hoiyoung Jung,Euiin Choi, Dept of computer engineering , Hannam University.

[4] IEEE paper on Knowledge-Based Decision Support System For Competitive Software Audit by Maya daneva,Juliana Peneva,Rossen rashev,Radostina Terzieva.

[5] IEEE paper on The Experience of Auditing Software for safety Critical railway Signalling Equipment by Tapan Kumar Ghosal,samar Bhattacharya,Kalyankumar Datta , centre for knowledge based system, jadavpur University, Kolkata .

[6] IEEE paper on Repository Software Evaluation Using the Audit Checklist for Certification of Trusted Digital Repositories by Joanne S. Kaczmarek,Thomas G. Habing,Janet Eke.

[7] IEEE paper on Software Security Analysis-execution Phase Audit by Bengt Carlsson , Dejan Baca.

[8] US Patent Number 5,398,196 Titled "Method And Apparatus For Detection Of Computer Viruses".

[9] US Patent Number 5,671,412 Titled "License Management System For Software Applications".

[10] US Patent Number 6,009,518 Titled "Computer System For Providing Improved Security for Stored Information".

[11] US Patent Number 6,029,256 Titled "Method and System for Allowing Computer Programs Easy Access To features Of A Virus Scanning Engine".

[12] US Patent Number 6,415,280 Titled "Identifying and requesting data in Network Using Identifiers Which Are Based on contents of data".

[13] US Patent Number 6,577,920 Titled "Computer Virus Screening".

[14] US Patent Number 6,721,721 Titled "Virus checking and Reporting for Computer Database Search Results".

[15] US Patent Number 6,735,700 Titled " Fast Virus Scanning Using Session Stamping".

[16] Auditing Information Systems by Mario Piattini

[17] Data Encryption Standard - Wikipedia, the free encyclopedia,

http://en.wikipedia.org/wiki/Data_Encryption_Standard

[18] http://www.tropsoft.com/strongenc/des.htm

[19]http://www.comms.scitech.susx.ac.uk/fft/crypto/des_algorithm_details.txt

[20]http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci344944,00.html(ECB)

[21] Cryptography and Network Security Principles and Practices 3rd Edition by William Stallings

[22]http://www.yourdictionary.com/hacker/electronic-code-book

[23] Java remote method invocation - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Java_remote_method_invocation

[24] Introduction to Java RMI , www.javacoffeebreak.com/articles/javarmi/javarmi.html

[25] List of Java APIs - Wikipedia, the free encyclopedia en.wikipedia.org/wiki/List_of_Java_APIs (java api table)