Soni J Balwir *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 11, November- 2015, pg. 31-40 **ISSN: 2321-8363**

Security Issues in Mobile Computing

Soni J Balwir[1], Dr. Mahendra Kondekar[2]

[1]*Student Of TY MCA MIT (E) Aurangabad(M.S), sonibalwir7@gmail.com*
[2] *Asst. Prof. Of MCA Dept. MIT (E) Aurangabad(M.S), mhkondekar@gmail.com*

Abstract
In the present mobile communication environment, lot of research is going on, to improve the performance of issues like handoffs, routing etc. Security is another key issue that needs to be considered, which comes into picture once the communication channel is set- up. Many security protocols are being proposed for different applications like Wireless Application Protocol, 802.11 etc. most of them are based on the public and private key cryptography. This paper provides an insight on these cryptographic protocols and also looks into the current research project going on at Sun Microsystems Lab on wireless security.
***Keywords*:** Mobile computing, mobile computing security.

1. Introduction
The birth of "Mobile Computing" has signalled a new era in the field of computing and information systems. The concept of mobile computing is derived from the realization that as computing machinery decrease in size and increase in computing power users will demand these machinery to be part of their everyday life, accompanying them in the carrying -out of their everyday tasks. Researchers in this new field envisage that mobile computing units, such as today's laptops and palmtops, in the future will be communicating with each other via wireless networks, whilst providing location transparency to the user. This notion of transparency is carried-over from that in distributed computing, in which the user is unaware of the remote physical location of resources being used by the distributed computing system.
With the rapid growth in the wireless mobile communication technology, small devices like PDAs, laptops are able to communicate with the fixed wired network while in motion. Because of its flexibility and provision of providing ubiquitous infrastructure, the need to provide security increases to a great degree. As wireless communication takes place mainly through the radio signals rather than wires, it is easier to intercept or eavesdrop on the communication channels. Therefore, it is important to provide security from all these threats. There are different kinds of issues within security like confidentiality, integrity, availability, legitimacy, and accountability that needs to be individually taken care off.

2. Why is Security an Issue?
Security is a prerequisite for every network, but mobile computing presents more security issues than traditional networks due to the additional constraints imposed by the characteristics of wireless transmission and the demand for mobility and portability. We address the security problems for both infrastructure-based WLANs and infrastructure-less ad hoc networks.

2.1 Security Risks of Infrastructure-Based WLANs
Because a wireless LAN signal is not limited to the physical boundary of a building, potential exists for unauthorized access to the network from personnel outside the intended coverage area. Most security concerns arise from this aspect of a WLANs and fall into the following basic categories:
Limited Physical Security: Unlike traditional LANs, which require a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an access point (AP) device. As shown in Figure 1 an access point communicates with devices equipped with wireless network

adaptors and connects to a fixed network infrastructure. Since there is no physical link between the nodes of the wireless network and the access point, the users transmit information through the "air" and hence anyone within the radio range (approximately 300 feet for 802.11b) can easily intercept or eavesdrop on the communication channels. Further, an attacker can deploy unauthorized devices or create new wireless networks by plugging in unauthorized clients or setting up renegade access points.

Constrained Network Bandwidth: The use of wireless communication typically implies a lower bandwidth than that of traditional wired networks. This may limit the number and size of the message transmitted during protocol execution. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency, corrupting the signal until the network ceases to function. Since the aim of this type of attack is to disable accessing network service from the legitimate network users, they are often named denial of service (DoS) attack. Denial of service can originate from outside the work area serviced by the access point, or can inadvertently arrive from other 802.11b devices installed in other work areas that degrade the overall signal.

Energy Constrained Mobile Hosts: To support mobility and portability, mobile devices generally obtain their energy through batteries or other exhaustive means, hence they are considered as energy constrained mobile hosts. Moreover, they are also resource-constraint relative to static elements in terms of storage memory, computational capability, weight and size. In WLANs, two wireless clients can talk directly to each other, bypassing the access point. A wireless device can create a new type of denial of service attack by flooding other wireless clients with bogus packets to consume its limited energy and resources.

3. Security Issues

Many authors [7] have presented classifications of security issues in communication networks. There are five fundamental goals of security in information system.

• Confidentiality, preventing unauthorized users from gaining access to critical information of any particular user.

• Integrity, ensures unauthorized modification, destruction or creation of information cannot take place.

• Availability, ensuring authorized users getting the access they require.

• Legitimate, ensuring that only authorized users have access to services.

• Accountability, ensuring that the users are held responsible for there security- related activities by arranging the user and his/her activities are linked if and when necessary.

The way these goals are achieved depends on the security policy adopted by the service providers.

4. Authentication Protocols

In a wireless mobile communication environment, the messages transmitted over wireless medium are more susceptible to eavesdropping than in wired network. Also, it is possible for any user to access the mobile communication system using a false identity. In order to provide security from the above-mentioned situations, we use encryption, which provides confidentiality of the messages sent over wireless channel and to authenticate. There are two types of encryption techniques in cryptosystem, namely symmetric-key cryptosystem and asymmetric-key cryptosystem. The main idea in using these techniques is to conceal the content of the messages before transmitting them in the clear (radio signals). In this system, a common key is shared between the entities before any communication session begins and later these session keys are used to encrypt the data.

4.1 Symmetric-Key and Asymmetric Cryptosystems

In a symmetric-key cryptosystem, the encryption and decryption keys are the same. Since the encryption and decryption transformations are easily derivable from each other, a common secret key is shared between the

communicating entities in advance via a secure channel. Therefore, the security of symmetric-key cryptosystems depends on keeping the key secret. Some of the most important symmetric-key cryptosystems that are used presently are the American Data Encryption Standard (DES) and the Japanese Fast Data Enciphering Algorithm (FEAL). In an asymmetric-key (public-key) cryptosystems, the encryption and decryption keys differ. Each user has a private key and a public key. Let us consider a scenario, where Alice wants to send a message to Bob. Alice encrypts the message M using Bob's public key Pbob, which is exchanged before the session started. At Bob's side, this encrypted message is decrypted using Bob's private key Sbob, which is known only to Bob. Another function in public-key cryptosystem is the use of digital signatures. In this process, if Bob wants to send a message to Alice, he first signs the message M with his private key Sbob to obtain a digital signature S= [h (M) Sbob] of M, where h ( ) is one-way hash function. Here, hash functions like MD5 and SHA are used which accepts a variable size message and outputs a fixed sized representation h (M) of M. Alice decrypts this encrypted message by using Bob's public key. One of the widely used public-key cryptosystem is the RSA public-key cryptosystem proposed by Rivest, Shamir, and Adleman (RSA). The security of the RSA key is based on the difficulty of factoring large integers. Another public-key cryptosystem that is widely used is the Modular Square Root (MSR) public-key cryptosystem. This is a variant of RSA, where the public key is the modulus N, which is a product of two large primes. MSR requires only one modular multiplication for computing the encryption keys, and because of its low computational cost, is preferred over RSA.

4.2 Protocols based on Symmetric-Key Encryption

4.2.1 Encryption using Symmetric-key function

Because of its negligible computational cost, a symmetric-key encryption is preferred. In this protocol, the home network broadcasts a random number r.

Mobile user ⇐ Home Network: r

Mobile user ⇐ Home Network: IDms, f (k, r)

Then, the mobile user sends its identity IDms along with function f (k, r), where f () is a symmetric-key function such as DES or FEAL, k is the secret key of the mobile user that it shares with the home network. When the home network receives the secret key from mobile user, it fetches the key in the database and completes the authentication. Once the session keys are exchanged, the messages are encrypted using these keys before transmission.

4.2.2 Encryption using Diffie-Hellman Key Exchange

Diffie-Hellman key exchange is another protocol that is used in Cellular Digital Packet Data (CDPD). This method takes advantage of the ease with which exponentials can be computed in a Galois field GF (q), where q is a prime of elements. As mentioned in paper [1], if y= X mod q, for 1 < X < q-1, where is a fixed primitive element of GF (q), then X= log y mod q is referred to as the discrete logarithm of y to the base over GF (q). Consider a scenario, where Alice and Bob want to communicate. Here, Alice selects a random number Xa between 1 and q-1, which it keeps as a secret and sends Ya= Xa mod q to Bob. Similarly, Bob chooses a random number Xb and sends Yb= Xb mod q to Alice. Once the two entities receive the messages, they compute Ks = XaXb mod q and use it as their key. As no one except, Alice and Bob know their keys, any one trying to compute Ks has to do using Ya and Yb alone. The security of this system is based on the difficulty of taking the discrete logarithm.

4.3 Protocols based on Public-Key Certificates

In this protocol, a universally trusted certificate authority (CA) is used. This CA can be a single large service provider. Whenever the mobile user registers with a home network, it is provided with a certificate that contains the mobile user's identity, the expiration date of the certificate, the certificate authority's signature and lastly the certificate authority's private key, Sca. Each home network has its own certificate.

The certificates of the mobile m user (Certms) and the home network (Certhn) will be as follows:

Certhn = {IDhn, phn, datehn, [h (IDhn, phn, datehn)] Sca,
Certms = {IDms, datems, [h (IDms, datems)] Sca,
where h () is the one-way hash function
date is the expiration date of the certificate
phn is the private key of the Home Network
Sca is the secret key of the certificate
In this scenario, the home network broadcasts its certificate Certhn and the mobile user authenticates the home network by verifying the signature with the public key pca of the certificate.

Mobile user ⇐ Home network: Certhn

Mobile user ⇐ Home network: [Ks] phn, f (Ks, Certms

Later, the home network chooses a session key Ks randomly and encrypts it with the public key of the home network. Also the certificate of the mobile user is encrypted with Ks and together both are sent to the home network. When the home network receives the messages, it decrypts the message with its secret key Shn. Since the security is based on the certificates, any personnel who get to know the certificates has a chance to impersonate the mobile user at home network side. To avoid this kind of security breach, Beller, Chang, and Yacobi suggested using an additional mutual authentication step where another session-key derived from Diffie-Hallman key exchange is used. In Diffie-Hallman key exchange method, the certificates of the home network and the mobile user contain some additional information as shown below.

Certhn = {IDhn, phn, Yhn, datehn, [h (IDhn, phn, Yhn, datehn)] Sca,

Certms = {IDms, Yms, datems, [h (IDms, Yms, datems)] Sca,

Yms = Xms mod N and Yhn = Xhn mod N are the public values for the Diffie-Hellman key exchange of mobile user and home network respectively. Xms and Xhn are the secret key values. In this method, the mobile user computes Ks`= (Yhn) Xms mod N and chooses a random key Ks to encrypt the certificate Certms. After receiving the encrypted message the home network computes Ks' = (Yms) Xhn mod N. Now, both the entities use their session keys Ks` to encrypt the message before sending them on the communication channel. As the session keys are computed using their individual secret keys, any impersonation can be identified. But there are other problems involved in this method. The session keys generated are identical for all sessions, which is not a good sign from a security point of view. To improve on this method, where it is possible to generate variable session keys, a new protocol was proposed. In this improved method, the secrecy of the certificates is not a priority. This protocol is similar to the one above, the only difference is in the certificates where the value of Yms is equal to -Xms mod N and Yhn is equal to -Xhn mod N.

Mobile user ⇐ Home network: $\alpha^{Rhn+Xhn}$, $Cert_{hn}$

Mobile user computes $Ks` = (Y_{hn} * \alpha^{Rhn+Xhn} X\ hn)^{Rms} \bmod N$

Mobile user ⇐ Home network: $R_{ms}+X_{ms}$, $[Ks]_{phn}$, f (Ks, $Cert_{ms}$)

Home network computes $Ks` = (Y^{ms} * \alpha^{Rhn+Xhn})^{Rhn} \bmod N$

Mobile user ⇐ Home network: f (Ks, [IDhn, IDms])

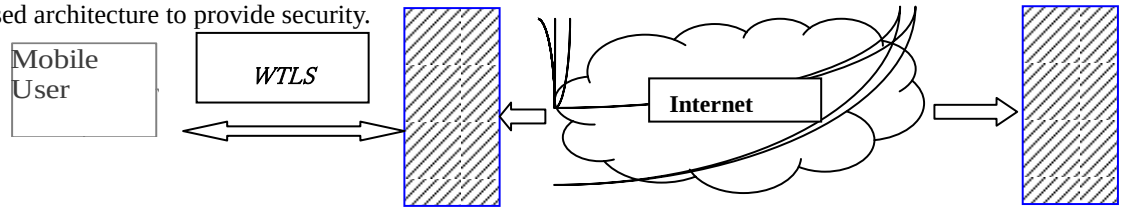
In this method, a random numbers Rhn and Rms are used. The home network calculates Rhn+Xhn and along with its certificate Certhn broadcasts the message to mobile users. After receiving the message, the mobile user calculates Ks` using Yhn present in the certificate. Later, the mobile user generates a random session key Ks and encrypts it with public key phn and sends it to the home network together with f (Ks, Certms) and Rms+Xms. Then the home network generates its session key Ks` using the public key Pms. Once both the

entities establish their session keys they start exchanging the messages using these keys. The advantage of using this method is that each time a session is set-up, a different session key is generated because of the use of random number Rms and Rhn. There are also situations where communication between two mobile users needs to be considered. To handle this situation an end-to-end security protocol was proposed. In this scenario, communication between the mobile users should be protected from both outsiders and insiders of the mobile networks, which also includes the home network. In order to support this kind of security, two levels of mutual authentication and session key exchange are used, one between the mobile user and the network and the other between the mobile users.

Consider two mobile users MS (A) and MS (B) that are registered to home networks HN (A) and HN (B) respectively. Also these mobile users are considered to be outside the home networks, in visiting network VN (A) and VN (B) respectively. Initially, both, the mobile users and the visiting network authenticate each other thereby sharing a common session key using the Diffie-Hellman key exchange mechanism. If the visiting network finds the mobile users certificate to be invalid, it checks with the home network to get the valid certificate for that particular mobile user. The main role of the visiting network here is to deliver the messages securely to the other visiting network involved in the communication process. After a call set-up is made, the network is no longer involved in any cryptographic computations. It just passes the encrypted messages to the required destination.

4.4 KSSL Security Protocol

New technologies like Wireless Application Protocol (WAP) and PalmOS, which are used on small mobile devices like mobile phones and Palmtops, do provide some kind of security in a wireless environment. But, the authors of this paper [2] listed out some problems in this WAP protocol, the primary being the use of proxy-based architecture to provide security.



All the data that the mobile user sends to a particular destination goes through this proxy- based server provided by the service provider. As shown in figure1, the WAP server decrypts the encrypted data using Wireless Transport Layer Security protocol (WLTS) and re-encrypts it using SSL before forwarding to the destination. Some concerns that were raised are, on issues like scalability, where a performance bottleneck comes-up with large number of users using a single service provider besides being a single point of failure, the need to maintain large data buffers to compensate the flow between a low bandwidth wireless channel and a high bandwidth wired channel, and security, where-in the proxy gets to see the process of encryption and decryption, which raises questions on security of sensitive data.

In contrast to the proxy-based architecture, the authors proposed a new protocol named "Kilobyte" Secure Socket Layer (KSSL), which is currently under research at the Sun Microsystems Lab. This protocol is an extension of Secure Socket Layer (SSL) Protocol, which is widely used in a wired network to provide security. Before discussing about the KSSL protocol, we will discuss about the SSL protocol.

4.4.1 Secure Socket Layer (SSL)

As mentioned in paper [2], SSL provides encryption, source authentication, and integrity protection of application data over insecure public networks. This protocol uses the service of TCP, which provides a bi-directional byte stream service.

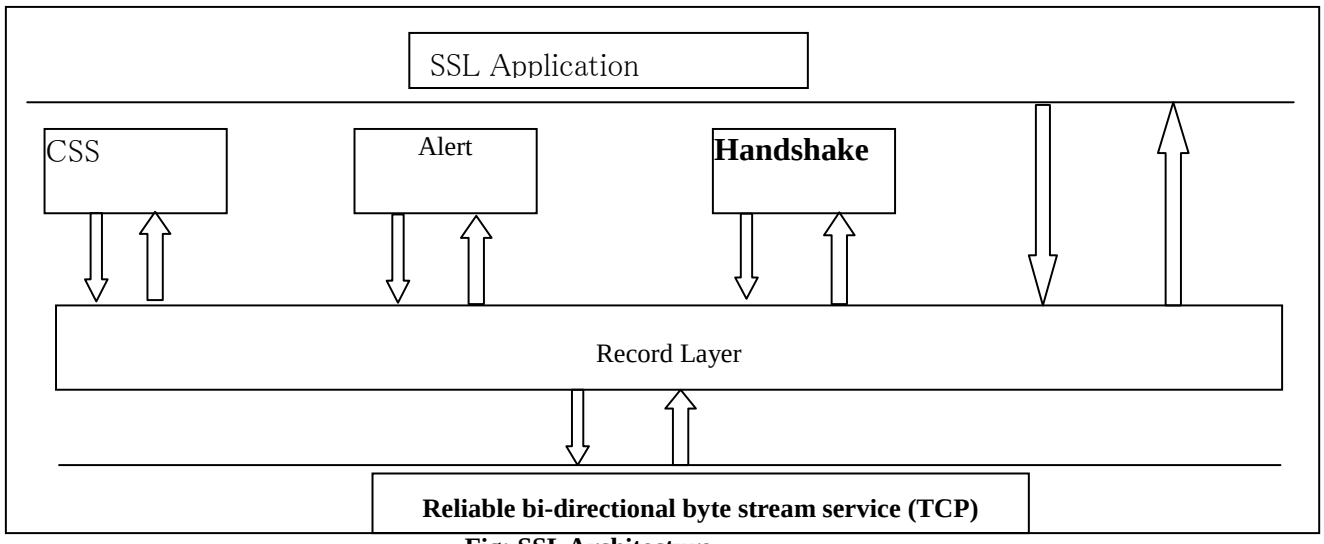


Fig: SSL Architecture

As shown in figure 2, SSL is a layered protocol. The Record layer, placed above the TCP layer, provides encryption and authentication services using symmetric-key algorithm. These keys are established by handshake protocol, which uses public-key algorithms to generate master secret between the SSL client and server. As mentioned in paper [2],this master secret is further used to derive cipher keys, initialization vectors, and message authentication code (MAC) keys for use by Record Layer. The other two protocols that are in the same layer as Handshake are Change Cipher Spec (CCS) and Alert protocols. CCS is used to signal successful completion of the handshake, and start of bulk encryption and authentication and Alert is used to notify if any failures occur. Because of its flexibility, SSL can support a variety of algorithms, for key agreement (RSA, Diffie-Hallman (DH), etc.), encryption (RC4, 3DES etc.), and hashing (Message Digest (MD5), Secure Hashing Algorithms (SHA), etc.). A standard is been specified that explicitly lists the combinations of these algorithms, together they are called cipher- suites. In our discussion, we use RSA key exchange form. Though SSL protocol supports, client and server side authentication, only server-side authentication is done, as maintaining certificates on the client-side requires maintenance. And the authentication process on the client side is done using passwords sent over an SSL-protected channel. Full Handshake The process begins with the client sending a ClientHello message containing a random number, a session ID and a set of supported cipher-suites to the server. The server accepts the message and checks whether it can support the proposed cipher-suite. If no, it aborts the handshake and sends a failure message back to the client. Otherwise, it generates a random number, and along with a session ID and the selected cipher-suite sends them in a ServerHello message to the client.

FULL HANDSHAKE

Client		Server
ClientHello ----->		(Includes proposed cipher suites)
	ServerHello	
	Certificate*	(Server's RSA Certificate)
	ServerKeyExchange*	
	CertificateRequest*	(Rarely used)
	<--------ServerHelloDone	
ClientHello		(Only if requested)
ClientKeyExchange		(RSA encryption of 48-byte random)
CertificateVerify*		(Only with Certificate)
[ChangeCipherSpec]		
Finished------->	[ChangeCipherSpec]	

Fig:Abbreviated SSL Handshake

In the abbreviated handshake protocol, the communication starts with client sending a ClientHello message containing a random number, a non-zero ID of a previously negotiated session, and the proposed cipher-suite. After receiving, the server checks whether it has the session information with it and is ready to use the corresponding master key. If yes, hoes back the session ID in the ServerHello message. Otherwise,it sends a new session ID signaling the client that a Full handshake process needs to be initiated. As the abbreviated handshake protocol doesn't involve certificates or public key cryptographic operations, fewer messages are exchanged and as a result the process is faster compared to a full handshake process.

4.4.2 KSSL and KSecurity

New technologies like Wireless Application Protocol (WAP) and PalmOS, which are used on small mobile devices like mobile phones and Palmtops, do provide some kind of security in a wireless environment. But, the authors of this paper [2] listed out some problems in this WAP protocol, the primary being the use of proxy-based architecture to provide security.

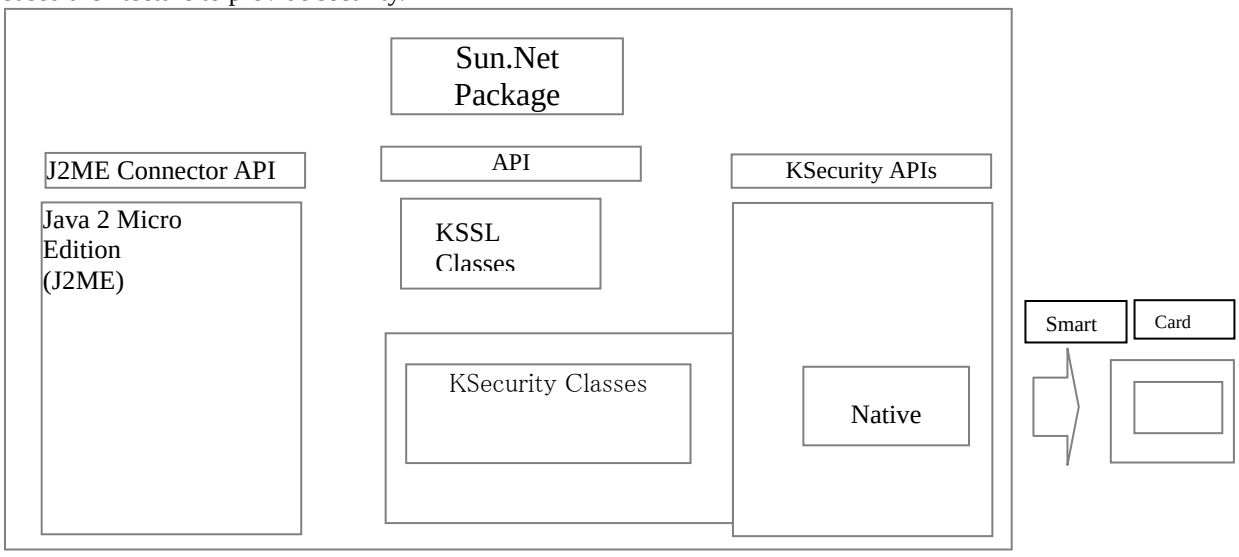


Fig.: **KSSL Architecture**

The KSecurity classes provide all the basic cryptographic functions such as random number generation, encryption, and hashing. It also contains a Java Card API, which on some occasions is used as a hardware crypto accelerator with minimum changes to the KSSL code. In this model the SSL protocol (KSSL) is written purely in Java and its

functions can be accessed using J2ME Connector API. The Connector API in addition to KSSL is used to support HTTPs and URLs. Another API is also used, which is yet to be standardized, for offering greater control over the SSL protocol like seeking user input upon encountering problematic certificates. Some of the features that KSSL and KSecurity offer are discussed below. They support symmetric keys of different lengths and RSA public/private keys with modulus lengths up to and including 1024 bits. For ciphers, they use RSA for keyexchange and RC4 for bulk encryption. For Signatures, they support RSA with both MD5 and SHA. Only X.509 certificates containing RSA keys and signed using RSA with MD5or SHA are supported. The client offers only two cipher-suites, RSA_RC4_128_MD5

and RSA_RC4_40_MD5, as they are fast and universally accepted by the SSL servers. Also client SSL supports session reuse and works on J2ME running on PalmOS, Solaris, and Windows.

5. **Performance**

The certificate-based security protocol is considered to be more secure than symmetric key protocol in terms of key management. Because of its computational complexity, public key cryptosystem is considered to be a burden on a mobile user with limited-resources. Instead, a MSR with RSA system and low component can be used for mobile users. Once a smart card containing the secret value, the certificate and the public key of the CA is issued to a mobile user, no secret information ever leaves the smart card. As specified in the paper [1], the recently announced smart card chip contains an 8-bit CPU as a standard smart card controller and an additional arithmetic coprocessor optimized for modular exponentiation of long operands.

The performance of the KSSL protocol was tested using PalmOS. The results are as follows: the bulk encryption and authentication algorithms are adequately fast on Palm's CPU. On a 20MHz chip (found in Palm Vx, Palm IIIc, etc.) RC4, MD5, and SHA all run at over 100Kbits/s. When measuring SSL Handshake Latency, a typical key with size of 768 or 1024 bits using RSA takes 0.5-1.5 seconds on a 20MHz Palm CPU.

The table shown below gives the performance of KSSL cryptographic primitives on PDAs.

	Palm Vx(20MHz)	Visor (33MHZ)
RSA(1024-bit) Verify+Sign	1433ms 80.91sec	806ms 45.11sec
RSA(768-bit) Verify+Sign	886 36.22	496 20.19
MD5 1024bytes 4096bytes	 292 Kbits/s 364 Kbits/s	 512Kbits/s 655Kbits/s
SHA-1 1024bytes 4096bytes	 124Kbits/s 140Kbits/s	 277Kbits/s 256Kbits/s
RC4 1024bytes 4096bytes	 117Kbits/s 190Kbits/s	 215Kbits/s 351Kbits/s

6. Discussion

Presently many wireless technologies are being used with each having their own approach to provide security. In this section we will discuss some of the current approaches and industry standards that are being followed.

The IEEE 802.11 wireless LAN uses a wired equivalent privacy protocol (WEP) mechanism to provide security. Here, the wireless network administrator provides a WEP-algorithm-based key for each authorized user. Any user without an assigned key is denied access.

The WAP application provides security, using a Wireless Transport Layer Security protocol (WTLS). This protocol uses RSA-based cryptography. However another protocol is also under consideration called Elliptic-Curve Cryptography (ECC). This protocol provides high level of security and using less memory resources and computation.
Another widely used authentication protocol is the wireless public-key-infrastructure mechanism (PKI), which is based on the wired PKI mechanism. Some of the products that use this mechanism are Certicom, eTrust, VeriSign.

Some of the new wireless-security standards that are under development are:
Pre-IKE Credential (PIC), where IKE stands for Internet Key Exchange: It is a protocol proposed by the IETF's IP Security Remote Access Working Group. This protocol provides additional features like flexibility and ease of configuration to the IPSec (IP Security) standard.

Open Multimedia Applications Protocol (OMAP): This protocol was developed by Texas Instruments. "It is a library of software from various vendors that will permit secure transactions on wireless devices that use TI's digital signal processors"[3].

Biometrics: It is a new system that identity's authorized user using their unique physical characteristics like finger prints, voice patterns, facial geometry, or retinal images.

Conclusion

Initially, when the wireless mobile environment came into existence security was not given a priority. But, as the time passed by, the extent to which this technology is used increased. This created a need to protect the information from unauthorized users and control the fraud. In the beginning, many security protocols where proposed, which were based on cryptographic techniques. With new loopholes coming up each time, a new protocol was proposed based on the existing one, to answer the problem. Presently, many researchers are concentrating on using the wired based security protocols over the wireless mobile communication. One such research is taking place at Sun Microsystems Labs, where the KSSL protocol is being tested within the corporate campus, using concepts like smart card and certificates.

According to me, the present research that is going on, that is trying to extend the security protocols used in wired networks to wireless mobile environment is a good step in providing high-end security. As the security protocols used in wired network have undergone heavy scrutiny over the years from various ends using these protocols in the mobile environment, would help in achieving good performance results.

Also, many wireless communication service vendors are developing new protocols and standards to provide a secured medium for the mobile users. With these efforts relatively new and not yet developed to its full extent, service providers are hoping to keep security development in pace with other developmental aspects of wireless technology.

References:

[1] Chang-Seop Park, " On Certificate-Based Security Protocols for Wireless Mobile Communication Systems."IEEE Network 1997
[2] Vipul Gupta and Sumit Gupta "Securing the Wireless Internet" IEEE Communications 2001.
[3] Asokan, "Security Issues in Mobile Computing," Univ. of Waterloo, Dept. of Computer Science, Technical Report CS690B, Apr. 1995.

