Security Services In Wireless Personal Area Networks. (December 2003)

Venkata Koonaparaju, Ramaseshan Iyengar, ECE Department, George Mason University.

Abstract— The days of using a mobile device for organizing schedules and contacts have given way to applications that can connect to the corporate backbone via a number of different methodologies, both wired and wireless. A mobile device is now a powerful tool that not only delivers the power of the enterprise in hand, it also provides all of the same vulnerabilities in a much more portable format. This paper represents the security issues related to the use of wireless personal area network technology and recommends a number of key implementation guidelines to ensure the secure deployment of WPAN services.

Initially, this paper compares the various implementations of WPANS and then looks at the different security threats for wireless networks. We then analyze the current protocols used in wired networks and test their compatibility with wireless networks. This paper then delves into the security requirements of current WPANS involving Personal Digital Assistants (PDA). The paper also gives an overview of typical wireless network security architecture and finally presents certain recommendations for the security services implementation.


I. INTRODUCTION

A new network paradigm concerning a short-range wireless connectivity attracts researchers and industrial attention in the last few years. Wireless personal area networks (WPANs) presents the person centered network concept, which allows a person to move, surrounded by its personal space (PS) and devices, and to communicate with them and through them with the outside world. The coverage area of WPAN is in the range of 10 meters. A standard communication method must be agreed between the hardware and software vendors to implement.

II. WPAN TECHNOLOGIES OR PROPOSED STANDARDS

The three candidates for use in WPAN systems are shares Shared Wireless Access Protocol – Cordless Access (SWAP – CA), Bluetooth and Infrared Data Association’s (IrDA) IrDA Protocol. The challenge in developing a wireless personal area network (WPAN) standard is that it must allow devices to communicate in a wireless environment while keeping in mind issues such as cost, power consumption, size and simplicity of use/deployment. Additional criteria such as communications range, data rate, LAN integration, and support for voice communications were also compared. A summary of the comparison of the three technologies is given below.

<table>
<thead>
<tr>
<th>Properties</th>
<th>HomeRF</th>
<th>Bluetooth</th>
<th>IrDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Spectrum</td>
<td>2.404 – 2.478 GHz</td>
<td>2.402 – 2.460 GHz</td>
<td>Infrared, 660 nm</td>
</tr>
<tr>
<td>Physical layer</td>
<td>FHSS 50 hops/s, 2 FSK and 4 FSK</td>
<td>FHSS 1600 hops/s, GFSK</td>
<td>Optical</td>
</tr>
<tr>
<td>Channel Access</td>
<td>CSMA/CA and TDMA</td>
<td>Master-slave, polling</td>
<td>Polling</td>
</tr>
<tr>
<td>Maximum Data Rates</td>
<td>0.8 to 1.6 Mbps</td>
<td>0.721 Mbps</td>
<td>4 Mbps</td>
</tr>
<tr>
<td>Range</td>
<td>50 Meters</td>
<td>10 Meters</td>
<td>2 Meters</td>
</tr>
<tr>
<td>Standby and Peak current</td>
<td>&lt; 1 mA and &lt; 300 mA</td>
<td>&lt; 1 mA and &lt; 60 mA</td>
<td>&lt; 10 uA and &lt; 300 mA</td>
</tr>
<tr>
<td>Data Support</td>
<td>Via TCP/IP</td>
<td>Via PPP</td>
<td>Via PPP</td>
</tr>
<tr>
<td>Voice Support</td>
<td>Via IP and PSTN</td>
<td>Via IP</td>
<td>Via IP</td>
</tr>
<tr>
<td>Power conservation</td>
<td>Yes</td>
<td>Yes</td>
<td>Distance based</td>
</tr>
<tr>
<td>Speech Encoding</td>
<td>32 kbps ADPCM</td>
<td>64 kbps CVSD/Δ,</td>
<td>^</td>
</tr>
<tr>
<td>Topology</td>
<td>Peer-to-peer, MS-to-BS</td>
<td>Master-slave</td>
<td>Master-slave</td>
</tr>
<tr>
<td>Price Point</td>
<td>Medium ($100)</td>
<td>Medium to Low ($10)</td>
<td>Low (&lt; $10)</td>
</tr>
</tbody>
</table>

Table 1 Technical Summary of Home RF, Bluetooth, IrDA (Source of Table: Wireless Personal Area Networking Systems: Comparison of Bluetooth, IrDA Data and HomeRF by Aurangzaib Kaleem)
exceeds the requirements of the WPANs and IrDA specification is far less than the required. Another limitation which impacts the range of IrDA Data is the use of Infrared, which is susceptible to blockage due to the objects or the angle between the two communicating devices, is off by 15°. IrDA could implement a protocol, which will meet the range of 10 meters but the cost, and power requirements of hardware would not meet the desired values of WPANs.

2) Data Rate

Bluetooth allows for up to eight devices to operate in a single piconet and transmit data in symmetric mode (up to 432.6 kbps) or asymmetric (up to 721 kbps and 57.6 kbps) mode. The eight-piconet devices must share the bandwidth and cannot transmit at that rate simultaneously. SWAP-CA supports 1.6 Mbps using a CSMA/CA scheme, which provides a peak effective throughput of 1 Mbps under lightly loaded conditions. The IrDA provides the fastest data rate at 4 Mbps, which is more than enough for large file transfers, print jobs, or Internet sharing.

In terms of data rate all three systems are satisfactory. It is difficult to place a number on what would be an adequate data rate for a WPAN. The concept of a WPAN is relatively new and applications for the technology have not matured enough to push the limits of the data rates available. The developers of SWAP-CA and IrDA both have hinted at support for higher data rates and it can be assumed that once an 802.15 standard is approved higher data rate versions of the standard will be development in the future.

3) Support for Voice

Of the three protocols only SWAP-CA and Bluetooth provide adequate support for voice. SWAP-CA’s implementation of DECT and integration with the PSTN is very good. The only drawback is that a Connection Point must be used. For the purposes of home networking SWAP-CA is adequate where the existence of a Connection Point can be planned. For ad hoc networks having to need an additional device that provides the voice services is not ideal. Bluetooth provides the same services as SWAP-CA but without the need for a specialized device. In a Bluetooth WPAN a single node (master node) can act as the aggregator to the PSTN and support the communication needs of other piconet nodes. For the purposes ad hoc networking Bluetooth is a better choice for voice support.

4) Support for LAN Integration

The three systems provide equal support for LAN integration. All three systems require some type of device that is WPAN protocol aware and LAN protocol aware and will be used as a gateway to the LAN. The IEEE 802.15 WPAN Group is looking at implementing protocols in 802.15 to access an 802.11 directly but the need for additional hardware may impact the size and power constraints of WPAN devices.

5) Power Management

For purposes of a WPAN, Bluetooth’s ability to allow any node to become a master and provide power management for the other nodes is superior to what is offered by SWAP-CA and IrDA. The SWAP-CA protocol offers an adequate method but the need for a Connection Point limits the ability to have this function available to nodes in ad hoc WPANs.

From the above discussion it is clear that Bluetooth is best suited for WPAN systems. This is because Bluetooth is specially designed for short-range network scenarios.

III. SECURITY ARCHITECTURE.

In this section we describe the overview of the security architecture. We start this by first describing the trust model on which we base the architecture.

Trust Model

The trust model we use describes the basic security relationships between the components in a PAN. On component level we use a model with one component as reference. We view all other components in relation to this single component. This allows us to describe the trust relations between any component and all other components in a PAN. We only distinguish between three different basic trust levels:

1) Untrusted Components

Untrusted components are by definition all PAN components that the reference component has no security relations with and that it has not (yet) been able to identify and/or verify the identity of. For example any new component that a user buys is an untrusted component from the perspective of all the other components belonging to the same user.

2) Second Party Components

A second party component has an owner different to that of the reference component. Second party component identities can be verified, i.e., authenticated. It is also possible to make a secure key exchange with a second party component. A second party component might be trusted for some actions while still be untrusted for other actions. The fine grain level of trust given to a particular second party component is determined by the security policy of the reference component and is part of the service level trust model.

3) First Party Components

A first party component has the same owner as the reference component. Furthermore, all first party components are able to identify all other first party components and distinguish a first party component from a second party component or untrusted component. It is possible to make a secure authenticated key exchange with a first party component without any manual user interaction.
IV. COMPONENT INITIALIZATION

A prerequisite for secure communication and authentication of components is a common security association. A security association can either be a shared secret or shared public key root key(s). The creation of security association, i.e., generation or transfer of key(s), we call "component initialization". The cryptographic initialization or what is also called imprinting, is a procedure of equipping the component with a secret value of a cryptographic parameter. The procedure of imprinting, where the initial secret cryptographic parameters are set in the component, is the most sensitive part of the communication.

1) Protocols for Manual Authentication

In PAN context it is assumed that the initial identification of the devices is based on the action of the users of the PAN components. For this purpose a protocol for conveying the result of the identification to the components is required. Using such a protocol two PAN components can verify that they share the same information. Let us now assume that two components have exchanged some information consisting of data items D. We shall describe a protocol, Manual Authentication Protocol (MANA) using which the users of the components can verify that the two components share exactly the same data items D. There are three different protocols MANA-I, MANA –II, MANA – III out of which MANA – III is the mostly used one and is discussed below.

a) MANA III

We now consider two PAN components with the following user interfaces. Both components have input interfaces for entering short strings of alphabetic and/or numeric symbols. Additionally, both components have a simple output interface. The steps of the manual authentication protocol with commitment are as follows (see also Figure 1):

1. Both components output a signal as to acknowledge that they have received data D and that they are now ready for the verification. User receives the signal from both components and generates a short random key K, where K is suitable for use with a MAC function shared by the two components. The user enters the key in both components, and enters a signal in one of the devices (called the first component in the sequel) to notify that the protocol can start.

2. The first component generates a random number R1. Using the key K, the first component computes a MAC1 as a function of the data D and the random number R1. The first component transmits the MAC1 to the second component over the insecure wireless link.

3. The second component generates a random number R2. Using the key K, the first component computes a MAC2 as a function of its stored version of data items D and the random number R2. The second component transmits the MAC2 to the first component over the insecure wireless link.

4. The first component sends its random number R1 to the second component.

5. The second component verifies that the received MAC1 corresponds to the MAC value computed using the stored values of K and D and the received value R1. If verification is successful the component outputs accepted (OK) and sends its random number R2 to the first component.

6. The first component verifies that the received MAC2 corresponds to the MAC value computed using the stored values of K and D and the received value of R2. If verification is successful the component outputs accepted (OK).

7. The user verifies that both devices accepted the verification, and enters OK in both devices.

Manual Authentication Protocol III
(Source: www.ist-shaman.org)

2) Personal Certification Authority

In a "conventional" Public Key Infrastructure (PKI) model, a Certification Authority (CA) issues a public key certificate. The CA is responsible for checking that the public key in an issued certificate corresponds to a private key that the holder (with the ID given in the certificate) of the certificate possesses. This is necessary in order to maintain the security of a global or very large PKI. The drawbacks of a central CA include:

1. It must issue all certificates used by the communication units, and all units must share trusted public root keys; this can be a tedious process that the user of a communication unit would like to avoid;

2. It is very costly to maintain a well-controlled
highly secure certification process that can handle thousands of users;
3. A user that wants to manage his/her own local environment, such as a PAN, will gain few benefits within the PAN from employing a centralized CA.
4. The user might not want, for privacy reasons, to delegate the CA operation to a centralized entity outside his personal environment.

A personal CA is different from large scale or global CA functions. An ordinary user for home or small office deployment uses the personal CA. As with any other PKI, we would like all units in a communication network to share common root public keys and use certificates issued by a trusted CA corresponding to the public root key. In order to use PKI technology in such an environment we need to reconsider the CA policies. One of the personal components must act as a “personal CA”. Such a component is able to issue certificates to all other personal components. Hence, since all the personal components can be equipped with certificates issued by the same CA, i.e., the personal CA, they will all share a common root public key. Consequently, the public keys in the certificates can be used to exchange session keys or authenticate personal components in a PAN.

V. EXISTING SOLUTIONS OF PAN COMMUNICATION SECURITY

A Link Layer Solution:
Link layer security provides point-to-point security between directly connected network devices. Link layer security provides secure frame transmissions by automating critical security operations including user authentication, frame encryption, and data integrity verification. In a wireless network, link layer protection defines a network that is secure to outsider intervention. Link layer protection starts with an authentication service and includes link layer encryption and integrity services. As a result, only authenticated users can actively use the link layer, and all data traffic on the link layer is encrypted and authenticated. Allows higher-level protocols, such as IP, IPX, etc., to pass securely. This provides security for all upper layer protocols.

The Wi-Fi Alliance has taken work done by the IEEE 802.11TGi and adopted key portions to create a new standard called Wi-Fi Protected Access (WPA). WPA is an industry standard for providing strong link layer security to WLANs, and supports two authenticated key management protocols using the Extensible Authentication Protocol (EAP). WPA also requires data frame encryption using TKIP (Temporal Key Integrity Protocol) and message integrity using a Message Integrity Check (MIC) called Michael. WPA provides strong, robust security on wireless connections, which addresses some widely, publicized security holes in older wireless LAN standards.

B Network Layer Solution:
Internet protocol IP is the most likely network layer protocol. IPsec protocols provide security services at layer 3. Two IPsec protocols exist: Authentication Header (AH) and Encapsulating Security Protocol (ESP). AH provides proof-of-origin on received packets, data integrity, and anti replay protection. ESP provides all that AH provides; in addition ESP provides data and limited traffic flow control confidentiality.

IPsec has the advantage, that it protects the network layer and is independent from the transport protocol. Actually IPsec is invisible on higher layers like transport and application layers. So users who operate only on these higher layers do not recognize IPsec; therefore, the IPsec solution can provide virtual private network (VPN).

When a network entity receives an IP packet, it checks on IP header the initiator’s and final receiver’s IP addresses. Next it checks on security policy database SPD, how this packet should be treated. It may be dropped, decrypted, further routed etc. Needed keys come from security associations (SAs) that describe not just keys, but also lifetimes of keys etc. IKE or son-of-IKE protocols can be used to negotiate SAs and negotiated SAs are stored on security association database.
IPsec can provide confidentiality of IP datagrams, when ESP protocol is used. The ESP header immediately follows an IP header, regardless of the mode that ESP is in. The ESP header is followed by a trailer, which contains protected data, padding, length of padding, next header information and authentication data. Protected data consist of the following things: the original IP header (if tunnel mode is used) and the IP payload, consisting of the transport layer header and the transport layer payload.

![ESP Header and Trailer](Source: www.ist-shaman.org)

The security parameter index (SPI) specifies the used cryptographic algorithms. The initialization vector is used for initialization of the ciphering algorithm. Therefore, these values are not encrypted, but only authenticated. The sequence number, which is 32-bit long, gives assurance that all packets are different and, therefore, it provides anti-replay protection.

3) Disadvantages of IPsec

It protects only the network layer and upper layer protocols, it leaves the link layer vulnerable. The following four types of attacks that might be effective against a network layer IPSec
- Denial of Service Attack
- Man-in-the-Middle Attack
- Peer-to-Peer Attack
- Limited Network Access Protection

VPN sessions may be broken when users move among access points since the IP address changes. This can cause other applications to freeze, requiring users to reboot their machines.

### C Comparison of Link Layer and Network Layer protection

<table>
<thead>
<tr>
<th>Security Parameters Index (SPI)</th>
<th>Link Layer</th>
<th>Network Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Parameters Index (SPI)</td>
<td>Authenticates interface to the network. Normally based on user of the system.</td>
<td>Authenticates an IP address to the network. Normally based on user of the system.</td>
</tr>
<tr>
<td>Sequence number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initialization vector</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authenticated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protected data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pad</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pad length</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Next header</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

V. POLICIES AND ACCESS CONTROL

A component that offers services to other components has to make access control decisions on which of its services are available to what components under what conditions. Such decisions are made based on policies, which can be expressed in some form of “authorization statement(s)”.

The following conceptual elements in authorization statements for access control:

**Issuer ID**: an identifier of the entity (or entities) that made the authorization statement. The serving component must recognize the identifier and be able to cryptographically verify that the authorization statement originated from the issuer.

**Subject authenticator**: authentication information for the entity (or entities) being authorised. The serving component must be able to interpret the authenticator and successfully authenticate the subject before access may be granted. To avoid resource stealing, this authentication must allow for subsequent integrity and replay protection of all messages in the access-controlled session.

**Resource descriptor**: the specification of the controlled service/object. All potential serving components (if there are more) must be able to map the resource descriptor unambiguously to a local service/object.

**Validity**: side conditions that must be satisfied at the time the access control decision is made. Conditions can be set, for example, on dates, times of day, length of session, required encryption strength, mutual authentication, user confirmation, etc.

**Delegation**: a statement of whether or not further delegation is allowed. Typically a single bit.

### A PAN Security Domain Specification

(Source: [www.ist-shaman.org](http://www.ist-shaman.org))
PAN Secure Domain, is “a group of components inside a PAN where each component can be authenticated, trusted and securely communicated by means of some common security association”.

The security association could be in the form of a shared secret key or a shared group key based on public key techniques with the trust being established by a personal CA within the PSD (certificates issued to all PSD members will indicate the device as a member of that PSD). Note that the “group key” will not be used for secure bilateral communications in the PSD, which should still take place using bilaterally established keys, but will be used only for proof of PSD membership, secure PSD-wide broadcasts and PSD-wide secure communications.

The simplest example of group trust is when a single user owns all devices in a PSD and treats them equally (this directly follows from the current trust model when all devices are first party devices). Such a configuration of devices will not contain any restrictions based on the identity of a device. All shared resources will be made available to all the group member devices.

1) PSD Controller

From a user’s point of view, it is tedious to update and manage the policy on each and every device, especially when the user wants to change the behaviour of the entire PSD. In order to make the PSD more manageable to a user, we introduce the role of a PSD controller. The PSD controller is a role that could be assumed by any one of the devices in the PSD provided it contains the necessary hardware to support the role, for example a secure key store and/or a display. The user may decide to move the controller role from one device to another depending on the usage.

The PSD controller is responsible for configuring and managing the policies governing the devices in the PSD. Additionally it is responsible for enrolling new members in the PSD. The PSD controller could also contain the personal CA that is responsible for issuing certificates to the PSD members.

2) Resource Sharing Using PSD

If PSD membership is limited to devices from a single user, two users will not be able share any resources. The only way this could be achieved is if they reconfigure their existing PSDs such they have matching policies and trust each other equally. This is not always practical and nor is it safe. Furthermore, from a PSD owner’s point of view, restricting resource sharing between his own devices in order to share resources with another user is not a very attractive proposition.

An effective way for the two users to share resources is to establish a new PSD, depending on the situation, this PSD could be a temporary or a permanent PSD (as outlined in yellow in the diagram below) involving the devices with the resources they want to share. Alternatively, the users could pair two devices (one from each user) and then add further members as required using one of the original devices as the PSD controller.

When forming a PSD with devices from different users, it is not always straightforward to assign a PSD controller. It might have to be mutually agreed by all parties in the PSD. Alternatively, the device that initially created the PSD could assume this role. Nevertheless, if required it could be handed over to another device in the PSD.

A temporary PSD is established between user 1 and 2 in order to share resources between devices B, C and E (Source: www.ist-shaman.org)

3) Forming a PSD

Consider three devices B, C, E with identities ID_B, ID_C, ID_E. We need to establish a group key, KPSD. In order for these devices to form a PSD, we need first to have two security associations between the three of them. We assume these to be, {B, C} and {C, E}. Based on these associations, it is possible for B and C, and C and E to communicate securely. C then generates the PSD membership key KPSD. C then communicates the identities of all PSD members to each other, i.e. forwards ID_B and IDE to E and B respectively. Together with KPSD, B and E are now in a position to generate KBE to establish secure communications between them.
Possible exchanges of information between the devices
(Source: www.ist-shaman.org)

4) Building on PSDs Using Policy

A PSD can be used as a foundation to build on some rules on resources sharing and device behaviour. Devices belonging to a PSD contain the fundamental requirements needed to support rules that would ensure coherent behaviour at the application layer. These rules are essentially the policy governing the devices in the PSD (or PSD policy). The policies on a device dictate how resources should be used and how the device should behave under different circumstances.

5) The Contents of the PSDs Policy File

The PSD policy file should be in a standardised format to achieve interoperability and it should contain information about the resources available to different devices depending on which PSD they belong to.

An example of the PSD policy file is shown below

<table>
<thead>
<tr>
<th>Res. Type &amp; ID</th>
<th>Auth. ID</th>
<th>Target ID</th>
<th>Perm. Type</th>
<th>Validity</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPRS</td>
<td>C</td>
<td>Component</td>
<td>1 day</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

(Source: www.ist-shaman.org)

Resource Type & ID: This contains information about the ID of the resource and its type. The ID is required to uniquely identify the resource within a component. The type of the resource is important when enforcing “Permissions Types” applicable to a resource.

Different resources on a component can be divided into four broad functional areas depending on their impact on the hosting component and its user.

1. Local Services – Printers, projectors, etc… or similar
2. Network Interfaces – GSM, GPRS, BT, IrDA, WLAN, etc… or similar resources related network connectivity
3. Personal Information Management – Calendar, Phonebook, Location information etc… which are of personal value and will have privacy issues associated
4. Executables – refers to code downloaded from another component on to the target device

Target ID: Uniquely identifies the component where the resource is located. It is useful to identify resources within the PSD when the resource is available from more than one component in the PSD.

Authorization ID: PSD members have access to all PSD resources that have been made available via the policy file. If the PSD relies on a PSD controller, then the Authorization ID should be the ID of the component assuming the role of the PSD controller. If the component is to have the autonomy to authorize other components access to its resources, then the Authorization ID same as the Target ID.

Permission Types: The permission types are made available to different components will depend on the Resource Type etc.. In order to cater for different usage scenarios and patterns there are different permissions types depending on the type of the resource.

Component – Will use the targeted component’s default access control rules applicable. The component’s local security policy is consulted when making the access control decision.

User – Will prompt the user to grant permission from a range of permissions types available for a device of that trust level (see below).

Allowed – The indicated resource is given access to the resource until further notice

Validity: Contains information on validity periods that a request can be granted to components of various trust levels. If the access control information is communicated to the target component using PAN tickets, then short validity periods could be used to address revocation requirements.

VI. VENDOR SPECIFICATIONS FOR SECURE SOFTWARE
Vendor: Utimaco
Product: Safeware
Key Features:
- Encryption Algorithm: AES, AES
- Infrared Protection: Provided
- PIN: Symbol PIN
- OS Compatibility: Pocket PC
- Required Memory: 1.8MB
- Cost: $37.63

Vendor: F-secure
Product: Pointsec Tech
Key Features:
- Encryption Algorithm: AES
- Infrared Protection: Not Provided
- PIN: Numeric PIN
- OS Compatibility: Pocket PC
- Required Memory: 500KB
- Cost: $39.87

Vendor: Trust
Product: Digital
Key Features:
- Encryption Algorithm: AES, AES
- Infrared Protection: Provided
- PIN: Numeric PIN
- OS Compatibility: Palm OS
- Required Memory: 600KB
- Cost: $39 (Premium Edition)

Vendor: CDL
Product: CDL-82 single chip configuration
Key Features:
- Infrared Protection: Provided
- PIN: Symbol PIN
- OS Compatibility: Pocket PC
- Required Memory: 1.8MB
- Cost: $37.63

Vendor: CDL
Product: m-Shield Crypto Card Processor
Key Features:
- Infrared Protection: Provided
- PIN: Numeric PIN
- OS Compatibility: Pocket PC and Palm OS
- Required Memory: 500KB
- Cost: $39.87

Vendor: Trusted Computing Platform Alliance (TCPA)
Product: TCPA chip
Key Features:
- Encryption Algorithm: AES, AES, AES
- Infrared Protection: Provided
- PIN: Numeric PIN
- OS Compatibility: Pocket PC and Palm OS
- Required Memory: 200KB
- Cost: $39 (Premium Edition)

Source: Link Layer And Network Layer Security For Wireless Networks (white paper from www.interlinknetworks.com)

From the above table it is clear that PDA Secure is better choice than the remaining software’s. It provides us with 6 encryption algorithms and needs a memory of 200 KB, which is a very important factor when used in wireless constrained devices like PDA.

VII. VENDOR SPECIFICATION OF SECURE HARDWARE.

Vendor: CDL
Product: CDL-82 single chip configuration
Key Features:
- Full Security Evaluation 0.35 micron technology, 3.3V CMOS
- ROM storage of math functions and algorithm software
- Battery-backed RAM for secret key storage DSA, SHA-1
- DES, Triple DES
- Random Number Generator
- USB interface
- 12 mm x 12 mm dimension

Vendor: CDL
Product: m-Shield Crypto Card Processor
Key Features:
- Provides Data Privacy, User Authentication, Data Integrity, Non-Repudiation, Time Stamping
- Provides applications like Access control, e-mail encryption, VPN remote access, digital signature
- Ideal for laptops/notebooks and mobile applications

Vendor: Trusted Computing Platform Alliance (TCPA)
Product: TCPA chip
Key Features:
- On-chip key pair generation, using hardware random number generator, along with public key signature, verification, encryption and decryption
- Master Encryption key for encrypted files stored in Platform Configuration Registers (PCR) ensuring the data is protected against virus attacks and hacking
- User can generate an RSA public/private key pair on the TCPA chip and configure the private key to never leave the chip
- TCPA formed by Compaq, HP, IBM, Intel and Microsoft

Vendor: IBM
Product: Embedded Security Subsystem (ESS)
Key Features:
- Hardware-Software based technology which protects vital information like passwords, encryption keys and electronic credentials while guarding against unauthorized user access
- User defined security policy settings
- Password Manager replaces multiple passwords by one password or fingerprint
- IBM Client Security Software, used in ESS, is easily downloadable

VIII. RECOMMENDATIONS

This section will recommend the usage of layer 2 or layer 3 security services to provide secure internal PAN communications for existing wireless technologies.

A Authentication
Authentication is an essential part of the PAN security and must be implemented at layer 2. Existing authentication (such as Bluetooth) mechanisms that are considered adequate can be used

In cases (such as IEEE 802.11) where link layer authentication may not be considered adequate, network layer authentication should be used to ensure the authenticity of the communicating partners. IPsec with ESP in transport mode should be used to authenticate the links between PAN devices.

B Confidentiality
Confidentiality must be provided at the link layer for internal PAN communications. End-to-end confidentiality must be achieved in a PAN environment. Confidentiality at the link layer will provide security to all upper layers if used in an all-first hop environment.
The majority of existing wireless technologies (Bluetooth, IEEE 802.11) support confidentiality (i.e. encryption) by default. If the encryption that is provided by the link layer is considered to be adequate then the default encryption mechanism provided by the wireless technology must be used.

C Integrity Protection

Ideally integrity protection for signaling messages and user data must be provided at the link layer. Unfortunately, the majority of the existing wireless technologies do not provide reliable integrity protection mechanisms. Some rely on encryption (Bluetooth) to provide integrity where as some (IEEE 802.11 with WEP) use error correction codes with encryption. Usage of only encryption for integrity protection should be avoided at the link layer. Alternative solution would be to use a network layer protocol such as IPsec (in transport mode) and ESP with integrity protection to provide data integrity.

If IPsec is also used to provide other security services such as confidentiality or authentication then IPsec overhead to provide integrity protection will not be an issue. However in cases where the wireless technology provides adequate authentication and confidentiality and does not provide reliable integrity protection, usage of IPsec can be considered as a significant overhead. This overhead should be traded off with the security required for the communication. Services that require strong integrity protection, such as financial transactions, synchronization services, must use IPsec in cases where layer 2 integrity is not provided.

D Identity and Location Privacy

Similar to integrity protection the majority of current wireless technologies do not provide identity and location privacy services. Existing technologies should develop this functionality to provide these services. Network or higher layer protection mechanisms cannot be used to provide this service as the identities (MAC, IP, etc) for each layer are individual.

ACKNOWLEDGMENT

We would like to take this opportunity to thank our professor Dr. Kris Gaj for his unconditional support. He motivated us throughout the project and we owe this entire effort to him.

REFERENCES


