Mobile computing

Technology, Computer

Today security is the biggest barrier faced by mobile computing on the way to their progress. It's not a new matter of discussion. It remained a threat from beginning of computer systems. Even since humans started communicating with each other, there has been a need to keep secrets. Same techniques of keeping secrets are required, when computers interact with one another. Actually technology is using in both positive and negative senses. Here is an example how it is using in negative sense.

Whenever we hear the word hacker or cracker we get a negative image in our minds, everyday in newspapers, magazines, movies, TV etc we hear that some one got hacked due to which they had to suffer heavy looses. In general a hacker is considered to be a person who uses his skill with computers to try to gain unauthorised access to computer files or networks. Chris Brenton (2001) described that " Active Defence states that a hacker is a person who has deep understanding of computers and networking" further he says that hacker is some one who feels the need to go beyond the obvious.

Means they are not the dumb person, it is different matter how they are using their capabilities. Following are the briefly explained some security techniques using in distributed network systems. SSL is a secure layer of protocols which runs between the layers of TCP/IP and higher-level protocols such as HTTP or IMAP. TCP/IP on behalf of the higher-level protocols helps to authenticate SSL- enabled client over SSL-enabled server. That also results to create an encrypted connection between client and server. SSL security technology not only helps to improve the safety of Internet communications but also on intranet.

That's why SSL is a standard for encrypted client/server communication between network devices. It has ability to maintain secure data traffic over the network that has very importance in the distributed environment. SSL generates a key after each encrypted transaction, which comes in two strengths, 40-bit and 128-bit. This strength refers to length of key generated by transaction. As the key length will increase it will difficult to break the encryption security. Data encryption is generally considered the best technique securing data storage and transmission.

According to techWeb (1999) statement " Encryption is the transformation of data using an algorithm, from one form to another utilizing one or more encryption keys during the transformation process". It is the art of storing information in a form that allows it to be revealed to those you wish to see it yet, hides it from all others. The original information to be hidden is called " plain text". The hidden information is called " cipher text". Encryption is any procedure to convert plain text into cipher text. Decryption is any procedure to convert cipher text into plain text. Public and private are key types of encryption.

Encryption and decryption are two ways conversion of data from one form to another. While encryption, data changes to its original form depends on its algorithms. On the other hand if we run the same algorithm in reverse condition, then data again comes to its original form. Supposing some wants to send credit card information from one computer to another over the Internet, what he will do is use public key to encrypt it and then the private

key to decrypt it. Public key algorithms are very complex maths problems some are based on prime numbers, factoring, elliptic curves, logarithms etc.

In the public key cryptosystem, the public can only determine private key if you solve the problem. There for the most important thing is that the problem should be so complex and time consuming that the attacker would think twice even before proceeding. Digital signature is another way to make the system secure. " Digital Signature is an electronic code that is attached to a message or file that gives it a unique identity and allows you to certify that a message or file that is sent by you actually came from you".

(Felix Weber, 2001) In order to truly understand the implications of digital signatures one must understand what a digital signature is and how it works. Simply, a digital signature is a way for you to identify yourself electronically. Just like a hand-written signature identifies a person separately, a little piece of computer data will do the same for a computer. But how do digital signatures work and what do they protect or sign. Well suppose you want to send someone an email and you want the recipient to know that the email did in fact originate from you.

The way you would do that is by using a digital signature. But in order for the digital signature to ensure authenticity there must be some way to verify that this signature came from you. This is accomplished by using key pairs. When you get a digital signature of your own you are assigned a public key and a private key. The private key is used to sign the document, which is then sent to the recipient. The recipient then uses your public key to verify

the signature. Here is an example of how digital signature works in distributed environment.

Let's say computer A want to send a signed documents to computer B. A uses his private key to generate his digital signature or fingerprint. The private key creates a code series based on a complex mathematical algorithm that is embedded in the message that A sends. When B gets the electronic document he then uses A's public key which he got from a public key server to then verify the digital signature and ensure that the message or document that he has received is in fact from A. The whole communication process between both of them is secure communication.

Different Internet security companies issue a PIN number that is unique to a computer. 2. 2 How we can make a system secure? While developing a security policy an organisation must identify those entities that are considered valuable enough to undergo security measures, with in these entities certain resources are more valuable than others and more focus should be given to them. Like in an electronic funds transfer system the exposure of the financial transactions likely will have more severe impact than the exposure of a personnel record of a customer.

Following these principles would help in avoiding a lot of common security problems. That is true that this set of principles will not be able to cover every possible flaw that could show up, but it will minimise the chances of any kind of hacking or cracking and make the system more reliable. Here I am going to discuses a few important ones. One of the most common analogies in the security community is that security is a chain of links. A

secure system is most likely secure as the weakest link. Hackers will always look for and attack weakest parts of the system.

It's probably no surprise that the hackers will always tend to go after low hanging fruit. If they target your system for whatever reason, they're going to take the path of least resistance. That means they'll try to attack the parts of the system that look weakest, and not the parts that look strong. A similar kind of logic is widely applicable to the physical world. There is always more money in a bank than a general store, but which one is more likely to be robbed? , the general store, of course. Why? Because banks tend to have much stronger security precautions; general stores are much easier targets.

This principle has is hundred percent applicable in the software world, but most people don't pay any attention. In particular, Kirk Job-Sluder (2002) concluded that " Cryptography is always considered to be the weakest part of a software system". Even if you use Secure Socket Layers1 with 512-bit RSA keys and 40-bit RC4 keys, which are considered incredibly weak cryptography, an attacker can probably find much easier ways to break in a system rather tan just attacking Cryptography. Sure, it is breakable, but doing so still requires a large computational effort.

If the attacker wants access to the data that travels over the network, then they'll probably target one of the end points and try to find a flaw like a buffer overflow or memory leakage, and then they dig out the stage of data when it gets encrypted or decrypted. All the cryptography in the world cannot secure data if there is a buffer overflow. Sometimes it is not the software that is the weakest link in your system; it could also be the general

surrounding considers social engineering when an attacker uses social manipulation to break into a system.

Typically, a service centre will get a call from a sincere sounding user, who will talk the service professional for a password that should not be given away. This sort of attack is generally quite easy to launch, because customer service representatives do not like to deal with stress. If they are dealing with someone is really mad about not being able to get into his account, most of them will give away the password and will try to calm the situation down. One good strategy is to limit the capabilities of technical support as much as possible.

Like the entire Customer service representatives wouldn't be allowed to peep or change the passwords of the users only a selected few persons should do it after a lot of questioning and enquiries. I remember when someone hacked my hotmail account I mailed hotmail's technical staff for help and they asked me a few but very complex questions which could only be answered by a real account user, the questions were like, name the last three passwords you used, what date the account was last accessed by me, what approx. date did I create my account etc.