PGP trust model example

Ok that was the full trust I know this guys a and b but I dont have full trust in this case it is 50 % some ti ames I do trust and some ti ames I don't, even these 50% trust as concept is not very descriptive it is fuzzy concept ,how you will trust some one 50% you cannot assign those kind of stuffs, some ti ames this kind behaves ok someti ames he doesn't that is 50% trust and b is also 50% but look at these two guys , they can sign a's key and you can say it is dot's version of circle that means it could be valid key y during the key signed by a , then you an get the key i ammediately i am going to look fro another entity who sends the key and have the 59% trust that is b for example both of the m make 100%trust and if you have 25% trust then you have sign 2 25% and 1 50% trust but if you have 75% trust 1 25 and 1 75 is going to make this guy legiti amate it is signed by a only I don't see any full trust or half trust who signs g's key there is no way for you to make g's key legiti amate and that's why you are not going to use it ,j like that k is like that and key is signed by c and I don't see anyone signed for s we call that idle mode this is the new guy he doesn't know anyone in this web and no one can make the key of web legiti amate , we have to break the wishes circle by signing it yourself, some one has to sign it and make it legiti amate for this network and r the key of r is not going to be again legiti amate there is not signature that I can trust , that's going to be your decision , you know that guy and its your decision to assign some level trust so that means that this guy is waiting signature from you if he signs then its the first level the guy you know and the kind of third parties known by the guys , there is no direct contact so you will decide whether to make it c's key legiti amate or not legiti amate are you clear with this ?.. so this the way we are distributing ht keys in PGP and that's why this is called web of trust we have web of trust in PGP , these aer ways jus register the keys in key server and whoever need your key will go to key server and this makes the PGP very powerful you saw the packet structure and everything ,the key distribution encryption algorithm and they are using DS, it is a pretty secure algorithm and it comes with this kind of key distribution stuffs that requires any 23rd party involvement it does require relationship or something , i amagine that you are spy agent or something and you want to try to monitor the mails of the people and if you are using x509 kind of thing then things could be a little bit problematic and but this one no third party and i amplementation is done by open source and this key distribution it could be PGP, so that's why it is called pretty strong algorithm and that's why lot of algorithm got really angry to the government as it was available to the public and everybody start using it whether it is encryption or strong security ,when we see SMI AME , SMI AME is a standard email security and it will come with the weakness and that is put intentionally just to make it available to the big brother kind of thing but with the PGP ,I will explain , don't forget that when you start or readoing the email PGP will ask your passphrase but i amagine if you are using SMTP email ,you left your station and screensaver and they can read your mail if you are commit to inbox but with PGP if the message will come tot the inbox and it is encrypted you are not goin to s anything expect a black page if you try to read it then it will ask the passphrase but if you don't know the passphrase then they cant read the mail , smmie will come with all the security and things but they are asking any password when you start treading the mail when you receive the mail you will decipher the plaintext of the mail , it doesn't require any passphrase entry from the user that is the drawback of the SMI AME there is not security for your email but PGP there is always a security if some one even access to your inbox ,in the email or there was an attack and intruder managed to gain access to the email server with SMI AME they are going to be able to read it but with

PGP they are not able to do it everything depends on passphrase and that is the end of this topic and we will go to next topic.

SMI AME (Secure multipurpose internet mail extension)

We are going to start with SMI AME in lab then we are going to go to PGP in reverse the first thing is SMI AME and the second the PGP , but you are going start when we finish the chapter I m going to post it on my website every detail don't do anything right now ,SMI AME is the standard security protocol for email security , security enhancements to mi ame email ,mi ame is the multipurpose internet mail extensions ,mi ame provides support for varying content types and multipart messages what they did si this remember I talked about the email protocol SMTP , we said it is text base and the encrypted email was binary file , remember in radix 64 the encrypted email file was in binary into text so that we can send it with the smpt ,SMTP is text base when it is text based it doesn't support any enriched text format key bolds like italics and all we cant do it in SMTP and third you cant transfer nay videos in the mail but you can by attachment i amagine you are sending a email there is a camera here, i am typing something for the email , and the video is capturing my email and i am talking at the same ti ame ,I have the voice input , video input and while i am writing bold italics all those kind of stuffs, all the styles everything is going to go in one mail and i amagine when I want to read the mail and I click on that one video will play automatically and voice and ani amated thing will be displayed automatically i am not going to click on each and everything separately when I say video and voice there are different kind of videos and voice so which one it is going to be separated as I said there are lot of different formats available and also for text like doc, pdf and these are different formats and we cannot do this scenario with SMTP what they did is they defined content type they are going to split the mail in two parts first they are going to say they want the text form of the email and the second part lets say that's a video part , so the video starts from this point and end stat this point but the content type is video or voice and they defined different content types and put it in e mail saying that this part of the mail is video and this part is video that way they embed the info into SMTP and they convert into text file and net it ,so that's why theyare called multipurpose means lot of format video is going to be handled extension to the SMTP, with encoding binary data to textual form , like RADIX 64 and we will see what type of encoding schemes only dilemma is it is not like PGP that I m going to use radix 64 , no , these guys say that i am going to use radix ansi or ber or some option and also content type what type of video formats are there??..mpeg, jpeg , what about voice?. Mp3 and there is called nuela or something you see different encoding for this , and also text pdf, doc and these guys will come from different format , SMTP has no security we i amprove it using MI AME so that we can embed all the videos and voice into the mail so then we are going to add security in mi ame by adding content type ,content type signed datas ,this is the part of the mail ,lets have a look at it ,this is quite a good stuff you are not going to see anywhere because this thing right now comes with microsoft outlook ,every email client that you are using like outlook ,outlook express what else anything else as email client , firewall, thunderbird one more safari , there are different email client available al of them will have mi ame , as of now but they are going to come with security enhancements as well in other words SMI AME is standard for todays email security

RFC822

What is this? That is the standard definition of SMTP ,you can find all the details of SMTP in this document RFC822 defines a format for text messages that are sent using electronic mail some thing like this date, message id ,but someti ames email servers cannot deliver the message and you get some error reports if you check those reports you will see the message id ,from , subject ,cc, bcc, fields in SMTP protocol and there is text message ,this we are going to change as it is quite limited.