2005

Issues relating to the Forensic Analysis of PDA and Telephony (PDAT) Enabled Devices

Craig Valli
Edith Cowan University

Issues Relating to the Forensics Analysis of PDA and Telephony (PDAT) Enabled Devices

Craig Valli
Edith Cowan University, Perth, Western Australia
c.valli@ecu.edu.au

Abstract: An emergent technology is the PDAT (Personal Digital Assistant & Telecommunicator) a hybrid of a mobile phone and coupled with a PDA's computing and storage abilities. Potentially every mobile phone is now an alternate or possibly primary computing and data repository for individuals. This paper explores current issues with the analysis of PDA technologies and the possible emergent issues forensic computing issues relating to its merger with mobile phone technology.

Keywords: forensic, PDA, telephone, mobile

1. Introduction

PDA (Personal Digital Assistants) in various forms have been in the marketplace for over a decade. These devices initially acted as little more than electronic calendars and address books with limited if any computational capacity beyond editing and storage. The current range of PDAs namely PalmOS, WindowsCE and Linux based appliances have similar computational and processing capabilities to that of desktop PCs less than 5 years old. This level of processing power enables the PDAs to run applications such as word processors, spreadsheets, database query engines and access networks including the Internet. Similarly, the memory capacity of these PDA devices when combined with current memory storage technology such as SD and Compact Flash Memory can easily approach several gigabytes of stored data. Traditionally, these types of appliances have been purchased to complement conventional desktop/laptop computing platforms.

An emergent technology is the marriage of mobile computing and mobile telephony. These devices combine the mobile phone with mobile computing abilities of a PDA a hybrid that could be called a PDAT (Personal Digital Assistant & Telecommunicator) . Potentially every mobile phone is now an alternate or possibly primary computing and data repository for individuals.

PDAs have crept into organisations often without the knowledge of IT support staff. Their relatively small size and ease of concealment make these devices ideal conduits for the transmission of contraband or covert data. With the current merger of phone and PDA technology the detection and mitigation of PDAs as a security risk to organisations will only increase. This level of use will eventually allow for would be perpetrators to transmit data covertly through multiple channels and at high speeds using a single device.

Due to the lack of transparency and even recognition of PDA technology in many organisations the possible last best hope for protecting an enterprise is recovery or mitigation through forensic computing techniques. This is largely a contemporary case of hope over experience with many forensic analysis tools been found sadly lacking in capability when it comes to analysis of PDAs (NIST, 2004).

These new PDAs/PDATs present significant challenges for the forensic computing community. This paper will outline some of the current problems with analysis of PDA and PDAT technologies and proffer some suggestions or possible solutions to some of the issues.

2. Current forensic issues with PDA technologies

The American based National Institute of Standards and Technology (NIST) in the report "PDA Forensic Tools: An Overview and Analysis" outline commonly available forensic analysis tools for WindowsCE, PalmOS and Linux based PDAs. In this report the authors from NIST tested various forensic software against actual acquisition scenarios. In most cases, the software that was tested highlighted significant issues with the software correctly acquiring material in sound forensic manner from PDAs. The level of problems varied from software to software, but the overall

analysis by NIST gave the impression that as forensic software goes most if not all had some way to go before being acceptable for use.

PDAs and PDATs by their nature are small devices often less than 100mm wide and 120 mm long and less than 10mm thick and weighing less than 150grams. There is not a lot of space left for the battery and often after the screen the battery is the next largest single component. Consequently, due to their diminutive size, power is a major concern on these devices and technology is used to minimise power consumption and maximise battery life. This maximisation from the point of view of the PDA user is optimal but for the forensic examiner this poses some unique problems.

One of the highest consumers of power in these devices is memory. Most PDA platforms operate on the principle of semi-volatile memory technology to store the base operating systems such as FLASH ROM and a volatile area for computation normally some form of RAM. The RAM normally requires a trickle charge to maintain integrity. So it is logical that one of the primary areas that has regular optimisation of usage is memory i.e. the less active memory the less power consumed. So optimisation of RAM usage can have significant savings of power which in turn impacts on battery life.

PalmOS optimises memory by dividing available RAM into dynamic and storage heaps. As their name implies dynamic heaps change dynamically as memory is required in the same way that conventional RAM works on a desktop computer however, these dynamic heaps are powered down and reactivated on a needs basis. Storage heaps are areas of memory that are used by PalmOS in a manner consistent with data stored on a hard drive Wilson(2004).

Traditional forensic computing methods mandate the use of some method of proving the unaltered state of a memory device this is normally achieved through the use of cryptographic hashes such as the MD5 algorithm. An investigation by Frichot(2004) saw that a PalmOS based PDA gave inconsistent MD5 image hashes when forensically imaged. This was determined to be as a result of the movement of dynamic heaps and data within the memory of the PalmOS PDA. The dynamic heaps moved/changed so the resultant MD5 hash was inconsistent, triggers for this can be date changes, temporary file deletion etc even though no individual file was changed by the user. These changes occur all the time as a PDA device is never truly turned off except when it has totally discharged its batteries at which point all memory in RAM is lost. This has a significant impact for the way in which evidence integrity for this style of device should be undertaken. It would be prudent to suggest that a more extensive and granular approach to forensic acquisitions and subsequent cryptographic hash verification of PDAs needs to be undertaken.

Furthermore, Frichot (2004) and NIST(2004) encountered problems recovering deleted files when a PalmOS device was acquired after a synchronisation. The reason for this was that certain files are no longer recoverable as one of the steps that PalmOS performs after a synchronisation is to restart and reorganise the file space and make deleted spaces available to the system. This process undertaken by PalmOS is analogous to defragmenting a conventional hard disk on every reset of the computer. This form of garbage collection while efficient memory wise removes any chance of recovering files in free space or slack space as can be undertaken in conventional forensic analysis.

On WindowsCE it would logically follow that similar problems in file recovery would be a problem as a result of PDA synchronisation this hypothesis is untested by the author at this time. This is because WindowsCE devices have similar methods for storing applications and data. WindowsCE 2.1 separates RAM into 2 main separate areas the Object Store and the Program Memory. Program Memory is the RAM used for application execution, stacks and heaps and its size is dependent upon the configuration of the system but it is managed by using a virtual memory system(Intel, 2004). In WinCE as with PalmOS an application dynamically allocates memory for run-time data. Hence, it is therefore valid to conclude at some stage a reorganisation of this memory space must occur altering contents. The alteration which then in turn alters hash values and the ability to recover deleted data.

The Object Store in WindowsCE uses the other major section of RAM which is divides into 3 categories the File System (RAM) – files and directories, Registry and Database. The File System contains applications and data created or stored by the user and it is persistent as long as the back-up battery provides charge. All of these files are stored in a compressed state. This compressed state also could have significant impacts on file integrity and subsequent re-compression by system utilities.

It should be noted that newer copies of system software that are stored in RAM would override ROM contents. This presents a problem for forensic analysis particularly in the replay of applications on different devices. This means that for proper forensic analysis the PDA not only has to have the same base operating system but also the exact same ROM contents for reliable playback and analysis.

The Registry in WindowsCE is a RAM based heap file that contains systems information about users, applications and configuration. Unlike a conventional PC based Windows registry this is operated and stored in RAM it should be noted that newer APIs allow for back up to more permanent media (Intel, 2004). A cold reboot and reinitialisation sees all files stored in RAM deleted.

3. The Merger Phone + Camera+ PDA - PDAT

Recently, the merger between the telephone and PDA (PDAT) has started to occur with main players in the PDA marketplace and telecommunications space offering PDAs capable of usage as mobile phones. In addition to extended telecommunications abilities there are also photo digital capabilities including still photography and streaming video.

This merge is changing the forensic landscape for these devices not only does one need to be expert in the acquisition and running of PDAs but now also telecommunications and photo digital technologies. It is fair to say that this development space is moving more rapidly than the conventional computing space as telephony is an established technology and hardware vendors are constantly trying to gain strategic market advantage by innovation or feature adding.

As these PDAT devices are integrated they will share memory, processing and other technologies, which will cause a multitude of analysis problems. For instance, take a SD memory storage card at any one time it may have a multitude of disparate data sources and types. The card could hold streaming movie data from a camera, SMS messages, email, email attachments, phone specific data and the list goes on. The memory on the actual devices themselves could likewise be inundated with a similarly large cacophony of data types and files. If compared to the situation 2 years ago to get the same effect you would have had to possess a phone, camera and PDA capable of handling a SD memory card and use the same card for the operation of all three devices. This trend will have major impacts on how data must be analysed for these particular PDAT devices.

One of the first impacts is the latency of free spaces on memory media. In a conventional forensic computing scenario as media is becoming larger it reasonable to assume that the latency of free space and slack space is increasing i.e because the amount of available free space on the devices in relation to workspace is actually increasing. This in turn increases the ability of the forensic examiner to find evidence that has been "deleted" from the device. However, with increased demand on the small memory space as a result of the multi-partite nature of these PDAT devices free space will be overwritten more often both on primary and secondary memory devices. This will minimise one of the avenues for forensic analysis available to conventional forensic computing analysis, which is the recovery of evidence from free and slack space.

Another impact of the developing multi-partite nature of the PDAT is that the complexity of analysis on these devices will increase and that much of the expert knowledge will have to be embedded into forensic analysis software. It is unlikely that a forensic examiner will be an expert in PDA design and operation, photographic and video forensics and telecommunications with a bent on

telephony. The expertise therefore has to be competently embedded into software and the indicators from the NIST(2004) report is that this is currently far from realised.

The ubiquity of connection will also present unique challenges for forensic analysis. Currently most PDAs are typically used to synchronise with a larger computing appliance such as a desktop pc, laptop or mail server normally through a serial, USB or infrared connection. In current usage profiles most PDA users have a tightly defined locus of data exchange/interchange with other devices. The PDAT device potentially allows connection to any modern network on earth i.e 802.11(LAN, WAN, Internet), Bluetooth (local and other PDA/Bluetooth enabled devices) and now the global telecommunications networks. This ubiquity of interconnection would make it difficult in determining conduits of travel for evidence or material sent by one of these devices. Every person you walk past with your powered up PDAT is a potential infector or malicious destroyer of your data and systems.

As an example, how would you track the spread or origin of a potential backdoor oriented malware that allows for remote control/retrieval of data from a PDA. Already there is proof of concept worms or viruses for PDA/Phones such as the Cabir Worm (BBC, 2004). The Cabir worm utilised low range Bluetooth as an attack vector it could have as easily been 802.11 or telephony. In contrast, a current forensic computing case of malicious code propagation would normally have attack occur from one potentially traceable network communications conduit, the organisational Internet router. The PDAT has more potential covert channels available for compromise in a singular instance than any device we have tried to secure before, coupled with the fact that is intended to be highly portable makes for an interesting analysis trail.

4. Possible solutions

One of the biggest issues will be finding software that is suited to the range of analysis that will be required to analyse these multi-media, multi-access devices. Traditional forensic computing analysis tools are focused squarely at the analysis of hard disks from desktop PCs or servers. The current range of tools for analysis of PDAs is noted to have problems as indicated in the NIST report pertaining to these tools (NIST,2004). Many of these tools are simply modified versions of existing forensic analysis tools and this is insufficient. To analogise for a moment this current approach by several software vendors is about as logical as a mechanic trying to fix a small car with the same socket and tool sets they would use for a large bulldozer, granted the principles of operation are the same but something is lost in the translation to reality. Furthermore, on this issue of software suitability there is a need for PDAT forensic analysis tools to be more comprehensive and complete due to device complexity.

The traditional usage of cryptographic hashes such as the use of macro MD5 hash signatures for verifying device and image integrity will largely become an obsolete *modus operandii* for PDAs and PDATs. Work conducted by Frichot (2004) and unpublished work by the author indicates that there is a major problem in using macro signatures for these devices. One possible way of assuring integrity will be to generate hash signatures for individual files based not only on file contents but also memory location and register at point of calculation. In essence the signature must become multi-partite.

Separation of function, or security controls within the devices themselves may go some way to aiding in the forensic analysis of the devices. By having finite areas of memory or access within the systems for particular functions then the ability to analyse for anamoly etc should become an easier task.

5. Conclusion

The emergence of telephony enabled PDAs (PDATs) and existing PDAs present interesting and varied challenges for forensic computing as a discipline. The high rate of change and adoption in this particular new space is causing significant stasis in skill acquisition and tool production to address forensic issues with the new PDAT devices.

The relatively fixed boundaries we as forensics examiners have been accustomed to are rapidly imploding the days of a single drive on a computer being your main evidence repositories are increasingly finite. Having PDAT devices with high market penetration and usage similar to or the same as existing mobile phones in itself is a large security issue. These PDAT devices unlike their static desktop bound computing ancestors will suffer from true network effects, viral infection, Denial of Service and other general forms of attack will occur at exponential rates on these devices with the limiting factor being bandwidth. Every person you walk past in the street is a potential attacker, intruder or hapless transmitter onto your PDAT data appliance. The PDAT is a multi-media, multi-channel digital device that will change the nature of forensic computing as we know it for some time to come.

References

BBC (2004) "First mobile phone virus created", [online] http://news.bbc.co.uk/1/hi/technology/3809855.stm

Frichot, C. (2004) An Analysis of the Integrity of PALM Images acquired with PDD, Proceedings of the 2nd Australian Computer, Network and Information Conference, Fremantle, Western Australia, pp. 66-75

Intel (2004) PSM Users Guide - Appendix B- Microsoft Windows* CE Memory Models and Usage Intel, [online] Intel Corporation http://www.intel.com/design/flcomp/manuals/psm/appendb.pdf

NIST (2004) PDA Forensic Tools: An Overview and Analysis [online]

Wilson, G. (2004). Exploring Palm OS: Memory, Databases, and Files. Sunnyvale, CA: Palmsource Inc.