Consiglio Nazionale delle Ricerche

Realizzazione di un applicazione per l'incremento della sicurezza dei dispositivi mobili

A. Falleni, F. Martinelli, C. Vallati

IIT B4-05/2006

Nota Interna

Ottobre 2006

Istituto di Informatica e Telematica

“Realizzazione di un applicazione per l'incremento della sicurezza dei dispositivi mobili”

Alessandro Falleni, Fabio Martinelli, Carlo Vallati

Indice

Abstract

Usually, operative systems in mobile devices do not offer native security solutions to protect sensible data of the users. To this aim, we show the development of an application for improving the security of mobile devices. This paper presents Data Defender, a security multiplatform application for PDAs and smartphones which improves the security of user data, like agendas, address books, personal contacts and files, by using criptographic techniques.

Data Defender allows the creation of private areas and the capability to send/receive chiphered messages to/from mobile devices.

Keyword: Mobile Security.

Introduzione

Il mondo delle comunicazioni mobili sta subendo una profonda rivoluzione tecnologica: alla sempre più massiccia diffusione degli apparati fa riscontro una radicale evoluzione dei terminali e delle possibilità di connessione offerte all'utente. I cellulari stanno lasciando rapidamente posto agli smartphone ed ai PDA con le funzionalità tipiche della telefonia mobile. Questi dispositivi appaiono avere prestazioni sempre migliori per capacità di calcolo e di memoria: il software, di conseguenza, si è evoluto offrendo servizi sempre più sofisticati e complessi.

Tali dispositivi, sempre più potenti e versatili stanno ormai, in molte situazioni, sostituendo i laptop, in quanto contengono sempre più spesso al loro interno dati sensibili e file di lavoro. Questo può rivelarsi potenzialmente pericoloso per la tutela della propria privacy e delle informazioni riservate memorizzate al suo interno.

In questa ottica è stato progettato e implementato Data Defender, un'applicazione java per smartphone e PDA che offre la possibilità di cifrare i propri file, appuntamenti e contatti ed offre un elevata protezione dei dati contenuti nel dispositivo.

I sistemi operativi di smartphone e PDA non offrono all'utente particolari strumenti per rendere i loro contenuti sicuri.

Descriveremo un'applicazione java multipiattaforma per la protezione del proprio smartphone o PDA che utilizza tecniche crittografiche al fine di cifrare rubrica, agenda e file ritenuti sensibili. Il software consente di creare sul proprio dispositivo aree di lavoro private e di inviare o ricevere messaggi di testo cifrati.

In particolare, ad una prima analisi, si possono individuare le seguenti aree che dovrebbero essere messe in sicurezza:

- Accesso al dispositivo. I dispositivi PDA non forniscono particolari accorgimenti contro gli accessi non autorizzati al sistema.

- Sicurezza dei file in RAM e in FLASH. I dati vengono memorizzati nelle memorie esterne o interne al palmare in chiaro senza particolari attenzioni riguardo alla sicurezza.
- Protezione del database interno. Il database interno del palmare contiene dati sensibili come appuntamenti o contatti che vengono memorizzati in chiaro e possono così essere letti da chiunque entri in possesso del dispositivo.
- Installazione delle applicazioni. I dispositivi mobili non impongono particolari limitazioni alla possibilità degli utenti di installare nuove applicazioni in memoria. Alcune di queste possono mettere a repentaglio l'integrità del sistema stesso o la riservatezza delle informazioni contenute in esso.
- Impostazioni di sistema. Le impostazioni del sistema solitamente possono essere cambiate da chiunque possa mettere le mani sul dispositivo.
- Sincronizzazione. La procedura di sincronizzazione con i PC desktop a volte avviene senza particolari accorgimenti riguardo alla sicurezza.

Nella realizzazione della applicazione abbiamo fatto particolare riferimento a dispositivi con sistema operativo Windows Mobile.

Studio preliminare

Obiettivo

L'obiettivo è quello di realizzare un applicazione per dispositivi PDA col fine di incrementarne la sicurezza, in particolare realizzando le seguenti funzioni chiave:

- **Autenticazione** , tramite un autenticazione obbligatoria all'accesso del dispositivo si cerca di verificare l'identità dell'utente in modo da permettere o negare l'uso del sistema.
- **Autorizzazione** , utilizzando l'identità fornita dall'utente durante la fase di autenticazione l'applicativo dovrà negare o permettere la lettura delle informazioni sensibili contenute in memoria non volatile. Non volendo implementare un file system si vuole raggiungere l'obiettivo tramite l'uso della cifratura dei file in modo da rendere leggibili gli stessi solo all'utente autorizzato.
- **Accounting** , rimanendo in esecuzione in background , l'applicativo deve effettuare su file il log di tutte le azioni compiute dall'utente durante la sessione di lavoro. Le informazioni ottenute devono essere memorizzato in maniera cifrata in modo tale da renderle leggibili solo agli amministratori.

Prima di passare alla fase di realizzazione si preferisce procedere inizialmente con uno studio preliminare strutturato in due fasi.

Una prima fase in cui, analizzando la situazione attuale, si cerca di ottenere un quadro completo dello stato dell'arte, studiando prima gli strumenti messi a disposizione dal sistema operativo all'utente finale e poi ricercando la presenza in commercio di applicazioni già sviluppate con funzionalità simili a quelle richieste.

Questa prima fase ha lo scopo di assicurarsi la necessità di sviluppare un applicazione ex novo

rispetto alla possibilità offerte dall'uso degli strumenti del sistema operativo.

La seconda fase si preoccuperà invece di studiare la panoramica delle tecnologie offerte al programmatore al fine di scegliere la migliore per lo scopo prefissato.

Stato dell'arte

Lo studio preliminare parte dalla ricerca delle possibilità che il sistema operativo Windows Mobile offre per risolvere le problematiche sopra citate.
Riguardo all'autenticazione il sistema, anche nella sua ultima versione, non sembra offrire all'amministratore strumenti particolari. L'unica strumento offerto dal sistema operativo è la possibilità di poter richiedere, al momento dell'accensione del dispositivo, l'inserimento di un codice numerico PIN prestabilito senza il quale l'utente non può accedere al sistema.
Il sistema operativo Windows Mobile 5.0 (l'ultima versione uscita) inoltre aggiunge la possibilità di poter bloccare il sistema con una password alfanumerica dopo un certo periodo di inattività scelto dall'utente.
Anche per quanto riguarda l'autorizzazione, il sistema non offre alcun strumento per la protezione dei dati sensibili o di altre risorse. La memoria non volatile è infatti caratterizzata da un file system privo di un qualsiasi criterio di protezione.
Infine, anche per quanto riguarda l'accounting, non si hanno a disposizione strumenti tali da rendere inutile l'uso di un applicazione esterna per lo svolgimento di una tale funzione.

Applicazioni già esistenti

Data l'assenza di strumenti offerti all'utente dal sistema operativo, è stata svolta una ricerca è stata svolta una ricerca delle applicazioni già disponibili in commercio.
Dalla nostra ricerca sono emersi i seguenti prodotti :
Il primo è il Mobile Defense della SureWave chiamato anche PDADefense commercializzato in due versioni, enterprise e professional (www.pdadefense.com).
L'applicazione si propone appunto di incrementare la sicurezza dei PDA equipaggiati con Palm OS e Windows mobile.
Le funzioni offerte dal prodotto, nella versione enterprise, sono le seguenti:

- Cifratura di file, anche su memory card, con chiave da 64 a 512 bit.
- Lock del palmare tramite password , il PDA può essere bloccato dall'amministratore tramite una password richiesta al reset del dispositivo e dopo un tempo di inattività prestabilito. La password è inoltre memorizzata in maniera cifrata nel file system.

- L'utente ha una propria password personale e una serie di politiche di sicurezza associate. Ogni cambio di password è memorizzato in maniera tale da non permettere la ripetizione di una già scelta in precedenza. L'amministratore può inoltre specificare una durata massima per la stessa e una sua lunghezza minima.
- L'inserimento delle password nelle form del dispositivo è mascherato tramite l'uso di asterischi.
- Tentativi di accesso al palmare tramite attacchi “bruteforce” sono evitati con il blocco del dispositivo dopo un certo numero di login errati.
- Ogni utente può protegge i propri documenti con la possibilità di cifrare cartelle e file e può proteggere il proprio PDA impedendo l'esecuzione di alcuni applicativi bloccandoli con una password.

La versione enterprise differisce da quella professional dalla mancanza di alcune funzioni (nella versione professional) e dall'abbinamento (nella versione enterprise) del programma con un applicazione per pc utile all'amministratore del sistema a configurare più facilmente il palmare.

La seconda applicazione trovata è la SafeBoot Device encryption per Pocket PC della Controlbreak (www.safeboot.com).

Anche questo è un programma esterno al sistema operativo che si prefigge di incrementare la sicurezza dei PDA; le funzioni offerte da tale prodotto sono:

- Cifratura dei dati sensibili contenuti in memoria interna o in memory card esterne in maniera trasparente e automatica.
- Richiesta obbligatoria di un pin o una password per ogni utente che vuole accedere al dispositivo.
- Possibilità di ibernazione sicura del PDA.
- Blocco del sistema dopo un certo numero di login falliti.
- Possibilità di recupero delle password perdute tramite un sistema di domanda/risposta.
- Controllo centralizzato delle politiche di sicurezza a disposizione degli amministratori possono globalmente controllare cosa, all'interno del dispositivo, può essere cifrato o meno.
- Trasferimento dati sicuro tra PC e palmare.

In maniera addizionale l'applicazione fornisce all'amministratore la possibilità di sincronizzare le politiche di sicurezza con Active Directory di Microsoft.

Il programma in questione è commercializzato in diverse versioni a seconda del sistema operativo presente; si ha infatti una versione per Palm OS, una per Pocket PC o windows mobile e una per

Symbian OS.

Il terzo programma è invece il Trust Digital 2005 mobile edition appunto della Trust Digital (www.trustdigital.com).

Questo applicativo si inserisce in un gruppo di soluzioni che la Trust Digital ha realizzato per incrementare la sicurezza dei vari dispositivi di una rete aziendale. Insieme alla versione per dispositivi mobili, si ha anche una versione del programma per PC desktop.

Le funzionalità del prodotto in questione sono le seguenti:

- Gestione delle password di accesso, con una serie di criteri di validità associati come la lunghezza minima, vita massima e grado di complessità.
- Gestione delle restrizioni all'interno del sistema. Tramite questa funzionalità si può inibire a/agli utenti l'accesso a determinate risorse di sistema come memorie SD, Bluetooth, WiFi, infrarossi, Camera, Video, registrazione della voce e sincronizzazione con PC.
- Cifratura dei dati anche su memorie esterne.
- Gestione delle applicazioni. Il programma permette all'amministratore di impostare in maniera dettagliata una politica di sicurezza riguardo alla possibilità degli utenti di eseguire o meno programmi o di installarne di nuovi.
- Supporto alla gestione remota del dispositivo. Il programma fornisce all'amministratore la possibilità di poter bloccare il PDA o di cancellare tutti i dati in esso contenuti da remoto tramite una connessione sicura.

Anche questo prodotto è commercializzato in più versioni per adattarsi ai diversi sistemi operativi esistenti al giorno d'oggi coma Palm OS o Pocket PC / windows mobile.

Il quarto prodotto presente in commercio offre sempre la possibilità di cifrare i dati di un determinato utente riconosciuto tramite una fase iniziale di autenticazione, differisce però dagli altri per il metodo adottato.

Il KeyCrypt della KeyCript (www.kecrypt.com) fornisce infatti la possibilità di un autenticazione biometrica basata sul riconoscimento della forma, densità e velocità della scrittura dell'utente. Il riconoscimento può essere richiesto all'accesso al dispositivo o semplicemente al momento dell'esecuzione di operazioni particolari come, ad esempio, il trasferimento di denaro tramite un determinato software.

Una volta fatta l'autenticazione i dati dell'utente vengono cifrati attraverso l'algoritmo Blowfish con una chiave fino a 448 bit.

Le applicazioni illustrate in precedenza offrono soluzioni di sicurezza complete per i dispositivi

mobili. Ci sono comunque altri programmi che forniscono delle soluzioni riguardanti uno o più ambiti. In particolare, una serie di applicazioni fornisce solamente il supporto all'utente o all'amministratore per la cifratura dei dati sensibili. Alcune di queste sono:

- Pointsec for mobile platforms della POINTSEC (http://www.pointsec.com/products/smartphonepda/).
  Questa soluzione fornisce la possibilità di mettere in sicurezza i dati sensibili dell'utente in maniera trasparente per mezzo della cifratura delle informazioni. L'applicazione infatti dopo una preliminare identificazione cifra i dati della memoria interna ed esterna che lo stesso crea. Il programma è disponibile per windows mobile e per Symbian OS.
- Sentry 2020 della SoftWinter (http://www.softwinter.com/sentry_ce.html).
  Sentry 2020 permette la cifratura dei dati contenuti in MMC, SD o compact flash tramite algoritmi come il Twofish-256 e il CAST-128. La chiave di cifratura inoltre può essere memorizzata in anche in memorie differenti. Esso supporta tutte le varie versioni dei sistemi operativi della famiglia windows mobile.
- PE Encrypt della Vieka (http://vieka.com/peexplorer.htm#peencrypt).
  Fornisce la possibilità di cifrare i dati tramite gli algoritmi DES e AES. Disponibile solo in versione per windows mobile.
- PocketLock della Applian mobile (http://www.applianmobile.com/pocketpc/pocketlock/index.php) .
  Come gli altri prodotti fornisce la possibilità di cifrare i dati in memoria con chiavi fino a 168 bit scegliendo anche l'algoritmo usato.

Un altra schiera di applicazioni si limitano invece a fornire strumenti per il blocco del dispositivo all'avvio o dopo un certo periodo di inattività. Queste applicazioni infatti, obbligano l'utente a inserire un PIN o una password per poter lavorare non impedendo però la lettura dei dati in memoria che rimangono quindi in chiaro.

Esempi sono:

- 1-Pass della Omega One Software (http://www.omegaone.com/pda/pocketpc/1p.html). Si limita a bloccare il palmare all'accensione o dopo un tempo di inattività. Lo sblocco avviene solo dopo l'inserimento di un codice.
- Touch Password Protection della JGUI (http://www.jgui.net/touch/index.html). Anche questo programma blocca il palmare e richiede un autenticazione non basata su password ma su una sequenza di pressioni su diverse aree dello schermo che l'utente deve compiere in

un ordine stabilito a tempo di configurazione.

Altre soluzioni

In commercio esistono comunque altre soluzioni in aggiunta a quelle illustrate fino ad ora. A fianco delle soluzioni fornite da software di terze parti installato sui dispositivi, esistono anche delle soluzioni realizzate da hardware costruito ad hoc.
L'esempio più convincente è il dispositivo HP iPAQ hx2750 (www.hp.com); questo dispositivo è infatti dotato di un lettore di impronte digitali che può essere usato per proteggere i dati contenuti in memoria. Il lettore viene usato per la procedura di autenticazione all'accensione o dopo un certo periodo di inattività. Se la verifica dell'identità fallisce per un certo numero di volte consecutive, il sistema cancella tutti i dati contenuti nella memoria principale e nella ROM.
L'unico punto debole di questo sistema sono le memorie esterne, i dati contenuti in esse vengono memorizzati in chiaro e non vengono cancellate, come le altre, dopo una serie di tentativi di accesso non riusciti.

Osservazioni

La prima fase ha evidenziato l'assenza di soluzioni fornite direttamente dal sistema operativo.
Questa lacuna porta quindi la necessità dello sviluppo di un applicazione che svolga le funzioni di sicurezza prima descritte.
Lo studio preliminare ha però evidenziato anche la presenza sul mercato di applicativi che già raggiungono parzialmente gli obbiettivi previsti inizialmente.
Le applicazioni già in commercio infatti coprono i primi due obbiettivi realizzando le funzioni di autenticazione e di autorizzazione tramite l'uso della cifratura e di password.
Nessuna soluzione copre comunque l'ultima funzione richiesta cioè quella di accounting.

Tecnologie disponibili

Per la realizzazione dell'applicazione abbiamo a disposizione due tecnologie alternative:

- Tecnologia **.net framework** offerta direttamente dal sistema operativo. Consiste nel

realizzare l'applicazione direttamente in c++ richiamando le API di windows mobile edition.

- Tecnologia **java ME** , l'applicazione scritta in java e viene poi eseguita sui vari sistemi dalla VM solitamente installata su tutti i PDA attualmente in commercio.

Ognuna delle due soluzioni ha naturalmente vantaggi e svantaggi. Un applicazione realizzata in java ME ha il grande vantaggio della portabilità che la rende indipendente dall'hardware e dal sistema operativo utilizzato. L'uso della tecnologia .net framework invece rende l'applicazione inutilizzabile su macchine non equipaggiate dal sistema operativo windows mobile.
La tecnologia java è quindi preferibile rispetto al .net framework; prima di prendere una decisione vanno però analizzati gli strumenti offerti da tutte e due le soluzioni per verificare che siano entrambe equivalenti tra di loro.

Soluzione .net framework

La soluzione .net framework offre al programmatore un insieme di API ben fornito riguardo alla sicurezza. In particolare sono presenti una serie di chiamate di sistema per l'utilizzo di servizi crittografici e di servizi per l'autenticazione.
I servizi crittografici danno al programmatore la possibilità di cifrare e decifrare i dati sensibili utilizzando i più comuni protocolli di crittografia. Il sistema offre inoltre una serie di funzioni che implementano i più diffusi algoritmi di hashing e che permettono l'uso dei certificati.
Il “Local Authentication Subsystem” offre invece una serie di primitive utili all'autenticazione dell'utente al momento dell'accensione del dispositivo o al momento dell'accesso ad una risorsa protetta.
Per una panoramica più dettagliata riguardo alle possibilità offerte dal sistema operativo al programmatore in materia di sicurezza si rimanda ai seguenti link:

- http://www.opennetcf.org/library/OpenNETCF.Security.Cryptography.html ontiene l'elenco dei servizi crittografici di windows mobile;
- http://msdn.microsoft.com/mobility/understanding/articles/default.aspx?pull=/library/en-us/dnnetcomp/html/PPCSignatureApp.asp è un riferimento a MSDN riguardo alla sicurezza contenente soprattutto esempi di programmazione tramite l'uso del compact .net framework.

Soluzione java ME

La soluzione java ME offre al programmatore la possibilità di poter utilizzare una serie di librerie, le SATSA (JSR 177) o le Bouncy Castle Crypto APIs, utili per applicare i più comuni algoritmi crittografici ai dati sensibili. Per capire a fondo le potenzialità di questo tipo di tecnologia si è però deciso di testarla direttamente utilizzando un PDA con una VM installata.
Riportiamo qui di seguito le operazioni compiute.

Installazione di WebSphere Everyplace Micro Environment 6.0

La maggior parte dei PDA, al momento della vendita non ha una VM installata. L'utente deve quindi cercarne o comprarne una e installarla sul palmare.
Per il nostro test abbiamo scelto WebSphere Everyplace Micro Environment 6.0 della IBM. Abbiamo deciso per questo prodotto rispetto ad altri perchè la versione evaluation è gratuita e liberamente scaricabile da internet per scopi non commerciali.
Questo prodotto inoltre presenta le seguenti caratteristiche:

- Supporto per CLDC 1.1, MIDP 2.0 e JSR-75
- Compatibilità con windows mobile 2003/5.0, Palm OS e Linux

Illustriamo passo dopo passo le operazioni che si sono dovute compiere sul palmare per l'installazione di questo prodotto.

1. Installazione di ActiveSync sul Pc host.
2. Utilizzare il software di Microsoft appena installato per connettersi al dispositivo tramite il cavo USB in dotazione.
3. Scaricare l'installer dal sito IBM all'URL
   www-128.ibm.com/developerworks/websphere/zones/wireless/weme_eval_runtimes.html
   Noi abbiamo scelto la versione 6.0 (l'ultima) dal profilo CDC 1.0, Foundation 1.0, Personal 1.0, la più adatta per le prove iniziali.
4. Installare il package sul pc host.
5. Collocarsi sulla cartella di installazione (solitamente

C:\Programmi\IBM\WEME\runtimes\60\wm50-arm-midp20) e scompattare l'archivio weme-wm50-arm-midp20_6.0.0.20051117-110708.zip (il nome potrebbe cambiare a seconda della versione o tipo del package iniziale scelto).

6. Cliccare sull'icona “File Explorer” di ActiveSync e collocarsi sulla root directory.
7. Creare una cartella “J9” e una sottocartella “MIDP20”.
8. Copiare in “MIDP20” le tre directory bin , lib e example ottenute dall'estrazione dell'archivio.
9. L'installazione è completata, possiamo testare la buona riuscita facendo girare sul palmare uno degli esempi. Per farlo basta entrare nella directory /J9/MIDP20/examples dal palmare tramite FileExplorer e cliccare due volte su `GolfScoreTrackerSuite.jad` che è la MIDlet di esempio. Se il programma parte allora l'installazione è andata a buon fine.

La versione 6.0 di websphere che abbiamo inizialmente installato si è però rivelata troppo recente. Per l'ultima versione non è infatti disponibile il pacchetto opzionale contenente l'implementazione delle librerie FileConnect (JSR 75). Si è quindi deciso di installare una versione più collaudata del prodotto dell'IBM la 5.7.1.

La procedura per l'installazione di questa versione è differente e riportiamo qui di seguito le operazioni svolte:

1. Download di Websphere device developer 5.7.1 dal sito dell'IBM e installazione dello stesso.
2. Trasferimento dei file j9-midp20-wm2003-arm_22.CAB e j9-midp20_it-wm2003-arm_22.CAB dal PC host al palmare. I due file sono contenuti nella directory C:\Programmi\IBM\DeviceDeveloper\wsdd5.0\ive-2.2\runtimes\wm2003\arm\midp20\cab .
3. Installazione dei due pacchetti sul palmare semplicemente avviando i due installer direttamente dal dispositivo.
4. Avvio del device developer. Download dei pacchetti opzionali (contenuti nella sezione WebSphere Studio Device Developer) “WEME Windows Mobile 2003 ARM PDAP-FC (Runtime 2.2) 5.7.1", "WEME Windows Mobile ARM PDAP-FC (Runtime 2.2) Language Pack 1 5.7.1", "WEME Windows x86 PDAP-FC (Runtime 2.2) 5.7.1" and "WEME Windows x86 PDAP-RC (Runtime 2.2) Language Pack 1 5.7.1." direttamente dal gestore degli aggiornamenti del programma.
5. Copia di C:\Programmi\IBM\DeviceDeveloper\wsdd5.0\ive-2.2\runtimes\wm2003\arm\midp20\lib\jclMidp20\ext\fc.jar nel dispositivo mobile nella

posizione My Device\Program Files\J9\MIDP20\lib\jclMidp20\ext.

6. Copia di C:\Programmi\IBM\DeviceDeveloper\wsdd5.0\ive-2.2\runtimes\wm2003\arm\midp20\lib\jclMidp20\ext\fileconn.dll nel dispositivo mobile nella posizione My Device\Program Files\J9\MIDP20\bin.

Per l'installazione invece delle api PIM (sempre facenti parte del Jsr 75) bisogna ripetere la procedura scaricando i pacchetti opzionali “WEME Windows Mobile 2003 ARM PDAP-PIM (Runtime 2.2) 5.7.1” e “WEME Windows Mobile ARM PDAP-PIM (Runtime 2.2) Language Pack 1 5.7.1” e poi copiando nella memoria del dispositivo i relativi file dll e jar.

A questo punto la VM è installata sul palmare. Possiamo passare all'installazione di alcune midlet di esempio per testare a fondo le potenzialità di questa tecnologia.

Per prima cosa abbiamo testato la possibilità di poter creare file in ogni directory della memoria del dispositivo tramite il seguente codice:

```
...
import javax.microedition.io.Connector ;
import javax.microedition.io.file.*;
...
try {
    FileConnection fconn=(FileConnection)Connector.open("file:////iamhere.txt");
    //verifico che il file esista
    if (!fconn.exists())
    //se il file non esiste lo creo
          fconn.create();
    fconn.close();
 }
 catch (Exception ioe) {
 }
...
```

Il codice sopra illustrato se inserito all'interno di una midlet crea un file vuoto dal nome iamhere.txt nella directory radice della memoria principale del PDA.

Dopo aver cambiato la directory di destinazione abbiamo verificato che la midlet che utilizza la libreria FileConnect può creare file in tutto il file system.

Con il seguente codice invece abbiamo verificato la possibilità di accedere ai file in memoria creati precedentemente anche con altri programmi:

```
...
import javax.microedition.io.Connector ;
import javax.microedition.io.file.*;
...
try{
          FileConnection fc = (FileConnection) Connector.open(file:////prova.txt);
          is = fc.openInputStream();
          int len = is.read(b, 0, 2048);
          fc.close();
 }
 catch (Exception ioe) {
 }
 ...
```

Dopo una serie di tentativi abbiamo visto che tramite una midlet è possibile accedere alla maggioranza dei file del file system tranne alcuni file di sistema a cui è negato l'accesso dal sistema operativo.

Conclusione

Viste le possibilità offerte dalla soluzione java ME con profilo cldc 1.1 e midp 2.0 con jsr 75 installato si decide di preferire questa soluzione rispetto a quella offerta dal .net framework soprattuto alla luce della grande portabilità offerta. Un applicazione realizzata con la tecnologia java ME può infatti girare non solo su PDA equipaggiati da windows mobile ma può essere installata su tutti i dispositivi aventi una VM come cellulari o PDA di qualsiasi tipo.
Visto quindi lo stato dell'arte e analizzate le tecnologie disponibili per lo sviluppo si decide di procedere con la progettazione dell'applicativo.

Progettazione dell'applicazione

Obiettivo

L'obiettivo è quello di realizzare un applicazione per PDA e smartphone di ultima generazione per la difesa dei dati e delle informazioni personali dell'utente.
Lo scopo principale è quindi quello di rendere inaccessibili i dati dell'utente a persone diverse dal proprietario o utilizzatore abituale del dispositivo tramite la cifratura delle informazioni e un'autenticazione iniziale obbligatoria.
I dati che si vogliono difendere sono i file sulla memoria (anche esterna) e le informazioni del PIM come i contatti, gli eventi e il calendario.

Caratteristiche dell'applicazione

Le funzionalità che l'applicazione dovrà offrire all'utente sono le seguenti:

1. Possibilità di cifratura di file o cartelle del file system del dispositivo.
   La cifratura/decifratura degli oggetti può avvenire in automatico all'accensione/spegnimento del dispositivo o solo dopo un esplicita richiesta dell'utente a seconda delle impostazioni scelte.
2. Possibilità di cifratura delle informazioni personali. Con informazioni personali si intende la rubrica, il calendario e la lista degli appuntamenti. Le informazioni personali vengono rese accessibili in chiaro all'utente subito dopo l'avvio dell'applicazione.
3. L'accesso alle informazioni cifrate deve essere garantito solo dopo una fase di

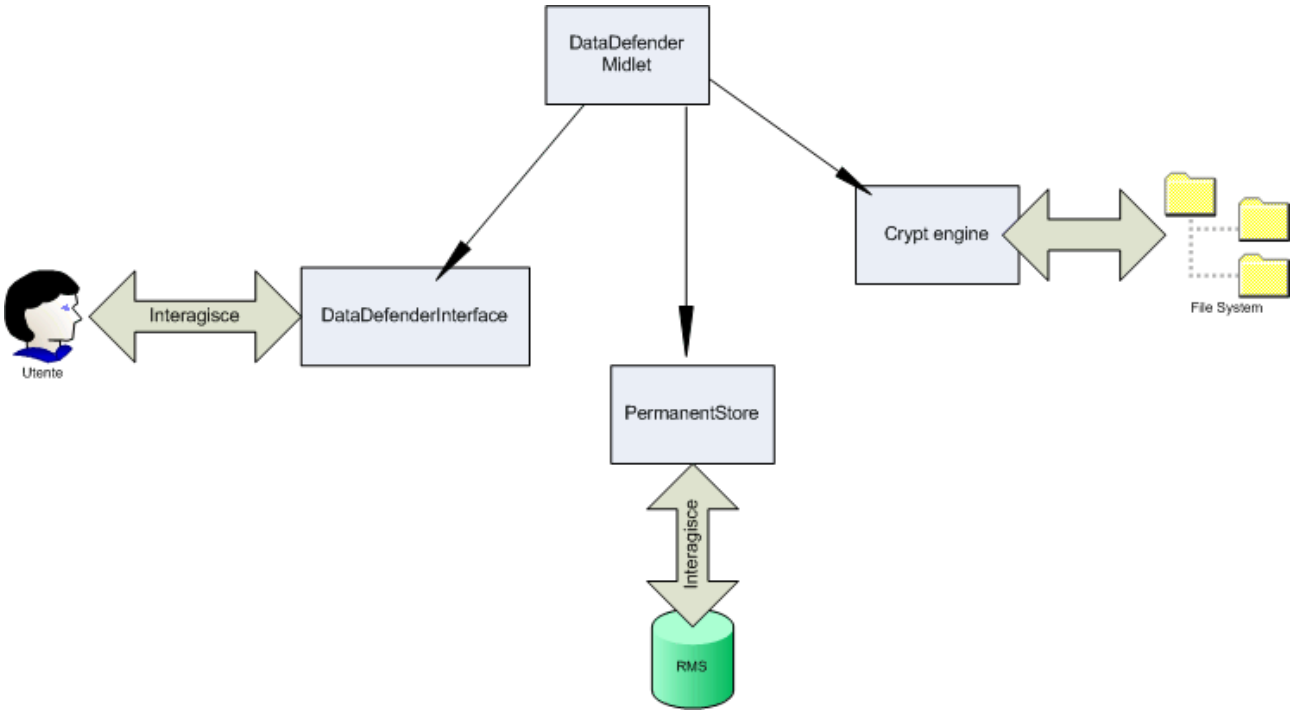
autenticazione iniziale in cui l'utente verifica la sua identità tramite l'inserimento di un nome utente e una password.

4. Le password immesse sono memorizzate tramite un sistema di cifratura reversibile in modo tale da rendere possibile il recupero delle stesse tramite un account di amministrazione.
5. I dati che l'utente decide di proteggere devono devono essere cifrati al momento della chiusura dell'applicativo o al momento dello spegnimento del dispositivo in maniera automatica.
6. L'applicazione dovrà fornire un supporto per il recupero da crash in seguito allo spegnimento accidentale del dispositivo durante la fase di elaborazione dati.

Aspetti implementativi

Per la realizzazione si è scelto la tecnologia java ME che, come evidenziato nella fase di studio preliminare, offre vantaggi in termini di portabilità rispetto alle altre tecnologie disponibili.
Per implementare la cifratura degli oggetti si pensa di utilizzare una crittografia basata sull'algoritmo di cifratura simmetrica Blowfish. Per l'implementazione di una cifratura reversibile si è scelto di memorizzare le password utente su record cifrati, in maniera tale da renderle leggibili solo all'utente amministratore del sistema. Per il calcolo dei digest si è pensato di ricorrere all'algoritmo SHA1.
Per la realizzazione dell'applicazione verranno usate le Bouncy Castle in versione lighweight
come appoggio per le funzioni crittografiche.

Struttura dell'applicazione



La midlet è composta da tre moduli principali:

1. **DataDefenderInterface;** è quella parte che si preoccupa dell'interazione con l'utente. Tramite di essa la midlet comunica e scambia dati con l'utente finale.
2. **PermanentStore;** serve ad interagire con l'RMS per la memorizzazione delle informazioni in maniera permanente. Tramite questo modulo il programmatore accede alla memoria non volatile al fine di memorizzare tutte le strutture necessarie al corretto funzionamento.
3. **Crypt engine;** si preoccupa dell'interazione col file system e di cifrare e decifrare i dati memorizzati in esso. Tramite questa componente la midlet realizza il proprio compito principale, cioè quello di mettere in sicurezza le informazioni personali dell'utente.

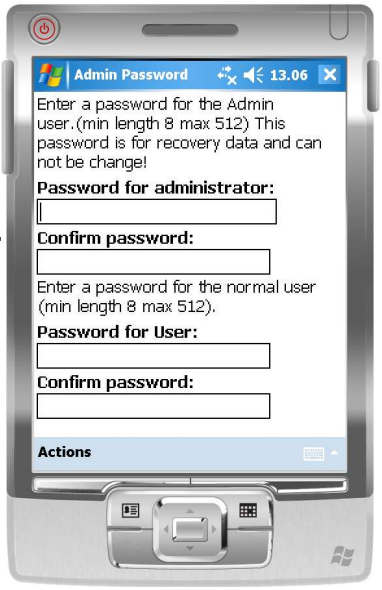
Utilizzo dell'applicazione

Prima esecuzione

Al momento della prima esecuzione dell'applicazione su un nuovo dispositivo la prima schermata che si presenta ad un nuovo utente è quella nella figura a destra.

Il programma richiede ad un nuovo utilizzatore una password per l'utente e una per l'amministratore di sistema, usata per il cambio e il recupero della prima.

Dopo aver digitato le chiavi scelte l'utente deve cliccare su Confirm Password per proseguire.



Esecuzione normale

Durante una esecuzione normale dell'applicazione invece il sistema richiede semplicemente la password utente.

Dopo averla digitata l'utente deve cliccare su Login per accedere al menu principale.

In caso di smarrimento l'utilizzatore può ricorrere al sistema per il recupero della password cliccando su Recovery Password.

Per il recupero della password bisogna conoscere la chiave di amministratore.

Recupero della password utente

Si ricorre al recupero della password utente in caso di smarrimento della stessa. Per avviare la procedura di recupero all'avvio dobbiamo scegliere l'opzione del menu "Recovery Password" senza dover inserire alcuna chiave.

Per far si che il recupero sia completo bisogna inserire la password di amministratore. E' bene ricordare che la password di amministratore non è recuperabile in alcun modo e quindi deve essere conservata con cura.

Se la chiave immessa è corretta verrà garantito l'accesso all'applicazione e in alto sopra al menu verrà mostrata la password utente scelta inizialmente.

Menu principale

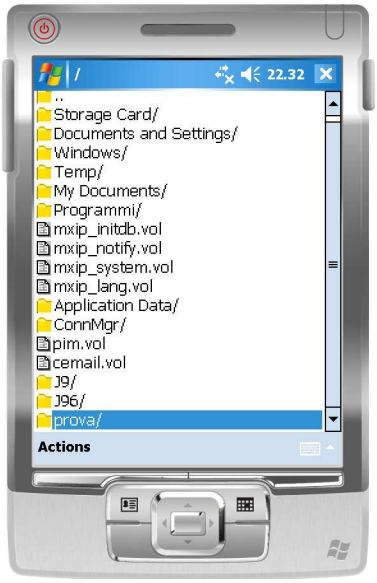
La figura a destra mostra il menu principale dell'applicazione. Le cinque voci che compongono il menu principale rappresentano ognuna una possibile azione che l'utente può svolgere:

- Cifrare o decifrare un file o una cartella singolarmente;
- Aggiungere selezionare una cartella come area di lavoro personale;
- Rimuovere una directory dall'elenco delle home directory;
- Cambiare la password utente;
- Selezionare la cifratura delle informazioni personali.

Vediamo nel dettaglio ciascuna di queste funzioni e le operazioni che l'utente deve compiere.

Cifratura/decifratura di un file o di una cartella singola

Se viene selezionata l'opzione "Encrypt or decrypt one file" si apre una finestra con cui viene visualizzato l'intero file system. L'utente può quindi navigare all'interno delle cartelle contenute nel dispositivo per scegliere la cartella o il file da cifrare o decifrare.



Una volta selezionato l'obbiettivo l'utente può procedere cliccando su "Perform Action"; a questo punto il file o la cartella selezionata vengono cifrati o decifrati a seconda che siano in chiaro o meno.

Lo svolgimento dell'operazione viene segnalato da una barra a scorrimento orizzontale che indica la percentuale di lavoro attualmente svolta e il nome del file attualmente sotto elaborazione.

L'elemento una volta cifrato viene contraddistinto da un icona blu

raffigurante un lucchetto.

Definizione di una home directory

La seconda opzione invece permette all'utente di selezionare una directory da aggiungere all'elenco delle home directory. Come per la prima funzione all'utente viene mostrata una finestra che rispecchia la struttura del file system. L'utilizzatore può quindi navigare tra le cartelle e i file per selezionare la directory voluta. La selezione di un singolo file non è naturalmente permessa.

Rimozione di una home directory

Tramite questa opzione l'utente può rimuovere una home directory dalla lista all'interno del sistema. All'utente viene mostrato l'elenco di tutte le cartelle personali a lui associate.
Dopo averne selezionata una l'utente può rimuoverla dall'elenco cliccando su "Remove Directory".

Cambio della password utente

Nel caso in cui l'utente voglia cambiare la password inizialmente scelta si può ricorrere a questa funzione che permette all'utente di cambiare la chiave di accesso.

Occorre sottolineare che il cambio della password è un procedimento piuttosto lungo in quanto comporta la decifratura e la ricifratura di tutti i file e cartelle messe sotto sicurezza al momento.

Il cambio della chiave di accesso può essere consentita solo agli utenti che conoscono la password di amministratore.

L'utente dopo aver scelto la penultima opzione dal menu principale deve inserire la password di amministratore e successivamente la nuova chiave utente come viene mostrato nella schermata sulla sinistra. Dopo aver digitato la nuova password l'utente deve selezionare la voce "Select pwd". A questo punto l'applicazione procede con la decifratura e ricifratura dei dati a partire dalla nuova password inserita.

La chiave scelta naturalmente deve rispettare i criteri iniziali e cioè deve avere una lunghezza minima di 8 caratteri e massima di 512.

Cifratura delle informazioni personali

La cifratura delle informazioni personali avviene solo su esplicita richiesta dell'utente. Di default questa funzione risulta disattivata, deve essere l'utente ad attivarla selezionando l'ultima voce del menu principale. L'attivazione della messa in sicurezza dei dati personali può essere vista dall'utente tramite il valore booleano visualizzato nel menu principale.

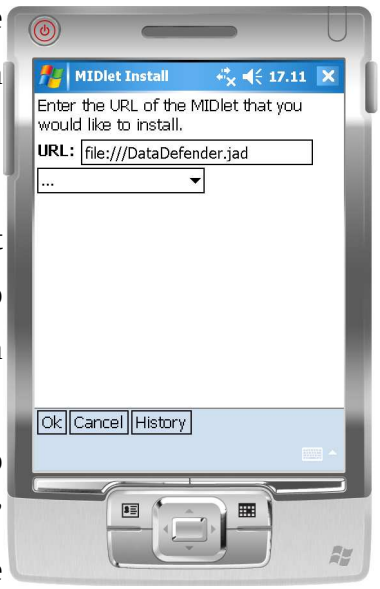
Installazione dell'applicazione

Prerequisiti

Per l'installazione di DataDefender l'utente ha bisogno di un palmare o cellulare dotato di una java virtual machine che implementa i profili CLDC 1.1 e MIDP 2.0 con il pacchetto opzionale JSR 75 contenente le api FileConnect per la connessione al file system e le api PIM per l'accesso alle informazioni personali.
Per l'installazione su palmari si consiglia l'uso della JVM WebSphere Everyplace Micro Environment almeno versione 6.0 che è stata pienamente testata con il nostro applicativo.
Per i ragguagli riguardanti l'installazione della JVM dell'IBM si rimanda alla prima parte della relazione dove si possono trovare tutti i passaggi da compiere per effettuare il setup manuale o automatico.

La seguente procedura di installazione del programma si applica per il setup su palmari equipaggiati di windows mobile 5.0 con IBM Websphere già installata.
L'installazione su altri tipi di dispositivi o palmari comporta la parziale modifica di alcuni passi.

Installazione



Per l'installazione dell'applicazione occorrono i file “DataDefender.jar” e “DataDefender.jad” che vanno caricati sulla memoria del dispositivo in un path qualsiasi.

Noi abbiamo caricato i due files nella root directory per semplicità.

Adesso, per procedere all'installazione, dobbiamo lanciare il midlet manager della JVM. Se abbiamo precedentemente usato il setup automatico dell'interprete java allora basta un doppio click sulla corrispondente icona del menu.

Se abbiamo invece effettuato un installazione manuale, dobbiamo lanciare il programma manualmente cliccando sul file “emulator.exe” situato nella cartella “bin” all'interno della directory contenente websphere. Una volta lanciato il midlet manager la procedura di installazione viene avviata cliccando sul pulsante “Install”. All'utente viene quindi mostrata un'apposita form sulla quale dovrà specificare il path del file “DataDefender.jad” (figura a destra). La procedura ha inizio dopo il click sul pulsante “Ok”.

Durante l'installazione l'utente deve acconsentire alle varie richieste della java virtual machine riguardanti la sicurezza fino al completamento dell'installazione stessa. Alla fine del setup il midlet manager ha l'aspetto mostrato sulla destra.

A questo punto per lanciare la midlet basta selezionare DataDefender dall'elenco delle applicazioni installate e poi cliccare sul pulsante “Launch”.

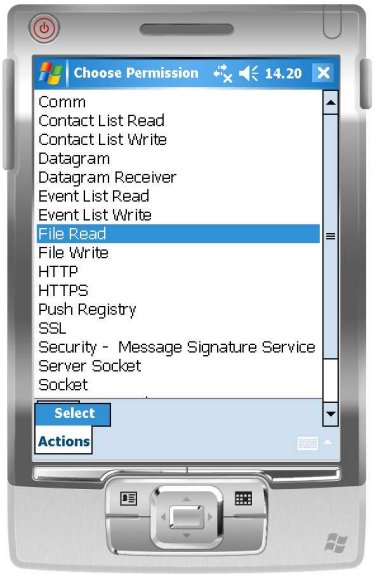
Durante l'esecuzione dell'applicazione la JVM potrebbe richiedere alcuni permessi all'utente, in particolare prima di compiere operazioni sensibili come l'accesso alla memoria e alle informazioni personali.

L'utente deve sempre acconsentire l'esecuzione di queste azioni al fine di permettere il corretto funzionamento del programma.

Per impostare in modo permanente i permessi dell'applicativo, al fine di non vedere più visualizzati questi messaggi, l'utente deve una volta per tutte modificare alcune impostazioni della JVM seguendo la procedura mostrata nel paragrafo successivo.

Impostazione dei permessi

La seguente procedura mostra come impostare i permessi associati al programma appena installato in modo da consentire, in maniera permanente, l'accesso alle informazioni personali e alla struttura del file system sia in scrittura che in lettura.



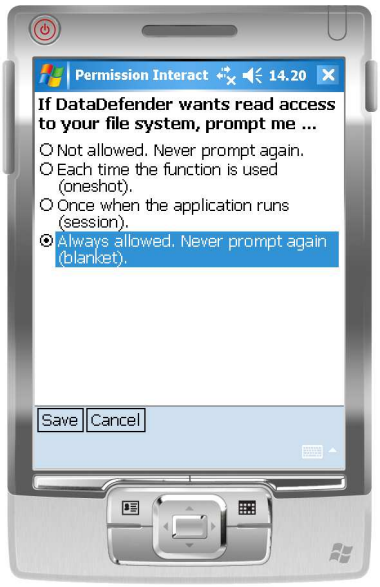
Per cambiare i permessi associati ad una midlet installata l'utente deve entrare nel midlet manager e dopo aver selezionato l'applicazione cliccare sul pulsante “Manage”.

A questo punto verrà mostrata una nuova schermata (nella foto a destra) contenente l'elenco delle possibili azioni sensibili che una midlet può compiere.

Per funzionare correttamente DataDefender ha bisogno del permesso di compere le seguenti azioni:

- File Read e Write
- Event List Read e Write
- Contact List Read e Write
- ToDo List Read e Write

Prima di utilizzare l'applicazione quindi l'utente deve, per ciascuna delle azioni precedentemente elencate, abilitarne l'esecuzione ripetendo la procedura qui esposta.



Dopo aver selezionato l'azione e cliccato su “Select” l'utente deve selezionare l'ultima voce del menu a scelta multipla mostrato nella figura a destra cliccando poi su “Save” per rendere effettiva la modifica. L'ultima voce, se selezionata, permette all'applicazione di poter svolgere senza problemi l'azione selezionata senza particolari restrizioni. Le altre opzioni permettono al programma di compiere l'azione ma con restrizioni (la terza), solo dopo un esplicito consenso dell'utilizzatore (la seconda) o non permettono affatto il suo svolgimento (la prima).

Dopo aver ripetuto la procedura per tutte le azioni elencate in precedenza, l'applicazione può essere eseguita tranquillamente dall'utente.

In altri dispositivi, in particolare in quelli che hanno una java virtual machine già installata in

fabbrica, l'assegnazione dei permessi da parte dell'utente potrebbe essere più restrittiva, permettendo una scelta meno ampia limitata alle sole prime due voci. Altri dispositivi invece, come ad esempio gli smartphone, assegnano automaticamente i permessi al momento dell'installazione, in base alla firma digitale dell'autore contenuta nel file jar non permettendone una successiva modifica.

Ad esempio, se una midlet non è digitalmente firmata in maniera corretta, la propria esecuzione viene permessa ma ogni azione sensibile deve essere accompagnata dal consenso esplicito dell'utente.

Sviluppi futuri

Di seguito riportiamo alcune considerazioni sui possibili sviluppi futuri, elencando le modifiche e le migliorie che potranno essere apportate al programma realizzato.
Elenchiamo qui di seguito le varie considerazioni per punti:

- Il cuore del programma è l'**algoritmo crittografico**, per migliorare la sicurezza si potrebbe cambiare l'algoritmo di cifratura scelto, il blowfish, con un altro più sicuro e immune da attacchi. La scelta dovrà naturalmente tenere conto anche della potenza di calcolo offerta dai dispositivi, in modo tale da non appesantire troppo il programma e rendere ragionevoli le attese dell'utente durante le elaborazioni. Un futuro incremento della potenza di calcolo può comunque aprire nuovi scenari e permettere l'uso di algoritmi più complessi ma più sicuri che in questa prima versione sono stati scartati.
- Le possibilità attualmente offerte all'**utente amministratore**, in questa prima versione del programma sono poche. In futuro si potrebbe voler permettere all'amministratore del sistema una gestione più particolareggiata e minuziosa dell'account utente. All'utente privilegiato infatti potrebbe essere aggiunta la possibilità di dare una scadenza alla password utente, di stabilire criteri di complessità per le chiavi oppure di bloccare l'accesso ai normali utilizzatori in caso di necessità.
- Per come è costruita la prima versione del programma un utente può prendere e spostare i dati cifrati da un dispositivo mobile ad un altro, senza particolari problemi di incompatibilità anche per scopi maliziosi. Se si vuole impedire questo possibile attacco sarebbe necessario implementare una cifratura legata non solo alla chiave utente come è adesso ma anche ad una caratteristica fisica dell'hardware che ospita il programma, come ad esempio un codice IMEI del dispositivo oppure al MAC address della scheda di rete. Se la caratteristica scelta individua in maniera univoca il dispositivo, allora i dati spostati su un altra macchina diventeranno illeggibili.

- Per i dispositivi con un lettore di impronte incorporato potrebbe essere implementata una nuova versione che usa il lettore per garantire o negare l'accesso.
- Per evitare il successo di attacchi di tipo **brute force** potrebbe essere implementato un sistema per il blocco sistematico dell'applicazione dopo l'inserimento di un numero prefissato di password utente o amministratore errate.

Bibliografia

Articoli sulle tecnologie Java http://developers.sun.com/

Bouncy Castle Crypto APIs www.bouncycastle.org

Li Gong – Inside Java 2 Platform Security: Architecture, API Design, and Implementation

James Keogh – J2ME: The Complete Reference

JSR118 Expert Group – Mobile Information Device Profile: for Java™ 2 Micro Edition Version 2.0

MSDN for Windowe Mobile – http://msdn.microsoft.com/windowsmobile/

JSR 75 API – http://jcp.org/en/jsr/detail?id=75

Runtime MIDP per Pocket PC

IBM WebSphere Everyplace Micro Environment – http://www-128.ibm.com/developerworks/websphere/zones/wireless/weme_eval_runtimes.html

ACCESS JV-Lite2 Wireless Profile – http://www.accesschina.com.cn/products/midp.htm

Tao Group Intent Platform, Midlet Manager – http://taogroup.com/main.php?pageid=254911.php&temptype=t1