Global Information Assurance Certification Paper

Eddie Henrard
GSEC
Version of assignment: GSEC version 1.3
Online

Encrypting PDAs with AES – why do it?

Eddie Henrard
GSEC version 1.3

Summary

More PDAs are being used to store sensitive data, so more are being lost or stolen, with potentially serious implications.

Unless the information they contain is encrypted, it may be easily recovered, so the new AES is an appropriate algorithm to use to protect it.

A number of different software applications are now available for these devices that utilise this standard effectively.

Introduction

As computer-using professionals spend more time travelling or commuting, away from their office or home desktop machines, they have more 'free' time, on trains, planes and buses, frequently having to make the choice to either 'waste' or utilise these valuable hours.

Even with the reducing size and weight of laptop computers, and the increasing availability of small high-resolution LCD screens, many have been turning to smaller, more portable personal devices (such as the 3Com Palm Pilot, Handspring Treo and PocketPC machines).

These lightweight machines enable users to draft documents, read and compose replies to email (sometimes wirelessly), plan projects and keep track of appointments (and eliminate the top shirt-pocket-full of scraps of paper!).

As convenient (and now in many cases, essential) as they are, mobile handheld

devices such as P.D.A.s (Personal Digital Assistants) are vulnerable to damage, loss, theft and corruption.
They can contain many types of personal or commercially-sensitive information, so adequate protection of this data is a minimum safeguard for users that take the potential threats seriously.

Although the advantages of P.D.A.s are manifold, on the flip side however, the fact that each one can potentially contain such a concentration of information in one place, makes it even more imperative that the data they contain (whether personal or confidential, maybe even classified!), is kept secure.

Unless measures have been taken to encrypt important data, it could be easily recovered.

With the recent introduction of the new AES, new applications are now available that utilise this algorithm and might better protect Palm devices.

The Chinks in the Armour ("The Problem")

Increased use of mobile devices

The wider acceptance and use of these devices for personal and corporate information management has led to a rapid growth in the numbers of PDAs being used, and subsequently being lost or stolen.

According to Informationweek.com, *"Global PDA shipments rose 17% in 2001 over the previous year and are poised to grow another 18% this year,.. Key drivers in boosting sales, include … the increased use of short-range wireless technologies, such as Bluetooth."* [1] (which itself presents other security issues!).

Wireless access (via infrared and radio frequency)

Since the events of late 2001, the threats to data from mis-configured or default-installed wireless-network access points and mobile radio-based handheld devices, have been emphasised in many security forums, among the issues the potential "grabbing" of such confidential data as medical records.

PDAs used between and by Ambulance personnel and Doctors in A & E departments are one such example of a security vulnerability, and if "*information, ... can be transferred to the emergency department from the scene via wireless cellular modem or at the hospital by "beaming" it from the Palm handheld to a printer that supports infrared technology*" [2] then it can also be intercepted by another similar device in the near vicinity, raising privacy and safety concerns!

Theft of data

However well the security of handhelds can be augmented, the need for physical security still exists; it's almost impossible to prevent them being lost or stolen from briefcases, bags and pockets. Even the Gartner Group estimates that *"more than a quarter million P.D.A.s and mobile phones were lost or stolen in airports world-wide in 2001."* [3]

Passwords

Although built-in password-based access control is most commonly relied on to protect PDAs, they are particularly vulnerable because, in most cases without encryption, their passwords are not secure, [3] and in earlier versions of the Palm OS, are not stored locally.

AES; (a "Solution"?)

The AES has been a co-operative four-year effort to develop the next accepted standard of encryption and is "*a Federal Information Processing Standard (FIPS - specifically, FIPS Publication 197),* (specifying) *a cryptographic algorithm for use by U.S. Government organizations to protect sensitive, unclassified information".* [4]

It is expected that AES will be implemented for use domestically and internationally in both the federal and private sectors to protect information.

The Rijndael (pronounced "rain-dahl") encryption algorithm, (by J. Daemon and V. Rijmen), is the numerical procedure chosen by NIST to be the AES, is

"a simple self-supporting cipher that does not depend on or use other cryptographic components, [5] and specifies three key sizes: 128, 192 and 256 bits.

When encryption is to be considered for P.D.A. devices, two factors especially – code density (and hence memory usage [4], limited in most PDAs) and speed are important, in order to maintain their "usability", especially as key length increases; AES performs well on both counts.

So why a new algorithm?

- Kyle Jones offers one possible reason: "*AES is set to replace DES, has been in use for over twenty years, and … is currently only approved for use in Legacy systems."* [5]

- There was a perceived need (by NIST) for a more flexible system that would adapt to a variety of platforms and devices,

- the absence of a secure Palm OS *(that is, at least, until v 5.0 with RSA encryption becomes available)* [6]

Even though Palm's OS v4.0 features enhanced support for the built-in security application, it appears to only go part of the way to securing the OS, (in that it doesn't encrypt the data).

However, Palm.com do encourage third party applications development, and list a number of resources in to their online article "Securing the handheld environment- An Enterprise Perspective", including NTRU (www.ntru.com), whose Security Toolkit for PalmOS uses the AES encryption algorithm. [7]

The company are also in the process of developing (as mentioned earlier) OS v5.0, with *"RSA (encryption) BSAFE® Micro Edition Software".* [6]

"Locking it down" (or What applications are available?)

So, what can be done to prevent information being recovered "in the clear", as an understandable format, and not encrypted?

The handheld security world is now seeing a new range of AES-containing utilities and applications, such as those next described, which can help take personal data security a step further.

Products that utilise AES:

- Certicom's MovianCrypt
- F-Secure's FileCrypto
- GoAti's PDASecure and ForeverSecure
- AstaWireless' PDA Safe
- Corsoft "Aileron Personal Access"
- Trust Digital's PDA Secure Premium
- Crypotomathic Secure Memorizer 2.0

The characteristics of each product are outlined in the summary table following these descriptions.

MovianCrypt:

Certicom's MovianCrypt uses a fast AES encryption algorithm to not only encrypt individual records in all user databases on the handheld, but also all of the application preferences and clipboard contents.

To further improve performance, MovianCrypt decrypts only records that the user requests re-encrypting them using idle CPU time once the user is finished.

F-Secure's FileCrypto

F-Secure has taken a slightly different approach, supporting the Pocket PC and Symbian platforms as well as Palm OS, with its FileCrypto software.

The 128bit (AES) encryption it uses requires a password to decrypt files, with the encryption being controlled via policy administration tools, which lets IT managers retain some control over the way users handle sensitive data, and "*takes the decisions out of their hands*." [8]

GoAti PDASecure and ForeverSecure (similar to Trust Digital's version)

PDASecure enables secure password and data encryption for all Palm devices. Among these is that in the event that a Palm device is stolen, PDASecure will restrict unauthorised synchronisation, which can easily be achieved without access to the user's PC.

It allows selection from six different security algorithms, including the Rijndael algorithm. ForeverSecure provides security to desktop PC applications, including Palm data on the PC. [9]

AstaWireless' PDA Safe

PDASafe uses either RSA or AES encryption methodologies to secure ALL of a P.D.A.'s data, but whichever solution is installed, the method of operation is identical. Database files are selected, a password is entered, and those ones chosen are encrypted. Prior to HotSyncing though, they must be decrypted.

Support for the utility is available via public newsgroups for PdaSafe that can be found by directing your newsgroup reader software to news.astawireless.com and then posting on the news.astawireless.pdasafe newsgroup.

Corsoft "Aileron Personal Access" secure email access

Version 3.1 of Corsoft Aileron Personal Access has an easy to use graphical user interface (GUI) and offers 192-bit encryption, the ability to receive both text and HTML messages and fax e-mail with e-mail attachments via the P.D.A. It supports various Palm hardware devices using Palm OS 3.1 or higher, and uses compression to enhance performance.

It is available for a free 14-day trial at ftp://ftp.corsoft.net/Ail4Palm.exe [10]

Trust Digital's PDA Secure Premium

Along with network-wide support, unobtrusive background performance, and the option of five alternative encryption algorithms, PDASecure protects handheld devices from the likes of "infrared oversight".

This is achieved because only the password-protected device itself, or the network that it is connected to have the key to unscramble it, so data encrypted on PDAs with this application cannot be copied or "beamed" (via Infra Red link) to another system that could read it.

PDASecure also provides a degree of Virus Protection, (where an unauthorized user or application or virus cannot delete protected application data), and is available in four different product versions:

- ***PDASecure™***,
- ***PDASecure™* Standard**, with more features and encryption algorithms.
- ***PDASecure™* Enterprise**, providing a unique and comprehensive solution for small to large PDA networks &
- ***PDASecure™* Policy Editor**, which deploys, manages, and secures networks containing PDA devices, using an enterprise centralized management solution. [11]

Crypotomathic Secure Memorizer 2.0


[12]

This tool keeps sensitive information secure and easily accessible, and uses a novel approach to entering a passphrase.

"*A key is used to enter the safe area where your information is stored, this being a sequence – of (the user's) choice -- of four to 16 nodes and major faces of* ***the company's logo****. This key is then used to AES-encrypt the contents of the edit area".*[12]

Whenever the program is closed, the contents of the safe area are encrypted. The encrypted data is also backed up during Hot Sync operations.

Product summary table:

(Please note; this table is not totally comprehensive, as details may have changed since submission).

Function or feature	MovianCrypt		FileCrypto		GoAti (same as *?)		PDA Safe		Aileron Personal Access		PDA Secure Premium *		Secure Memorizer 2.0	
AES encryption algorithm	Y	Bits: 128	Y	Bits: 128	Y	Bits: ?	Y	Bits: ?	Y	Bits: 192	Y	Bits: ?	Y	Bits: ?
Option for other algorithms	N		Y, five		Y (same as PDA Secure Premium?)		Y, one		N		Y, RC4(128 bit) –Default, TEA(128 bit) Twofish (128 bit,) Blowfish (Up to 448 bit) XOR		N	
Encrypts: - individual records	Y				Y		N				Y		N	
- all databases	Y		Y		Y		Y				Y		N	
- all applications	Y						N						N	
- passwords	NA				Y		Y				Y			
"Disable encryption on per-application basis	Y				N(ot) K(nown)		N							
Password required to enter	Y		Y		Y		Y				Y		N –phrase	
Password stored on device	N						NK						Y	
Key stored on:					Device or network		NK				Device or network			
Decrypts individual records	Y						N						Y	
Effect on performance	Negligible		Negligible if AES		Negligible		Negligible		Negligible		Negligible if AES		Negligible	
Memory used					76kB						76kB		24kb	
C/w policy admin' tools?			Y		N						Y		N	
HotSync protection					Y						Y		N	

Beam protection (IR port)			N			Y	N
Supports other platforms		Y Symbian, Pocket PC					N
Secures desktop applications?			Y, with "Forever Secure"				N
Online support?			Y	Y, newsgroup			Y
Uses compression to enhance performance			N		Y		
Support for hardware using Palm OS			Y		Y, v3.1 or better		
Wireless support			N			Y	N
Free trialware?			NK		Y		Y
On demand encryption	Y					Y	Y
Configurable by enduser		Y				Y	Y
Configurable by end user and administrator		Y				N	N
Managed security		Y				N	N
Wipe password						Y	N
Displays owner info						Y	N
Full control with time features						Y	
Antivirus protection	Y						N
Company URL	http://www.certicom.com/	http://www.f-secure.com/	http://www.goati.com/	http://www.astawireless.com/products/pdasafe	www.corsoft.net/home.asp	www.trustdigital.com/prod1.htm	Www.cryptomathic.com/secure-memorizer/index.html

Conclusion

From the material researched, the opinions studied, and looking objectively at the reasons summarised in this article, I believe it is imperative that to maintain the confidentiality, integrity and availability of data on handheld devices, a tested, reliable encryption standard should be used to protect PDAs.

In my opinion, (when appropriately deployed and configured), the Rijndael algorithm is ideally suited to this task, being flexible and versatile enough to integrate with various operating systems, having low processing and memory requirements, and as such meeting the security needs of mobile PDA users.

The matter of which particular application is chosen, will depend very much on individual and corporate needs, but may be more easily made by comparison of the features summarised previously.

Regardless of whichever path (or 'flavour') is chosen, encryption with an AES-enabled application will, with reasonable cost and effort, offer greater surety and 'peace of mind' to PDA users and information owners.

References

1. PDA Sales remain Strong Feb. 7, 2002, informationweek.com, URL: http://www.idg.net/idgns/2000/08/28/StudyPDASalesToDoubleIn.shtml (3/5/2002)

2. Palm.com Press Releases, "**Palm Powered Handhelds Improve Emergency Medical Response** " URL: http://www.prnewswire.com/cgi-bin/micro_stories.pl?ACCT=153400&TICK=PALM&STORY=/www/story/11-26-2001/0001621506&EDATE=Nov+26,+2001

3. Gardner, Dale, "WIRELESS INSECURITIES - Control mobile computing vulnerabilities before they get control of you." Information Security, January 2002, published by TrueSecure. URL: http://www.infosecuritymag.com/2002/jan/cover.shtml

4. "ADVANCED ENCRYPTION STANDARD (AES) Questions and Answers", Paragraphs 7, 15, URL: http://csrc.nist.gov/encryption/aes/aesfact.html

5. Jones, Kyle, "Who's Who in AES?", SANS Information Security Reading Room, August 16, 2001 URL: http://rr.sans.org/encryption/who.php

6. RSA® CONFERENCE, SAN JOSE, Calif., Feb. 21, 2002 - RSA Security Inc. "RSA Security Encryption Software Embedded in Palm OS 5; RSA BSAFE® Micro Edition Software Helps Secure Newest Version of Palm OS®", URL: http://www.rsasecurity.com/news/pr/2002/RSA2002/020221.html (30/4/2002)

7. Palm.com file securing_env.pdf, "Securing the handheld environment – An Enterprise Perspective", URL: http://www.palm.com/pdfs/securing_env.pdf (26/3/02)

8. Fisher, Dennis, "PDA security to get stronger", ZDNet Saturday 18th June 2001,
URL: http://www.zdnet.com.au/newstech/news/story/0,2000025345,20233109-1,00.htm

9. McDermott, Matthew, "PDA (Personal Digital Assistant) Security." ITS Med. Tuesday, 26-Feb-2002,
URL: http://its.med.yale.edu/security/PDA/#sdmupda

10. Corsoft product announcement, http://www.corsoft.net/home.asp, (25/3/02)

11. Trust Digital Security Software - TRUST DIGITAL! "Secure your PDA and Palm using PDA Secure" URL: www.trustdigital.com/prod1.htm (25/3/02)

12. Cryptomathic.com article: "Security On P.D.A.s - And The Possibilities For Enabling Them With PKI", NewsOnInk April 2001,
URL: http://www.cryptomathic.com/pdf/news6.pdf (26/3/02)